ETHICS AND TECHNOLOGY/ETHICS REPORT

J. Heal Ethics Admin
Volume 4 | Number 2 (Fall/Winter 2018)
www.jheaonline.org
ISSN 2474-2309 | doi:10.22461/jhea.6.7162
https://doi.org/10.22461/jhea.6.7162
Published Dec. 20, 2018

The Current Ethical and Regulatory Status of the Internet of Medical Thing (IoMT) and the Need of a New IoMT Law.

WILLIAM OSEI-BONSU[1] AVIEL STEIN[2] AND MICHAEL BOSWELL[3]

wo23@drexel.edu,[1] ajs568@drexel.edu,[2] mab669@drexel.edu[3]

[1. 2. 3.] Electrical and Computer Engineering Department, Drexel University, Philadelphia, Pennsylvania, U.S.A.

***Keywords**: Cybersecurity, digital pill, internet of medical thing (IoMT), privacy violation.*

I. INTRODUCTION

Many decades ago the telephone was our only means of connection to the outside world from the privacy of our homes. Policymakers enacted regulations to protect individual privacy with the explicit purpose of preventing unauthorized eavesdropping of private conversations. Decades later, the Internet revolutionized our connectivity, and similarly, regulation was passed to protect personal communication over the Internet. Today, with the advent of ubiquitous connectivity and the emerging Internet of Things (IoT) paradigm, all manners of devices can be connected to the Internet. Among these IoT devices is the so-called Internet of Medical Things (IoMT) which are medical devices ranging from personal health monitoring devices like Fitbit, to life-critical devices like pacemakers, and even a new emerging phenomenon of digital pills – a pill with embedded tracking sensor which communicates with a wearable patch to determine if a pill is taken as prescribed. While these innovations in medical device technology have many positive aspects, they also share cybersecurity threats that any Internet-connected device faces. These threats include breach of data privacy and other adversarial threats like stealing or destroying information, causing personal injury, and in some cases digital extortion. Many of these IoMTs are available through legal distribution channels that exclude them from existing data privacy and cybersecurity regulations.

Broadly speaking, there are two domains of cybersecurity threats: those perceived at a personal level, facing consumers of IoMT, and those related to public security issues including national security. However, the two domains cut across each other because they are closely related to each other. The entire world is already connected in a complicated manner. Different layers of connectivity exist from governmental through organizational to personal levels. In the U.S. alone, it has been a while since the Food and Drug Administration (FDA) began "tracking millions of medical devices, from pacemakers to hip replacements, using a new electronic system designed to protect patients by catching problematic implants."[1] The FDA even published new rules in Sept 2013 that required "most medical devices sold in the U.S. to carry a unique code, identifying its make, manufacture date, and lot number" so that the codes … stored in a publicly accessible database [could] help regulators, doctors and companies monitor safety issues with

[1] Matthew Perrone, "FDA Requires Tracking Codes on Medical Implants," *NBC News* September 20, 2013, https://www.nbcnews.com/healthmain/fda-requires-tracking-codes-medical-implants-4B11215906

*Address correspondence to: William Ose-Bonsu, Electrical and Computer Engineering Department, Drexel University, 3175 Chestnut St, Philadelphia, PA 19104, U.S.A. E-mail: wo23@drexel.edu.

+To cite this article: William Osei-Bonsu, Aviel Stein, and Michael Boswell, "The Current Ethical and Regulatory Status of the Internet of Medical Things (IoMT) and the Need of a New IoMT Law, " *The Journal of Healthcare Ethics & Administration* 4, no. 2 (Fall/Winter 2018): 32-38, https://doi.org/10.22461/jhea.6.7162

devices."[2] In 2017, the FDA approved pills with a digital tracking device in it.[3] The pill with embedded tracking sensor which communicates with a wearable patch to determine if the pill is taken as prescribed will, of course, be tracked by the governmental organizations, device makers, doctors, and the patients themselves.

