VULNERABILITY OF MEDICAL DEVICES AND MEDICAL INSTITUTIONS

IN THE AGE OF IOT AND CONNECTED NETWORKS

Technology Practice Group @ NovoJuris Legal

3/18/2019

Contents

Introduction 2

What is meant by Vulnerability? 4

PART I – Medical Device 5

International Medical Device Regulators Forum 5

UNITED STATES OF AMERICA 8

EUROPEAN UNION 10

INDIA 13

PART II- Cybersecurity Framework 15

Global Cybersecurity Standards 15

United States of America 16

European Union 17

India 18

INTRODUCTION

Medical devices have taken quantum leaps in terms of their functionality, intelligence and precision in the last decade or so. Improved design, better and cheaper production materials, and the inclusion of more sophisticated software have all contributed to this improvement and have made medical devices more adaptable and user-friendly. However, perhaps the most significant development that has greatly enhanced the capabilities of medical devices is the use of connected networks by these medical devices to accomplish machine-to-machine communication.

The modern age medical devices do not function in isolation anymore; they function as integrated medical devices, where the medical device, networks, software, operating systems, and other various technologies are integrated to serve the ever-changing needs of the healthcare industry. An unintended consequence of this interconnectivity is the increased susceptibility of the devices/networks to cyber-attacks as any weak point in the network may be exploited by cyber offenders, leaving all the devices in the network vulnerable.

In the year 2016, Johnson & Johnson had to inform its users that they have learned about cyber-security vulnerability in one of their diabetic insulin pumps, by exploiting this vulnerability a hacker could trigger an “overdose” of insulin in a diabetic patient. At the beginning of 2017 cybersecurity vulnerabilities were identified in St. Jude Medical's implantable cardiac devices and merlin@home transmitters. The transmitters’ inductive model allowed for ‘MerlinOnDemand’ to allow healthcare professionals to read patients’ data remotely. This feature, if exploited, could have allowed an unauthorized user, i.e., someone other than the patient's physician, to remotely access the implanted medical device (radio frequency enabled) by altering the Merlin@home transmitter. The altered Merlin@home Transmitter could then be used to modify programming commands to the implanted device to deplete the battery life of the device or administer inappropriate pacings or shocks.

As mentioned above due to the interconnected nature of medical devices and clinical systems/networks, even clinical systems/networks established in medical institutions have become vulnerable to cyber-attacks. Most of the cyber-attacks on such interconnected clinical systems/networks in medical institutions are initiated to extract the electronic health records (EHRs). These EHRs may contain personal health information of the patients, their medical history, diagnosis codes, billing information, etc. which can be exploited by the cyber offenders in various manners, for instance to extort money from medical institutions or to create fake IDs to buy medical equipment(s) or medication which are not accessible to the public at large.

One of the most well-known examples of such cyber-attacks on interconnected clinical systems/networks was the ransomware attack, known as ‘WannaCry’. The WannaCry attack affected more than 200,000 computers in at least 100 countries. The WannaCry attack also affected 80 out of 236 trusts (medical institutions under the National Health Service, UK) 603 primary care, 595 general practitioners and other National Health Service organizations in the UK. The trusts which were affected by the WannaCry ransomware faced issues like patient appointments being cancelled, computer being locked out, patients from accidents and emergency departments being diverted to other departments among other things.

In India, as reported by multiple news agencies, last year in the month of June, Mahatma Gandhi Memorial hospital, in Mumbai (MGM Hospital) was affected by a similar cyber-attack where the hospital administrators found their systems locked, and noticed an encrypted message by the attackers demanding ransom in Bitcoins to unlock it. It was reported that the MGM Hospital had lost 15 days' data related to billing and patients' history, though the hospital didn't face any financial loss. More recently on February 1, 2019, a cyber-attack on Easton hospital in Easton, Pennsylvania led to a breach of 4.5 million patients' records.

The incidents discussed above clearly indicate that the healthcare industry as a whole has become a prime target for cyber-offenders. Hackers are not only exploiting vulnerabilities present in various modern medical devices, but they are also targeting interconnected clinical systems/networks. Asserting the dual nature of cyber-attacks on the medical and healthcare industry at large, it is clear that the cyber vulnerability of the industry as such has to be addressed at two fronts i.e. (i) modernizing laws and regulations governing manufacturing, sale and distribution of medical devices to specifically address issues related to software and software functions, and (ii) formulating and implementing robust cybersecurity standards specifically for healthcare institutions' networks.

