SAVANNAH LAW REVIEW

VOLUME 5 | NUMBER 1

DEUS EX MACHINA: REGULATING CYBERSECURITY AND ARTIFICIAL INTELLIGENCE FOR PATIENTS OF THE FUTURE

Charlotte A. Tschider[·]

"You asked the impossible of a machine and the machine complied."[1]

Introduction

Translated as "god from a machine," the *deus ex machina* mechanically suspended Greek gods above a theatre stage to resolve plot issues by divine intervention.[2] The implement's name has since extended to the rapidly expanding Artificial Intelligence (AI) field, as AI has similarly promised miraculous resolution to any number of human challenges, including chronic health conditions.

Modern medical devices and other health applications use AI to automate computer functionality, including Internet-connected medical devices, ubiquitous mobile device use, and individual self-monitoring consumer health devices.[3] Unlike human algorithmic programming of the past, AI enables more powerful

[·] Charlotte A. Tschider is the Lead Affiliated Professor for the Mitchell Hamline School of Law's Cybersecurity and Privacy Law Program and Owner/Principal for Cybersimple Security, an international cybersecurity and privacy law consulting firm. I would like to thank the excellent *Savannah Law Review* editors and the annual *Savannah Law Review* Colloquium participants and presenters for their thoughtful questions and suggestions on this topic.

[1] KURT VONNEGUT, THE SIRENS OF TITAN 306 (2007).

[2] *See* Elias Karayannakos, *Deus ex Machina*, GREEK THEATRE WEBSITE (2015), http://www.greektheatre.gr/on-stage/deus-ex-machina/; Anthony Cohn, *Deus ex Machina*, 109 J. ROYAL SOC'Y MED. 284 (2016).

[3] Over one hundred Artificial Intelligence (AI) startups are currently in the healthcare sector, illustrating a movement towards heavy AI use in this sector, not including big name medical device AI investments. *From Virtual Nurses To Drug Discovery: 106 Artificial Intelligence Startups In Healthcare*, CB INSIGHTS (Feb. 3, 2017), https://www.cbinsights.com/research/artificial-intelligence-startups-healthcare/.

and automated dynamic algorithmic calculation, or automation, which surpass human data science in accuracy.[4]

AI has the potential to revolutionize modern medicine, yet exceptionally large data volumes coupled with automated functionality and Internet connectivity will likely introduce previously unanticipated device safety issues. [5] Although businesses increasingly integrate AI services into medical devices worldwide, the United States and the European Union, typically global leaders in regulating health and medical device technology, have not established legal frameworks to adequately address big data, cybersecurity, and AI risks.[6] With new technology, the principles informing medical device risk management activities no longer effectively manage patient safety risks.[7]

Neither the U.S. nor the E.U. has effectively developed a standardized approach to regulating AI in traditional medical devices, and consumer health devices receive considerably less attention.[8] Wearables and other medical devices produced by general product manufacturers and mobile application ('app') developers have become tremendously popular; yet, no regulatory body has established predictable standards-based regulatory requirements for these devices.[9] Once a tightly regulated field with limited competition and substantial barriers to entry, any start-up may now develop these devices, which health care providers increasingly use for medical purposes.[10]

In Part I, the Author will explain the technology of medical device AI and specific areas of concern for patient safety: big data, cybersecurity, and artificial intelligence engineering. [11] In Part II, U.S. and E.U. medical device legal frameworks and associated risk management principles will be evaluated for

---

[4] *See* Michael Wu, *Artificial Intelligence Is the New Business Intelligence*, CMS WIRE (Aug. 10, 2017), https://www.cmswire.com/information-management/artificial-intelligence-is-the-new-business-intelligence/.

[5] *See* Robert Hart, *When Artificial Intelligence Botches Your Medical Diagnosis, Who's to Blame?*, QUARTZ (May 23, 2017), https://qz.com/989137/when-a-robot-ai-doctor-misdiagnoses-you-whos-to-blame/. Although AI should dramatically reduce safety issues in theory, if the "opacity of AI" makes it difficult for humans to understand how systems function, preventing humans from reviewing AI decisions.

[6] *See infra* Part III and accompanying notes.

[7] *See infra* Part II(C) and accompanying notes.

[8] *See infra* Part II(A) and (B) and accompanying notes.

[9] *Id.*

[10] Steve Blank, *Reinventing Life Science Startups: Medical Devices and Digital Health*, FORBES (Aug. 19, 2013), https://www.forbes.com/sites/steveblank/2013/08/19/reinventing-life-science-startups-medical-devices-and-digital-health/#ccda13c6ac64. Many startups come from technology backgrounds with less experience in healthcare.

[11] This article attempts to respond, at least in part, to further exploration of cybersecurity considerations and more detailed understanding of machine learning algorithm design and its impact on FDA regulation. *See* W. Nicholson Price II [hereinafter Price 2], *Regulating Black-Box Medicine*, 116 MICH. L. REV. 421 (2017); Roger Allan Ford & W. Nicholson Price II [hereinafter Ford & Price], *Privacy and Accountability in Black-Box Medicine*, 23 MICH. TELECOMM. & TECH. L. REV. 1 (2016) (both articles calling for further exploration on topics of cybersecurity and fully opaque algorithms in machine learning).

effectiveness for devices using new technologies. Part III will propose key areas of focus for the medical device legal frameworks to establish an "AI-safe" health device regulatory approach.[12]

I: Medical Devices, Artificial Intelligence Technologies, and Cyber Attacks

Modern software-based medical devices increasingly require additional technologies to create innovative and market-leading solutions to improve patient health outcomes. Big data, distributed cloud computing, and mobile devices have revolutionized technology, making AI not only possible, but probable.[13] Although AI has the potential to improve overall health outcomes, it may also introduce additional threat vectors that could compromise patient safety without appropriate cybersecurity measures.[14]

Cybersecurity safety concerns stem from Internet connectivity, where such connectivity could compromise data confidentiality, availability, integrity, and ultimately patient safety.[15] AI amplifies existing cybersecurity issues because it necessitates ubiquitous data collection, involves reinforced or codified algorithmic calculation, and automates decision-making.[16]

A. IoT Devices and Associated System Architectures

Prior to 2007, when the iPhone transformed the use of Internet-connected mobile services, the first medical devices functioned as largely stand-alone machines.[17] Engineers designed these devices to run for specific durations after

---

[12] It is duly acknowledged that self-regulation, marking/labeling, or independent verification could present unique solutions to this challenge. However, the U.S. and E.U. have not pursued medical device co-regulation schemes historically. Therefore, the Author does not present these solutions. *See* Katherine Wellington, *Cyberattacks on Medical Devices and Hospital Networks: Legal Gaps and Regulatory Solutions*, 30 SANTA CLARA HIGH TECH. L.J. 139, 188–90 (2014); Michael Woods, *Cardiac Defibrillators Need to Have a Bulletproof Vest*, 41 NOVA L. REV. 419, 441–43, 444 (noting potential third-party testing, national data sharing solutions, and external industry standards); H. Michael O'Brien, *The Internet of Things*, 19 J. INTERNET L., no.12, 2016, at 1, 19. The Online Trust Alliance (OTA) created the Internet of Things Trustworthy Working Group that has developed a framework for home automation and wearable technologies.