There are no easy solutions for security problems. In this paper, we intend to help healthcare professionals, health administrators, and bioethicists understand where we are situated in the light of the advance of medical technology related to cybersecurity problems and how effective our current regulatory measures are. To do so, we will outline some of the main cybersecurity challenges facing connected medical devices powered by the IoMT technology, discussed the status quo concerning regulations and healthcare consumer data protection, and discussed the price of inaction to the healthcare consumers. We will also highlight the fact that there is no single governmental or industry entity entrusted to ensure cybersecurity integrity of IoMT devices leaving consumers with uncertainties about who owns their healthcare data (device manufacturer, app developer, etc.) and how to protect them. In the end, we make policy proposals to overcome the introduced difficulties as a way of setting a regulatory paradigm of IoMT to improve the delivery of healthcare.

II. BACKGROUND

A. The internet of Medical Thing (IoMT)

In recent years, the medical field has been able to make huge strides in providing curated healthcare to individuals that has been the direct result of the explosion of connected medical devices which are able to collect troves of information on individuals and transmit the data back to a healthcare provider or application for analysis and more accurate treatment. These devices, commonly known as IoMT devices, can connect to other devices over a public or private network (Johnson, 2018). IoMT devices may be assistive devices like hearing aids, life-sustaining devices like pacemakers, and personal fitness tracking device. An emerging class of smart digital pills has ingestible sensors that can detect when it is swallowed and connect to a wearable patch to record the medication time and dosage taken. The recorded information can then be reviewed later on to ascertain compliance to the prescription regimen. Such connected medical devices allow consumers and healthcare providers alike to monitor trends in lifestyle continuously and effectively manage healthcare needs.

B. The ubiquity of IoMT in Near Future

According to *Forbes* magazine, IoT spending will approach $267 billion by 2020 with healthcare industry accounting for $15 billion and is expected to increase up from $4 billion in 2015.[4] By 2025, it is expected that 12.5% of the world's population will be considered elderly, which naturally comes with higher healthcare costs and treatment. As a result, IoMT is seen as a potential combatant to the growing number of healthcare concerns and associated costs because it has the potential to provide preemptive medical attention by using the data to be collected and transmitted over the network. It currently has a projected market cap of $136.8 billion by 2021 with 3.7 million devices currently connected to the Internet.[5] In the U.S. alone, the healthcare industry represents 18% of U.S. GDP and has the second highest GDP share in the U.S. economy. The use of IoMT devices and its spending would be the topics of discussion among health industry leaders and medical professionals shortly.

[2] Ibid.

[3] Susan Scutti, "DA Approves Pill with Digital Tracking Device You Swallow," *CNN*, November 15, 2017 https://www.cnn.com/2017/11/14/health/fda-digital-pill-abilify/index.html

[4] Louise Columbus, "A Roundup of 2018 Enterprise Internet of Things Forecasts and Market Estimates," *Enterprise CIO*, January 3, 2018, https://www.enterprise-cio.com/news/2018/jan/04/roundup-of-internet-of-things-forecasts-and-market-estimates-2018/

[5] Bernard Marr, "Why the Internet of Medical Things (IoMT) will Start to Transform Healthcare In 2018," *Forbes*, January 25, 2018, https://www.forbes.com/sites/bernardmarr/2018/01/25/why-the-internet-of-medical-things-iomt-will-start-to-transform-healthcare-in-2018/#2ed8af0f4a3c

C. The IoMT Cybersecurity Problem

There are many cybersecurity risks associated with the use of IoMT devices. These range from compromising device safety, data privacy violation, and information theft and destruction, to abuse and misuse of consumer healthcare information. The security needed to protect these connected devices has not been able to keep up with the technological advancements that enable attackers to compromise the devices. One report indicates that in 2017 the healthcare industry saw an average "of almost 32,000 intrusion attacks per day" with the IoMT representing two of the top ten vulnerability exploits of attackers.[6]

One of the most publicized cyber-attacks against the industry was the “WannaCry” ransomware in 2017 which resulted in a significant disruption in medical service to patients such as the cancellation of surgeries and ambulances being diverted from areas of need.[7] It affected many hospitals, requiring them to take many crucial services offline such as MRI and X-Ray machines. Although the WannaCry attack mainly affected servers and desktop computers, a similar attack to personal wearable medical devices is expected to occur because such devices are essentially portable computers often with simple hardware and software that attackers can easily break into. The WannaCry ransomware demanded payment of $300 to $600 from victims and while it is unknown exactly how much payout the attackers received, infecting thousands of computers increases the odds of gaining substantial payouts from victims.