This article identifies the problem of cyber vulnerability of the medical and healthcare industry and analyses regulatory approaches undertaken by United States of America (USA), European Union (EU) and India to lower the susceptibility to cyber-attacks. Further, the article assesses the impact of each regulatory framework implemented by the legal jurisdictions mentioned above.

Part I of the article assesses the laws, regulations and various guidelines in USA, EU, and India with regards medical devices, specifically focusing on inclusion and assessment of software and software functions in relation to medical devices. Further, Part I also discusses various guidance documents/ guidelines published by the International Medical Devices Regulatory Forum (IMDRF) for regulating SiMD and SaMD.

Part II of the article focuses on various cybersecurity guidelines and frameworks recommended/implemented in the USA, EU, and India to protect interconnected networks especially in relation to medical and healthcare institutions. Part II concludes by analyzing various global cybersecurity standards that can be implemented by medical device manufacturers to mitigate cyber vulnerabilities related to medical devices.

What is meant by Vulnerability?

Any cyber-attack aimed at medical devices or institutions may expose the systems to the following vulnerabilities:

- Compromised medical records leading to:
  - Reputational damage
  - Litigation
  - Financial loss
  - Extortions
- Corruption of data or systems leading to:
  - Disruption of medical services
  - Misdiagnoses and mishaps
- Loss of control over medical devices leading to
  - the threat to patients' life if the device has some critical functionality
  - inability to monitor the patient or to inform the patient regarding any risks

Gaining unauthorized access to any medical device or medical institutions' systems can be very simple at times. A cyber-offender may gain access by (a) using a USB drive, (b) exploiting vulnerable or expired software, (c) stealing medical personnel's mobile devices, (d) hacking emails, or (e) phishing. Outdated medical infrastructure, untrained staff and lackadaisical attitude of medical institutions towards cyber security lead to the susceptibility of medical institutions to such attacks.

PART I – MEDICAL DEVICE

INTERNATIONAL MEDICAL DEVICE REGULATORS FORUM

International Medical Device Regulators Forum (IMDRF), is a group of medical device regulators who work together to harmonize the regulatory requirements for medical products which may vary from country to country. IMDRF has issued various guidance documents explaining the requirements to be kept in mind while developing and deploying Software as a medical device (SaMD) in the healthcare market.

IMDRF defines SaMD as "*software intended to be used for one or more medical purposes that perform these purposes* ***without being part*** *[emphasis ours] of a hardware medical device*". Such software should be capable of running on general purpose (non-medical purpose) computing platforms. However, if the software's intended purpose is to drive a hardware medical device, it doesn't satisfy the definition of SaMD. However, it may be used in combination (e.g., as a module) with other products including medical devices. SaMD is one of the three types of software associated with medical devices. The other two types of software are i) software that is integral to a medical device (Software in a medical device- SiMD) and software which is used in the manufacture or maintenance of a medical device.

One thing which one should be watchful of is that SaMDs have to undergo through the process of updating, or alternation while they are in use. With this in mind, the IMDRF has defined what constitutes as a SaMD change. SaMD change refers to any modification which is made throughout the lifecycle of the SaMD including its maintenance phase. ISO/IEC 14764:2006 is the standard which should be adhered to while maintaining software. The above-mentioned standard establishes the maintenance requirements and provides guidance related to planning, execution and revaluation processes. As a result of changes to the SaMD during its lifecycle, the category of the SaMD may have to be regulated again.

IMDRF has issued four specific documents to guide the stakeholders including the manufacturers and developers in developing their software and apps. In 2013, IMDRF's SaMD Working Group had released *Software as a Medical Device (SaMD): Key Definitions* to create a standard terminology for SaMD. The following year, IMDRF adopted *Software as a Medical Device: Possible Framework for Risk Categorization and Corresponding Considerations* which proposes a method for categorizing SaMD based on the following considerations (a) significance of information provided by the SaMD to healthcare decision i.e. the intended use of the information provided by SaMD in clinical management which has different significance on the action to be taken by the medical institutions, and (b) the health care situation or condition that it aims to address. In 2015, the SaMD Working Group published *Software as a Medical Device (SaMD): Application of Quality Management System*, outlining how manufacturers should follow Quality Management System (QMS) Principles for medical devices as well as good software engineering practices. Lastly, IMDRF recently published *'Software as a Medical Device (SaMD): Clinical Evaluation'* to indicate to the manufacturers the importance of Clinical Evaluation.

The following paragraphs briefly explain these documents.

