Health Policy and Technology 10 (2021) 100549

Contents lists available at ScienceDirect

Health Policy and Technology

journal homepage: www.elsevier.com/locate/hlpt

Review Article

Cybersecurity in the Internet of Medical Things

Nicole M. Thomasian *, Eli Y. Adashi

The Warren Alpert Medical School, Brown University, Providence, RI, United States

ARTICLE INFO

Keywords:
Cybersecurity
Internet of things
Public health preparedness
Health policy

ABSTRACT

Background: The Internet of Things has spawned a new fleet of medical devices replete with improved sensing and actuating capabilities. Preemptive mitigation of the cyber risks that arise in this hyperconnected space is needed to ensure continued patient safety.
Objective: The aim of this paper is to analyse the robustness of existing policy measures in securing the Internet of Medical Things technologies. The regulatory ecosystem in the US is primarily discussed herein and includes regulatory frameworks for industry, public-private partnerships, and transparency initiatives.
Methods: A qualitative review of the medical cybersecurity literature was performed with collation of federal and international legal documents, policy reports, industry frameworks, cyberbreach analyses, and scientific journal articles.
Results: Regulatory guidance documents introduced to date that address cybersecurity in the Internet of Medical Things place a key emphasis on device identification, legacy device management, enhanced physical security, and breach detection. Recent oversight trends aim to bolster federal authority around the enforcement of baseline security safeguards.
Conclusions: Additional regulatory guidance is needed to mitigate risks in the Internet of Medical Things devices conferred by retrofitted IT infrastructures, edge-to-cloud interfaces, and off-the-shelf device components. Recent advancements in the cyber realm also raise the possibility of novel attack vectors, autonomous cyber-physical systems, and quantum computing threats. Interventions to promote awareness and security hygiene around the Internet of Medical Things devices can empower end users and facilitate smooth incident response.
Lay summary: The rise "Smart" technologies such as voice assistants and adaptable at-home appliances moves us closer to a more personalized world that can enhance our daily lives. The field of medicine will be changed by these next generation "Internet of Things" technologies that possess the ability to interact with their users and their surrounding environment. These technologies are important because the precision with which medical devices interact with patients, healthcare workers, and other technology can have huge impact on patient care. For all of their promise, the increased interconnectivity that these devices possess also confers additional cybersecurity risks. Policy regulation and public health preparedness are critical for ensuring the benefits of these emerging technologies do not come at the expense of patient safety and privacy. In this Review, we discuss cybersecurity regulation in the Internet of Medical Things and highlight novel threats still in need of address at the policy and public-health levels.

Introduction

The degree to which devices are able to optimally interface with patients, healthcare providers, and other technology can significantly impact delivery of care. In a transition that mirrors industry at-large, medical devices now often take advantage of networks that can offer enhanced communication, safety, and feedback control. Indeed, medical technology has secured a place amongst the Internet of Things (IoT) in the ever growing body of embedded devices that automate our world. But this digital revolution is not one only of scale but also of proximity. What was once a network of devices is now a human device network. For all of its appeal, this recent push for interconnectivity also confers additional security risks. A single weak point in these convoluted networks could very well cripple vital health infrastructure. What's more, with humans directly in the loop, the stakes of cyber subterfuge are higher than ever. Risks are further complicated by the shifting ground

* Corresponding author.
E-mail address: nicole_thomasian@brown.edu (N.M. Thomasian).

https://doi.org/10.1016/j.hlpt.2021.100549

Available online 4 July 2021

underneath. New technology lends itself to new targets, imploring a need for agile cybersecurity systems that can combat these emergent threats in real-time.

More than just technically feasible, the widespread takedown of medical devices is an imminent threat [1]. Recent malware campaigns on hospitals have clearly demonstrated that health data are already under attack globally [2]. There is nothing to preclude similar events from happening in the context of medical devices. It is against this evolving backdrop that we evaluate the existing cyberthreat landscape. Of note, the scope of the term "medical device" is vast and refers broadly to items used for the prevention, diagnosis, treatment, or cure of disease (See Table 1). We hone in on the Internet of Medical Things (IoMT) specifically, which refers to a cyber-physical ecosystem of interconnected sensing and actuating objects within the health sector (See Fig. 1) [3]. These devices constitute a major security risk owing to their ubiquity and relatively immature safeguards [4,5]. Below, we discuss potential sequelae of cyber harm in medicine, discuss regulatory efforts to date, and outline emerging threats in "Smart" security for healthcare.

Taxonomy of harm

Any device that utilizes a network or information system runs a risk of being hacked. Cyberattacks fall on a continuum of brazen to imperceptible, which has implications in terms of detection and response. Also worth noting, while the term "cyberattack" is often conflated with malicious intent, accidental security breaches can equally threaten patient safety. We illustrate the effects of cyberattack by way of a canonical security framework, drawing from both counterfactual and past examples (see Fig. 2). Of note, this classification schema is not meant to be exhaustive, and the mechanistic principles of cyberattack are illustrated in broad strokes as they are intended as a general overview for policymakers and healthcare practitioners.

Table 1
Glossary of Key Terms and Abbreviations.

Term	Definition
Cybersecurity	Measure to safeguard the confidentiality, integrity, and availability of digital data and technology.
Medical device	Items used for the prevention, diagnosis, treatment or cure of disease.
Internet of things (IoT)	A cyber-physical ecosystem of interconnected sensing and actuating objects.
Sensor	An entity that detects physical indicators and converts it to a digital signal.
Actuator	An entity that manipulates a physical output in response to a digital signal.
Bluetooth	Wireless technology that enables device communication by transmitting packets of data over short distances.
Wearables	Devices that externally interface with the human body, thus enabling them to be easily worn and removed.
Implantables	Devices with a component(s) that interfaces internally within the human body.
Malware	Software of code that can be used to damage or disable devices.
Denial of service (DoS)	An attack that overloads the IoT bandwidth, memory, and battery limitations, usually by flooding the network with traffic.
Botnet	An army of devices that are hijacked to flood a network in a denial of service attack.
Bluetooth Low Energy (BLE)	A variant of Bluetooth with lower power consumption that maintains a similar operational range.
Off-the-shelf (OTS)	Components made by external vendors that manufacturers can use to associate with or embed into their devices for operational control, functionality, or energy sourcing.
Artificial intelligence (AI)	The application of computer algorithms to perform tasks generally associated with human intelligence.
Cloud computing	Use of servers on the Internet to run software and databases.
Edge computing	Use of servers close to the device for data processing.
Quantum computing	Use of quantum mechanics to generate parallel processing states that operate simultaneously to increase computing power and functionality.
Cryptography	Protection of communications by converting data in (encryption) and out (decryption) of a secure format.
Blockchain	A digital leger for decentralized storage of data that utilizes cryptographic techniques.