[13] Giulio Coraggio, *Are You Ready for Artificial Intelligence?*, TECH. L. EDGE (Feb. 2, 2017), https://www.technologyslegaledge.com/2017/02/are-you-ready-for-artificial-intelligence/ (quoting Ginny Rosmetty, Chairman and CEO of IBM).

[14] Roman V. Yampolskiy, *AI Is the Future of Cybersecurity, for Better and for Worse*, HARV. BUS. REV. (May 8, 2017), https://hbr.org/2017/05/ai-is-the-future-of-cybersecurity-for-better-and-for-worse (discussing the role of AI in perpetuating cyberattacks and guarding against such attacks). AI capabilities could be attacked via AI cyberattacks or by human cyberattackers.

[15] *See* James Scott & Drew Spaniel, *Assessing the FDA's Cybersecurity Guidelines for Medical Device Manufacturers*, INST. CRITICAL INFRASTRUCTURE TECH. 2, 4 (2016), http://icitech.org/wp-content/uploads/2016/02/ICIT-Blog-FDA-Cyber-Security-Guidelines2.pdf.

[16] *See infra* Part I and accompanying notes.

[17] *See* John G. Browning & Shawn Tuma, *If Your Heart Skips a Beat, It May Have Been Hacked: Cybersecurity Concerns with Implanted Medical Devices*, 67 S.C. L. REV. 637, 641–46 (2016).

which time patients or health care providers (HCP) returned the devices to the manufacturer or medical doctors for updates or replacement.[18] This involved purchasing new diagnostic tools for the hospital and replacing implantable devices in surgery. As of 2010, an estimated 2.6 million people had implanted medical devices alone, an industry value of at least $52 billion.[19]

Devices may have software and storage on the device, or devices may rely on Internet connectivity for some features. Modern devices have many of the same standalone features that enable a device to work effectively when disconnected from an Internet connection or mobile device, yet features may also update software on-demand when connected to the Internet.[20] Pervasive connectivity facilitates data aggregation across devices and enables a device to receive new instructions or information based on insights from data analyses occurring outside of the device, while still maintaining critical functions (e.g. a pacemaker does not stop working when disconnected from a hospital or home network).[21]

Due to integrations with hospital networks, patient mobile devices, and web applications that provide real-time data to providers, modern medical devices and other health devices introduce more complexity to backend systems while, in some cases, simplifying the device itself. The "medical device" or "health device" does not just include the physical hardware interfacing with the human body.[22] Instead, devices today have become Internet of Things (IoT) devices, or devices designed to pervasively connect to the Internet, whether through a hospital network, outpatient networks, or a mobile data connection.[23] Due to their connected status, IoT devices are vulnerable to cyberattack.[24]

Connectivity, or the ability to transmit data outside of a device, is a common attribute of modern medical devices.[25] Medical devices generate a tremendous volume of useful data, which can improve device responsiveness and capabilities while simultaneously creating tremendously useful health data, such as effects of multi-device implantation, recovery time, or unanticipated side effects, that might not be observable during testing or clinical trials. Connectivity also reduces data storage needs, as devices may store large data sets within a database outside the device, reducing hardware costs and device size or weight and creating new device

---

[18] *See* 21 C.F.R. § 806 (2017) (establishing reporting procedures for device removal prior to end-of-life); *Easing the Medical Device Life Cycle with Virtual Instrumentation*, NAT'L INSTRUMENTS [hereinafter NAT'L INSTRUMENTS] (Feb. 24, 2014), http://www.ni.com/white-paper/5711/en/ (describing the historically relevant medical device lifecycle, including 'obsolescence').

[19] *See* Browning & Tuma, *supra* note 17, at 641–42.

[20] Univ. of the Basque Country, *Pacemakers With Internet connection, a Not-So-Distant Goal*, SCIENCEDAILY (Jan. 28, 2015), https://www.sciencedaily.com/releases/2015/01/150128113715.htm (reporting on new security protocols to protect Internet-connected pacemakers).

[21] *Id.*

[22] *See* O'Brien, *supra* note 12, at 1, 12; Browning & Tuma, *supra* note 17, at 643.

[23] O'Brien, *supra* note 12.

[24] *Id.*

[25] U.S. FOOD & DRUG ADMIN: DIGITAL HEALTH (Sept. 6, 2017), https://www.fda.gov/MedicalDevices/DigitalHealth/default.htm.

applications and functionality.[26] Reduced device size will support new size-constrained applications capable of performing previously unimaginable tasks: mapping of human internal systems, stimulating healing and repairing tissues, or providing camera images.[27]

IoT devices include not only the hardware itself, but associated mobile apps, Web applications to review data, and backend servers, databases, and utilities.[28] These devices have developed precisely due to low-cost sensors, mobile device use, and wireless Internet access.[29] The "medical device" now includes substantially more systems and components that ever before, including the physical device with sensors, actuators, housing; a hub, gateway, or mobile device where data are transmitted; and data storage and tool processing systems, often residing in third-party cloud storage.[30]

IoT device manufacturers create hardware capable of remote system updates to improve device functionality, fix software bugs, or upgrade systems. Manufacturers also create devices with less in-device storage because IoT devices routinely transfer and receive data feeds from remote systems.[31] The benefit of such remote systems lies in the ability to leverage live, real-time data from devices across a human population, rather than relying on only clinical data or anticipated device functionality in the engineering process.[32] Remote data feeds, to work effectively, usually require very large data sets, or big data, stored in remote databases to reliably provide insights to IoT devices.[33]

Manufacturers leverage utilities on backend data sets to effectively process, interpret, and organize data for use within medical devices. These utilities may include algorithms created by data scientists to decipher data trends and provide specific instructions or changes to medical devices. In more advanced implementations, these utilities may include supervised or unsupervised AI utilities.[34]

Backend servers often provide different functionality, such as Web or mobile app services or database storage, depending on the server type. Web or mobile app service servers provide functionality for Web applications, such as running a Web application that enables a physician to view historical device activity for all

---

[26] Waqaas Al-Siddiq, *The Impact of Artificial Intelligence on Medtech*, MED. PROD. OUTSOURCING (Apr. 7, 2017), https://www.mpo-mag.com/contents/view_online-exclusives/2017-04-07/the-impact-of-artificial-intelligence-on-medtech/.

[27] *Id.*

[28] *See* O'Brien, *supra* note 12.

[29] *Id.*

[30] Swaroop Poudel, *Internet of Things: Underlying Technologies, Interoperability, and Threats to Privacy and Security*, 31 BERKELEY TECH. L.J. 997, 1002 (2016).