Risk Categorization

State of Healthcare situation or condition	The significance of information provided by SaMD to healthcare decision		
	Treat or diagnose	Drive Clinical Management	Inform Clinical Management
Critical	IV	III	II
Serious	III	II	I
Non-Serious	II	I	I

IMDRF has categorized SaMDs in four categories according to their risks. These categories are based on the levels of impact that these devices may pose to the patients or public health where accurate information provided by the SaMD to treat or diagnose, drive or inform clinical management is vital to avoid death, long term disability, or other serious deterioration of health, mitigating public health. Category I is the least impact these devices can have whereas Category IV is the highest. The *Software as a Medical Device: Possible Framework for Risk Categorization and Corresponding Considerations* explains each category by providing detailed examples so as to help the manufacturers identify what kind of risks their product might pose and thereby what precautions are required to be taken. One key thing which the guidance document prescribes is that SaMD will have its own category according to its SaMD definition statement even when a SaMD is interfaced with other SaMD, other hardware medical devices, or used as a module in a larger system.

Quality Management System

Quality Management of any product is essential. QMS principles are essential to maintain good practices and control the quality of products in organizations. This document complements the previous document published by IMDRF regarding the risk categorizations of SaMDs. This document integrates the Quality Management Principles required in Software and Medical Devices to create a fit model for SaMDs. They address the need for good software quality and engineering practices as well as ensuring that these QMS principles are used to minimize and manage unintentional outcomes related to patient safety.

According to the IMDRF guidance, an effective QMS for SaMD should adhere to the following principles:

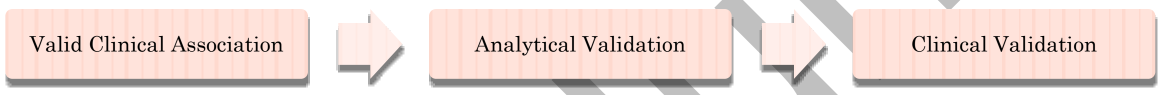
- An organizational structure that provides leadership, accountability, and governance with adequate resources to assure the safety, effectiveness, and performance of SaMD;
- A set of SaMD lifecycle support processes that are scalable for the size of the organization and are applied consistently across all realization and use processes; and
- A set of realization and use processes that are scalable for the type of SaMD and the size of the organization; and that takes into account important elements required for assuring the safety, effectiveness, and performance of SaMD.

Clinical Evaluation

Increased usage of SaMD would result in doctors putting in more reliance on the decisions made by these software. In such a scenario, it is vital that the SaMD predict the best scenario to reduce the chances of misdiagnosis. Thus IMDRF has recommended that the developers follow the process of clinical evaluation so as to have a precise diagnosis.

Clinical evaluation is a systematic and planned process to continuously generate, collect, analyse, and assess the clinical data pertaining to a SaMD in order to generate clinical evidence verifying the clinical association and the performance metrics of a SaMD when used as intended by the manufacturer. The quality and breadth of the clinical evaluation is determined by the role of the SaMD for the target clinical condition and assures that the output of the SaMD is clinically valid and can be used reliably and predictably.

To perform a clinical evaluation, the manufacturers, depending on different SaMDs, needs to do the following:



Valid Clinical Association

Analytical Validation

Clinical Validation

- Valid Clinical Association: The manufacturer needs to check whether there is a valid association between the SaMD outputs, based on the inputs and algorithms selected, with the SaMD targeted clinical condition. This needs to be done only if required, this depends on the type of SaMD in question.
- Analytical Validation: This is to ensure that the SaMD meets the technical requirements, it checks whether the output is what was technically expected from the SaMD.
- Clinical Validation: The manufacturer needs to ensure that the SaMD generates clinically valid outputs. Measures of clinical validation may be sensitivity, specificity, positive predictive value, etc.

These processes need to be validated by generating evidence via already existing research or novel clinical association.

It is recommended that the manufacturer may get evidence of clinical evaluation independently reviewed. In case of high-risk SaMDs, this becomes more important in providing users with the confidence in the performance metrics including but not limited to, identification of design errors or limitation, broadening technical competence, testing the appropriateness of assumptions, and management of bias.

