*Intersect*, Vol 10, No 3 (2017)

# New Dangers in the New World: Cyber Attacks in the Healthcare Industry

Caleb J. Kumar
*Stanford University*

## Abstract

The Internet of Things, IoT, is one of the developments in the new world that has impacted humanity in an unbelievable way. Most noticeably by the connections it has created between devices and the information-sharing network it has established. The implementation of this revolutionary technology, while creating many positive outcomes, also has the threat of privacy invasion by hacking, making individuals vulnerable to loss of private data. The greatest impact of this invasion is experienced by the healthcare industry. A hacking attack on medical records, or on biomedical devices can have lifelong implications, and in the case of implantable devices, have the potential to be fatal. Since there is the involvement of several persons in the maintenance and sharing of medical records as well as in the invention, design, development, and utilization of a medical device, preserving the security of data that is shared presents an enormous challenge. Additionally, the cyber security of devices and records in the healthcare industry comes under the purview of many agencies, and thus, no one department has been held responsible for their protection. The government has initiated several actionable items and the cyber security experts have suggested techniques for cyber defense. Regulatory protocols, safety measures and emergency procedures have not yet been developed and instituted, but much work has begun and is being sustained by the interaction of the biomedical industry, cyber defense experts, government agencies, and healthcare providers. The future of cyber security in the healthcare industry looks promising even as investment, infrastructure, and regulations have commenced in all the interconnected agencies.

## Introduction

The Internet of Things, (IoT), is the "network of physical objects accessed through the Internet that can identify themselves to other devices and use embedded technology to interact with internal states or external conditions" (Weber, 2010). IoT is used to describe an environment where technology is able to connect to surrounding objects, such as cars, fridges, and thermostats, and capture all relevant data. With the IoT, the physical world is becoming a large database-like information system that has the ability to improve quality of life by managing everything from transportation (e.g., self-driving cars) and healthcare to consumer and business environments. IoT has the potential to generate new business models because of improved sharing of information that will allow businesses to better customize their products to their customers' needs. The optimal performance of IoT devices can increase safety, comfort, and efficiency as well as providing better decision-making and increased revenue generation. In fact, Cisco has said that IoT "has the potential to grow global corporate profits by 21% in 2022" (Maddox, 2015). Gartner Inc. predicts that more than 50% of new business processes will contain devices connected to the IoT, resulting in total economic impact expected to be between 3.9 to 11.1 trillion dollars by 2025 (Manyika, 2015). These organizations may be considered to have a vested interest in IoT and are therefore not a reliable source of information regarding the growth of IoT. The true evidence of the potential of magnitude of IoT growth is indicated by the financial investment in its prospective growth. In September 2016, the Global X Internet of Things ETF was launched. Such a large investment could not have been made unless there are several investors who believe in the future growth of IoT. The expansion of IoT means that personal information and business data will exist in the Cloud and will be passed back and forth through thousands of devices that may have exploitable vulnerabilities. A single weak link in the security system could provide hackers with nearly limitless backdoors that could potentially be unlocked, enabling them to access private and personal data.

The privacy of individuals is a serious concern not just in the IoT, but also in all the applications, devices, and systems where information is shared. Even when users take strong precautions to secure their information, there are conditions that arise that are beyond their control. People with malicious intentions can now target many different types of gadgets including smartphones and home-automation systems. Currently, more objects are linked to the Internet than people—at present, 25 billion devices are connected and it is expected that by 2020 more than 50 billion devices will be linked to the Internet (Sundmaeker et al., 2010). In this rapidly changing world, all the things that connect to the Internet are exponentially expanding their vulnerability for hackers and intruders. A recent study released by Hewlett Packard showed that 70 percent of IoT devices are vulnerable to hacking (Middleton, 2013). There is undeniable evidence that our dependence on interconnected technology warrants the

need to secure the devices for their safety and optimal performance. This paper highlights one of the new critical dangers facing the medical industry today, emphasizes the need for the immediate development of safety measures and an impenetrable cyber defense systems for all IoT applications of the healthcare industry, presents the current status of protection in IoT devices used in the medical world industry, draws attention to some of the progress made towards meeting this challenge, and urges greater impetus towards regulation and policy for adequate cyber protection.