[31] DANIEL KELLMEREIT & DANIEL OBODOVSKI, THE SILENT INTELLIGENCE: THE INTERNET OF THINGS 11 (2013) (statement of Assaf Biderman) ("Computers are becoming so small they are vanishing into things. It's not machine-to-machine, it's thing-to-thing.").

[32] *See, e.g.*, *Medical Device Connectivity: Remote Patient Monitoring*, LANTRONIX (2018), https://www.lantronix.com/solutions/healthcare/.

[33] *Id.* at 1005–06.

[34] *See infra* Part I (B).

patients from the physican's laptop computer. Mobile app services might also transmit data from these servers to a caregiver's mobile device so a caregiver can adjust treatment for a patient.[35]

Cyberattack threat models consider three functions with respect to technology architecture: data storage, data transmission, and third-party risk models.[36] Architectures involve the device itself, connectivity to internal Intranet or the public-facing Internet, and data storage/analytics on which AI-enabled services may run.[37] Although device architectures vary tremendously depending on the system architecture and device hardware, of these functions, architectures passing information over the open Internet (transmission) poses the greatest direct cybersecurity risk to patients.[38]

Devices that transmit information over the open Internet include a device that connects with the human body temporarily or permanently and a wired or wireless connection between the device and the Internet via a wireless or wired network (usually a home network).[39] Whether the device provides sensor technologies for remote monitoring of a patient or more biologically invasive, implanted devices, the device's ability to transmit and receive information is often dependent on a home wireless network.[40] Most devices designed for home use store information on a device during service interruption. Some devices may connect to a mobile device that affords additional data storage and occasionally more reliable Internet connectivity.[41] In contrast, medical devices in a hospital setting typically connect to internal healthcare provider intranets through internal

---

[35] *See, e.g.*, PHILLIPS, *IntelliVue Mobile Caregiver* (2018), https://www.usa.philips.com/healthcare/product/HCNOCTN197/intellivue-mobile-caregiver-mobile-app-for-patient-monitoring-data (the IntelliVue product enables clinicians to review data on personal and hospital-issued devices to monitor patients remotely).

[36] *See* Cwalina et al., *Privacy and Security in Mobile Apps, the Cloud and the Internet of Things: The Role of In-House Counsel in Mitigating New Class Action and Regulatory Risks*, HOLLAND & KNIGHT (2013), https://www.hklaw.com/files/Publication/7a8a6d5a-6064-43e2-ae25-ad9f5a0c57c8/Presentation/PublicationAttachment/b67bcc84-4c8a-4115-a4e6-30b9d71470b1/MahonyEdits.pdf.

[37] *See* John A. Rothchild, *Net Gets Physical: What You Need to Know about the Internet of Things*, BUS. L. TODAY (2014), https://www.americanbar.org/publications/blt/2014/11/03_rothchild.html.

[38] *See* Shaun Sutner, *White House CIO warns health CIOs to beware the internet of things*, SEARCHHEALTHIT (Nov. 4, 2016), http://searchhealthit.techtarget.com/news/450402422/White-House-CIO-warns-health-CIOs-to-beware-the-internet-of-things (quoting Tony Scott's warning to closely investigate connectivity for devices due to the cybersecurity risk).

[39] Vijayakannan Sermakani, *Transforming Healthcare Through the Internet of Things*, Project Management Practitioners' Conference (Nov. 20, 2014), http://pmibangalorechapter.in/pmpc/2014/tech_papers/healthcare.pdf (slideshow).

[40] *See* Scott R. Peppet, *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent*, 93 TEX. L. REV. 85, 98–99 (2014). Professor Peppet identifies five types of health monitors: 1) countertop devices, 2) wearable sensors, 3) intimate contact sensors, 4) ingestible sensors, and 5) implantable sensors.

[41] *See* Al-Siddiq, *supra* note 26.

Ethernet or wireless connections, although some devices may directly connect over the Internet when a manufacturer uses cloud technologies.[42]

B. Big Data, Cloud, and Artificial Intelligence Architectures

The most common architecture for modern devices involves transmitting data over the open Internet to a cloud service, which captures large volumes of data in shared databases.[43] If data scientists can structure data in a useful way, or big data, these large data stores can dramatically change what the medical field can learn about certain conditions and effectiveness of specific medical devices on these conditions.[44] Big data necessitates ubiquitous data collection to store the volume necessary for complex data insights, and availability of large data sets dramatically improve the effectiveness of AI utilities, as well.[45] Manufacturers often use cloud technologies in medical device implementations involving big data because cloud technologies reduce overall cost to run or maintain big data infrastructure and databases.

In medical device manufacturing, AI is a form of automation, or digitizing a previously manual decision or human interaction without human intervention or with very limited human interaction.[46] Automation seeks to reduce costs through increasing efficiency of care, reducing human workload, and improving overall health outcomes by leveraging ever-increasing machine computing power. AI builds on this concept by coupling automation's enormous power with decision-making capabilities, in some cases modeled after the human brain, as in neural networks.[47]

---

[42] *See, e.g.*, *CloudMinds, the World's First Cloud Robot Operator, Launches Mobile-Intranet Cloud Services, Enabling Secure Cloud Robotic Deployments, and Data A1 Handset, World's First Mobile Phone Robotic Control Unit*, BUSINESSWIRE (Sept. 12, 2017, 1:17 PM), http://www.businesswire.com/news/home/20170912006534/en/CloudMinds-World%E2%80%99s-Cloud-Robot-Operator-Launches-Mobile-Intranet (describing cloud-based robotic deployments). Cloud technologies include applications, infrastructure, and storage technologies managed by a third party, rather than a health care provider's own server room or data center. *See Categories of Cloud Providers*, SERVICE ARCHITECTURE (2017), https://www.service-architecture.com/articles/cloud-computing/cloud_computing_categories.html.

[43] Lisa Mays, *The Cloud and Cloud-Computing: Pharma and Medical Device's Biggest Trend for 2012*, BASECASE (Feb. 1, 2013), http://basecase.com/blog/cloud-computing-pharma-and-medical-device (positing that cloud computing has become the biggest trend, starting in 2012).

[44] The collection and use of large data stores involves a data trade: patients provide data to a manufacturer, and big data may reveal unanticipated information about a person. Without effective, complementary, privacy restrictions, this data could be purchased for recombination with other data sources, providing unanticipated insights. *See* Peppet, *supra* note 44, 121–23.

[45] The need for substantially high data volume and ubiquitous data collection in AI informs architectures. In other words, without connectivity, medical devices must include substantial storage capacity, which increases their overall size. *See* Al-Siddiq, *supra* note 26.

[46] *Id.*

[47] STUART J. RUSSELL & PETER NORVIG, ARTIFICIAL INTELLIGENCE A MODERN APPROACH 740–41 (2015).