Confidentiality

Loss of confidentially traditionally refers to unauthorized disclosures of patient information protected under federal legal code. In the context of external threats, this usually occurs due to unauthorized access, device theft, or malware attack. First, a hacked device could be used as conduit to eavesdrop on health information by an unsanctioned actor. Network access authentication and encryption of IoT device data may be able to curtail this type of attack, but past incidents have shown that these best practices are not always in place [6–8]. Even if the Internet of Medical Things are properly secured, the advent of Smart environments also raises the possibility of health-adjacent IoT as new attack vectors. This principle is no better illustrated than by the infamous casino cyber heist of 2017 [9,10]. In this hack, adversaries used a Smart fish tank in the lobby to gain access the casino network and were then able to exfiltrate several gigabytes of information from the high-roller database. The theft of IoT is another method that can be used to lift data or credentials from the device and highlights the importance of physical security [11]. This risk is compounded by the fact that IoT devices are frequently concealable and are often found in areas with unrestricted physical access. Mitigations for theft might include equipping high-risk, portable IoT with location trackers linked to alerts for suspicious activity [12]. Finally, hackers can also infect devices with malware programs for use in data surveillance or extraction.

Internal threats can be classified as intentional or inadvertent and result from creation of a "backdoor" that introduces an opening for subsequent attack. Malware attacks often exploit this type of insider error. Take a phishing attack, for example, that – once clicked by an unsuspecting patient or medical staff – propagates spyware from a computer onto nearby devices. Education around cyberattack awareness is one way to help to curtail this type of attack [13]. Timely device upkeep and maintenance is also vital for good security hygiene [14]. These practices would include anything from the timely installation of updates or patches to device end-of-life care. Failure to properly purge a device prior to disposal, for example, could leave it vulnerable to data extraction. Misplaced devices would also carry a similar risk profile. Finally, an all-too-common example of an internal failure is neglecting to change the default passwords on Smart devices, which adversaries can exploit to gain access privileges [15,16].

Integrity

Integrity is the trustworthiness of a device. Broadly speaking, loss of device integrity can be due to corruption of functionality or data. A classic example is direct weaponization of a medical device through a reprogramming attack. This type of hacking can elicit a wide range of effects based on the device's clinical application. For example, commandeering of devices that intimately associate with the body such as implantables or pumps could directly result in death or bodily harm. Subtle cognitive manipulation, such as by tampering with neurostimulation devices, could be more difficult to pick up. In as early as 2008, researchers demonstrated that the malicious hacking of medical devices was technically feasible in the laboratory setting [17]. The group was able to tweak the device programmer of a pacemaker to eavesdrop, alter patient data, disrupt communications, produce interference, and manipulate the administration of shocks [17]. This is by no means an isolated incident, and recent examples have also entrenched the IoMT [18]. Take, for example, the 2016 vulnerability in the Owlet Smart sock, a baby monitor replete with sensors that parents can use to track their infant's heart rate and oxygen saturation on their phone [18]. A security researcher found that the Smart sock communications with the Owlet

