Legal Requirements towards Enhancing the Security of Medical Devices

Prosper K. Yeng[1]
Department of Information Security
and Communication Technology
NTNU
Gjøvik, Norway

Stephen D. Wulthusen[2]
Department of Information Security
and Communication Technology
NTNU
Gjøvik, Norway
School of Mathematics
and Information Security
Royal Holloway, University of London
Egham, United Kingdom

Bian Yang[3]
Department of Information Security
and Communication Technology
NTNU
Gjøvik, Norway

***Abstract*—Over 25 million Americans are dependent on medical devices. However, the patients who need these devices only have two choices, thus the choice between using an insecure critical-life-functioning devices or the choice to live without the support of a medical device with the consequences of the threats presented by the disease. This study therefore conducted a state-of-the-art on security requirements, concerning medical devices in the US and EU. Food, Drugs and Cosmetic Act, HIPAA, Medical Device Regulations of EU and GDPR were some of the identified regulations for controlling the security of these devices. Statutory laws such as computer Fraud and abuse Act (CFAA), Anti-Tempering Act, Panel Code as well as Battery and Trespass to Chattel in the civil law, were also identified. In analyzing the security requirements, there are less motivations on criminal charges against cyber criminals in addressing the security issues. Because it is often challenging to identify the culprits in medical device hacks. It is also difficult to hold device manufactures on negligence of duty especially after the device has been approved or if the harm on patient was as a result of a cyber attacker. Suggestions have been provided to improve upon the regulations so that both the regulatory bodies and MDM can improve upon their security conscious care.**

Keywords*—*Information security; medical device; legal requirement; healthcare; privacy

I. Introduction

Medical devices play significant role in the sustenance of human life in our society. In addition, the connection of these devices to the internet has transformed the medical device management and thereby, increasing their flexibility of management and use.

Implantable medical devices fused with network communications, such as pacemakers, have been adopted for essential treatment of critical conditions such as tachycardia [8], [9]. Tachycardia condition makes one heartbeat faster than the average per minute [8], [9]. This can occur when the electrical signals in the upper chambers of the heart misfires resulting in increased heart rate [4, 5]. In such a condition, the heart is not able to fill with blood before contracting, and this reduces the blood flow to the rest of the body [8], [9]. Other related conditions include ventricular (a condition in which the electrical signals in these chambers fire wrongly) and sinus tachycardia which occurs when the heart's natural pacemaker transmit electrical signals faster than normal [8], [9]. Patients experience symptoms such as dizziness, shortness of breath, chest pain and heart palpitation. Sever issues includes unconsciousness and cardiac arrest. Implanted medical devices known as pacemakers are used in the management of these conditions [8], [9].

These network-enabled medical devices can also enhance the implementation of other functionalities. Such as continuous care which is not possible with medical devices not fused with communication networks [8], [9].

Much as medical devices are sustaining millions of lives, they are associated with some vulnerabilities. Recent studies showed vulnerabilities with potential risks to patients who are using devices with medium- or long-range wireless systems [10]. According to the FDA, cybersecurity is the process of preventing unauthorized access, unauthorized use, unauthorized modification, or misuse of information, which is accessed, stored or transmitted from a device to an external receiver [1], [14].

Cyber criminals can be heartless to an extend of taking undue advantage of these vulnerabilities to hack into medical devices with the intention to cause harm.There have been similar instances where cybercriminals hacked epilepsy support websites and posted animated images which caused pain and seizures to photosensitive epileptic patients [11], [12]. So, the communications to and from pacemaker can be compromised. This can lead to injuries or death [10], [16], [17]. More to this, security loopholes have also been discovered in some class II medical devices. Insulin pumps were assessed to have the potential of delivering excess insulin if the vulnerabilities found in them are exploited[6]. Additionally, the serial number was used to hack into an insulin pump such that the device could be disabled by the hackers [18]. The impact of such an attack could be life-threatening for people with diabetes.

Attack surface on medical devices increase as the number of devices connected to the internet increase [19]. This has increased the possibility of endangering patient lives since attackers can be able to access sensitive information and can infect devices with malware [20]. IMDs such as pacemakers, neurostimulators, implantable cardiac defibrillators (ICDs), and drug delivery systems have become target of attacks in

recent times [21].

In a vulnerability assessment in medical devices [10], Shodan (a search engine for IoT devices) was used to obtain a large collection of IP addresses that were scan with Nessus (a vulnerability scanner) to determine the existence of vulnerabilities. The study identified 1,604/16,078 (9.97%) of devices with vulnerabilities. In general, about 3,964 vulnerabilities were found in 1,604 devices. 345 devices had 'Critical' vulnerabilities, 411 with 'High' vulnerabilities, 1,468 with 'Medium', and 1,740 with 'Low' vulnerabilities. Dropbear SSH (a software package that provides a Secure Shell-compatible) Server was found to be one of the most common and critical vulnerabilities which hackers can execute malicious codes to disclose sensitive information in database. Other devices which were found to have vulnerabilities include some radios designed to communicate with the medical devices such as cardiac pacemakers, implantable neurostimulators, and implantable infusion pumps.

Additionally, vulnerabilities were identified in Magnetic Resonance Imaging (MRI) scanners and X-Ray machines. Furthermore, the study found devices with Electronic Health Records (EHR) software that have default community names of Simple Network Management Protocol (SNMP) of which hackers can gain ingress into the respective networks of these devices and can be able to access other network nodes [15].

With all the enormous benefits of network enabled medical devices, they are life-threatening security issues for the patients [22] ranging from network failures to hacking of medical devices. This raises serious concerns about the security and privacy of patients [12], [22], [23]. Various legal requirements including regulations, directives and laws were examined in this study towards enhancing the security of medical devices.

1) Research problem, objective and scope: The double-stress of a patient who has to battle with the effect of a disease as well as the fear of being harm due to medical insecurity call for more research in medical devices to overcome this challenge. The objective of this work is to therefore identify, assess and analyse the legal requirements in medical devices towards enhancing their usage safety for patients.