AI, from a medical device perspective, consists of various utilities or software running on top of big data databases.[48] AI works adaptively by nature: reviewing data with respect to algorithms, or equations for interpreting data, then making decisions based on these data. Decisions can include what direction to give to a medical device client, to monitor for additional data, or to change the algorithm based on new data aggregated.[49] AI decisions might take the form of directly changing something about a medical device without human interaction or by recommending some action to a human recipient who then interacts with the medical device to accept or reject the recommendation.

The most applicable AI functions for medical and health devices include machine learning utilities. Machine learning is a system of learning that leverages data sets and substantial computing power to independently develop algorithms from structured and unstructured data, including data mining to interpret and learn from data patterns.[50] Machine learning utilities can include supervised and unsupervised learning environments.[51]

Supervised learning environments include human "training" or other evaluation of how machine learning utilities interpret data and create algorithms.[52] Supervised learning environments work well when a human clearly understands expected device functions and devices may collect relatively small data volumes.[53] Unsupervised learning, however, references a lack of human intervention at any point in the computing process, including in creation of algorithmic calculations without human intervention or even a human decipherability of algorithms that support or automate primary medical device functionality.[54] While supervised learning environments ensure humans control or guide AI decisions, unsupervised learning environments have the most potential for revolutionary

[48] AI is now possible due to advancements in foundational infrastructure technologies, the "stacking" anticipated by Ray Kurtzweil in his prediction of the AI singularity, or sentience. *See* Robert D. Kalinoski, *The Role of Law in Our Technological World*, 33 MD. B.J. 3, 7 (2000). AI used in medical devices today involves more structured learning than sentient machines.

[49] AI applications, whether supporting diagnosis or directly delivering instructions to a device, require access to sensitive medical data. Although under some circumstances data could be rendered de-identified, reducing "minimum necessary" privacy obligations, this could reduce the efficacy of AI. Further, the E.U. does not recognize de-identification as a valid method for establishing anonymization under the GDPR and requires both primary and secondary identifiers be removed from data sets to establish *impossibility* of re-indentification, while reinforcing the minimum necessary obligation. This poses a problem for AI utilities in the E.U. as well as the U.S. *See* Article 29 Data Protection Working Party, *Opinion 05/2014 on Anonymisation Techniques*, 0829/14/EN WP216, 6 (Apr. 10, 2014), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf.

[50] Pattern recognition is also known as data mining, which can be used for diagnosing an individual, providing treatment plans, or to gauge effectiveness. *Id.* at 8–10.

[51] ETHEM ALPAYDIN, MACHINE LEARNING 38–40, 114 (2016).

[52] *Id.* at 38.

[53] *Id.*

[54] An example includes "bootstrapping," where the computer is fed a large data set, which is then processed without human intervention. *See* RUSSELL & NORVIG, *supra* note 47, at 27–28.

health outcomes by identifying data relationships not previously discovered through human-created algorithmic investigation.[55] However, they also require substantially more data and little to no human oversight, which could pose safety issues, without appropriate implementation or monitoring.

Unsupervised learning improves previously established big data analytics and data science by leveraging a machine learning utility to develop the algorithms governing device activity, then monitors, analyzes, and adapts such algorithms as needed to improve function for one or all patients.[56] Machine learning incorporates probabilistic agency, or machine determinations made by calculating potential actions, their relative probability of success, and tolerance for negative outcomes.[57] Probabilistic agency mimics human decision-making, including risk appetite or tolerance. However, unlike human beings, who might fall victim to various cognitive biases, machines use pure data to make these decisions.[58]

C. Big Data Technology Risks

Big data, cloud services, and AI coupled with medical device technological improvements have already begun to revolutionize health care.[59] However, scholars have also raised consumer privacy concerns. David Vladeck has discussed the following considerations for big data collection that includes

---

[55] *Id.* at 28.

[56] Machine Learning accommodates variegated data types and unstructured or poorly structured data, unlike the limitations of data science. From this perspective, AI utilities organize and structure data for analysis. Where data science requires prior knowledge of data structure and effective organization, AI requires no prior knowledge of data structure: the AI utility determines structure from data by identifying relationships between data elements and complex relationships.

[57] The concept of agency matches similar conceptual underpinnings in economics (wealth maximization) and the social sciences. Humans act to increase pleasure and avoid pain; machine learning will incorporate this human trait within established ethical boundaries. For example, perhaps a ninety-nine percent chance exists for a patient to recover substantially using a new stimulation frequency, but a one percent chance exists that the patient will die. A machine will likely calculate these as "exceptionally good" odds, although a human might reject the stimulation frequency based on a known mortality probability (or otherwise advise the patient). When manufacturers consider fully automated systems without human interaction, manufacturers, in partnership with the FDA or other government regulators, must establish appropriate compliant and ethical limits.

[58] Of course, the concept of machines avoiding cognitive biases also requires "clean" data sets, or those without previously codified human biases. If machines learn and tune algorithms to an existing data set created by humans, presumably human-specific conditions will also be codified, including less desirable traits. For purposes of medical devices, codification of human traits is far less likely, as most databases receive pure device data, machine-to-machine.

[59] *See* President's Council of Advisors on Sci. & Tech., Exec. Office of the President, Big Data & Privacy: A Technological Perspective (May 2014), https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf (addressing the impact, from a policy perspective, of big data and associated broad technical developments on the future of health care).

algorithmic decision-making: 1) ubiquitous data collection, data breach, and identity theft; 2) unrestrained collection of sensitive, personal data; and 3) the use of algorithmic decision-making to make consequential decisions.[60]

Ubiquitous data collection and unrestrained collection of sensitive personal information (SPI) complicate the relationship between artificial intelligence and cybersecurity. Artificial intelligence, for its part, requires ubiquitous data collection in relation to medical device functionality, which may in some cases include substantial collection of SPI across populations, locations, and devices.[61] Without substantial and seemingly restrained data collection, AI machine learning utilities, especially unsupervised learning utilities, will reach inaccurate and, likely, dangerous results. For strict AI purposes, limiting data collection may lead to undesirable patient safety risks.[62]

Ubiquitous data collection, especially involving SPI, creates an undesirable risk of data loss and potential for data misuse and mismanagement.[63] SPI is valuable, not only because it is intrinsically private, but because it often has substantial value on the digital black market, or the Dark Web.[64] When SPI falls into criminal dealings via a breach of confidentiality, it can be sold for any purpose: blackmail, ransom, or bulk sales in the case of health data perpetuating insurance fraud schemes.[65] When value attaches to data, a built-in incentive exists for cyberattack.

---

[60] David C. Vladeck, *Consumer Protection in an Era of Big Data Analytics*, 42 OHIO N.U. L. REV. 493, 501–15 (2016) (describing how these three big data impacts apply in practice to impact consumers' private information). Of note, the European Union's General Data Protection Regulation (GDPR) has anticipated automated processing by adding an additional data subject right within the regulation: the right to be informed and object to automated processing. *See infra* Part II (E) and accompanying notes.