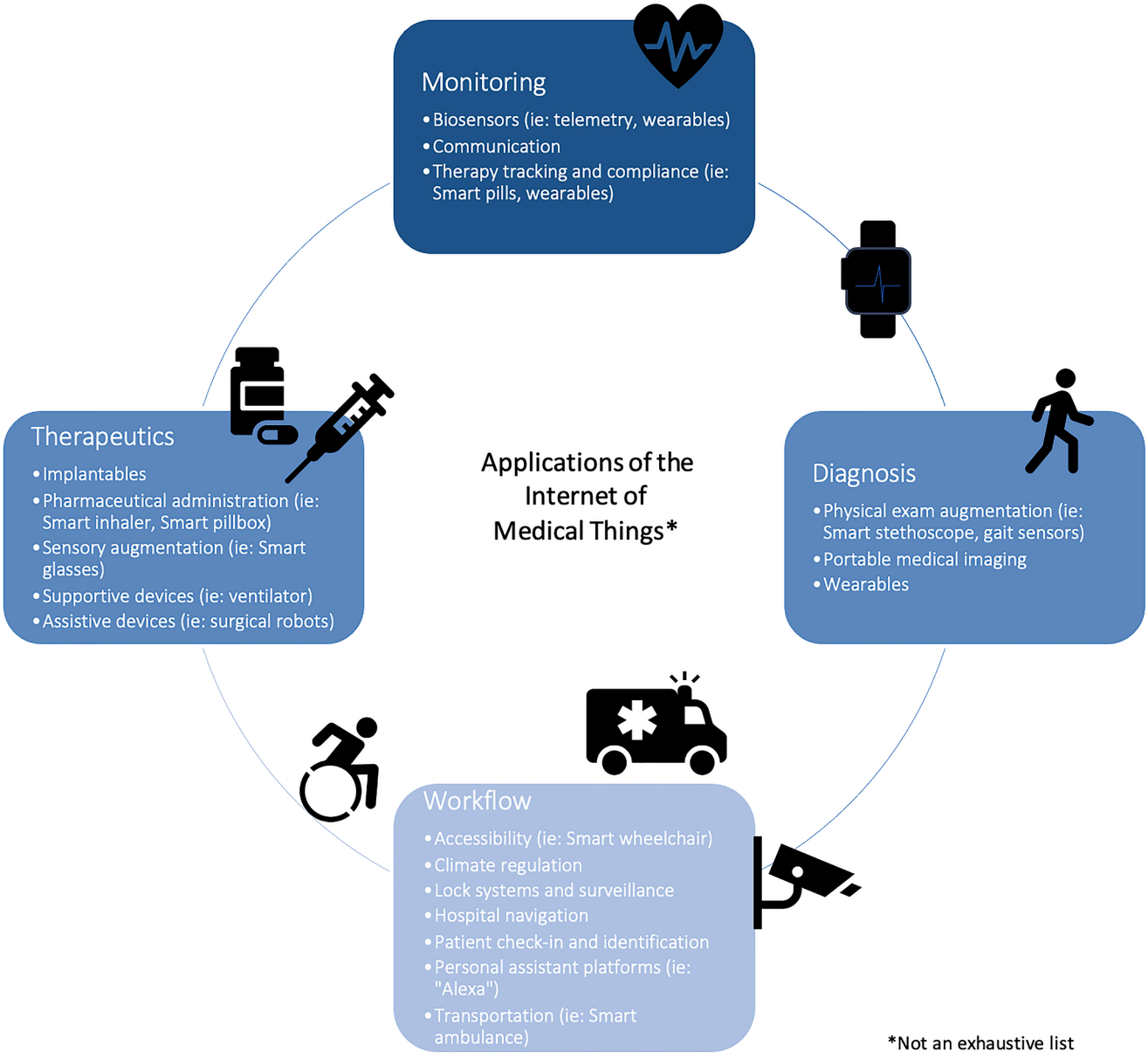

Fig. 1. Applications of the Internet of Medical Things.

data routing station were held on an unauthenticated network without encryption [18]. An adversary could have easily exploited the vulnerability to remotely silence, generate, or otherwise interfere with the baby monitor alarms.

Devices can also be compromised through sabotage of data integrity. For example, a malicious actor could deliberately inject inputs or install malware to corrupt device data. Thus, this type of attack disrupts any data-driven device process. Possible sequalae of such an attack might include inaccurate device calibration, misdiagnosis, or treatment errors [19]. Consider the hypothetical scenario of a patient with high blood pressure and chronic heart failure who is using a Smart pillbox to manage their multiple medications. A data injection attack on the pillbox could be used to double the dose of the patient's diuretic medication or to trick the device into thinking the drug had already been administered. This could induce deleterious effects on the patient's blood pressure that could result in hypoperfusion-associated injury or death.

Availability

Availability refers to the ability of a device to be used by an authorized party. This property is constrained by bandwidth, memory, and battery limitations. Denial of service (DoS) attacks overload a device, typically by flooding the network with traffic. A DoS attack could be utilized to drain the battery of a pacemaker, for example [20]. Alternatively, by saturating the memory of a Smart watch, one could render the device unresponsive or force a reboot. The latter is just one demonstrated sequalae of the March 2020 "SweynTooth" vulnerabilities in the Bluetooth Low Energy (BLE) "system on a chip" [21]. Generally speaking, the reduced power consumption of BLE make it an attractive and widely utilized option for resource-poor devices like IoT. However, a group of researchers from Singapore identified a number of flaws in the protocol stack of major off-the-shelf (OTS) BLE components that are used for device pairing [21]. The scope of SweynTooth was massive, implicating over 480 product lines across multiple sectors and highlighting the need for attention to security in OTS items [21]. The vulnerabilities are primarily exploitable by DoS tactics with an attack

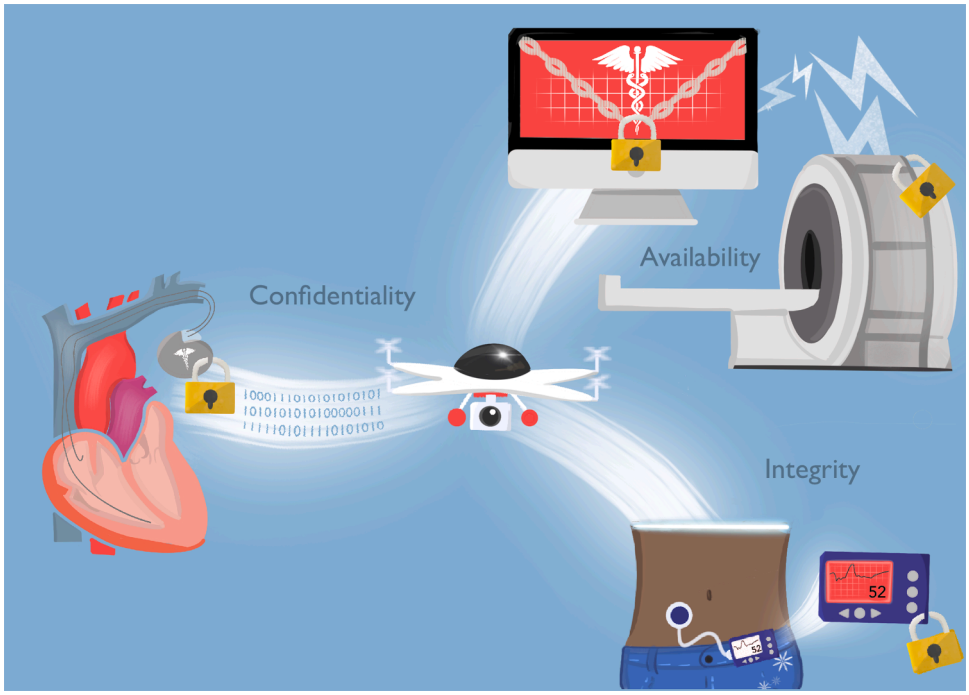

Fig. 2. Novel Attack Vectors in an Internet of Things world. The figure illustrates the three principles of the CIA security triad with an IoT device, in this case a drone, as the attack vector. (Left) Information is being siphoned from a pacemaker, which represents breach of confidentiality. (Bottom right) Integrity is represented by an unauthorized reprogramming into an insulin pump. (Top right) Lastly, the drone executes a DoS attack on an MRI machine, which renders it unable to be used.

radius restricted to the Bluetooth range [21]. Healthcare IoT devices potentially impacted ranged from wearables like fitness bands and hearing aids to Smart therapeutics like pacemakers and inhalers [21]. Of note, while most DoS attacks cause temporary service outages – as is the case for SweynTooth – other incidents have demonstrated that it is also possible to "brick" or permanently (PDoS) disable IoT devices [15,22].