UNITED STATES OF AMERICA

The US Food and Drug and Administration (FDA) through the Federal Food Drug & Cosmetics (FD&C) Act regulate medical devices. Section 321 (h) of Title 21 of the FD&C Act has defined a device as "*an instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, or other similar or related article, including any component, part, or accessory, which is-*

> *(i) recognized in the official National Formulary, or the United States Pharmacopeia, or any supplement to them,*
>
> *(ii) intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease, in man or other animals, or*
>
> *(iii) intended to affect the structure or any function of the body of man or other animals, and*
>
> *which does not achieve its primary intended purposes through chemical action within or on the body of man or other animals and which is not dependent upon being metabolized for the achievement of its primary intended purposes.* ***The term 'device' does not include software functions excluded pursuant to section 360 j (o) of this title [emphasis ours]****".*

Section 360 j (o) of the FD&C Act clearly stipulates that a device shall not include a software function which is intended for (a) administrative support of a healthcare facility including but not limited to billing information, appointment schedule, business analytic, (b) maintaining a healthy lifestyle and which is unrelated to the diagnosis, cure or treatment of a disease or a condition, (c) serving as electronic patient records including the patient provided information and so long as the records are part of the health information technology certified under the FD&C Act, and such function is not intended for analyzing or interpreting the records for the purpose of diagnosis, cure, mitigation, etc., (d) transferring, storing, displaying lab tests, findings of the lab test or the device, unless such function is intended to interpret or analyses the clinical lab tests or other device data, results or findings.

It is to be noted that except any software being used for the above-mentioned purposes as mentioned in Section 360 (j) (o) software can be termed as a device which can be a standalone device or also being used as a component of any other device. The statute is silent as to separately classifying the device and software when the software is used as a component of any other device.

The FDA in 2005 had released a *Guidance Document for the content of Premarket Submissions for Software Contained in Medical Devices* which is non-binding in nature. The document states that medical devices may contain one or more software components, parts, or accessories, or may be composed solely of software which is defined as a "*software device*". This guidance document applies to software devices regardless of the means through which the software is delivered to the end user. In a software development environment, "software verification**"** is the confirmation that the output of a particular phase of development meets the input requirements. Further, the software has to undergo through the process of software validation i.e. establishing by evidence that the software conforms to the user's needs and intended uses of the device. This involves the software being checked for proper operations in its actual or a simulated use environment.

As stated in "*Software as a Medical Device: Possible Framework for Risk Categorization and Corresponding Considerations*" the SaMDs are categorized through a formulation which is a combination of information provided by the manufacturer and the healthcare issue which it proposes to address. Based on the consideration the SaMDs are categorized into 4 categories. As per the framework category, category I SaMD has the lowest impact whereas category IV has the highest level of impact. Also when a SaMD is to be utilized across multiple healthcare situations or conditions it is categorized as per the highest category applicable. Further, when the manufacturer makes changes to the SaMD during the lifecycle the categorization of the SaMD should be revaluated appropriately. The framework for risk categorization also provides that IEC 62304 is the standard for life cycle development of medical device software. IEC 62304 provides for a risk-based decision model, which calls for certain testing requirements and highlights three major principles that promote the safety of SaMD:

- Risk management;
- Quality management; and
- Methodical and systematic systems engineering according to best industry practices.

Further, in 2016 the FDA released a guidance document on *Software as a Medical Device: Clinical Evaluation*.

While classifying the devices the FDA does not differentiate between software as a standalone device and software used as a component. The FDA has also published guidance documents containing recommendations on matters such as clinical evaluation of the device or the pre-market submissions if the software is contained in the device, which are good practices to adhere to but are not binding in nature.

EUROPEAN UNION

On 5th April 2017, 2 new Regulations on medical devices were adopted by the European parliament namely, Regulation (EU) 2017/745 ("Regulation 1") and Regulation (EU) 2017/746 ("Regulation 2") – collectively referred to as "Regulations".

Regulation 1 regulates all kinds of medical devices other than *in vitro* diagnostic medical devices, whereas Regulation 2 regulates *in vitro* diagnostic medical devices.

The new Regulations in their entirety will only apply after a transitional period- 3 years after entry into force for the Regulation on medical devices and 5 years after entry into force for the Regulation on diagnostic medical devices.

The EU through these Regulations has completely changed its regulatory stance towards medical devices; these Regulations now categorize medical devices as per the risk associated with a medical device.

Recitals to both Regulation 1 and Regulation 2 clarify that a software in its own right, when specifically intended by the manufacturer to be used for one or more of the medical purposes set out in the definition of a medical device, qualifies as a medical device, while software for general purposes, even when used in a healthcare setting, or software intended for lifestyle and well-being purposes is not a medical device. This position is similar to the one taken by the USA's FDA.