II. Background

A medical device per the World Health Organization, is an instrument, machine, object, or an apparatus that can be used for diagnosis, treatment, monitoring, and prevention of disease or illness [1], [2]. Similarly, in the EU, medical devices include "any instrument, software, or other tools, intended by the manufacturer to be used for diagnosis, prevention, monitoring, treatment, or alleviation of disease" [3]. Medical devices vary from each other based on their design, implementation and application. These devices can be made of software only, hardware only or a hybrid of both [3]. But most of the critical medical devices are made of both hardware and software to enable them to be more fit for vital use. Additionally, most of these medical devices are incorporated with communication technologies and networks to enhance their performance. Medical devices which are integrated with communication networks provides better ways of diagnosing, treating and monitoring of different kinds of medical conditions including heart related conditions and chronic diseases.

Such devices include wearable, connected-on-site equipment and implantable medical devices. These advanced medical devices have transformed diagnosis, treatment and monitoring of various medical conditions and have even increased life expectancy in the United States to about 10 years [1]. Many of such devices include vital sign monitoring devices, glucose monitoring, infusion pumps, electrocardiograms (ECG), implantable pacemakers, insulin pumps, blood pressure monitors, radiology equipment, ventilator machines embedded sensors, ECG sensors, acidometers and intensive care unit (ICU) equipment [1], [5]. Medical devices fused with communication technology have tremendously improved the efficiency of healthcare facilities. Currently, medical devices collect, process, analyze, measure, share and transfer biological signals in real-time.

Implantable medical devices (IMDs) including pacemakers and implantable cardioverter-defibrillators (ICDs) are developed to boost the physiological functioning of some organs such as the heart. Heart related problems could result in slow heartbeat rate, fast heartbeat rate and irregular rhythms in the heartbeat [6]. In 2001, about 25 million people in the US were recorded to be dependant on these devices for life-threatening functions [7]. Currently most of these devices are wirelessly made such that they can be able to communicate with remote equipment of about 5 meters away. ICDs and IMDs can now be remotely configured by doctors while avoiding the need for numerous invasions into patients. This may also reduce infecting sterilized operating rooms due to the need for the proximity of configuration equipment. Additionally, IMD devices transmit alerts to remote monitoring stations in which reports can be generated for the patient's physician to be analysed without causing interference to the patient' activities. But the adoption and usage of these devices require some legal considerations.

Legal requirements in this context include the laws and directives which are enforcing medical device security [51]–[53]. Laws are rules which are established by the appropriate bodies to control behaviours [51]–[53]. These can be categorized into regulatory law, statutory law, constitutional law and common or case law [51]–[53]. Statutory laws are enacted by governmental organs such as the legislation or the parliament [51]–[53]. Regulations are written to primarily implement specific aspects of the law [51]–[53]. Regulations and directives such as FDA, HIPAA, GDPR and EU MDR provides a framework for regulating medical device manufacturers and healthcare providers. Within the EU, when regulations are issued and implemented, all EU and their affiliate European Economic Area (EEA) members can directly apply the regulations without the need for the governments of the EU member states to pass legislation to implement the regulations [24], [25], [33], [35], [36]. On the contrary, directives are legal acts in the EU which are written to enable member state to obtain a desired result. Each member state is given the opportunity to define their ways and details of implementations of the directives [24], [25]. Essentially, a directive cannot be directly applied in member states in EU unless it is passed through legislation [24], [25]. Common Law, which is often used interchangeably with case law, refers to the precedents and authorities which have been set by previous court rulings, judicial decisions and administrative legal findings or rulings [53], [54]. In the U.S., constitutional law comes from the U.S. constitution, a state

constitution or local constitution, bylaws or charter [52], [53].

Statutory law is subdivided into criminal law, and civil law. Criminal law has various laws between individuals and organizations or among these parties. Criminal laws are deterrence in structure, with the primary objective to deter adversaries who are responsible for cyberattacks [24], [25], [51]–[53]. Some of the civil laws are contract law, employment law, family law and tort law [51]–[53]. Tort is a behaviour that causes harm to the complainant (in this context, the patient who is using the medical device) leading to legal liability for the involved person who committed the act (the malicious actor) [24], [25], [51]–[53]. Tort law therefore enables parties to seek redress in the event of injuries pertaining to physical, personal or financial injuries. Other related laws include Battery and Trespass to Chattels. Battery involve deliberate touching of the claimant which is tantamount to the physical invasion of the injured patients [27], [28]. Trespass to Chattels is violated when there is a deliberate interference with one's personal property which has resulted in the cause of an injury [27], [29].

Due to widely adoption of networked medical devices, legal requirements have become important in dealing with security-related challenges. This study therefore surveyed for the most common and recent regulations, laws and directives of medical devices in the US and EU towards enhancing the security of medical devices [24], [25], [51]–[53].

III. Related Work

Realizing the need to improve on the cyber security of medical devices, various researches have been conducted to strengthen the security of medical devices. In that light A.J. Burns et al. presented the legislative timeline and the evolving threats to information security in medical devices in the US with the aim to provide attention for future action [59]. Katherine Booth et al., also analyzed the legal gaps in medical devices in the US towards addressing medical device security and privacy issues [27]. These studies significantly contributed knowledge towards enhancing the security of medical devices.

Additionally, various studies [1], [31], [44], [45], [62] focused on the regulatory aspect. Daniel et al studied into how medical device regulation Perform in the United States and the European Union. This compared medical regulations in both US and EU, however, legal requirements of medical requirement is not limited to device regulations alone [45]. Additionally, Halperin et al developed a framework towards security and privacy measures in medical devices for the adoption of manufactures and regulatory bodies, having analysed the general operations of medical devices [62]. Additionally, Mariela Yaneva et al also identified some legal regulations of biomedical devices pertaining to EU [31]. Tahreem Yaqoob et al conducted a study into information security vulnerabilities in medical devices and other applicable regulations to provide suggestions towards enhancing the security and privacy of healthcare devices [1]. Jon et al work focused on vulnerable software in medical devices regarding patching and updating, manufacturers responsibilities towards assisting FDA processes to address security issues [44].

While these studies contributed to the body of knowledge in the context of medical device security, some of the studies [27], [59] focused their scope on only US and other studies focused on only regulations of the legal aspect [1], [31], [44], [45], [62].

IV. Method

A literature survey was conducted in Google Scholar, Science Direct, Elsevier and IEEE XPlore for legal requirements of medical devices. The most popular legal requirements of US and EU were identified and assessed towards enhancement of the security measures in medical devices. Keywords and phrases such as medical device, regulations, laws, directives and vulnerabilities were used in searching for the related literature. These words and phrases were combined with Boolean functions of AND, OR and NOT.