The above examples can be linked to direct consequences for patient safety, but DoS attacks are also known to cause disruptions in workflow. This can manifest as delays in care or financial damages, which place a strain on the healthcare system [23,24]. Of particular concern here is the potential for a large-scale distributed denial of service (DDoS) attack exploiting the Internet of Medical Things. Take the "Mirai" DDoS campaign on the internet infrastructure company Dyn in 2016 as an example. The attack conscripted numerous household IoT that used default passwords into a "bot" army that was used to flood the Dyn network [25,26]. The cyber assault resulted in widespread service outages across many sites including Amazon, Netflix, Twitter, and Spotify, amongst others [26]. The responsible party later released the Mirai code as open-source on the web, spawning a number of successive iterations that continue to advance in terms of scope and complexity.

US regulation

The Food and Drug Administration (FDA) is the national gatekeeper of medical device cybersecurity in the US. In as early as 2005 and in keeping ahead of the issue, the FDA first broached the topic of medical device security. Their "Cybersecurity for Networked Medical Devices Containing Off-the-Shelf Software" took the form of a brief Q&A guidance [27]. Full pre and postmarket guidance documents for industry would later follow in 2014 and 2016, respectively [28,29]. The premarket guidance leverages the National Institute of Standards and Technology's (NIST) "Framework for Improving Critical Infrastructure Cybersecurity," to promote a "security by design" approach to device manufacturing [30]. The framework's deliberately broad focus prioritizes general security principles over adherence to rigid requirements in order to foster flexibility and innovation [30]. In September 2017 and in response to an industry-wide trend towards more complex device architectures, the FDA issued a "Design Considerations and Premarket Submission Recommendations for Interoperable Medical Devices". Manufactures were asked to document the intended purpose for device communications, additional anticipated users, authentication controls, and approved partner devices [31]. Finally, in an effort to promote transparency, the FDA releases public communications about device cyber vulnerabilities that, if acted on, could result in patient harm (see Table 2) [32]. The FDA has yet to receive any reports of patient harm associated with cyber vulnerabilities in medical devices [32,33].

Other landmark initiatives with a focus on Smart Security include the NIST's "Interagency Report on the Status of International Cybersecurity Standardization for the IoT", which was released November 2018. This document maps risks in the IoT threat landscape to relevant security guidance documents across all sectors, with the healthcare sector receiving the highest marks on the availability of core cybersecurity standards in network and physical security [34]. Key items on the exploratory agenda are blockchain for cryptography, handling of incidents not amenable to patching, spontaneous network connectivity management, and security automation [34]. The "IoT Device Cybersecurity Capability Core Baseline" was later released by the NIST in June 2019 as an agnostic and easily digestible guide for manufacturers that consolidates properties for minimally securing IoT devices . These core principles include device identification, authorized configuration, data protection, restricted access, software updates, and detection (See Fig. 3) [35]. Future oversight directions in the cyber realm at-large aim to bolster federal authority around IoT [36]. Indeed, the recent IoT Cybersecurity Improvement Act was signed into law on December 4, 2020 will require all government purchased devices to meet minimum cybersecurity standards to-be-defined by the NIST, raising the possibility of further modifications to existing FDA measures [36].

It should be noted that, while the aforementioned federal guidance documents serve as excellent conceptual frameworks, they do not map explicitly to existing manufacturing design processes. To better reflect standard industry practices, the private sector has also developed a number of consensus standards that offer more detailed language and

Table 2
US Food and Drug Administration Cybersecurity Safety Communications To Date *Note the changes in scope and device type over the years.

Year	Manufacturer	Device(s) Type	Scope	Vulnerabilities
2015	Hospira	Hospital drug infusion pump	–	Remote unauthorized user could remotely manipulate drug dosage
2017–18	Abbott (Formerly St. Jude Medical)	Implantable pacemaker	465,000 implanted devices in the US	Remote unauthorized user could reprogram the device to result in battery depletion or unsanctioned pacing/shocks
2018	Medtronic	Implantable pacemaker	–	Remote unauthorized user could attack during software updates if using internet connection to the software distribution network
2019	Medtronic	Implantable pacemaker and defibrillator	–	Unauthorized user could alter device settings when telemetry in use when within close-range
		Insulin pump	400,000 pumps in use	Unauthorized user could wirelessly manipulate insulin delivery when within close-range
2019	Multiple, Health Sector "Urgent/11″	Devices containing operating systems with IPnet software component	200 million+ devices and IoT	Remote unauthorized user, DoS, or information leak attacks
2020	GE Healthcare	Telemetry device for hospital monitoring of patient vital signs	- -	Remote unauthorized user could remotely silence, generate, or otherwise interfere with alarms
2020	Multiple, All Sectors "SweynTooth"	Devices with affected BLE system-on-a-chip sold by seven industry vendors	480+ product lines	Unauthorized user, DoS, or information leak attacks when within the BLE range

alignment. The most influential documents in this arena are arguably the Association for the Advancement of Medical Instrumentation (AAMI) TIR57 and UL 2900 series, both of which have been formally endorsed by the FDA. A strength of the AAMI TIR57 series lies in its comprehensive approach to risk management as it relates to the identification of device-specific threats and their preemptive evaluation, design controls, and longitudinal monitoring [37]. The UL 2900 series contains both pre and postmarket considerations but is widely recognized for the robustness of its testing and mitigation strategies that leverage the Common Vulnerability Scoring System (CVSS) for uniform indexing of incident severity [38].