Regulation 1 defines a medical device as *any instrument, apparatus, appliance, software, implant, reagent, material or other article intended by the manufacturer to be used, alone or in combination, for human beings for one or more of the following specific medical purposes:*

- *diagnosis, prevention, monitoring, prediction, prognosis, treatment or alleviation of disease,*
- *diagnosis, monitoring, treatment, alleviation of, or compensation for, an injury or disability,*
- *the investigation, replacement or modification of the anatomy or of a physiological or pathological process or state,*
- *providing information by means of in vitro examination of specimens derived from the human body, including organ, blood and tissue donations,*

and which does not achieve its principal intended action by pharmacological, immunological or metabolic means, in or on the human body, but which may be assisted in its function by such means.

The following products shall also be deemed to be medical devices:

- *devices for the control or support of conception;*
- *products specifically intended for the cleaning, disinfection or sterilisation of devices as referred to in Article 1(4) and of those referred to in the first paragraph of this point.*

Regulation 2 defines *in vitro* diagnostic medical devices as *any medical device which is a reagent, reagent product, calibrator, control material, kit, instrument, apparatus, piece of equipment, software or system, whether used alone or in combination, intended by the* *manufacturer to be used in vitro for the examination of specimens, including blood and tissue donations, derived from the human body, solely or principally for the purpose of providing information on one or more of the following:*

- *concerning a physiological or pathological process or state;*
- *concerning congenital physical or mental impairments;*
- *concerning the predisposition to a medical condition or a disease;*
- *to determine the safety and compatibility with potential recipients;*
- *to predict treatment response or reactions;*
- *to define or monitoring therapeutic measures.*

It is pertinent to note that the Regulations recognise software both as a medical device and as a component integrated into a medical device. This regulatory approach makes it evident that if the vulnerabilities of medical devices, as discussed at the beginning of this article are to be mitigated, it is important to regulate and set standards for the development of SiMDs and SaMDs.

The Regulations while discussing software under the 'Classification Rules' state that a "*Software, which drives a device or influences the use of a device, shall fall within the same class as the device*. *If the software is independent of any other device, it shall be classified in its own right*". This classification of SiMD and SaMD reflects that while allowing a SiMD or a SaMD to be developed and sold in the EU markets, it is of utmost importance to assess the vulnerabilities and risks associated with such medical devices. The Regulations also show the importance of setting standards and regulations for these medical devices basis the risk assessment.

Medical device manufacturers under the Regulations prior to placing their medical device in the EU market and prior to putting them into service have to adhere to certain 'General Safety and Performance Requirements' ("Requirements"). The purpose of making every manufacturer adhere to these Requirements is that any medical device made available in the EU should be safe and effective and should not compromise the safety of patients or other persons. While addressing software in specific, these Regulations state that medical devices should be manufactured in such a manner that reduces the risks associated with the possible negative interaction between software and the IT environment within which it operates.

Further, the Requirements, in particular, emphasis on reducing and removing risks associated with medical devices which incorporate *electronically programmable systems including software* that are medical device themselves. The Regulations clearly state that manufacturer of a medical device, which incorporates an electronically programmable system including software, should ensure repeatability, reliability and performance in line with their intended use. In the event of a single fault condition, appropriate means shall be adopted to eliminate or reduce as far as possible consequent risks or impairment of performance. Any such software should be manufactured taking into account the principles of the development life cycle, risk management, including information security, verification and validation. If a software is intended to be used in combination with a mobile computing platform the software should be manufactured in accordance with the specification of such mobile platforms (e.g. size and a contrast ratio of the screen) and the external factors related to their use (varying environment as regards the level of light or noise). The manufacturers are required to provide minimum requirements of hardware, IT networks, and IT network security measures including protection against unauthorised access, necessary to run the software as intended.

Regulations also define the compatibility and interoperability of medical devices. The Regulations state that any device which is intended to be used with other devices should be manufactured in a manner that allows for safe interoperability.

INDIA

The Medical Devices Rules, 2017 ("Rules") formulated under the Drugs and Cosmetics Act, 1940 regulates the manufacturing, distribution and clinical tests related to medical devices in India. Rule 3 (zb) defines a medical device as follow:

> *"medical device" means,- (A) substances used for in vitro diagnosis and surgical dressings, surgical bandages, surgical staples, surgical sutures, ligatures, blood and blood component collection bag with or without anticoagulant covered under sub-clause (i),*
>
> *(B) substances including mechanical contraceptives (condoms, intrauterine devices, tubal rings), disinfectants and insecticides notified in the Official Gazette under sub-clause (ii),*
>
> *(C) devices notified from time to time under sub-clause (iv), of clause (b) of section 3 of the Act;*

Medical devices under the Rules are classified into 4 risk-based classes as per their intended use and risks associated therewith. The classification of medical devices determines the procedure to be followed to procure the licenses required to manufacture or distribute the medical devices.