V. Findings of Legal Requirements

In the US, the Food and Drugs Administration (FDA) is the main regulatory body, responsible for regulating the development and certification of medical devices [10], [27]. Federal Communications Commission (FCC) [10], [27] and the Centers for Medicare and Medicaid Services (CMS) [10], [27] [10], [27] are other auxiliary agencies which are supporting the FDA in the regulations of medical devices. The FDA uses Federal Food, Drug, and Cosmetic Act (FD&C Act) in regulating the medical devices [10], [27], [54].

There are various categories of medical devices [10], [24] as depicted in Fig. 1 and Table I. Some of them do not present unreasonable risk of illness or injury while others could present unreasonable risk of illness or injury [10], [24] and are intended to be use in supporting or sustaining human life. So, regulatory classification was developed based on these risks that the devices pose to humans as shown in Table I. The level of controls required to ensuring the safety and effectiveness of the devices were also considered. The medical devices have hence been categorized into Class I, Class II and Class III. The Class I devices are basic and common medical devices which have low to medium risk, low complexity and consist of about 47% of the total medical devices [1]. The class I devices are basically not internet enabled and are exempted from regulatory controls based on their low security risk [10]. Example of class I devices include Lancet, and dental floss [10]. The cybersecurity issues are mostly around the class II and class III medical devices [10], [20]. The class II devices pose medium to high risk to patients. Class II devices are more complex and partially implantable [10]. They form about 43% of the total number of medical devices [1] and these devices include Syringe, Insulin pump and blood glucose meters (BGM) [1], [10], [24].

The class III medical devices consists of only 10% of the total medical devices and are categorized into the highest security level, requiring the most strict security measures [1]. They are fully implanted to regulate body functions. The class III medical devices include Artificial pancreas, Continuous glucose monitoring (CGM), pacemaker and Replacement Heart valves

The relevant regulations of FDA on medical devices and the processes therefore involve:

TABLE I. MEDICAL DEVICE CLASSES [10], [27]

Medical Device Class.	Attributes	Example Devices
Class I	Common, low risk, low complexity	Lancet, Dental Floss
Class II	More complex, greater risk to patient, partially implanted	Syringe, Insulin Pump, Blood Glucose Meter
Class III	Fully implanted, greater risk, regulate body functions	Artificial Pancreas, CGM, Replacement Heart Valves

- Medical device listing and establishment registration: The manufacturers and distributors of medical devices must register their organization with the FDA to be able to market their product. Organizations must provide full details of the medical devices being manufactured.
- Labeling: Labeling must be in accordance with information and description of the device usage.
- Medical Device Reporting (MDR): manufacturers/importers/healthcare facility must report events of device malfunctions or causes of serious injuries or death to the FDA. This will enable FDA to detect and correct issues.
- Quality System (QS) regulations: Indicates requirements relating to controls, facilities, and methods used in the entire medical device life-cycle. These indications include designing, purchasing, manufacturing, labeling and packaging, servicing, and installation of the devices. The FDA is responsible to ensure that the devices fulfill important specifications and requirements.
- Investigational Device Exemption (IDE) for clinical studies: This enables manufacturers to provide device-specific effectiveness and safety data to support Pre-market notification (510-k) or post-market approval (PMA)application.

FDA satisfies medical devices after going through a total product life cycle method which has two important phases thus pre-market notification/510-k approval and post-market approval (PMA). Manufacturers need to provide detailed information with evidence of the device use safety and effectiveness as shown in fig 1. FDA then validate the information in addition to sharing identified security vulnerabilities, monitoring and examination of connected medical device's effectiveness and safety.

Medium risk related devices are mostly routed through the 510-k approval process. Significant assurance of the medical device's safety and effectiveness are normally provided by the manufacturer who submits a 510-k application. Basically, the 510-k application is exempted from non-clinical and clinical data of showing the effectiveness and safety of the device. But the high risk devices goes through PMA, which involve a complete review of the device including the device's clinical and non-clinical trials and testing data.

Health Insurance portability and accountability act (HIPAA) privacy and security rules were passed for protecting personal health and medical records in the United States of America (USA). The HIPAA rules covers healthcare providers, health plans and healthcare clearing housing entities. HIPAA

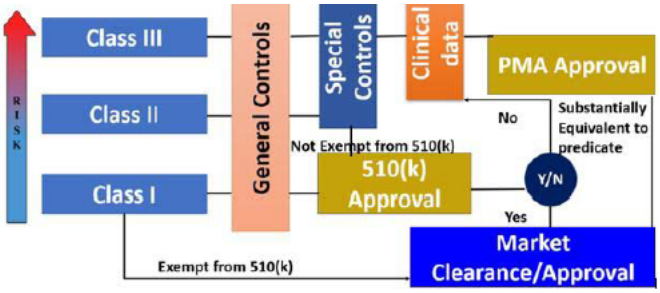

Fig. 1. FDA Medical Device Regulation Process [10]

privacy and security rules primarily protect personal identifiable health information (PHI) including names, diagnosis and identifiable numbers of medical device [27]. This rule therefore demands for appropriate privacy and security protection controls. However, the mandate of the HIPAA rules excludes the protection of pharmaceutical companies and medical devices [1], [27]. As HIPAA concentrates on the protection of PHI, it does not extend its mandate to include the protection of cyber-attacks against medical devices. The regulation of medical device manufacturers are not also covered by HIPAA regulations [27].

Cybersecurity issues should be addressed by the manufactures at the design and development stages. The process should involve [59], [60]

- Identifying assets, threats and vulnerabilities.
- Assessing the impact of the threats and vulnerabilities on device functionality and patient or user.
- Assessment of the likelihood exploitation of the threats and vulnerability.
- Assessing residual risk and risk acceptance criteria.
- cybersecurity documentation should be done to include.
  - Traceability matrix between security controls and their risks.
  - Hazard analysis, mitigation and design consideration.
  - Documented plan for validating software update in the life-cycle of the device.
  - Documentation of controls that have been implemented to assure the integrity of the device.
  - Instructions for the device use and specification on cybersecurity controls needed for the

intended use environment.

- Appropriate standards should be followed and documented.