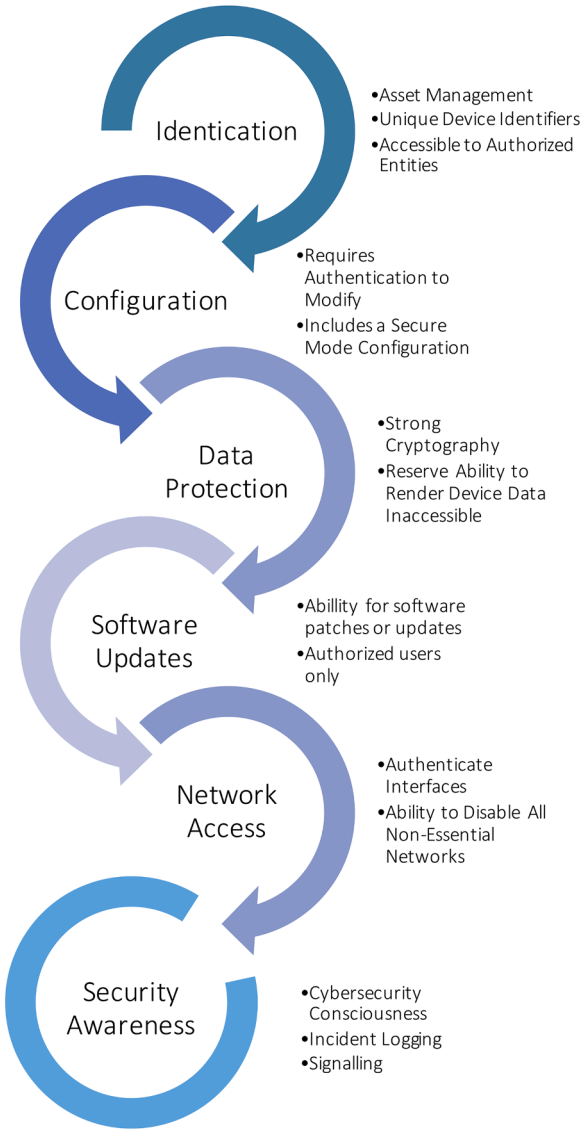

Fig. 3. US National Institute of Standards and Technology's IoT Device Cybersecurity Capability Core Baseline Principles.

International governance

The International Medical Device Regulators Forum (IMDRF) is a collective of global leaders from the public and private sector working to develop worldwide consensus standards. The IMDRF's new Cybersecurity Working Group, co-chaired by Canada and the US, first convened in the fall of 2019. Initial efforts culminated in the IMDRF's "Principles and Practices for Medical Device Cybersecurity" guidance document. With regards to premarket considerations, the IMDRF underscores the importance of comprehensive risk assessments and highlights traceability matrices that link each threat to its respective cybersecurity controls as a gold standard approach [11]. Another key premarket control noted by the IMDRF is robust security testing. These assessments should take into account any known vulnerabilities in any of the device components through targeted approaches and also attempt to identify potential unknown vulnerabilities in the device or its ecosystem, such as through penetration testing and variant analysis [11]. amongst postmarket items, there is a clear emphasis on international transparency and uniform indexing of cyber incidents [11]. Here the CVSS and "Computer Emergency Response Team Guide to Coordinated Vulnerability Disclosure" are noted as reference examples [11]. The group has

yet to delve into considerations for medical IoT specifically, but rather puts forth a broad principles for device security and coordination at-large [11].

Emergent threats

Artificial intelligence

The heterogeneity in IoT devices is conducive to a wide variety of takedown approaches. A human need not always be on the adversarial end. Increasingly sophisticated algorithms, bots, and drones are already capable of being used as attack vectors (see Fig. 2) [39–41]. Hackers can also leverage these technologies to enhance attack capabilities in terms of efficiency, accessibility, and scalability. Cyber weaponization of artificial intelligence could very well become a new norm. On the flip side, these features also have security tradeoffs [41,42]. Adaptive code relies heavily on incoming data. Therefore, a subtle adversarial attack into input data has the potential to alter algorithms in silence, leaving barely a trace. Furthermore, loss of static architecture relegates the traditional concept of "debugging" to a thing of the past [41]. Another security consideration surrounds the prospect of artificial intelligence algorithms as autonomously acting cyber-physical systems [43]. A classic example of this would be devices entrained by real-time visuo-spatial feedback, i.e.: surgical robot. This type of tech can be vulnerable to subtle physical manipulation of the device's visual field— such as by shining lasers – that can lead to decision making or classification errors [44,45]. While humans can typically catch these types of error, it may be difficult to pick up in physician out-of-the-loop devices [41,43]. Automated event monitoring with defence-AI may provide a solution to detection and possible countering of these breaches [46,47].

Cloud convergence

Next, we see that data as a commodity is a moving target [2]. While cyberattacks on device-held protected health information is still a major issue, hackers are diversifying their portfolios. Medical research, contractual agreements, non-health patient data, and enterprise information are now increasingly amongst the milieu of cyber targets [48]. The point to be made here is that compliance with privacy measures on health data alone cannot be conflated with adequate cybersecurity safeguards. Further, as consolidated computing platforms like the cloud manage more devices in order to build a Smarter world, this issue is likely to compound. Harmonization of device and cloud security is needed to ensure continued data protection. For example, while less robust security requirements for IoT may be acceptable in certain low-risk settings, they can create a backdoor for hackers if they share real estate with medical devices in the cloud. Appraising, restricting, and pruning cloud architectures so that they interact with only trusted interfaces can mitigate some of these risks. Similarly, data should be encrypted whenever possible with regular auditing to ensure non-repudiation.

Another space warranting attention is the area between the device and the cloud, known as a the edge. Edge computing refer to micro data centers where device data is locally processed, often prior to being routed to the cloud. This practice is gaining traction in the IoT sphere for its ability to reduce device latency and superfluous data transmission [49]. In terms of security implications, edge computing can be beneficial by reducing the total amount of data in-transit and by spreading risk across a number of distributed nodes, rather than centralizing it in the cloud. At the same time, this also has the untoward effect of increasing the overall surface area for attack. Avoiding persistent node-to-network connectivity by enabling a secure configuration for use during computing downtimes can bolster security. Direct edge-to-cloud communications should also generally be avoided or require authentication for necessary operations. Finally, dedicated, secure networks should be used for edge computing in mission critical IoT systems in lieu of more vulnerable public or virtual private networks.

Retrofitting

Recent advancements in IoT add another wrinkle of complexity to the ongoing practice of device stacking. Upcycling with IoT is an attractive option for vendors and end users because it can allow for improved device functionality that might otherwise be cost-prohibitive. However, weak security in newer IoT – quite conceivable given trends towards bare bones IoT with low computing power that can be quickly rushed to market– can introduce a conduit for attack. Conversely, simply retrofitting IoT to existing environments can propagate flaws in outdated technology to newer devices. This type of security pitfall was exemplified in the recent "Urgent/11" vulnerabilities in an old operating system that was carried forward and embedded into hundreds of millions of US-manufactured medical devices [50]. This flaw could have been exploited to enable mass takedown of devices that ran this common operating system, which ranged anywhere from infusions pumps to patient telemetry monitors. Large scale cybersecurity incidents like "Urgent/11" are likely to occur with greater frequency owing to trends towards increased IoT interconnectivity, use of common off-the-shelf items, and protracted utilization of outdated "legacy" technologies (see Table 2). Mandating adherence to supported device lifetimes, implementing pre-procurement security requirements for vendors, and conducting integrated and individual hazards assessments for device components may also help to mitigate poor retrofitting practices. Finally, increased government regulation over the cost of medical technology might be another strategy to curb the financial lock-in that promotes patchwork updates and IoT stacking in lieu of comprehensive upgrades.