The Rules recognise various kinds of medical devices i.e. the *in-vitro* medical device, in-vitro diagnostic medical device, invasive and non-invasive device, implantable medical devices etc.

What is interesting to note here is that the initial draft of the Rules, published for public comments included the term 'software' in the definition of medical devices, but the same was removed in the final draft of the Rules. The Rules may have removed software from the definition of medical devices but the Rules do regulate the same. Below is a detailed analysis of how software (integrated and standalone) in relation to a medical device is regulated in India as of today subject to if the respective medical device falls under the purview of the definition of a medical device as not all medical devices in India are regulated.

Under this section, we will discuss how software is placed for assessment along with the kind of medical device it is being used for. In case of medical devices other than *in vitro medical devices* software, which drives a device or influences the use of a device, falls automatically in the same class. Whereas in case of *in vitro* medical devices a software, which drives a device or influences the use of a device, falls automatically in the same class as the device. And in case of standalone software, which is not incorporated into a medical device and provides an analysis based on the results from an analyser, shall be classified into the same category that of the *in vitro* diagnostic medical device on the basis of its intended use.

Further, in case a medical device other than an *in vitro* medical device which falls under class B, C or D an applicant for procuring a license to manufacture the medical device has to submit a device master file ("File") along with manufacturing application submitted under the relevant form.

Appendix II of the Rules details what should form a part of the File. Among other things, the File should contain the device description and product specification, including that of variants and accessories, which include 'software'. Additionally, the File should contain details about software verification and validation. This information should typically include the summary results of all verification, validation, and testing performed both in-house and in a simulated or actual user environment prior to the final release of the medical device. It should also address all different hardware configurations and, where applicable, operating systems identified in the labelling.

An applicant who intends to procure an import license for medical devices has to submit a design analysis data pertaining to validation of software relating to the function of the device (if applicable). Similar norms are also applicable to any applicant who intends to manufacture a new *in vitro* medical device. Under the Quality Management System standards prescribed in Schedule 5 of the Rules for medical devices (including *in vitro* medical devices), a manufacturer is required to establish documented procedures for the validation of the application of computer software (and its changes to such software or its application) for production and service provision that affect the ability of the device to conform to specified requirements. Such software applications are required to be validated prior to initial use and the records of the same are supposed to be kept.

The Rules state that SiMDs and SaMDs should be classified under the same risk category as that of the respective medical device the software is integrated with or the same category of *in vitro* diagnostic medical device where it controls or influences the intended output of a separate in vitro diagnostic medical device. Unlike the EU Regulations, the Rules do not account for the interoperability/compatibility of devices. The Rules do not specify any norms regarding the use of the devices in an interconnected environment. The Rules are silent about the manufacturers/importers specifying the IT environment/platforms on which a given device/software can be used, making it amply clear that the regulators did not foresee medical devices being used in a network of other such devices.

PART II- CYBERSECURITY FRAMEWORK

GLOBAL CYBERSECURITY STANDARDS

There are a number of international standards that provide for pre-requisites for the certification of medical devices *vis-a-vis* the development and design risk assessment process. These standards do not focus on cybersecurity within the complex deployment setting. However, since many security flaws result from poor software design the list provided below includes certain standards related to software designs.

- ISO/IEC 27032:2012 Information technology – Security techniques – Guidelines for cybersecurity standard provides guidance on addressing cybersecurity issues and its relationship to other types of security to highlight the basic practices in cybersecurity.

- IEC 62304:2006 – Medical device software – software life cycle processes define the medical device software lifecycle requirements.

- IEC/ISO CD 82304 Health software – Part 1: General requirements for product safety (under development) is a standard for the safety of health software, and evolution of IEC 62304. This standard provides requirements for the safety of health software products, and while situations where health software is part of – or embedded in – a physical device are not part of this standard, where medical devices are software only, this standard should be used.

- ISO/IEC 80001 series of standards detail guidance for application of risk management for IT-networks incorporating medical devices.

- ISO/DTR 80002–2 Medical device software – Part 2: Validation of software for regulated processes is a technical report under development, which considers embedded and associated software with all medical devices.

- IEC/TR 80002–1:2009 Medical device software – Part 1: Guidance on the application of ISO 14971 to medical device software. This provides the risk management practitioner advice on meeting the requirements of ISO 14971 and is used as the principal standard for risk management regulation.

- IEC/TR 80002–3:2014 Medical device software – Part 3: Process reference model of medical device software life cycle processes (IEC 62304). This provides the description of the software life cycle processes and the associated safety class definitions, derived from IEC 62304.