[61] *See* Drew Simshaw et al., *Regulating Healthcare Robots: Maximizing Opportunities While Minimizing Risks*, 22 RICH. J.L. & TECH. 3, 14 (2016), https://scholarship.richmond.edu/jolt/vol22/iss2/1. Robots and medical devices leveraging AI functionality both create and use substantial data volumes.

[62] *See* RUSSELL & NORVIG, *supra* note 47. There is a substantial increase in performance accuracy with a dramatically larger data set.

[63] Ubiquitous data collection also complicates obligations related to information privacy and data protection obligations, as ubiquitous data collection conflicts with data minimization requirements under the Federal Trade Commission's Fair Information Practices and other international laws. *See generally*, Ira Rubinstein, *Big Data: The End of Privacy or a New Beginning*, 2 J. INT'L DATA PRIVACY L. 74 (2013), https://academic.oup.com/idpl/article-pdf/3/2/74/2090432/ips036.pdf (describing how big data will affect data minimization efforts under the FIPs and the E.U. Data Protection Directive).

[64] Browning & Tuma, *supra* note 17, at 638–39.

[65] *See id.* at 643–44, 654–57. Attacks specifically designed to collect confidential data are considered *passive*. Passive attacks although less dangerous have increased in frequency and pose serious privacy concerns. As M. Ryan Calo has noted, the "impact of technology on privacy is pervasive." *See* M. Ryan Calo, *People Can Be So Fake: A New Dimension to Privacy and Technology Scholarship*, 114 PENN ST. L. REV. 809, 818–19 (2010) (quoting Erwin Chemerinsky, Orin Kerr, Ruth Gavison, Michael Froomkin, and Jonathan Zittrain); *see also* Peppet *supra* note 44, at 121–23 (exploring the privacy impacts of the sensor fusion phenomenon). The "sensor fusion" phenomenon leads to circumstances where data from disparate devices together provide a greater degree of

SPI and other health data are essential to providing reliable health care. Attackers who seek to interrupt or negatively impact healthcare operations or harm an individual patient will target data integrity and availability.[66] Medical devices rely on accurate, available data; by making accurate data unavailable, devices will not likely function properly.[67] Therefore, large data stores connected to medical device data would likely attract this type of attacker, as well as criminals seeking financial gain. Essentially, the more sensitive data collected, the more attackers will seek to undermine the confidentiality, integrity, and availability of that data, which may lead to privacy and safety impacts: more data result in (potentially) more problems.

D. Cyberthreats and Device Vulnerabilities

Artificial intelligence, unregulated, poses unique and highly impactful risks for protecting individual health safety. The crux of safety concerns is the lack of human intervention and device automation when such devices: 1) instruct a human to behave in some way based on data analysis; 2) provide sensor data, which inform future health treatment; 3) directly interface with the human body, automatically performing according to human or AI algorithmic direction; or 4) engaging in complex robotic tasks.[68] Although exhibiting different risk profiles, each of these device functions directly introduce safety challenges when data integrity or data availability is compromised by an online attacker.

Unlike many devices within a hospital or health care provider, which may pass information over an internally managed network that employs some security controls, information passed over externally exposed networks without appropriate security controls, as with unregulated Internet of Things (IoT) medical devices, expose patient data to unauthorized change, interruption, or exposure.[69] Most patients and, in some cases, medical professionals, receiving instructions from a medical device trust the information provided. For example,

---

identifiability than alone. This concept, which is desirable from a medical device perspective, also could lead to more impactful data loss.

[66] Browning & Tuma, *supra* note 17, at 644. Attacks designed to interrupt or modify data are considered *active*. Active attacks are considerably more dangerous to a patient. Indeed, most manufacturing activities are spent preventing data loss rather than preventing active attacks. *See* Woods, *supra* note 12, at 423; *see also*, Andrea Peterson, *Connected medical devices: The Internet of Things-That-Could-Kill-You*, WASH. POST (Aug. 3, 2015), https://www.washingtonpost.com/news/the-switch/wp/2015/08/03/connected-medical-devices-the-internet-of-things-that-could-kill-you/?utm_term=.78232191b138.

[67] *See* Peterson, *supra* note 66.

[68] *See* Simshaw et al., *supra* note 61, at 10–11. Robots involved in complex tasks likely will require access to multiple medical devices for purposes of monitoring. It should be noted that for less complex operations, medical devices will likely develop either interoperable data sharing between devices in a human or a common interface for physicians or patients to review reports.

[69] Torsten George, *IoT: The Security Risk Iceberg*, SECURITYWEEK (Sept. 23, 2015), http://www.securityweek.com/iot-security-risk-iceberg (on file with Author). Internet of Things for medical devices are sometimes also known as Internet of Health Things (IoHT).

if a brain stimulation device signals to a patient that the patient is about to have a seizure, the patient will likely activate the device to prevent the seizure. However, stimulating the brain without a seizure impending could have a substantial safety impact. If instructions or information can be altered when passed over the Internet, injury could result.

Similarly, attackers could manipulate sensor data, which is used to inform future surgical or pharmaceutical medical needs.[70] When patients and their physicians rely on data, safety issues could result when patients undergo surgical procedures or are unnecessarily or inaccurately medicated.[71] Cybersecurity measures would ensure the integrity of information transmitted in both of these scenarios.

When devices continuously interface with the human body and the open Internet, whether implanted or tethered, additional cybersecurity risks result.[72] In addition to the same data integrity concerns described in relation to decision-making, unauthorized data changes, whether in transmission over the Internet or in backend big data systems, may result in incorrect instructions directly sent to a medical device.[73] As many medical devices do not have a user interface for a patient to make decisions regarding device functionality (e.g. a pacemaker), the medical device will act on incorrect instructions from the backend infrastructure.[74]

Lack of data availability for life-sustaining medical devices, critical diagnostic devices, or record-storing medical devices will physically harm patients.[75] Depending on the type of device, several known cyberattacks involve stopping existing services, including: ransomware, distributed denial of service (DDoS) attacks, malware, and others.[76] Cybersecurity network infrastructure and controls and a variety of other cybersecurity best practices can combat these attacks, so long as manufacturers build these programs.[77] Whether the medical device gives patient or physician instruction, provides output sensor data, or directly acts on the human body, Internet connectivity dramatically changes the safety profiles for

---

[70] *See* Lily Hay Newman, *Medical Devices Are the Next Security Nightmare*, WIRED (Mar. 2, 2017, 10:20 AM), https://www.wired.com/2017/03/medical-devices-next-security-nightmare/.

[71] *See* Patricia A.H. Williams & Andrew J. Woodward, *Cybersecurity Vulnerabilities in Medical Devices: A Complex Environment and Multifaceted Problem*, NCBI, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4516335/#b26-mder-8-305.

[72] *See* Newman, *supra* note 70.