Quantum computing

Quantum computing capable of producing a real-world threat to security could arrive as early as the next one to two decades [51,52]. An operational platform of this class can boast enhanced power and functionality by leveraging quantum mechanics to process data in parallel states. Quantum development is relevant to our discussion of security in the IoMT as these technologies have the potential to render many existing cryptosystems and their respective security safeguards obsolete (i.e: public key encryption, blockchain, etc.). An anticipated quandary lie in the fact that many encryption codes are based on the premise that the computational bandwidth needed to crack the cypher will be overly burdensome for the conventional computer to perform. Quantum computers would be able to overwhelm these hardened computations with their increased processing capabilities. While many conventional encryption algorithms would be irretrievably compromised, others could be made quantum-resistant. This "post-quantum" crytptography is an area of emerging research with prospective mitigations including modification of key size and parameters or via the use of redundant ciphers [53]. In the near-term, manufacturers should conduct hazards assessments around the quantum resilience of their technologies in order to manage their postmarket assets and to guide their subsequent development priorities. In the longer-term, a complete paradigm shift towards quantum-safe cryptography may be indicated to ensure continued health security [53]. Given that experts find that the "phasing out of an endangered encryption algorithm can take a decade or more", transition planning for mission critical IoMT technologies should begin now [53]. On the other hand, a definitive solution for quantum defence may be baked into the problem itself. Indeed, the prospect of quantum encryption also looms on the horizon, which would be able to yield a theoretically uncrackable cypher by leveraging the entanglement properties of quantum mechanics.

Empowering end users

One of the most impactful ways for end users and allied healthcare personnel to assist with cyber defence is through timely activation of the event reporting cascade. Swift identification of potential cyber breaches is essential to minimizing patient harm, streamlining threat mitigation, and preventing viral propagation to other devices. Institution event reporting pipelines and ad hoc response protocols for medical providers should be introduced during the onboarding process and reviewed on an regular basis. Such entities might include the IT department, relevant manufacturing personnel, and hospital incident management team who can subsequently activate the appropriate upstream channels [54]. Independent practitioners and patients often also have a direct line to central oversight though the US FDA's MedWatch reporting channel, which can be used to track nationwide trends in aberrant medical device behaviour [55]. Healthcare personnel, incident command officials, industry liaisons, emergency responders, and other relevant stakeholders should also participate in trainings intent on promoting cyberattack awareness and preparedness [56]. Such drills need consider activations in the field, inpatient, and outpatient settings and should be tailored to the institution's IoT inventory and local patient population. Examples might include a mass casualty incident resulting from a disseminated attack on IoMT in the community or a hijacked surgical robot, to name a few.

Healthcare professionals and allied personnel should also strive to foster an ethos of safety around medical device cybersecurity in their routine patient encounters. Medical providers or technicians who are co-managing devices with patients should set aside time during the initial or pre-implantation visit to establish a cyber safety plan in the event that the device malfunctions. Ensuring patient compliance with recommended operating systems and cybersecurity updates or patches is similarly vital. As health and technology literacy amongst patients cannot be assumed, healthcare workers and affiliated personnel will serve as critical knowledge translators for patients when cybersecurity vulnerabilities do arise. In this way, it is important for providers to maintain a working knowledge of next steps for technical mitigations, potential health implications, and emergency protocols in the event of a cyber emergency. Development of educational materials around personal IoT security promotion at the local or federal level can also serve as a preemptive mitigation strategy, such as is routinely done for other public health crises like drug addiction, gun violence, or COVID-19. These materials might include good personal security hygiene practices like safeguarding of device identifiers and password information, changing of default passwords, turning off of Bluetooth when IoT is not in use, and auditing of IoT on personal networks, to name a few (see Table 3). Indeed, we call for an adaption and synthesis of the health systems and cybersecurity literature to address emergent concerns in the increasingly ubiquitous IoMT technologies.

Table 3
Internet of Medical Things Threat Landscape.

Threat	Probable Mechanism	Primary Mitigations
Autonomous AI	A closed-loop system would be particularly vulnerable attacks that poison data or distort the visuospatial workspace, both of which can modify device outputs.	Systems: Conduct preemptive hazards and cost/benefit analyses prior to deployment to determine suitability and possible indications for supervision. Perform automated auditing, intrusion detection, and countering with defence AI. Equip IoT with emergency shutdown and manual override capabilities. End user: Conduct emergency simulations for high-risk scenarios (i.e.: surgical robots, ventilator).
Bluetooth/ Bluetooth Low Energy	An attack would most likely target the implementation of the protocol stack used in pairing devices.	Systems: Implement authentication controls to limit spontaneous connectivity. Use strong cryptography to secure communications. End user: Users should turn off Bluetooth when not in use to avoid spontaneous connectivity. Keep relevant IoT software up-to-date.
Cloud Convergence	An attack exploiting weak security in IoT as conduit to attack the cloud.	Systems: Maintain cloud security updates, authenticate communications, regularly audit assets, use isolated networks for mission critical operations, implement intrusion detection, and encrypt data and backups. End User: Protect account passwords.
Edge Computing	Distributed processing can increase the potential surface area for attack, with the edge-to-cloud interface particularly at risk.	Systems: Avoiding persistent node-to-network connectivity. Initiate direct edge-to-cloud communications only when absolutely necessary with authentication. Use dedicated, secure networks for mission critical IoMT systems.
IoT heterogeneity and ubiquity	The increasing diversity of the IoT introduces the possibility of new attackers and prey.	Systems: Extrapolate a wide range of scenarios during threat modelling. Implement user contracts for IoT to connect to networks in high-risk grids (i.e.: Smart Hospital) that can allow for ease of identification, asset management, and monitoring. End User: Survey IoT connected to personal networks for any unsanctioned devices.
Off-the-Shelf (OTS) Components	Widespread utilization of OTS components in IoT creates an optimal target for attackers.	Systems: Implement pre-procurement OTS security requirements for vendors. Perform integrated and individual security assessments for components.
Physical Environment	An attacker can exploit the device via direct access to IoT in public areas via theft of concealable IoT.	Systems: Equip all IoT with unique identifiers and tracking/guarding for those that are high-risk. Account for all IoT assets, particularly those in publicly accessible grids that share networks with institution assets (i.e.: fish tank heist). Isolate mission critical systems on dedicated,