It is evident that till now there has been no separate or specialized legislation or regulation in place which deals with new age medical devices integrating technologies like IoT and AI with modern healthcare. In addition to the guidance notes provided by the FDA, the FDA has put in place the following mechanisms to ensure that the IoT/AI enabled medical devices are safe to use. The FDA recommends that manufacturers of IoT/AI enabled medical devices to use NIST (National Institute of Standards and Technology) framework for improving 'critical infrastructure cybersecurity', based on the regulation of industrial control system. NIST Cyber Security Framework maps reference standards for specific elements and various other frameworks including the Health Insurance Portability and Accountability Act (HIPAA) 1996. The FDA came out with the draft guidance document on the *Content of Premarket Submissions for Management of Cybersecurity in Medical Devices* on October 18, 2018. This guidance document provides recommendations which should be considered and included in FDA medical device premarket submissions for effective cybersecurity management. The guidance document specifically states that it is applicable to premarket submissions for devices that contain software or programmable logic as well as software that is a medical device. As a part of the design controls, device manufacturers must "*establish and maintain procedures for validating the design of the device"* which "*shall include software validation and risk analysis, where appropriate"* and as a part of software validation a risk analysis the manufactures may need to establish a cybersecurity vulnerability and management approach. The FDA here defines two tiers of devices according to their cybersecurity risk:

Tier 1- High cybersecurity risk-(a) a device is capable of connecting to another medical or non-medical product, or to a network, or the internet; and (b) the cybersecurity incident affecting the device would directly result in patient harm to multiple patients.

Tier 2- Standard cybersecurity risk- other medical devices which cannot be categorized under Tier 1.

The guidance document makes it evident that the cybersecurity risk tiers may not track to the statutory risk classification as mandated by the FDA.

EUROPEAN UNION

ENISA was created in 2004 by EU Regulation No 460/2004 as **European Network and Information Security Agency** EU Regulation No 526/2013 which repealed the earlier regulation references it as the *European Union Agency for Network and Information Security (ENISA)*. The ENISA was formed with the objective to enhance the capability of the Member States to prevent, address and to respond to network and information security problems. The ENISA coordinates among the member states and assists them in developing legislation in the field of network and information security.

As a part of the EU cybersecurity strategy, the European Commission adopted the EU Network and Information Security Directive ("NIS Directive") on 6 July 2016 and the same came into force in August 2016. The NIS Directive mandates every member state of the EU to have certain cybersecurity capabilities, e.g. it is a mandate for every member state to have a national Computer Security Incident Response Team ("CSIRT"). The NIS Directive encourages collaborations between EU member states like the EU CSIRT network, the NIS cooperation group, ENISA, etc. As per the NIS Directive, every member state shall supervise the cybersecurity of critical market sectors in their respective country including the health sector.

Further, as a part of the NIS Directive the NIS cooperation group through ENISA has developed guidelines regarding (i) identification criteria of cyber-attacks, (ii) incident notification, (iii) security requirements for Digital Signal Processors (DSPs), (iii) mapping of operators of essential services (OES) security requirements for specific sectors including health, and (iv) audit and self-assessment frameworks for OESs and DSPs.

European Committee for Standardization (CEN) was formed with a view to prescribing certain standards of safety and quality. The CEN supports standardization activities in relation to a wide range of fields and sectors including healthcare.

The General Data Protection Regulations ("*GDPR*") specifically defines 'data concerning health', 'genetic data' and 'biometric data' and regards them as 'special category of data', this means that parties who process special categories of data shall comply with additional higher safeguards and process it legitimately. Recital 53 of the GDPR states that special categories of personal data which merit higher protection should be processed for health-related purposes only.

INDIA

Information Technology Act, 2000

Personal medical/health information in India is regarded as sensitive personal information as per the *Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 ("Rules").*

To strengthen the framework and to ensure that reasonable security practices and procedures are followed, the Department of Information Technology introduced Rules. The Rules requires each and everybody corporate including medical institutions which are collecting such sensitive personal information to have security measures as documented in their security policy/programmer which is considered to be a reasonable security practice keeping in mind the nature of their business and considering the fact that they are collecting sensitive personal information. One such international standard as recommended under the Rules is the IS/ISO/IEC 27001.