III. THE THREAT OF INACTION

Vulnerable IoMT devices pose a significant risk to the public. These risks include cyber threats from bad actors that can steal, destroy, or hold health information for ransom. They can also engage in unauthorized disclose the information to violate personal privacy. Meanwhile, some manufacturers of IoMT devices and software may lack the resources or financial motivation to invest in securing their devices. We discuss these threats in the following sections.

A. Cyber Threats

One risk to IoMT devices is a cyber attack. The *WannaCry* attack in 2017, as well as countless other attacks, have mostly been the result of well-calculated exploits in human and technical systems. Imagine a WannaCry-style attack where the target is not servers and desktop computers, but personal IoMT devices. The attacker can seek ransom payment from an IoMT consumer under the threat of disabling, say, a pacemaker in the middle of the night (a classic ransomware attack) or threaten to make available to the general public the private vital medical data collected by a wearable connected medical device (a leakware attack).

B. Lack of Vendor Responsibility

At the time of the "WannaCry" attack, there was an available patch developed by Microsoft that could have prevented the attack on most computer systems. However, many organizations went without updating their software for fear that "Windows updates can screw up their legacy software programs."[8] This type of thinking has led to many companies not proactively to update their software, leaving the public they serve exposed. The situation is even more dire for small personal and wearable computers. Unlike traditional software and device vendors like Microsoft and Apple with immense financial and technical resources, many wearable device manufacturers and small-scale app developers lack the resources or the business motivation to investigate and provide regular security patches to secure their devices or apps leaving these devices vulnerable to cyber-attack.

[6] Ladi Adefala, “Healthcare Experiences Twice the Number of Cyber Attacks as Other Industries,” *CSO*, March 6, 2018, https://www.csoonline.com/article/3260191/security/healthcare-experiences-twice-the-number-of-cyber-attacks-as-other-industries.html

[7] David Goldman, “Global Cyberattack: a Super-Simple Explanation of What Happened,” *CNN*, May 15, 2017, http://money.cnn.com/2017/05/14/technology/global-cyberattack-explanation/index.html

[8] Ibid.

C. Privacy Violation & Information Misuse

Another risk to IoMT devices is the breach of privacy. Many wearable medical devices collect health information from the user and push it into a cloud for storage or analysis on behalf of the user. However, it is not clear whether such healthcare information enjoys the same protection under the HIPPA privacy laws. The only protection seemingly offered to users is the Terms of Service (TOS) which is so onerous and riddled with legalese to the extent that the average user will acknowledge the TOS without reading it and thereby signing away their privacy. This can allow providers to use the information gathered to target users with an advertisement, sell the information to third parties for similar purposes, and even worse, allow an insurance company to screen or exclude people from services based on their publicly available personal health records.

D. Other Security Implications

Besides, as these devices become more ubiquitous with widespread use that rival cell phones, rampant security flaws can allow terrorists and state-sponsored actors to attack a large portion of the public simultaneously. Attackers can also target wearable IoMT devices of prominent public or political figures or pose a national security risk in some situations. For instance, the *New York Times* article, "Strava Fitness App Can Reveal Military Sites, Analysts Say," published in Jan. 2018, reports how a fitness app developed by the IT company named Strava can raise a serious national security concern in the U.S.[9] It is common nowadays that people use wearable technology like Apple Watch, Samsung Smartwatch, etc. to check their daily routines, track their physical activities, and so forth. Strava is a fitness wearable that tracks athletic activity. It uses satellites through which people can share their fitness activities including whereabouts. In this day and age, people, especially young generation, enjoy connectivity, and the corporation that can provide it can boast its power. However, that can be a serious problem. In Strava's the global "heat map," the locations of its 8 million members are tracked. Since the app is popular among the U.S. military, the U.S. bases in Afghanistan, Iraq, and Syria are exposed in detail, underscoring the far-reaching consequences of IoMT security breaches that can affect even national security.