(*continued on next page*)

Conclusion

Smart devices that leverage networks can achieve enhanced control over human physiology, giving a whole new meaning to the term precision medicine. Digital health nudges us closer to our goal of developing a learning healthcare system, but it also leaves patients increasingly susceptible to vulnerabilities in their device counterparts. This precarious alignment of motivation, means, and opportunity creates a perfect storm for the hacking of the IoMT. In this new climate, medicine would do well to keep cyberattack on its radar. Recognizing this clear and present danger, a number of public and private actors are engaged in cyber regulation intent on promoting safety without stifling innovation. Moving forward, unwavering vigilance and continued reworking of existing cybersecurity strategy is needed to keep pace with new attack vectors and prey in this emergent space.

Table 3 (*continued*)

Threat	Probable Mechanism	Primary Mitigations
		secure networks. End user: Enable tracking on devices where applicable and report lost or stolen devices.
Retrofitting	Vulnerability in an outdated device with serve as a point of compromise of the larger IoT grid.	Systems: Federal authorities can mandate adherence to supported device lifetimes, regulate the cost of medical technologies to alleviate financial lock. Institutions can conduct hazards analysis on legacy technologies and prune system architectures accordingly. End User: Survey IoT connected to personal networks for updates and consider removing devices no longer supporting updates (i.e.: old webcams and routers).
Quantum Computing	Computing capabilities would render many existing cryptosystems obsolete.	Systems: Viable encryption algorithms can often be made quantum-resistant by increasing key size or parameters. Consider transitioning existing mission critical technology to quantum-safe encryption in the near-term. Explore the development of quantum encryption as a potential definitive solution.

Ethical approval

Not required

Funding/support

None.

Competing Interests

Ms. Thomasian declares no conflict of interest. Professor Adashi serves as Co-Chair of the Safety Advisory Board of Ohana Biosciences, Inc.

References

[1] FDA informs patients. Providers and manufacturers about potential cybersecurity vulnerabilities for connected medical devices and health care networks that use certain communication software [press release]. MD: Silver Spring,; 1 October 2019.

[2] Cohen IG, Hoffman S, Adashi EY. Your Money or Your Patient's Life? Ransomware and electronic health records. Ann Intern Med 2017;167(8):587–8.

[3] European Union Agency for Cybersecurity (ENISA). Baseline security recommendations for iot. enisaHeraklion, Greece; 2017.

[4] Alsubaei F, Abuhussein A, Shiva S. Security and Privacy in the Internet of Medical Things: taxonomy and Risk Assessment. In: 2017 IEEE 42nd Conference on Local Computer Networks Workshops (LCN Workshops). IEEE; 2017.

[5] Dimitrov DV. Medical Internet of Things and big data in healthcare. Healthc Inform Res 2016;22(3):156–63.

[6] Ching K, Mahinderjit Singh M. Wearable Technology Devices Security and Privacy Vulnerability Analysis. Int J Netw Sec Appl 2016;8:19–30.

[7] Radcliffe J. Hacking medical devices for fun and insulin: breaking the human SCADA system. In: Black Hat Conference presentation slides; 2011.

[8] Mohzary M, Tadisetty S, Ghazinour K. A Privacy Protection Layer for Wearable Devices. In: International Symposium on Foundations and Practice of Security. Springer; 2019.

[9] Pelton JN, Singh IB. Challenges and opportunities in the evolution of the internet of everything. Smart cities of today and tomorrow. Springer; 2019. p. 159–69.

[10] Stremlau T. The financial motivation to keep information secure. Comput Fraud Sec 2020;2020(2):18–9.

[11] Medical device cybersecurity working group. principles and practices for medical device cybersecurity. International Medical Device Regulators Forum; October 1 2019.

[12] Qusa H, Allam H, Younus F, Ali M, Ahmad S. Secure smart home using open security intelligence systems. In: 2019 Sixth HCT Information Technology Trends (ITT). IEEE; 2019.

[13] Martin G, Martin P, Hankin C, Darzi A, Kinross J. Cybersecurity and healthcare: how safe are we? BMJ 2017;358:j3179.

[14] Ghafur S, Kristensen S, Honeyford K, Martin G, Darzi A, Aylin P. A retrospective impact analysis of the WannaCry cyberattack on the NHS. NPJ Dig Med 2019;2(1):98.

[15] Kolias C, Kambourakis G, Stavrou A, Voas J. DDoS in the IoT: mirai and other botnets. Computer (Long Beach Calif) 2017;50(7):80–4.

[16] MacDermott Á, Kendrick P, Idowu I, Ashall M, Shi Q. Securing things in the healthcare internet of things. In: 2019 Global IoT Summit (GIoTS). IEEE; 2019.

[17] Halperin D, Heydt-Benjamin TS, Ransford B, Clark SS, Defend B, Morgan W, et al. Pacemakers and implantable cardiac defibrillators: software radio attacks and zero-power defenses. In: 2008 IEEE Symposium on Security and Privacy. IEEE; 2008.

[18] Thomson I. Wi-Fi baby heart monitor may have the worst IoT security of 2016; October 13, 2016 [Available from: https://www.theregister.com/2016/10/13/possibly_worst_iot_security_failure_yet/?mt=1476453928163.

[19] Maggi F, Quarta D, Pogliani M, Polino M, Zanchettin AM, Zanero S. Rogue robots: testing the limits of an industrial robot's security. trend micro. Politecnico di Milano; 2017. Tech Rep.

[20] Hei X, Du X, Wu J, Hu F. Defending resource depletion attacks on implantable medical devices. In: 2010 IEEE Global Telecommunications Conference GLOBECOM. 2010. IEEE; 2010.