## Cyber Attacks on Medical Data

Hospitals are evolving into a paperless environment with the introduction of electronic health records (EHR) for patients. Currently, Epic is one of the major software providers for EHR. However, the existing system faces challenges in data sharing, data compliance and data security (Rosenbaum, 2015). The medical industry has become the target of hackers for whom medical identity theft by the unlawful access to electronic health records (EHR) is a new lucrative business. Healthcare hacking has become an epidemic because medical data is more valuable than financial information. Data stolen from a bank quickly becomes useless once the breach is discovered and the passcodes are changed. However, healthcare data, which includes medical histories and personal identification, can last a lifetime. The information collected can be used for ransom, to commit tax frauds, to provide supporting disability documentation, to send fake bills to insurance providers, to obtain healthcare, prescription drugs, medical treatment, and to obtain government benefits like Medicare and Medicaid. Therefore, stolen medical data sells for 10-20 times more than credit card data. Additionally, victims of medical identity theft have no legal recourse to recover their losses, unlike credit card identity theft where the credit card provider has a legal responsibility to accountholders for amounts exceeding fifty dollars. The U.S Department of Health and Human Services, as required by Section 13042 (e) (4) of the HITECH Act, has posted a list of breaches involving more than 500 individuals, and currently, there are 1893 organizations on the list (Blumenthal, 2010). Industry consultants predict that in the next five years, one in thirteen patients will have their medical information compromised and cyber attacks on medical data will cost hospitals in the vicinity of 305 billion dollars (Filkins, 2014). On February 4, 2015, there was a huge breach of medical data information when personal identifiable medical and financial information of 78.8 million individuals was compromised during a hacking of Anthem Inc, the nation's second largest health insurance company, supposedly by a foreign government (Greene, 2015). On June 9, 2016, ProMedica, a healthcare organization in Ohio, issued a statement about a healthcare data breach after several of its employees inappropriately accessed the private medical records of patients they were not treating (Belliveau, 2016). In 2014, Community Health Systems Inc,

one of the largest U.S. hospital operators, revealed that Chinese hackers stole 4.5 million patient records (Humer, 2014). On June 3, 2016, the University of New Mexico hospital informed patients of a data breach that could potentially impact some of their personal data (University of New Mexico, 2017). The intrusion of ransomware, "a category of malicious software which, when run, disables the functionality of a computer in some way" (O'Gorman, 2012), into the Presbyterian Hospital in San Bernardino, in 2016, is alarming with its potential loss of data privacy and the associated financial expenditure involved in recovering system operability. In the same year, two other hospitals in California, along with the Hollywood Presbyterian Medical Center in Los Angeles, paid in bitcoin to unlock the hospital computer systems and regain access to their own computers (Sedlack, 2016). "Cyber criminals are increasingly targeting the $3 trillion U.S. healthcare industry, which has many companies still reliant on aging computer systems that do not use the latest security features" (Humer, 2014).

## Cyber Attacks on Medical Devices

Numerous medical devices commonly used today may be vulnerable to unauthorized access. For example, there are programmable, implantable, internal and external biomedical devices (such as pacemakers, defibrillators, insulin pumps, pain management pumps, vagus nerve stimulators, and spinal cord stimulators) that are susceptible to hacking. Intrusions may lead to the compromise of confidential patient data or loss of control of the device itself, which may be fatal (Frenger, 2012). Security vulnerabilities are severe in wireless connected devices, where not only the confidentiality of the patients data is at risk but also the processing of unauthorized commands. Although many patients benefit from these implantable devices, their number, connectivity, and especially remote-communication increase their security vulnerabilities (Maisel, 2010). In 2011, cyber security researcher J. Radcliffe found vulnerabilities in a drug infusion pump that a hacker could exploit to alter the drug dosage, even to a fatal dose, without the pump issuing an alert (Goodin, 2011; Radcliffe, 2011)

Government authorities in the United States and other regulatory organizations around the world have yet to develop adequate protocols for the safety of the wireless technology incorporated into medical devices and for the regulatory procedures to be adopted to prevent a deliberate attack on a medical device. The complacency exists partly because there has been no established attack on individual devices; therefore, there is a void in established procedure (Fu, 2011). Though a number of articles, such as "Killed by Code: Software Transparency in implantable Medical Devices" (Sutter, 2016), have been written about the possibility of an IoT-based life-threatening attack on an individual's device, it is reassuring to know that to date there are no known cases of deliberate harm caused to a

patient by hacking into their biomedical device. And yet that good fortune is no reason not to consider improving the security of these devices.