[73] *Id.*

[74] *See, e.g.*, Browning, *supra* note 17, at 645–47 (describing demonstrations of hacking an IV infusion pump that changed dosage and shut down the pump).

[75] *See* Newman, *supra* note 70.

[76] *See* Michael Kassner, *How to Mitigate Ransomware, DDoS Attacks, and Other Cyber Extortion Threats*, TECHREPUBLIC (Aug. 13, 2016, 11:56 AM PST), https://www.techrepublic.com/article/how-to-mitigate-ransomware-ddos-attacks-and-other-cyber-extortion-threats/.

[77] The relevant acronym for medical device attacks is STRIDE: spoofing, or impersonation; tampering, or data change in transmission; repudiation, or the inability to prove valid changes; information disclosure, or data loss; denial of service, or halting device function; elevation, or privilege escalation, using credentials to increase access rights. *See* Browning, *supra* note 17, at 648–49.

medical devices. AI multiplies these risks by removing human involvement, once built, from the medical device system.

E. AI Threats and Vulnerabilities

Although AI may seem like a futuristic endeavor, machine learning applications have flourished for recent medical devices. In 2017 alone, at least six companies passed FDA review for machine learning applications, one of them with 13 different applications.[78] Despite an industry movement towards AI-enabled devices, the FDA appears focused on preserving a system built around traditional encapsulated medical devices.

Medical devices historically included software applications with algorithmic calculations and automated functionality, but these capabilities resided within the physical medical device rather than on backend systems, limiting the options for continuous learning applications. Clinical testing, then, could accurately observe static medical device functionality across a clinical trial population for a specific time period.[79] Clinical testing could, within a range of accuracy, anticipate potential safety hazards and disclosable side effects in a test environment so long as the medical device did not functionally change between testing and sale.

In contrast to encapsulated medical devices, the connected medical device using AI is dynamic and continuously evolving, rather than static.[80] AI not only informs human decision-making, it independently instructs device behavior and benefits patients as it uses data from all patients to learn and adapt, theoretically improving functionality and efficacy.[81] AI transforms the world into a continuous clinical test. As designed, AI adapts instructions, appropriate device ranges, or dosages, to what is most successful for a population.

Storing as much information as possible about an individual enables the AI utility to adapt these instructions to sub-populations in a recruitment pool or protocol designs that a human might never select for a traditional trial.[82] For example, perhaps an AI utility discovered that patients near the equator with a history of heart failure and current stent implantation required less insulin from their pump than patients in Northern Canada without heart failure as part of a continuous clinical trial. The vast majority of clinical trials would never test this level of granularity,[83] and most physicians would not have access to the data

---

[78] *See* infra, note 179.

[79] SHARONA HOFFMAN, ELECTRONIC HEALTH RECORDS AND MEDICAL BIG DATA 113–16 (2016). Existing clinical trials have limits for testing. For example, randomized trials are tightly controlled, while observational trials can fall to confounding bias. Big data and, presumably, AI operating on big data, can improve clinical trials substantially by offering a broader range of research.

[80] *See* Browning, *supra* note 17, at 642.

[81] See discussion in Part I(A)–(B) and accompanying notes.

[82] *See* RUSSELL & NORVIG, *supra* note 47. Part of why AI is so powerful is its ability to find relationships between data points in big data sets. When leveraged in medical devices, the AI utility might find correlative relationships that would be too expensive to traditionally test through clinical trials or are simply unanticipated.

[83] *See* HOFFMAN, *supra* note 79.

volume or have the computing capacity to identify causative relationships between so many seemingly disparate pieces of information.[84]

Despite the potential benefits of AI in these circumstances, the structure and function of AI alone presents a plethora of potential patient safety concerns. From an AI-cybersecurity perspective, the first consideration is whether the AI utility can rely on data integrity within applicable data sets. AI lives and dies by data: without sufficient data volume, AI utilities will identify inaccurate data relationships and provide incorrect instructions.[85] However, poor data integrity likely results in AI utilities providing incorrect instructions. Data must be both high volume and highly accurate to safely improve medical device functionality.

AI engineering requires specific expertise in design of learning environments. Most AI utilities in modern medical devices use supervised learning environments to ensure that AI decisions are reviewed and tuned before patient use. However, supervised learning environments require highly knowledgeable engineering of the database and environment, the ability to analyze highly complex computer-generated algorithms, and the knowledge to train these utilities to create algorithms closer to a range of acceptable medical device instructions. Although a medical device manufacturer might be able to construct these environments, manufacturers might not create the appropriate training environment, or the requisite data set to ensure reliable and effective medical device performance. Further, testing may not fully ensure a range of predictable behavior, potentially affecting performance and patient safety issues downstream.

From a cybersecurity perspective, if large data sets used by AI utilities include substantial volumes of incorrect or inaccurate data, the AI utility will assuredly provide incorrect instructions.[86] Manufacturers can prevent these issues through standard cybersecurity measures; further, they may install AI utilities to monitor for data value changes in a primary data set or otherwise for unauthorized access to the data set(s).[87] It only makes sense for manufacturers to consider AI utilities

[84] *See, e.g.*, Robert Rowley, *AI as a Way to Overcome Cognitive Bias in Physicians*, FLOW HEALTH (July 17, 2017), https://flowhealth.com/blog/2017/07/ai-as-a-way-to-overcome-cognitive-bias-in-physicians/ (describing how AI can overcome human biases and limitations).

[85] This argument is self-referential: If AI requires larger data stores for accuracy, it follows that data integrity issues could dramatically alter outcomes. In more advanced AI, it is possible that the utility itself could learn to identify integrity issues, but it is unknown whether that is currently possible.

[86] *See* Kevin Magee, *Has Healthcare Misdiagnosed the Cybersecurity Problem?*, HELPNETSECURITY (Aug. 7, 2017), https://www.helpnetsecurity.com/2017/08/07/healthcare-cybersecurity-problem/ (arguing that machine learning could provide a solution to validating data, such as identifying anomalies).

[87] Cybersecurity vendors are beginning to implement AI utilities to identify unauthorized changes. *See* Selma Dilek et al., *Applications of Artificial Intelligence Techniques to Combating Cyber Crimes: A Review*, 6 INTL. J. ARTIFICIAL INTELLIGENCE & APPLICATIONS 21 (2015) (describing the viability of AI functions for cybersecurity applications).

to ensure the integrity and availability of the databases on which AI utilities rely.[88] The solution to AI safety concerns could be more AI.[89]

Although less common in medical device manufacturing, unsupervised learning also presents unique issues for patient safety. Unsupervised learning leverages substantially large data sets to define algorithms from the data, rewriting algorithms as needed and communicating between multiple machine learning utilities using shorthand communication.[90] The potential for unsupervised learning can, under the right circumstances, eclipse benefits of supervised learning: transforming medical device functionality, providing personalized medicine, and continuously improving functionality.[91] However, unsupervised learning also has fewer structural limitations, potentially posing safety issues. For example, it is possible that, in the name of efficiency, AI code and associated algorithms will become unreadable and undecipherable due to their complexity and communicative efficiency.[92] Without an opportunity to review and consider AI instructions or decisions, both patients and operators may be unable to understand calculations and conduct root cause analyses after unanticipated safety issues or undesirable outcomes.[93] Algorithms, then, become increasingly more opaque when even those who created the AI infrastructure running the algorithms cannot understand them.