[21] Matheus E. Garbelini S.C., Chundong Wang. SweynTooth: Unleashing Mayhem over Bluetooth Low Energy: Singapore University of Technology and Design; [Available from: https://asset-group.github.io/disclosures/sweyntooth/sweyntooth.pdf.

[22] United States Computer Emergency Response Team (US-CERT). BrickerBot Permanent Denial-of-Service Attack; April 12, 2017 [Available from: https://us-cert.cisa.gov/ics/alerts/ICS-ALERT-17-102-01A.

[23] Martin G, Ghafur S, Kinross J, Hankin C, Darzi A. WannaCry—A year on. BMJ 2018;361:k2381.

[24] Tully J, Selzer J, Phillips JP, O'Connor P, Dameff C. Healthcare challenges in the era of cybersecurity. Health Sec. 2020;18(3):228–31.

[25] Newman L.H. What We Know About Friday's Massive East Coast Internet Outage: Wired; October 21, 2016 [Available from: https://www.wired.com/2016/10/internet-outage-ddos-dns-dyn/.

[26] D. FitzGerald and R. McMillan. Cyberattack Knocks Out Access to Websites: Wall Street Journal; October 24, 2016 [Available from: https://www.wsj.com/articles/denial-of-service-web-attack-affects-amazon-twitter-others-1477056080.

[27] US Food & Drug Administration. Cybersecurity for networked medical devices containing off-the-shelf (OTS) software. MD: Silver Spring; 2005.

[28] US Food & Drug Administration. Content of premarket submissions for management of cybersecurity in medical devices. Guidance for Industry and Food and Drug. Administration Staff; 2014.

[29] US Food & Drug Administration. Postmarket management of cybersecurity in medical devices. Guidance for Industry and Food and Drug Administration Staff; 2016.

[30] National Institute of Standards and Technology. Framework for improving critical infrastructure. Cybersecurity 2014.

[31] US Food & Drug Administration. Design considerations and premarket submission recommendations for interoperable medical devices. MD: Guidance for Industry and Food and Drug Administration Staff Silver Spring; 2017.

[32] US Food & Drug Administration. Cybersecurity [Available from: https://www.fda.gov/medical-devices/digital-health/cybersecurity].

[33] Us Food & Drug Administration. FDA informs health care providers. facilities and patients about potential cybersecurity vulnerabilities for certain GE Healthcare Clinical Information Central Stations and Telemetry Servers; January 23, 2020 [Available from, https://www.fda.gov/news-events/press-announcements/fda-informs-health-care-providers-facilities-and-patients-about-potential-cybersecurity.

[34] Interagency International Cybersecurity Standardization Working Group. Interagency report on status of international cybersecurity standardization for the internet of things (IoT). National Institute of Standards and Technology; 2018.

[35] Fagan M, Megas KN, Scarfone K, Smith M. IoT Device Cybersecurity Capability Core Baseline. Nat Inst Stand Technol 2020:S. 734.

[36] TIR57 A. Principles for medical device security—Risk management. Arlington, VA: Association for the Advancement of Medical Instrumentation; 2016.

[37] UL. UL 2900. Standard for Software Cybersecurity for Network-Connectable Products; September 01, 2017.

[38] Greenberg A. Watch a drone take over a nearby smart tv. Wired; 11 August 2019 [Available from: https://www.wired.com/story/smart-tv-drone-hack/].

[39] Nassi B, Shamir A, Elovici Y. Xerox Day Vulnerability. IEEE Trans Inf Forensics Sec 2018;14(2):415–30.

[40] Brundage M, Avin S, Clark J, Toner H, Eckersley P, Garfinkel B, et al. The malicious use of artificial intelligence: forecasting. Prevention, and Mitigation; February 2018.

[41] Jang-Jaccard J, Nepal S. A survey of emerging threats in cybersecurity. J Comput Syst Sci 2014;80(5):973–93.

[42] Schneier B. Click here to kill everybody: security and survival in a hyper-connected world. WW Norton & Company; 2018.

[43] Comiter M. Attacking artificial intelligence: ai's security vulnerability and what policymakers can do about it 2019.

[44] National Protection and Programs Directorate Office of Cyber and Infrastructure Analysis. The future of smart cities: cyber-physical infrastructure risk. US Department of Homeland Security; August 2015.
[45] Babic B, Gerke S, Evgeniou T, Cohen IG. Algorithms on regulatory lockdown in medicine. Science 2019;366(6470):1202–4.
[46] Ten C-W, Hong J, Liu C-C. Anomaly detection for cybersecurity of the substations. IEEE Trans Smart Grid 2011;2(4):865–73.
[47] National Institute of Standards and Technology. Considerations for managing internet of things (IoT) cybersecurity and privacy risks. Gaithersburg, MD; June 2019.
[48] D.R. Jg, J. Rydning. The Digitization of the World: From Edge to Core Framingham, MA; November 2018 [Available from: https://www.seagate.com/files/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf.
[49] US Food & Drug Administration. URGENT/11 cybersecurity vulnerabilities in a widely-used third-party software component may introduce risks during use of certain medical devices. FDA Safety Communication; 1 October 2019 [Available from, https://www.fda.gov/medical-devices/safety-communications/2019-safety-communications.
[50] Arute F, Arya K, Babbush R, Bacon D, Bardin JC, Barends R, et al. Quantum supremacy using a programmable superconducting processor. Nature 2019;574(7779):505–10.
[51] National Institute of Standards and Technology. Post-Quantum Cryptography; January 03, 2017 [Available from: https://csrc.nist.gov/projects/post-quantum-cryptography.
[52] Princeton University Center for Information Technology Policy. Implications of quantum computing for encryption policy. Washington, DC: Carnegie Encryption Working Group; April 2019.
[53] Medical Device Innovation Consortium. Medical device cybersecurity report. Advancing Coordinated Vulnerability Disclosure; 2018.
[54] US Food & Drug Administration. MedWatch Online Voluntary Reporting Form [Available from: https://www.accessdata.fda.gov/scripts/medwatch/index.cfm?action=reporting.home.
[55] Dameff CJ, Selzer JA, Fisher J, Killeen JP, Tully JL. Clinical cybersecurity training through novel high-fidelity simulations. J Emerg Med 2019;56(2):233–8.