## Vulnerability of the Insulin Pump

In the 1960s, the first insulin pumps were designed but were not implantable because they were the size of a backpack. The first insulin pump was implanted in a human on the 5th of July 1980 and was the size of a deck of cards. Since then, the pump has evolved to be even smaller in size and to possess software and wireless capabilities that can track and manage glucose levels by the automatic injection of appropriate amounts of insulin. Since July 2012, the Food and Drug Administration (FDA) of the United States has permitted the implementation of Bluetooth 4.0 into a small system that can be attached to the belt of a patient with an insulin pump and that allows the management of the device by the patient as well as the communication of bidirectional information about the status of the patient. Pacemakers and other biomedical devices have also followed a similar trajectory of development and alignment with technology. In 2015, the FDA acknowledged the potential for Hofstra insulin pumps to be hacked. These pumps, present in all kinds of medical facilities from hospitals to nursing homes, utilize IoT to update the programs they use to deliver insulin. The FDA mandated health-care providers to reconfigure existing pumps, update their drug libraries, increase security and close any unused ports on the pump in response to approximately 56,000 reports of adverse events that occurred between 2005-2009 (Mansfield-Devine, 2016). These adverse events were the result of software defects, user interface issues and mechanical or electrical failures, not due to hacking of the pumps or a cyber security breach. The regulations mandated by the FDA did not address the issue of hacking or cyber security of the device (Shafer, 1988).

## Vulnerability of the Cardiac Implantable Devices

The pacemaker was first successfully implanted in Sweden in 1958. Prior to the 1970s, a diagnosis of heart disease or diabetes was similar to a death sentence or at least a life with medical complications and definitely a shorter life expectancy. About fifty years ago, biomedical industries began emerging all over the country with the goal of prolonging life, improving the quality of the extended life and restoring health. Towards this objective and keeping abreast of current developmental trends in technology, they invested in the innovation and design of products that increasingly rely on Internet technologies to accomplish the original purpose.

This has led to the creation of a large number of biomedical devices that have become omnipresent in today's world for the management and treatment of disease. These devices are extremely reliable and capable of operating for years or even decades inside the body of a patient. However, the engineering of these devices did not include the parallel development

of adequate security features like data encryption and user authentication, to protect the integrity of both the device and its benefit to the recipient. The design of security features to be incorporated into devices is challenging since access by doctors and medical staff is required, while unsanctioned access needs to be prohibited (Howarth, 2014). As battery technology developed, the pacemaker evolved, and, in the 1990s, the most advanced form incorporated a process called cardiac resynchronization therapy. In 2009, the pacemaker with Wi-Fi capabilities was first introduced with the principal beneficial improvement of remotely testing the device to optimize it or to alert doctors and patients of any malfunction. In 2015, a group of researchers at the University of Alabama attempted to hack into iStan, medical mannequins which are used for testing. They successfully conducted attacks on pacemakers within two different iStan mannequins and concluded that those pacemakers were at risk (Storm, 2016). Medical professionals are opting to use Wi-Fi for medical device connectivity because of the numerous benefits it provides. Connecting between a device and a hospital network can help patients, medical professionals and even caregivers. For example, access to a complete profile of patient data allows doctors to evaluate changes in a patient's medical history over time. While this level of access seems dangerous, it lets healthcare providers treat patients better by making more well-informed treatment decisions, and avoid wasting time and money. The telemetric tracking of medical data and its daily fluctuations in a congestive heart failure patient can save periodic visits to the ER by adjusting the dosage of diuretics and other medications. The real time alert of cardiac arrhythmias can save lives if it is ventricular fibrillation (Noland, 2015). Another benefit of the interconnectedness comes from the ability of a network-connected medical device to download new, perhaps more sensitive, settings or response libraries. What is significant and of vital importance is that mobile devices and medical devices share the same wireless connectivity possibilities. This means that both devices can be linked for messaging of instructions, information and alerts. Mobile devices have had more time to resolve wireless security issues and develop security protocols than medical devices, which aligned with technology at a later date (Sansurooah, 2015).