The post-market management of cybersecurity in medical devices is to complement the premarket management, to form a comprehensive security measure. So the security measures cover the design, development, peoduction, distribution, deployment and maintenance stages [61]–[63]. As cyberseurity issues continue to evolve, it is not possible to put in measures to take care of all issues at one point in time. So after the device has been deployed on the market, the MDM, need to always document complaint handling, quality audit, corrective and preventive actions, software validation and risk analysis and serving, as specified in the quality system regulation. In addition, MDM need to [61]–[63]:

- Constantly identify vulnerabilities and risks and assessing their impact by monitoring cybersecurity information sources.
- Maintain software life cycle process such as monitoring third party software for vulnerabilities, design verification and validation for the software updates and patches.
- Using threat models and vulnerability handling process standards (e.g. ISO/IEC 30111:2013) to maintain safety and security.
- Adopting standard procedures (e.g. ISO/IEC 29147:2014) for vulnerability disclosure.
- Timely deployment of mitigation measures to address cybersecurity issues prior to exploitation.
- Other guidelines include, having a structure and systematic approach to risk and quality management, as provided in 21 Code of Federal Regulation, part 820.
- The MDM is to also follow procedures that are in line with the NIST framework for improving critical information cyber security (Identify, Protect, Detect,Report and recover).
- Maintaining safety and core functionality of the device to prevent patient harm.
- Adopting appropriate for managing cybersecurity risks.
- Assessing the exploitability of vulnerabilities.
- Assessing the severity of harm to patients.
- Assenting and controlling risk of patient harm.
- Mitigating and reporting vulnerabilities.

Aside the regulatory laws, statutory laws were also identified in the U.S. to have protection for medical devices. These include Computer Fraud and abuse Act (CFAA) and Anti-Tempering Act [1], [27], [51]–[53]. CFAA punishes cybercriminals who access medical devices or transmits code which resulted in causing harm [27], [53].Within the scope of this law, the medical device manufacturer(MDM) or hospital network is not charged with negligence of duty [27]. But the cyber-criminal under this behaviour is fined, imprisoned for not more than 10 years or both [27]. Under the Anti-Tempering Act, it is a criminal offence to temper with consumer products including medical devices [27]. This Act directly applies to cybercriminals in a breach scenarios but does not apply to MDM or hospital networks. In the context of common or case law, [27] there exist tort liability in which the cybercriminal can be liable to Trespass to Chattels or Battery. When a patient is injured through medical device attacks, the patient can take a civil cause of legal action against the malicious attacker, the device manufacturer and the hospital. The hospital can be charged if the compromised device was as a result of cyber attacks on the hospital's network. A medical device manufacturer or a hospital may be held accountable for negligence if they fail to comply with established cyber security measures [27], [53].

In the European Union (EU), Medical Device Directives (MDD) was responsible for regulating the marketing and safety of medical devices as far back as 1990 [1], [24], [32]–[36], [40]. But this has been changed to regulation 2017/745 of EU [1], [24], [31], [39]. EU also classified its medical devices but what is different is that, EU has four number of classes in accordance to their risk level and purpose. The classes are I (Is and Im), IIa, IIb and III with respective increases in the level of assessments.Before a medical device is advertised in any EU country, it must first go through the systematic regulatory assessment in order to obtain the Conformite Europe (CE) mark [1], [31]. CE mark means the device satisfied the safety criteria and can be sold without further controls.

The national competent authorities which is formed by EU member states, observe, appraise and nominates notifying bodies (NBs) to be responsible for these conformity processing [1]. Other vital responsibilities of this body are device certification, class designation, quality system verification, and assessment, and design profile reviews. The approval process of a device involves the selection of an NB by the manufacturer to grant certification of a new device for CE marking [30]. The NB then obtain technical details of the device based on its class [1]. The information is used to review the safety of the device [1]. Usually, devices in each class must declare its conformity to the EU directives and the specific conformity assessment plan [1]. Also designs of devices in the highest class have to be assessed however, devices in the lower class I are exempted from such regulations [1]. In Spite of that, these class1 devices must follow vital propositions of efficacy and safety in their design alongside with labelling and construction requirements. After a medical device is approved, there is post-market surveillance by competent authority through the authority of member-state [1].

As the devices are getting sophisticated, better regulations are much needed since the current directives have not catch-up with the technical and scientific developments pace in the healthcare domain. Currently devices are not thoroughly assessed in the pre-market phase except medium to high-risk devices which go through conformity assessment for the NB to decide on the needed controls of the device safety [1], [40].

The regulation (EU) 2017/745 which has recently been written [1], [39], will enable NBs to visit manufacturers on their site without prior notice towards ensuring safety, security, quality, and performance of the medical devices. The Medical Device Regulation of EU have incorporated some security

measures for device manufactures. These security measures are [39]:

- Under Regulation 17.2. Medical device manufactures (MDM) shall follow state-of-the-art development and manufacturing process, including the principles of development life cycle, risk management, including information security, verification and validation.
- In regulation 17.4, Medical Device Manufacturers(MDM) shall specify minimum requirements to run the medical device and software as intended and the specification should include hardware, IT networks characteristics and IT security measures including protection against unauthorized access.
- In regulation (39) of the MDR, MDM are to provide clear and easily accessible essential information to patients who are on implanted medical devices. Information that should be provided include information concerning how the implanted device can be identified, any necessary health risk warnings or precautions to be taken. Such warnings or precautions includes information as to whether or not the device is compatible with certain diagnostic devices or with scanners used for security controls.
- Under regulation 4.5, MDM are required to provide description of the arrangements that fulfil existing rules controlling the protection and confidentiality of personal data, such as [39]:
  1) organizational and technical arrangements that will be implemented to avoid unauthorized access, disclosure, dissemination, alteration or loss of information and personal data processed;
  2) a description of measures that will be implemented to ensure confidentiality of records and personal data of subjects; and
  3) a description of measures to be adopted towards mitigating potential adverse impact in the event of data security breach.
- Under Section 4.1, a signed statement must be provided by the natural or legal person responsible of the MDM satisfying that the medical devices is in conformity with the general safety and performance requirements and that precautions has been taken to protect the health and safety of the subject.
- In Section 4.3, MDMs are to provide and proof insurance cover or indemnification of subjects in case of injury, pursuant to Article 69 and the corresponding national law.