Professors W. Nicholson Price II and Roger Allan Ford pioneered exploration of "black box medicine" in relation to opacity and privacy in algorithmic decision-making.[94] Price articulates two separate types of algorithms used in "black box medicine," research algorithms that help to identify data relationships and

---

[88] *Id.*

[89] *Id.*

[90] Adrienne LaFrance, *What an AI's Non-Human Language Actually Looks Like*, THE ATLANTIC (June 20, 2017), https://www.theatlantic.com/technology/archive/2017/06/what-an-ais-non-human-language-actually-looks-like/530934/. Facebook shut down an unsupervised AI utility after it created its own language. Short-hand creation is an important development for AI bots because it enables more efficient communication between bots in an AI utility.

[91] The categories of supervised learning are "known" and established by a human. This makes possible "discoveries" less possible in a supervised learning environment. In an unsupervised learning environment, relationships and cause/effect relationships are not limited by established boundaries, making more dynamic findings possible. *See What Exactly is the Difference Between Supervised and Unsupervised Learning?*, COMPUTER SCI. STACK EXCHANGE (2018), https://cs.stackexchange.com/questions/2907/what-exactly-is-the-difference-between-supervised-and-unsupervised-learning (noting, in particular, the answer by Dave Clarke on July 25, 2012, and related comments).

[92] *See* LaFrance, *supra* note 90.

[93] *Id.*

[94] *See* Price 2, *supra* note 11, at 429; *see also* W. Nicholson Price II [hereinafter Price 1], *Black-Box Medicine,* 31 JOLT 419 (2015), http://jolt.law.harvard.edu/assets/articlePDFs/v28/28HarvJLTech419.pdf (introducing the concept of black-box medicine algorithmic decision-making); Ford & Price, *supra* note 11 (articulating potential impacts to patient privacy due to substantial data aggregation and potential regulatory approaches for protecting privacy while driving accountability for algorithmic decision-making).

potential outcomes and predictive algorithms that drive decisions or action.[95] Both of these algorithms in a medical device AI environment may be even more opaque than previously imagined: AI engineers create the infrastructure and conduct limited training, then the utility uses data to create algorithms that conduct research, which feeds predictive algorithm and specific action. Algorithms once designed or discoverable by experts now have the potential to be completely indecipherable to anyone but the machine.[96]

II: New Technology Gaps in U.S. and E.U. Regulatory Frameworks

Despite new cybersecurity and AI safety risks, FDA classifications do not anticipate these risks in device clearance procedures and guidance. Likely due to historical classification based on previously submitted devices, or substantial equivalence, the FDA categorizes devices primarily in relation to its interaction with the human body rather than backend architecture. While details of the additional systems used might be disclosed during the device submission process, usually these details are not scrutinized during the FDA review process, as they do not directly interface with the human body. Further, risk management principles embedded in FDA procedure may introduce additional safety issues.

A. FDA and MDD Medical Device Types

Standing law for medical devices in the United States and the European Economic Area (EEA) include the Food, Drug, and Cosmetics Act (FD&C Act) and the Medical Device Directive (MDD), respectively. The Food and Drug Administration (FDA), the European Commission (EC), and relevant country-level authorities regulate medical devices in the U.S. and E.U.

Congress passed the FD&C Act in 1938, giving broad rule-making authority and medical device oversight to FDA. Since this time, the FDA has established clearance processes, which involve categorization of medical devices into classes and specific panels, which review medical devices within a designated medical specialty and help to classify a particular device into a class for a particular use within that panel.[97]

The FDA classifies medical devices as:

> An instrument, apparatus, implement, machine, contrivance, implant . . . or other similar or related article, including a component part, or accessory which is . . . intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease

[95] Price 2, *supra* note 11, at 426.

[96] *Id.* at 435.

[97] U.S. FOOD & DRUG ADMIN.: DEVICE CLASSIFICATION PANELS, https://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/Overview/ClassifyYourDevice/ucm051530.htm (last updated June 26, 2014).

> . . . or intended to affect the structure or any function of the body of man.[98]

The FDA classification for medical devices illustrates the FDA's intention to ensure maximum breadth of enforcement authority and occupy the medical device regulatory field.[99] These devices, however, must be classified in such a way as to balance manufacturing discretion and federal oversight. As a result, the FDA has established a classification scheme that creates fewer compulsory obligations for lower risk medical devices, while increasing upfront clearance requirements and downstream monitoring activities for high risk medical devices.[100]

Despite differences in backend functionality, the FDA establishes device type through historically established clearance procedures, which in turn inform downstream device reviews and testing stringency.[101] Required processes, testing, and disclosure obligations become more stringent with a higher classification, with the highest classification a Class III device.[102] These devices pose the most potential risk to human subjects usually evaluated based on the degree of physical contact and expected, direct changes to human body function.[103] The FDA exercises the most authority over Class III devices.[104] This classification-based approach embraces a risk management approach to regulation, one that focuses on promoting device safety while balancing oversight with self-management and product costs.

Medical devices fall into three FDA groups from least to most invasive in relation to the human body, and organizes devices into specific panels, or expertise classification. Class I devices support human decisions regarding the body (such as Web applications or mobile apps) through completely indirect means.[105] Class I devices might require an individual to input data rather than by directly capturing data from the human body. According to the FDA, Class I devices typically do not introduce substantial human health and safety risks, and therefore do not receive a comprehensive FDA inquiry.[106] However, Class I and II devices may support decision-making about diseases or diagnoses, which could substantially impact human life.[107]

---

[98] U.S. Food & Drug Admin.: Medical Device Overview, https://www.fda.gov/ForIndustry/ImportProgram/ImportBasics/RegulatedProducts/ucm510630.htm (last updated Dec. 1, 2017).

[99] Although this article does not explore methods of tort recovery following AI injury, future analysis of AI tort recovery should include considerations of FDA preemption, taking into account FDA oversight limitations discussed in detail here.

[100] U.S. Food & Drug Admin.: Classify Your Medical Device, https://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/Overview/ClassifyYourDevice/default.htm (last updated July 29, 2014).

[101] *Id.*

[102] *Id.*

[103] *Id.*

[104] *Id.*

[105] *Id.*

[106] *Id.*

[107] *See* Price 2, *supra* note 11 at 443. Most devices fall into Classes I and II, rather than requiring full review in Class III. Although this classification is designed to reduce

Class II and Class III devices classically present more potential safety hazards for a human subject.[108] Class II devices often interface with the human body, yet are less invasive than devices implanted in the human body.[109] Class II devices might include both technologies that gather information from the human body, such as sensing or other diagnostic and biological mapping technologies. Class III devices may include implantable devices connected to additional sensors or Class I devices, such as a drug delivery pump connected to a mobile application.