IV. THE POLICY CONTEXT

While any underlying security solution to the IoMT cyber threat will be technical, effective policies are necessary to guide the industry to protect consumers from the usage of this technology. Several existing agencies in the U.S. could regulate aspects of this industry yet there are still gaps in the system. Among these are:

- The US Federal Drug Administration (FDA) of the Department of Health and Human Services
- The Federal Communication Commission, an independent body within the US government
- The Federal Trade Commission, another independent body within the US government
- The Health Insurance Portability and Accountability Act (HIPAA) enforced by the Office for Civil Rights (OCR) of the Department of Health and Human Service

We describe below the jurisdictions of these regulatory bodies, how they impact the security of IoMT devices, and the limitations and any policy loopholes of the existing policies and regulations.

A. The FDA & IoMT Security

In recent years, the FDA has taken more aggressive steps to ensure that IoMT devices are secure. However, they have stopped short of providing mandatory requirements and had mostly provided recommendations only. The FDA, in consultation with the Center for Devices and Radiological Health and the Center for Biologics Evaluation and Research, has developed guidelines for mobile medical applications (The FDA, 2015). While this is a step in the right direction, FDA's oversight is limited to regulating a subset of medical

[9] Richard Pérez-Peña and Matthew Rosenberg, "Strava Fitness App Can Reveal Military Sites, Analysts Say," *The New York Times*, January 29, 2018, https://www.nytimes.com/2018/01/29/world/middleeast/strava-heat-map.html

devices and software that fall under section 201(h) of the Federal Food, Drug, and Cosmetic Act (FD&C Act). This limits the regulation to devices and software whose malfunction could pose a physical health risk to patient safety. Many apps and IoM devices on the market that monitor, collect, analyze, and store personal medical data fall outside the purview of the FDA.

B. The FCC, NIST & IoMT Security

The Federal Communications Commission (FCC) is another regulatory agency that has oversight over IoMT devices simply because they contain electronics and wireless technology. The FCC is mainly concerned about possible harmful radiation from the devices that can affect people or interfere with proper operation of other devices. FCC does not mandate or enforce compliance of these devices with any cybersecurity standards. Similarly, the National Institute of Standards and Technology (NIST) defines cybersecurity standards that must be met by connected devices. NIST publishes guidelines and best practices with regard to security of connected devices but does not enforce or mandate compliance.

C. The FTC & IoMT Security

The Federal Trade Commission is tasked with enforcing laws that protect consumers. For IoMT devices that fall outside the regulatory authority of the FDA, the FTC perhaps comes the closest to ensuring the protection of consumer information which includes IoMT devices that create, collect, or share consumer health information. However, the FTC does not directly deal with cybersecurity risk posed by such devices.

D. HIPAA & IoMT Security

The HIPAA security laws, another option to consumers regarding privacy and security of their healthcare information, is not applicable if the collector of the healthcare information is not a HIPAA covered entity such as healthcare providers in the business of collecting and using such information to provide a service to the consumer. For instance, if someone purchases a Fitbit device from Walmart for their personal use, the information collected and transmitted by such a device is not covered by the HIPAA regulation. However, the same device obtained through a healthcare provider to provide healthcare would likely fall under the HIPAA rules. This means mobile app developers and IoMT device manufacturers who are not in the business of providing healthcare services are outside the HIPAA regulations even though they collect similar personally identifiable health information.

V. POLICY RECOMMENDATIONS

As shown above, despite the presence of the different regulating bodies, there is no clear single policy goal or a set of regulatory measures that protect all manners of health information. Also, there is no solid set of governing rules that apply to the connected medical devices. All this would leave consumers at risk by exposing medically connected devices to cyber threats. Therefore, we offer the following policy recommendation and discuss potential drawbacks of these recommendations.