The general data protection regulations (GDPR) of EU's privacy-related regulation is concerned with the processing of personal data by a data processor or a data controller in EU. The GDPR defines personal data to include information which can be linked to an identifiable person [38]. Unlike the HIPAA regulation, the GDPR is application to all sectors that are processing personal information of the EU citizens. Biometric data, genetic data and PHI are classified under sensitive information. Explicit consent is required in order to process such data. The GDPR also applies to all healthcare organizations, health insurance companies, and medical device manufacturers [37].

Accordingly, there are no general Applicable laws as at now, which are serving the purpose of cybersecurity only in Norway [42], [43]. The cybersecurity regulations are fragmented into sector specific [42], [43]. In the context of common or case law, there exists a criminal code which is originally known as Penal code in Norway [42], [43]. This code is for handling criminal cases. On April 8, 2005, the penal code relating to cybercrime was amended and enacted to include various offences. The offensive provisions are [42], [43]:

1) Under Penal Code 151 b: [42], [43] Any person who is found guilty of destroying, damaging, or putting out of action any data collection or any installation for supplying power, broadcasting, telecommunication, or transport, causes comprehensive disturbance in the public administration or in community life in general shall be liable to imprisonment for a term not exceeding 10 years. If the aforementioned act was found to be negligent acts the person shall be punishable by fines or imprisonment for a term not exceeding one year.
2) In Penal Code 145b: "Any person who unlawfully disclose or make available a computer password or similar data, by which the whole or any part of a computer system is capable of being accessed, shall be sentenced for spreading of access data, to a fine or imprisonment not exceeding 6 months or both". If the act involves serious spreading of access data the culprit shall be sentenced to imprisonment not exceeding 2 years.

Also, Under section 204 of the Penal Code of 20 May 2005, some violations are punishable upto two years imprisonment or by fines. Some of these offensive activities include unauthorised access or hacking, Denial-of-service-attacks, phishing, infection of IT systems with Malware and possession or use of tools for committing cybercrime. Other punishable offences are identity theft, electronic theft and any activity that can have adverse effect on CIA of any IT system, infrastructure, communications network, device or data [41]–[43]. A summary of the findings are shown in Table II. where the legal requirements are listed with their respective origin.

A. Gap Analysis

In the European Union (EU),the GDPR and the EU Medical Device Regulations (Regulations 2017/745) [1], [39] have some intersections towards holding device manufactures to be responsible of negligence of duty in the event of device compromise [1], [24], [39]. However, there are gaps in the HIPAA privacy and security rules in the regulation of medical devices. HIPAA does not concern itself much with the security of medical devices [1]. Unlike the GDPR, which holds both hospitals and device manufacturers responsible for data protection in medical device regulations in EU, the HIPAA privacy and security rules are only limited to the healthcare entities such as hospitals and other healthcare providers. HIPAA provides heavy penalties for breaches against patient health information (PHI). MDM who deals with healthcare entities directly are

TABLE II. SUMMARY OF LEGAL REQUIREMENTS FOR MEDICAL DEVICES

#	Legal requirement	Origin
1	Food, Drug, and Cosmetic Act (FD&C Act) [10], [27], [54].	U.S.
2	Health Insurance portability and accountability act (HIPAA)	U.S.
3	General Data Protection Regulation (GDPR)	EU
4	Medical Device Regulation 2017/745 of EU [1], [24], [31], [39]	EU
5	Computer Fraud and abuse Act (CFAA) [1], [27], [51]–[53]	U.S.
6	Anti-Tempering Act [27]	U.S.
7	Trespass to Chattels [27], [53]	U.S. /EU
8	Battery [27], [53]	U.S. /EU
9	Penal Code [42], [43]	EU

covered by HIPAA but not when devices are directly sold to patients This does not adequately cover the protection of the entire medical devices against cyberattacks [1], [6], [24], [27].

In this shortfall of HIPAA, privacy concerns are not also addressed in medical devices. According to [1] safety and security issues are also affected in scenarios where devices are prone to safety and security risks. But FDA does not provide guidelines for MDM to explicitly deal with that [1].

Furthemore, FDA have some cybersecurty guidelines for controlling the security of medical devices and these guidelines dependent on NIST's recommended security framework for critical infrastructure [1]. Though the guideline is useful, it was not specifically developed for enhancing the security of medical devices. The severity of hazards pose by medical device malicious errors and non-malicious errors could be different from conventional IT systems [1]. Example, malicious error in water or power system could cause a substation to go off. But in the context of medical device, a malicious or non-malicious error could have direct harm on the patient ranging from pain to death in a short time [1]. Also, the Food, Drug and Cosmetic Act of U.S., have detailed description for safety controls for medical devices but specific security related controls are limited [1].

Additionally, quality and safety labelling of medical devices has been a requirement but cybersecurity labelling of medical devices have not been adopted [1], [27], [39]. This makes is difficult for patients to choose secure medical devices. Again, the FDA require hospitals and device users to report serious security issues within a time line. But this has been found to be violated due to lack of capacity and training in timely determination of security issues.

Within the confines of statutory and case laws, for a patient to establish a claim arising from harm of cyber attack, the patient must proof that the defendant deliberately interfered with his or her possessory interest without authorization [27], [45]–[49]. Also if there is an unauthorized access by the defendant which resulted in a harm to the involved patient, the defendant can be found liable in such scenario. The difficulty is that the patient or the plaintiff may not be able to provide justification for the intention of attacks. According to [1], a number of hospitals and MDMs have been fined for various offences including failure to report faults on medical devices [55], [56], failure to follow PMA regulations [55]–[57], safety issues with medical devices [27], [56], [58],and for selling unapproved medical devices [1], [57]. Apparently, this will deter others from committing related acts but security related offences were not seen.

VI. DISCUSSION

As threats to information security evolve, security requirements such as regulations, directives, statutory law and case laws are also revised accordingly. These requirements are usually updated to enhance their ability to mitigate current and foreseeable threats. This study was therefore conducted to identify the state-of-the-art legal requirements which are being used to control the security of medical devices. Medical devices serve critical functions in the sustenance of human life in the eHealth space [1], [2], [24], [27]. But the current laws that exist to safeguard these devices in terms of security and how adequate they are, need to be assessed. Regulations and their procedures, statutory law and case law or common law were identified and assessed in the study as shown in Table II.