## Summary

The prospect of the deliberate manipulation of a biomedical device to create harm to an individual is even more critical than patient privacy issues. Medical devices are now susceptible to hacking and other security issues due to their wireless communications. Although wireless communication offers a great number of health advantages with new ones awaiting development, the biomedical industry needs to be equally cognizant of cyber security innovation and link it to new products as it engineers devices that function inter-connectedly with the Internet. Security complexity arises from the realities that implanted medical

devices are difficult to access physically, applying updates are extremely challenging, and it is complicated to pack enough computational resources inside implanted medical devices to be able to manage the entire range of cryptographic operations necessary to authenticate commands (Fu, 2009). A security paradigm must be developed in the future that ensures the safety and well-being of these device recipients. Policy changes are needed to encourage the adoption and standardization of innovative security defense mechanisms, to accelerate manufacturers' responses to security threats and to require detailed security incident reporting.

## Challenges to Implementing Change

The world of medical devices includes the manufacturers, the software developers, the hospital, the government authorities and the patients. All these stakeholders need to be aware of the dangers of a security malfunction or breach or intentional intrusion and the consequences of such an event. Like in all industries, the paramount purpose of the biomedical industry is for profit sufficient to continue to provide a valued service for humankind. Due to the lack of any documented attacks on medical devices, in the past, manufacturers have adopted the stance that a breach in security is not a serious threat. Recently, these industries are becoming increasingly aware of the possible security threats and the risk of not addressing security issues adequately, as the public and the government are being made cognizant of these facts through conferences and media. As manufacturers comprehend the legal expenses they could face, it is hoped that they will develop a functional security system of high integrity to maintain patient safety, despite the fact that government authorities have not yet required regulatory protocols and strict testing procedures. Additionally, the risk management experts in the companies will surely consider investing time and money in the forecasting of future attacks, considering the long legal battle and the costly repercussions that could follow a security lapse.

Software developers who design the system and the technology that ensures proper functioning of the devices have not been assigned the objective of incorporating security into the device. The developers are given the task of creating a product that meets the need of a patient and contributes to patient care; they are not involved in post-development cybersecurity threats. These experts who create software solutions have a limited understanding of security threats and are accustomed to interpret code in an environment without security challenges, while also working under pressure to develop and deliver the product to a highly competitive market. The cybersecurity professionals are trained in threat modeling, remediation, pre- and post-market considerations of product safety and should work with the IT experts to create a safe product.

Hospitals have not been structured to include software security as part of their operations. Therefore, they are not equipped to deal with the invasion of the security of a medical device, which requires the

intervention of a specialist. The IT department understands security but not medical equipment, while the medical staff understand the devices but not necessarily the security technology. This mentality is a hindrance to the advancement of security development. For the investment in software security to occur in hospitals, there must be adequate policies and guidelines created along with mandated requirements issued by the Department of Health and a concern for the best patient outcome. The hospitals are the organizations that have direct access to all the different stakeholders, and they should be the driving force in this endeavor.

## Responses to Changes

*Response by Federal Agencies*: The extensive buzz about the cyber security of biomedical devices has brought awareness and visible reactions in many connected organizations (Schwartz, 2016). In 2012, the Department of Homeland Defense identified implantable medical devices as a potential target for hackers and issued a national security bulletin on potential risks to medical devices. In March 2012, the Information Security and Privacy Advisory Board (ISPAB), an American public private federal advisory committee, published a number of recommendations to the federal government regarding the security of medical devices offering wireless capabilities, such as the creation of a dedicated cybersecurity division (NIST, 2012). Furthermore, the hospitals under the jurisdiction of the Department of Defense, which require compliance with DIACAP (Department of Defense Information Assurance Certification and Accreditation), states that any medical device that is connected to a military network be evaluated and certified from an information security standpoint before it can be used (Sandler et al., 2010). The question is whether these recommendations are being adequately followed.