A. One Single Authority Responsible for IoMT Security Regulation

There should be one authority in the public or private sector responsible for ensuring that IoMT meets certain minimum standards for cybersecurity. We propose a policy position that will bring all stakeholders together to find a means to ensure the security of all wearable devices that have connectivity to the network. An example of such a policy direction is expanding the existing HIPAA laws to include all collection of medical information by non-consumers, regardless of the entity doing so. One way of making this happen is to expand the FDA's authority to require a minimum set of cybersecurity requirements defined by the industry under NIST guidance. This device certification will be based on physical health and cybersecurity risks. However, one concern about this is that, although NIST collaborates with industry when developing security guidelines, they have no enforcement authority. This means that an agency like the FDA and OCR will have to take the NIST recommendations and enforce them across the board.[10]

B. A New Regulation to Protect Universal Health Information

There should be a development of new regulations that define the ownership of health information collected by any third-party entity as well as what information is considered health information. This approach ensures a tailored solution to the problem and has a great opportunity to address all the current loopholes. We do realize that this recommendation has some potential drawbacks. That is, being a brand-new law, it will take time to be properly craft and vet it. The longer it takes to develop such new laws, the longer it will take to come with a solution to this urgent issue and leave consumers vulnerable. This problem could also be compounded by the fact that any new regulation runs the risk of not having the relevant experts and stakeholders involved in the conversation. However, while it is impossible to have everyone at the table and to account for all possible scenarios, the new regulation must be all-encompassing to address all the vast amounts of IoM originated health information that falls outside the reach of all regulations.[11]

VI. BIBLIOGRAPHY

Adefala, Ladi. “Healthcare Experiences Twice the Number of Cyber Attacks as Other Industries.” *CSO*, March 6, 2018. https://www.csoonline.com/article/3260191/security/healthcare-experiences-twice-the-number-of-cyber-attacks-as-other-industries.html

Columbus, Louise. “A Roundup of 2018 Enterprise Internet of Things Forecasts and Market Estimates.” *Enterprise CIO*, January 3, 2018. https://www.enterprise-cio.com/news/2018/jan/04/roundup-of-internet-of-things-forecasts-and-market-estimates-2018/

Goldman, David. “Global Cyberattack: A Super-Simple Explanation of What Happened.” *CNN*, May 15, 2017. http://money.cnn.com/2017/05/14/technology/global-cyberattack-explanation/index.html

Marr, Bernard. “Why the Internet of Medical Things (IoMT) will Start to Transform Healthcare In 2018.” *Forbes*, January 25, 2018. https://www.forbes.com/sites/bernardmarr/2018/01/25/why-the-internet-of-medical-things-iomt-will-start-to-transform-healthcare-in-2018/#2ed8af0f4a3c

Pérez-Peña, Richard, and Matthew Rosenberg. “Strava Fitness App Can Reveal Military Sites, Analysts Say.” *The New York Times*, January 29, 2018. https://www.nytimes.com/2018/01/29/world/middleeast/strava-heat-map.html

Perrone, Matthew. “FDA Requires Tracking Codes on Medical Implants.” *NBC News,* September 20, 2013. https://www.nbcnews.com/healthmain/fda-requires-tracking-codes-medical-implants-4B11215906

[10] There is also the concern of industry treating the standard as the limit of what they must do to secure IoMT devices and information. To combat this and encourage stronger security above the minimum, the government could create a database of manufacturers and rank them based on meeting and exceeding the minimum-security standard.

[11] The policy recommendations we make affect the following stakeholders: 1. Individuals Healthcare Consumers: Individual healthcare customers will have concerns about how the devices will affect their everyday life, what risks may arise from using one devise, what alternatives to that device exist, and what future options might look like. 2. Healthcare providers: Although currently covered under HIPAA, providers will want to make sure the new policy does not add undue administrative overhead to their operation. They will also be key early adopters of any new security technologies and help with patient education to ensure healthcare data is protected everywhere. 3. Medical Device Manufacturers: they will be concerned with any technological solutions and the impact it can have on their cost of manufacturing and supporting the IoMT devices. 4. National Agencies (HHS, DHS, FDA, FTC): As gatekeepers of the any ensuing regulation these agencies must be involved to ensure that any regulations can be smoothly enforce without administrative hurdles. These stakeholders must be brought together to discuss the existing problem and implications of the each of the recommended policies.

Scutti, Susan. "DA Approves Pill with Digital Tracking Device You Swallow." *CNN*, November 15, 2017. https://www.cnn.com/2017/11/14/health/fda-digital-pill-abilify/index.html