With reference to Table II, in the U.S., the FDA is the main body that is regulating medical devices, using FD&C Act [1], [13], [24], [27], [44], [45]. In this regards the effectiveness of the security regulations were assessed. Also in the event of a device compromise, the responsible bodies or were also analysed. For example, who will be liable if a patient's medical device was hacked? Per the state-of-the-art studies, those who will be liable include the attacker, the MDM and the hospital if the medical device was compromised due to attacks on the hospital network [1]–[4], [27], [28]. In recent prosecutions of offenders of FDA regulations and HIPAA privacy and security rules in the U.S., those who were found liable are hospitals and MDA [1], [56]–[58]. None of the liabilities involve security issues left alone to charging a cybercriminal on the account of medical device compromised. Some of the legal structures have not fully addressed the threat of cyberattacks. For instance, it is sometimes difficult to identify and indict culprits of cyber criminals [27], [46], [47]. In some cyberattack instances, the adversaries conceal their identity, cover their tracks or at worse can divert the act on others through source spoofing [27], [47]. Much as it remains challenging to identify and get hold of the perpetrators behind cyberattacks, the criminal law remains insufficient as a deterrent measure [27], [47]–[49].

In comparing the medical device regulations of EU and that of FDA, the EU has comparative placed a higher responsibility for device manufacturers to be proactive in both pre-market and post-market release of the medical device [1], [39]. Literally, the EU ask their device manufacturers to take insurance cover for patients who are using their devices [1], [39]. In order for them not to pay claims,MDM in the EU will be encouraged to enhance security. The Insurance company of the medical device will also want to mitigate risk by charging the appropriate premium based on the severity of vulnerabilities in the medical devices. So the insurance company will also have interest in the level of security of the device. With all these

actors involve, the level of security in medical devices can be greatly improved.

Common law principles can descend on MDM on liabilities relating to negligence of duty to protect medical devices against cyberattacks [1], [27], [47]. If an MDM fails to implement acceptable cybersecurity measures then that MDM can be liable to negligent of duty of care. But the duty of care is relative in cybersecurity breaches [27]. Standard and guidelines changes as the threats in cyberspace changes. This complicates the identification and specification of duty of care. For instance, under Regulation 17.2 of EU MDR, MDM shall follow state-of-the-art development and manufacturing process, including the principles of development life cycle, risk management relating to information security, verification and validation [39]. The point in time where MDM becomes liable for negligence of duty in cyberattack of a medical device may be difficult especially in phases where standards and guidelines are undergoing changes [1], [27]. In some states in USA, where the patients' injury was directly caused by the acts of the adversary, the MDM was exonerated from acts of negligence liability [27]. Further to this, on the basis that an MDM was certified by FDA, through the PMA process, injured patients cannot hold the MDM liable [26], [50]. Based on these, there are uncertainties regarding negligence of duty actions against an MDM.

Furthermore, there is a gap on the share responsibility of regulators and bodies that certify medical devices. In the literature studies [1], [6], [24], [27], [39], [56], none of them blame the regulatory bodies in the event of cyberattack. But regulatory bodies need to be hold accountable for attacks on medical devices which they have approved. For instance, if a medical device was approved to be safe and secure by a regulatory body like the FDA when in fact it has some security loopholes, it could be that the regulatory body did not do due diligence. Notwithstanding, FDA and HIPAA were not primarily provided to safeguard against cyberattacks of medical devices and could lacks adequate regulatory safeguards [1], [27]. So the regulatory body may not be liable if the security assessments of the device was not part of their mandate [27]. The FDA and HIPAA need to improve upon their regulations to fully cover the security of medical devices such that the MDM and regulatory bodies can directly be responsible to vulnerabilities found in medical devices. In this way, the circle of efficiency maybe getting completed. Regulatory bodies would want to comprehensively assess a medical device for vulnerabilities in medical devices such that they will not be liable in the event of breaches. This would also compel MDM to want to put in the necessary measures to have their medical devices approved.

But, with this approach, there are also ethical hurdles that need to be cleared. If a potentially unsecure medical device is approved for use, patients can be vulnerable to attack[11]. On the contrary, if a device is not approved due to security reasons, that device may never be available for patients [23]. This implies that many more patients would be harmed since there would not be any effective treatments for the conditions [23], [27].

Comparing the legal requirements of U.S. and EU, the EU general data protection regulation(GDPR) highly complements the medical device regulation of EU. That is not the case, between the FD&C Act and HIPAA privacy and security Act OF U.S. The HIPAA has distanced itself a bit when it comes to medical device regulations [1], [6], [24], [27]. This has weakened the regulatory security controls in enforcing security measures in medical device. This is because aside the NIST's guidelines on critical infrastructure, FDA do not have tailored guidelines for controlling the security of medical devices [1], [6], [24]. A combined effort of FDA and HIPAA will greatly enhance the security of medical devices since HIPAA privacy rules will be extended to handle privacy issues of device manufacturers and while the HIPAA security rules handle the security concerns of the hospital and device manufactures [1].

A. Conclusion

Patients who are dependent on medical devices such as pacemakers and artificial pancreas are vulnerable to cyberattacks. This study therefore conducted a state-of-the-art on security requirements, concerning these devices in the US and EU. Food, Drugs and Cosmetic Act, HIPAA, Medical Device Regulations of EU and GDPR were some of the identified regulations for controlling the security of these devices. Statutory laws such as computer Fraud and abuse Act (CFAA), Anti-Tempering Act, Panel Code as well as Battery and Trespass to Chattel in the civil law, were also identified.

In analysing the security requirements, there are less motivations on criminal charges against cybercriminals in addressing the security issues. Because it is often challenging to identify the culprits in medical device hacks. It is also difficult to hold device manufactures on negligence of duty especially after the device has been approved or if the harm on patient was as a result of a cyber attacker.

Suggestions have been provided to improve upon the regulations so that both the regulatory bodies and MDM can improve upon their security conscious care.

However, this raises an ethical issue of balancing the practice of using a very secured medical devices which may take a long time to develop, versus causing more harm to patients who may not have the device to use due to stringent security regulatory processes. Future studies will analyse these ethical dilemmas to provide a balance point of enforcing security requirements while ensuring availability of the medical devices.