The FDA declares that "medical device manufacturers and health-care facilities should take steps to ensure appropriate safeguards" (US FDA, 2013). They believe manufacturers are responsible for identifying risks and potential exploits associated with their medical devices. They place responsibility for mitigation and device performance in the hands of the manufacturers. They "look for and encourage reports of cyber security issues through our surveillance of devices already on the market" as stated in their 2017 cyber security guidelines for medical devices (FDA, 2017). In a guidance document released by the FDA on January 22, 2016, the FDA states that cyber security risk management is a shared responsibility among stakeholders such as the "medical device manufacturer, the user, the Information Technology (IT) system integrator, Health IT developers, and an array of IT vendors that provide products that are not regulated by the FDA". The FDA guidance is merely a guidance that manufacturers and providers are not obliged to follow (Coronado & Wong, 2014). The FDA seeks to encourage collaboration among stakeholders by clarifying, for those stakeholders it regulates, recommendations associated with

mitigating cyber security threats to device functionality and device users. In an FDA report published in 2013, the FDA has identified cyber security vulnerabilities and challenges that hospitals could be facing in the future. They include malware on hospital networks, uncontrolled distribution of passwords to hospital personnel, failure to provide timely software updates and updates to medical devices and hospital networks, and addressing vulnerabilities in legacy devices. Keeping the objective of mitigating and managing cyber security threats, the FDA has recommended that medical device companies and healthcare facilities ensure that adequate safeguards are in place to prevent the risk to patients from becoming a reality (Sandler et al., 2010).

The true commitment of the government in dealing with a perilous and high-risk challenge is demonstrated by the allocation of funding that is earmarked to resolve the issue. In January 2016, President Obama signed into law, legislation that requires the United States Department of Health and Human Services (HHS) to impanel a Healthcare Industry Cybersecurity Task Force to hammer out standards for healthcare cyber security (Public Health Emergency, 2016). Despite this legislation, the National Institutes of Health (NIH), did not specifically earmark any funding in its $31.3 billion 2016 budget for cyber security in biomedical devices. The National Science Foundation (NSF) in its $7.724 billion 2016 budget has a 16% investment in Secure and Trustworthy Cyberspace (SaTC) that focuses on long term, foundational cyber security research, "to protect and preserve the growing social and economic benefits of cyber systems while ensuring security and privacy" (NSF, 2017). It attempts to meet the needs of the Computer and Information Science and Engineering (CISE) Directorate, interdisciplinary projects with Math and Physical Science (MPS) and Engineering (ENG), to fund proposals on hardware security with semiconductor research programs, to sponsor proposals that are focused exclusively on transitioning existing research to practice, and to provide scholarships for cyber security education and research. There is no emphasis on cyber security in medical devices; however, a Dartmouth proposal that designs cyber security measures for a home-based healthcare system has received funding.

*Response by Professionals:* Black Hat USA is a conference that has existed for about twenty years, and it sets the benchmark for all other security conferences. It brings together leaders from all facets of the information security world, including experts from the corporate, government and academic sectors and even includes underground researchers. The Black Hat conference is a global series of technical events and a premier venue for elite security researchers and prestigious thinkers that stay on the cutting edge of new security trends and challenges as they emerge. Information technology security experts have been warning the public about cyber-threats using conferences such as Black Hat to publicize new vulnerabilities in systems and software. At the 2014

Black Hat conference, discussions were focused on the security of the Internet of Things as they brought together the best minds in security to define the information security landscape of the future and showcased the latest tools and solution providers in the industry. The conference provided training courses to offer essential knowledge and skills to defend against current threats and delivered timely actionable security information in an easily accessible environment (Geer, 2014). At the conference, many sessions discussed the cyber security of medical devices. Additionally, they highlighted some of the challenges: security in all devices are not universal and in some devices it would be impossible to include strong authentication; it is not always clear which government agency hold the responsibility of the device security since some devices are regulated by the FDA, some by the FCC and others by the DHS (Rashid, 2014).