Computer Emergency Response Team

The Indian legislature took an important step in addressing issues relating to cybersecurity when it amended the *Information Technology Act, 2000* in 2008, through which they established an Indian Computer Emergency Response Team (CERT), a national agency for incident response. CERT has been entrusted with performing the following main functions (a) collecting, analyzing and disseminating information on cyber incidents, (b) forecasting and giving alerts on cybersecurity incidents, (c) laying down emergency measures for handling cybersecurity incidents, (d) coordinating cyber incident response activities, (e) issuing guidelines, advisories, vulnerability notes and whitepapers relating to information security practices, procedures, prevention, response and reporting of cyber incidents, and (f) performing any other functions relating to cybersecurity as may be prescribed.

CERT has been focused on making various institutions dependent on cyber/digital networks cyber-resilient. Being cyber resilient allows these institutions to anticipate various threats and have adequate safeguards in place to deal with the cyber-attacks. Anticipate, withstand, contain and recover are the four main contours of being cyber resilient:

- *Anticipate: Maintain a state of informed preparedness in order to forestall compromises of mission/ business functions from adversary attacks*
- *Withstand: Continue essential mission/business functions despite successful execution of an attack by an adversary*
- *Contain: Localize containment of crisis and isolate trusted systems from untrusted systems to continue essential business operations in the event of cyber attacks*
- *Recover: Restore mission/business functions to the maximum extent possible subsequent to the successful execution of an attack by an adversary*
- *Evolve: To change missions/business functions and/or the supporting cyber capabilities, so as to minimize adverse impacts from actual or predicted adversary attacks*

Digital Information Security in Healthcare Act (Bill)

Taking a step further, the Ministry of Health and Welfare ("Ministry") has introduced a draft bill for Digital Information Security in Healthcare Act ("DISHA") to safeguard EHRs. One of the key purposes of DISHA is to ensure reliability, data privacy, confidentiality and security of digital health data. DISHA prescribes that the storage of digital health data so collected would be held in trust for the owner and the holder of such data would be considered as the custodian of data thereby making such holder responsible to protect privacy, confidentiality and security of data.

DISHA's main purpose, as per its preamble is to *(i) establish National health Authority (NeHA), State health Authorities ("SeHA") and Health Information Exchanges; (ii) standardize and regulate the processes related to collection, storing, transmission and use of digital health data; (iii) and to ensure reliability, data privacy, confidentiality and security of digital health data.*

Further, these clinical establishments can only collect digital health information for certain particular purposes which are more or less related to providing medical and healthcare services to owners of the digital health information. DISHA clarifies that digital health information in any form i.e. whether identifiable or anonym zed, shall not be accessed, used or disclosed to any person for commercial purposes.

The primary functions of NeHA and SeHA ("Authorities") include:

- Formulation of standards, guidelines and protocols for the generation, collection, storage and transmission of the digital health data.
- Defining protocols to safeguard the data from any theft or breach and to provide for data security measures at each level of processing of data, which shall at least include access controls, encryption and audit trails.
- Laying down protocols for transmission of digital health data to and receiving it from other countries.
- Providing for standards for establishing necessary norms and standards for certifying digital healthcare data systems and stakeholders.
- Conducting regular checks and investigations to ensure compliance with the law.

One of the key aspects of DISHA is to establish digital health information exchanges ("DHIE(s)") which allow doctors, nurses, pharmacists, other health care providers and patients to access and securely share a patient's vital medical information electronically—improving the speed, quality, safety and cost of patient care. Any and all transmission of digital health information will happen through these exchanges. The intention under DISHA is to store and keep all the digital health data in these DHIEs located across India. This can only be possible if the digital health information is standardized i.e. it is maintained in the same format by all and therefore the Ministry primarily introduced the EHR standards and now through DISHA wants to integrate the EHR records and provide the digital healthcare system with a proper structure. While, DISHA is in the draft stage, and the standards for storing and transmitting health records are yet to be delineated, it is heartening to see the Ministry taking appropriate steps to ensure the safety of digital health records.

About NovoJuris

NovoJuris is an innovative new age law-firm, where clients leverage on update, in-depth knowledge to adapt to evolving business environment. With nearly a decade of its presence, NovoJuris has worked with numerous high impact technology companies, large corporates, high growth startups and disruptive business models.

NovoJuris has been consistently ranked amongst India's top 10 active legal counsellors in Private Equity.

The practice areas are private equity, technology laws, intellectual property, cross-border transactions, M & A, corporate advisory and compliances, startups and accelerators, employment laws, SEZ and real-estate, dispute resolution, mediation and settlements.

NovoJuris caters to an array of businesses including technology, startups, accelerators, R & D, electronics, e-commerce, trading, media, entertainment, BFSI, sports, real-estate, telecom, and many more.

Twitter: @NovoJuris

Contact: relationships@novojuris.com