REFERENCES

[1] Yaqoob T., Abbas H., Atiquzzaman M. Security Vulnerabilities, Attacks, Countermeasures, and Regulations of Networked Medical Devices—A Review. IEEE Communications Surveys & Tutorials. 2019;21(4):3723-68.

[2] Syring G. Overview: FDA regulation of medical devices, Accessed June 06 From: https://www.fda.gov/medical-devices/overview-device-regulation/history-medical-device-regulation-oversight-united-states

[3] Fatema, N. and Brad, R., 2014. Security requirements, counterattacks and projects in healthcare applications using WSNs-a review. arXiv preprint arXiv:1406.1795.

[4] Tanev, G., Tzolov, P. and Apiafi, R., 2015. A value blueprint approach to cybersecurity in networked medical devices. Technology Innovation Management Review, 5(6).

[5] Yu, B., Kang, S.Y., Akthakul, A., Ramadurai, N., Pilkenton, M., Patel, A., Nashat, A., Anderson, D.G., Sakamoto, F.H., Gilchrest, B.A. and Anderson, R.R., 2016. An elastic second skin. Nature materials, 15(8), pp.911-918.

[6] Denning T., Borning A., Friedman B., Gill B. T., Kohno T., Maisel W. H., editors. Patients, pacemakers, and implantable defibrillators: Human values and security for wireless implantable medical devices. Proceedings of the SIGCHI conference on human factors in computing systems; 2010.

[7] Pope A., Bouxsein P., Manning F. J., Hanna K. E. Innovation and invention in medical devices: workshop summary: National Academies Press; 2001.

[8] Fisher J. D., Kim S. G., Furman S., Matos J. A. Role of implantable pacemakers in control of recurrent ventricular tachycardia. The American journal of cardiology. 1982;49(1):194-206.

[9] TOIVONEN L., VALJUS J., HONGISTO M., METSO R. The influence of elevated 50 Hz electric and magnetic fields on implanted cardiac pacemakers: the role of the lead configuration and programming of the sensitivity. Pacing and Clinical Electrophysiology. 1991;14(12):2114-22.

[10] Halperin D., Heydt-Benjamin T. S., Ransford B., Clark S. S., Defend B., Morgan W., et al., editors. Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses. 2008 IEEE Symposium on Security and Privacy (sp 2008); 2008: IEEE.

[11] Ertl B.: coping-with-epilepsy.com; 2007 [Available from: Hooligans Attack Epilepsy Patients During Epilepsy Awareness Month.

[12] @wired. Hackers Assault Epilepsy Patients via Computer. 2020.

[13] McMahon E., Williams R., El M., Samtani S., Patton M., Chen H., editors. Assessing medical device vulnerabilities on the Internet of Things. 2017 IEEE International Conference on Intelligence and Security Informatics (ISI); 2017: IEEE.

[14] Food and Drug Administration, 2015. Content of Premarket Submissions for Management of Cybersecurity in Medical Devices-Guidance for Industry and Food and Drug Administration Staff.

[15] McMahon E., Williams R., El M., Samtani S., Patton M., Chen H., editors. Assessing medical device vulnerabilities on the Internet of Things. 2017 IEEE International Conference on Intelligence and Security Informatics (ISI); 2017: IEEE.

[16] Cybersecurity and Hospitals. American Hospital Association Accessed on June 7 2020 From:https://www.aha.org/system/files/2017-12/ahaprimer-cyberandhosp.pdf

[17] Peterson A. Connected medical devices: The Internet of Things-that-could-kill-you. Washington Post. 2015 Aug.

[18] Kaplan D. Black Hat: Insulin pumps can be hacked. SC Magazine. 2011 Aug 4.

[19] Lake D, Milito RM, Morrow M, Vargheese R. Internet of things: Architectural framework for ehealth security. Journal of ICT Standardization. 2014 Mar 31;1(3):301-28.

[20] Sametinger J, Rozenblit J, Lysecky R, Ott P. Security challenges for medical devices. Communications of the ACM. 2015 Mar 23;58(4):74-82.

[21] Halperin D, Heydt-Benjamin TS, Fu K, Kohno T, Maisel WH. Security and privacy for implantable medical devices. IEEE pervasive computing. 2008 Jan 16;7(1):30-9.

[22] Marchang J., Beavers J., Faulks M., editors. Hacking NHS Pacemakers: A Feasibility Study. 12th International Conference on Global Security, Safety & Sustainability; 2019: IEEE.

[23] Sokolsky O., Lee I., Heimdahl M., editors. Challenges in the regulatory approval of medical cyber-physical systems. 2011 Proceedings of the Ninth ACM International Conference on Embedded Software (EMSOFT); 2011: IEEE.

[24] Pesapane F., Volonté C., Codari M., Sardanelli F. Artificial intelligence as a medical device in radiology: ethical and regulatory issues in Europe and the United States. Insights into imaging. 2018;9(5):745-53.

[25] European Union Regulations, Directives and other acts, 2018. Available via https://europa.eu european-union/eu-law/legal-acts_en

[26] Medtronic, Inc. v. Lohr. US: Supreme Court; 1996. p. 470.

[27] Wellington K. Cyberattacks on medical devices and hospital networks: Legal gaps and regulatory solutions. Santa Clara High Tech LJ. 2013;30:139.

[28] Neal Hoffman, Battery 2.0: Upgrading Offensive Contact Battery to the Digital Age, 1 CASE W. RES. J.L. TECH. & INTERNET 61, 68 (2010).

[29] eBay, Inc. v. Bidder's Edge, Inc., 100 F. Supp. 2d 1058, 1069 (N.D. Cal. 2000).

[30] Fawaz K, Kim KH, Shin KG. Protecting privacy of BLE device users. In25th USENIX Security Symposium ({USENIX} Security 16) 2016 (pp. 1205-1221).

[31] Yaneva-Deliverska M, Deliversky J, Lyapina M. Biocompatibility of medical devices–legal regulations in the European Union. Journal of IMAB–Annual Proceeding Scientific Papers. 2015 Feb 13;21(1):705-8.