*Response by one of the major biomedical companies, Medtronic PLC:*
Medical devices have not historically been included in HIPAA compliance or healthcare security programs, yet their capabilities make them targets for cyber security attack. Like other computer systems, these devices can be vulnerable to security breaches, potentially impacting the effectiveness of the device and the safety and privacy of the patient. In the corporate world, Medtronic Inc., one of the largest manufacturers of biomedical devices in the US, takes device security and patient safety very seriously and accepts that the responsibility for the security of these devices rests with the manufacturer. Therefore, the company is working extensively with the FDA. Wendy Dougherty, spokeswoman for Medtronic Inc., in response to the comment that the company does not emphasize security of its devices, responded that the company is willing to work with the FDA to establish "formal device security guidelines." The company is aware of potential security risks to implanted medical devices, she said. "Safety is an integral part of our design and quality process. We're constantly evolving and improving our technologies." However, in a written statement, Dougherty described the risk of someone hacking into a wireless medical device as "extremely low" (Storm, 2016). Medtronic is actively engaged with security research firms and regularly conducts independent assessments to monitor the security of the devices and identify potential vulnerabilities without compromising the therapy that the device is designed to deliver (Medtronic, 2013).

Michael McNeil, global security privacy leader at Medtronic, emphasizes that the delicate balance between keeping medical devices secure and patient protection must be maintained, without overcompensation by adding an extra layer of security that reduces efficacy of the device. Medtronic has consolidated privacy and security under one governance structure and includes in this corporate division, the protection of intellectual property, of patient data, of customer privacy and of device integrity. There is a heightened awareness of cyber security in

medical devices in the regulatory landscape. As an industry, Medtronic is taking a holistic approach to the issue by continually performing internal and external testing and ongoing monitoring, remediation, collaboration with regulatory organizations, development of contingency planning and incident response management, and working with ethical hackers and IT experts to create a winning strategy (McGee, 2013).

## Conclusion

Many of the best security practices can be leveraged, such as hardening the systems, using secure protocols for communication or installing the latest updates, fixes and patches. Innovators need to consider that future security will be managed automatically by the system instead of users, and designing secure technology will require a new approach and a growth mindset. Kevin Fu, a graduate researcher at the University of Michigan whose research focuses on cyber security in medical devices, emphasizes that while this is a growing fear, it should be viewed in perspective, considering that most patients experience tremendous gain from the implantation of the device, far greater than the associated risk from a security breach. There are many facets to the problem: devices using outdated operating systems are easy targets for malware, plugging unverified USBs into devices, lack of safety awareness in hospital settings and many more. Despite all the security gaps existing, Fu is of the opinion that the benefits of medical devices to patients who desperately need them far outweigh the security hazards that potentially exist and that can and should be addressed (HealthTrust, 2015).

Frank Platt, information security consultant and Certified Information Security Systems Professional, comments, “To truly mitigate the risk, organizations need several layers of technical, operational and management controls around assets containing vital information. It’s what we call a defensive depth approach” (HealthTrust, 2015). Ultimately, as Fu adds, smarter thinking and action will help us stay ahead. Finally, several cyber defense and data security companies have jumped into the fray to prevent what is science fiction today from becoming tomorrow’s reality (Basu, 2013; Sansurooah, 2015).

## Acknowledgements

The author acknowledges, with grateful thanks, his mentor and advisor, Professor John Willinsky, who successfully guided him and provided expert advice during the independent study that led to the publication of this paper.

## References


Arora, S., Yttri, J., & Nilsen, W. (2014). Privacy and security in mobile health (mHealth) research. *Alcohol research: current reviews*, *36*(1), 143.

Basu, E. (2013). Hacking Insulin Pumps and Other Medical Devices from Black Hat. Retrieved May 1, 2014, from https://www.forbes.com/sites/ericbasu/2013/08/03/hacking-insulin-pumps-and-other-medical-devices-reality-not-fiction/#1f77da6121f8

Belliveau, J. (2016). Improper Employee Access Creates Potential Health Data Breach. *HealthITSecurity*. Retrieved June 9, 2016, from http://healthitsecurity.com/news/improper-employee-access-creates-potential-health-data-breach

Blumenthal, D. (2010). Launching hitech. *N Engl J Med*, *2010*(362), 382-385.

Clark, S. S., & Fu, K. (2011, October). Recent results in computer security for medical devices. In *International Conference on Wireless Mobile Communication and Healthcare* (pp. 111-118). Springer, Berlin, Heidelberg.

Coronado, A. J., & Wong, T. L. (2014). Healthcare cybersecurity risk management: Keys to an effective plan. *Biomedical instrumentation & technology*, *48*(s1), 26-30.

FDA. (2017, March 03). Digital Health - Cybersecurity. Retrieved April 16, 2017, from https://www.fda.gov/MedicalDevices/DigitalHealth/ucm373213.htm

Filkins, B. (2014). Health care cyberthreat report. *Widespread compromises detected, compliance nightmare on horizon.* Bethesda, MD: SANS Institute.

Frenger, P. (2013). Hacking medical devices a review-biomed 2013. *Biomedical sciences instrumentation*, *49*, 40-47.

Fu, K. (2009). Inside risks Reducing risks of implantable medical devices. *Communications of the ACM*, *52*(6), 25-27.

Fu, K., & Blum, J. (2013). Controlling for cybersecurity risks of medical device software. *Communications of the ACM*, *56*(10), 35-37.

Geer, D. (2014). Cybersecurity as realpolitik. *Black Hat USA 2014*.

Goodin, D. (2011). Insulin pump hack delivers fatal dosage over the air. *The Register*.

Greene, T. (2015). Biggest data breaches of 2015. *Network*, *10*, 14.

Halperin, D., Heydt-Benjamin, T. S., Fu, K., Kohno, T., & Maisel, W. H. (2008). Security and privacy for implantable medical devices. *IEEE pervasive computing*, *7*(1).

HealthTrust. (2017, March 01). Cybersecurity and Medical Devices. Retrieved January 30, 2017, from http://healthtrustpg.com/healthcare-innovation/cybersecurity-and-medical-devices/

Horowitz, B. T. (2017, July 09). FDA, DHS Warn Medical Device Makers, Hospitals on Cyber-Threats. Retrieved March 30, 2017, from

http://www.eweek.com/security/fda-dhs-warn-medical-device-makers-hospitals-on-cyber-threats

FDA. (2017). Digital Health - Cybersecurity. U S Food and Drug Administration Home Page. Center for Devices and Radiological Health.

Howarth, F. (2014, August 15). Black Hat 2014: Where the Internet of Things Meets Reality. Retrieved January 30, 2017, from https://securityintelligence.com/black-hat-2014-where-the-internet-of-things-meets-reality/

Humer, C., & Finkle, J. (2014). Your medical record is worth more to hackers than your credit card. *Reuters.com US Edition*, *24*.

Klitou, D. (2014). Human-Implantable microchips: Location-Awareness and the dawn of an "Internet of Persons". In *Privacy-Invading Technologies and Privacy by Design* (pp. 157-249). TMC Asser Press.

Maddox (2015, February 18). Cisco: The Internet of Everything is at tipping point. Retrieved March 30, 2017, from http://www.techrepublic.com/article/cisco-the-internet-of-everything-is-at-tipping-point/

Maisel, W. H. (2010). Improving the security and privacy of implantable medical devices. *The New England Journal of Medicine*, *362*(13), 1164.

Mansfield-Devine, S. (2016). Securing the Internet of Things. *Computer Fraud & Security*, *2016*(4), 15-20.

Manyika, J. (2015). *The Internet of Things: Mapping the value beyond the hype*. McKinsey Global Institute.

Manyika, J., Chi, M., Bisson, P., Woetzel, J., Dobbs, R., Bughin, J., and Aharon, D. (2015). The Internet of Things: Mapping the Value Beyond the Hype. *McKinsey Global Institute*.

Medtronic. (2013, October 19). Medtronic Statement on Medical Device Security. Retrieved from http://newsroom.medtronic.com/phoenix.zhtml?c=251324&p=irol-newsArticle&ID=1866063

Middleton, P., Kjeldsen, P., & Tully, J. (2013). Forecast: The Internet of Things. *Worldwide. Gartner*.