[32] Pesapane, F., Codari, M. & Sardanelli, F. Artificial intelligence in medical imaging: threat or opportunity? Radiologists again at the forefront of innovation in medicine. Eur Radiol Exp 2, 35 (2018). https://doi.org/10.1186/s41747-018-0061-6

[33] European Economic Community (1993) 93/42/EEC - Council Directive concerning Medical Devices. Official Journal of the European Communities. Available via http://ec.europa.eu/growth/ single-market/european-standards/harmonised-standards/medicaldevices_ en

[34] European Economic Community (1990) 90/385/EEC - Council Directive on the approximation of the laws of the Member States relating to active implantable medical devices. Council Directive. Available via https://ec.europa.eu/growth/single-market/europeanstandards/harmonised-standards/implantable-medical-devices_en

[35] European Commission (1998) Directive 98/79/EC of the European Parliament and of the Council on in vitro diagnosticmedical devices. Official Journal of the European Communities. Available via https:// ec.europa.eu/growth/single-market/european-standards/harmonised-standards/iv-diagnostic-medical-devices_en

[36] Patients and Privacy: GDPR Compliance for Healthcare Organizations, Accessed on June 8th 2020 From:https://www.trendmicro.com/vinfo/dk/security/news/online-privacy/patients-and-privacy-gdpr-compliance-for-healthcare-organizations

[37] D. Cicco et al. (2018). Toward an Enhanced EU Cybersecurity Framework: Political Agreement Reached on EU Cybersecurity Act—Security—European Union. Accessed: Nov. 17, 2018. [Online]. Available: http://www.mondaq.com/uk/x/709760/Security/ Toward+An+Enhanced+EU+Cybersecurity+Framework+Political+ Agreement+Reached+On+EU+Cybersecurity+Act

[38] (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons With Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation) (Text With EEA Relevance). Accessed: Dec. 13, 2018. [Online]. Available: https://publications.europa.eu/en/publication-detail/-/publication/3e485e15-11bd-11e6-ba9a-01aa75ed71a1/language-en

[39] (2017)REGULATION (EU) 2017/745 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC. Accessed: June 08, 2020. [Online]. Avialable: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017R0745

[40] Directive concerning Medical Devices. European Communities, (1993).

[41] Bastani F, Tang T. Improving security of wireless communication in medical devices. Massachusetts Institute of Technology. 2015.

[42] Cybercrimedata AS, Cybercrime Law, Norway. Accessed: June 09 2020, [Online].Available: https://www.cybercrimelaw.net/Norway.html#: :text=Penal

[43] ICLG.com, Norway:Cybersecurity 2020. Accessed: June 09 2020, [Online]. Available: https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/norway

[44] Martinez JB. Medical Device Security in the IoT Age. In2018 9th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON) 2018 Nov 8 (pp. 128-134). IEEE.

[45] Kramer DB, Xu S, Kesselheim AS. How does medical device regulation perform in the United States and the European union? A systematic review. PLoS medicine. 2012 Jul;9(7).

[46] Fouretier A, Bertram D. New regulations on medical devices in Europe: what to expect?. Expert review of medical devices. 2014 Jul 1;11(4):351-9.

[47] Handler SG. New cyber face of battle: developing a legal approach to accommodate emerging trends in warfare. Stan. J. Int'l L.. 2012;48:209.

[48] Jensen ET. Cyber deterrence. Emory Int'l L. Rev.. 2012;26:773.

[49] Richard Clarke, War from Cyberspace, NAT'L INT., Nov.-Dec. 2009, available at http://nationalinterest.org/article/war-from-cyberspace-3278.

[50] Riegel v. Medtronic, Inc., 552 U.S. 312, 128 S. Ct. 999, 169 L. Ed. 2d 892 (2008).

[51] Whitman ME, Mattord HJ. Legal, ethical, and professional issues in information security. Principles of information security (4th ed.; pp. 133–147). Boston, MA: Course Technology, Cengage Learning. Retrieved from http://www. cengage. com/resource_uploads/downloads/1111138214_259148. pdf. 2012.

[52] WARREN E. Legal, ethical, and professional issues in information security. 2011:89-116.

[53] Whitman M. E., Mattord H. J.Legal, ethical, and professional issues in information security. Principles of information security. 6th Edition ed: CENGAGE Learning; 2017: 127-143.

[54] Case Law - Common Law.Accessed: June 09 2020, [Online].Available: https://www.hg.org/case-law.html

[55] Federal Food, Drug, and Cosmetic Act (FD&C Act),June 13 2020, [Online].Available:https://www.fda.gov/regulatory-information/laws-enforced-fda/federal-food-drug-and-cosmetic-act-fdc-act

[56] V. Pollard and M. Davar. (2017). FDA's Evolving Civil Money Penalty Authority: Simple Violations Can Lead to Major Costs. [Online]. Accessed On June 14 2020 Available: https://www.mastercontrol.com/gxp-lifeline/civil_money_penalty_authority_0609/.

[57] A. Brino, Grisly Medical Errors, Some Deadly, Lead to 700K in Fines for 10 California Hospitals, Healthcare Finance, HIMSS Media, Portland, ME, USA, 2020. [Online]. Available: https://www.healthcarefinancenews.com/news/grislymedical- errors-some-deadly-lead-700k-fines-10-california-hospitals

[58] B. Zimmermann, California Fines 9 Hospitals $500k+ for Patient Safety Issues, ASC Commun., Chicago, IL, USA, Accessed on June 14 2020 [Online].Available: https://www.beckershospitalreview.com/quality/californiafines- 9-hospitals-500k-for-patient-safety-issues.html

[59] Burns AJ, Johnson ME, Honeyman P. A brief chronology of medical device security. Communications of the ACM. 2016 Sep 22;59(10):66-72.

[60] Food and Drug Administration. Content of Premarket Submissions for Management of Cybersecurity in Medical Devices-Guidance for Industry and Food and Drug Administration Staff. Accessed on June 14 2020 [Online].Available: https://www.fda.gov/media/86174/download

[61] US Food and Drug Administration. Postmarket management of cybersecurity in medical devices: guidance for industry and food and drug administration staff. 2016. Accessed on June 14 2020 [Online].Available: https://www.fda.gov/files/medical

[62] Halperin D, Heydt-Benjamin TS, Fu K, Kohno T, Maisel WH. Security and privacy for implantable medical devices. IEEE pervasive computing. 2008 Jan 16;7(1):30-9.

[63] Ransford B, Molina-Markham A, Stewart Q, Fu K, Kramer DB, Baker MC, Reynolds MR. Security and Privacy Qualities of Medical Devices: An Analysis of FDA Postmarket Surveillance.