Mientka, Matthew (2013). Body Hacking: Do Implantable Medical Devices Make Humans Susceptible To Cyber-Attacks? *Medical Daily.* Retrieved from http://www.medicaldaily.com/body-hacking-do-implantable-medical-devices-make-humans-susceptible-cyber-attacks-260395

NIST. (2012). Information Security and Privacy Advisory Board (ISPAB). Retrieved from http://csrc.nist.gov/groups/SMA/ispab/index.html

Noland, B. (2015, July 21). Real-time Analytics on Medical Device Data – Part 1 – Introduction. *phData.* Retrieved July 10, 2017, from https://www.phdata.io/real-time-analytics-on-medical-device-data/

NSF. (2011, December 2). Directorate for Computer & Information Science & Engineering. Retrieved January 30, 2017, from https://www.nsf.gov/mobile/funding/pgm_summ.jsp?pims_id=504709

O'Gorman, G., & McDonald, G. (2012). *Ransomware: A growing menace*. Symantec Corporation.

Public Health Emergency. (2017, June 16). Health Care Industry Cybersecurity Task Force. Retrieved July 10, 2017, from https://www.phe.gov/preparedness/planning/CyberTF/Pages/default.aspx

Radcliffe, J. (2011, August). Hacking medical devices for fun and insulin: Breaking the human SCADA system. In *Black Hat Conference presentation slides* (Vol. 2011).

Rashid, F. (2014, August 08). BlackHat 2014: Medical Device Security Not as High Risk as Previously Claimed. Retrieved March 30, 2017, from https://www.infosecurity-magazine.com/news/medical-device-security-not-as/

Rosenbaum, L. (2015). Transitional chaos or enduring harm? The EHR and the disruption of medicine. *N Engl J Med*, *2015*(373), 1585-1588.

Sametinger, J., Rozenblit, J., Lysecky, R., & Ott, P. (2015). Security challenges for medical devices. *Communications of the ACM*, *58*(4), 74-82.

Sandler, K., Ohrstrom, L., Moy, L., & McVay, R. (2010). Killed by code: Software transparency in implantable medical devices. Software Freedom Law Center, 308-319.15.

Sansurooah, K. (2015). Security risks of medical devices in wireless environments. *4th Australian eHealth Informatics and Security Conference.*

Schwartz, S. B. (2016, October 27). National Cyber Security Awareness Month: Understanding the Interdependencies of Medical Devices and Cybersecurity. Retrieved February 30, 2017, from https://blogs.fda.gov/fdavoice/index.php/2016/10/national-cyber-security-awareness-month-understanding-the-interdependencies-of-medical-devices-and-cybersecurity/

Sedlack, D. (2016). Understanding Cyber Security Perceptions Related to Information Risk in a Healthcare Setting.

Shafer, S. L., Siegel, L. C., Cooke, J. E., & Scott, J. C. (1988). Testing computer-controlled infusion pumps by simulation. *Anesthesiology*, *68*(2), 261-266.

Storm, D. (2015, September 8). Technology news | latest news about information technology & world IT. Retrieved January 30, 2017, from http://www.debtfree4ever.net/researchers-hack-a-pacemaker-kill-a-mannequin/

Sundmaeker, H., Guillemin, P., Friess, P., & Woelfflé, S. (2010). Vision and challenges for realising the Internet of Things. *Cluster of*

*European Research Projects on the Internet of Things, European Commision*, *3*(3), 34-36.

Sutter, J. D. (2016). Scientists work to keep hackers out of implanted medical devices. *CNN.* Retrieved from http://www.cnn.com/2010/TECH/04/16/medical.device.security/index.html

UNM Health sciences Center. (2016, June 03). UNMH notifies patients of limited data breach. Retrieved March 30, 2017, from http://hscnews.unm.edu/news/unmh-notifies-patients-of-limited-data-breach

US FDA (2014). "What we do". Retrieved from http://www.fda.gov/aboutfda/whatwedo/default.htm

US Food and Drug Administration. (2013). Cybersecurity for medical devices and hospital networks: FDA safety communication. Retrieved September, 19, 2014, from https://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm356423.htm

Weber, R. H., & Weber, R. (2010). Internet of Things (Vol. 12).

Williams, P. A., & Woodward, A. J. (2015). Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem. *Medical devices (Auckland, NZ)*, *8*, 305.