The E.U. manages medical devices under the MDD, which in 1998 became mandatory for countries in the E.U. and requires the use of a CE Mark to demonstrate compliance with the Directive.[110] The E.U. defines a medical device as:

> [A]ny instrument, apparatus, appliance, software, material or other article, whether used alone or in combination, together with any accessories, including the software intended by its manufacturer to be used specifically for diagnostic and/or therapeutic purposes and necessary for its proper application, intended by the manufacturer to be used for human beings for the purpose of: diagnosis, prevention, monitoring, treatment or alleviation of disease, diagnosis, monitoring, treatment, alleviation of or compensation for an injury or handicap, investigation, replacement or modification of the anatomy or of a physiological process.[111]

As in the 2007 medical device definition, the E.U. has explicitly noted that software, when used for medical device purposes, is classified as a medical device, regulated under the MDD.[112] Furthermore, validation of software functionality both within devices and as standalone devices is explicitly required.[113]

The E.U. has adopted a similar typology to FDA medical device classification and associated clearance processes, a "risk based," "graduated system of control" under the Medical Devices Guidance Document.[114] At a minimum, all devices must meet both requirements established in Annex I of the Medical Device Directive and receive CE Mark status established in Annex VIII.[115]

---

risk to human health by classifying based on invasiveness, some devices using AI may actually pose more risk than the classification scheme might immediately anticipate.

[108] *See* U.S. FOOD & DRUG ADMIN., *supra* note 100.

[109] *Id.*

[110] *See generally* Council Directive 93/42/EEC, 1993 O.J. (L 169) 1 (EC), http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:1993L0042:20071011:en:PDF.

[111] Council Directive 2007/47/EC, art. 1, § 1, pt. 1, para. a 2007 O.J. (L 247/21), http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L1148. Despite being drafted in 2007, this definition now explicitly includes references to the evolution of software in medical device applications.

[112] *Id.* at art. 6.

[113] *Id.* at art. 20.

[114] European Commission, *Medical Devices: Guidance document*, MEDDEV 2.4/1 Rev. 9, at 4 (June 2010) [hereinafter Eur. Comm'n, *Guidance* (2010)].

[115] *Id.* at 4–5. *See infra*, Part III and accompanying notes.

The E.U. organizes medical devices into Class I, Class II, and Class III, with sub-classes.[116] The manufacturer can either independently evaluate components of a device, such as an implantable portion of the device, separately from external device components and classify each component. [117] Class categorization considerations the duration of time a device will interface with the body and whether this connectivity involves an orifice or a surgical site.[118] However, nearly all direction for medical device classification explains the relationship with the body, rather than how data could affect, directly or indirectly, device function or user behavior.[119]

In addition to devices manufactured by the entity seeking clearance, the U.S. and E.U. require manufacturers marketing or selling third party devices and components to either include third party devices and components in the submission process or demonstrate previous clearances.[120] This process ensures that such devices and components are assessed for risks specific to applied use within or as a medical device when used for previously off-label use. Manufacturers purchasing products through acquisition or as components, then, must illustrate appropriate quality measures are met for disclosed use.

B. Medical Device Oversight – U.S.

The FDA has two different processes for device clearance: Pre-Market Acceptance (PMA) process and the 510(k) process. The PMA process requires full FDA evaluation for new medical devices and substantial changes to previous devices for Class III devices.[121] The 510(k) process is used for Class II devices and Class III devices leveraging substantial equivalence, or when a device has similar technical characteristics or new technical characteristics that does not raise new safety or efficacy concerns.[122] When changes to an existing product do not appear to significantly affect safety considerations, manufacturers likely do not require new FDA approval.[123] Devices changing backend infrastructure may qualify for the 510(k), avoiding comprehensive FDA review, even for Class III devices.

Outside the PMA process, FDA oversight is not comprehensive. Although all devices, regardless of classification, must comply with the FD&C Act and FDA oversight, many devices posing cybersecurity risks do not receive any direct FDA review prior to release on the open market.

---

[116] Eur. Comm'n, *Guidelines* (2010), *supra* note 114, at 5.

[117] *See id.* at 14, 16–22 (illustrating classification for specific examples).

[118] *Id.*

[119] *Id.*

[120] *Id.* Third-party devices and components must demonstrate clearance. If a third party has not already established clearance, the manufacturer will need to submit the third-party devices or components for clearance separately or as part of another device submission.

[121] 21 C.F.R. § 814 (2017). A supplement may be required if a software patch has an adverse effect on patient safety or effectiveness. *See* 21 C.F.R. § 814.39 (2017).

[122] Amanda Swanson, *510(K) Clearance: Opportunities to Incentivize Medical Device Safety Through Comparative Effectiveness Research*, 10 IND. HEALTH L. REV. 117, 128–29 (2013).

[123] 21 C.F.R. §§ 807.81(a)(3), 814.39 (2017).

Class I devices require application of general controls, or controls specified under the FD&C Act.[124] These controls include submission under the 510(k) process, notifications to the public, mandatory recalls, adverse event report management, good manufacturing requirements, and reporting on removals and corrections.[125] Overall, Class I devices require basic Quality Management System (QMS) operations and after-manufacture communication processes.

Class II devices require general controls and special controls. The special controls pertain individually to the type of device and its panel, including performance standards, post-market surveillance, registration of patients, data requirements for pre-market submission, and specific guidelines.[126] Class II devices require additional upfront and post-market rigor due to an increased safety risk.[127] For Class II and III devices, the FDA publishes guidelines for medical device pre- and post-submission practices, including for example, topics on cybersecurity and home care.[128]

Class III devices, except when determined substantially equivalent, will follow a rigorous PMA process.[129] PMA clearance essentially licenses an organization to market a Class III medical device.[130] To ensure a manufacturer includes appropriate safety measures, the PMA process requires clinical trials, data outcome submission, substantial documentation, and manufacturer engagement both prior to and following successful PMA submission.[131]

The FDA does, however, have discretionary authority to not review some devices. Class I devices receive very little review, and sometimes none whatsoever. The FDA, for example, has decided not to review Type I consumer health apps or Web application devices at this time.[132] Despite the FDA's intention not to review these apps, mobile health app downloads were estimated to have reached 3.7 billion in 2017, illustrating the magnitude of consumers relying on apps to support health management.[133]

---

[124] Jessica S. Allain, *From Jeopardy! to Jaundice: The Medical Liability Implications of Dr. Watson and Other Artificial Intelligence Systems*, 73 LA. L. REV. 1049, 1070 (2013).

[125] *See, e.g.*, 21 C.F.R. § 872.6855(b) (2017).

[126] U.S. FOOD & DRUG ADMINISTRATION, REGULATORY CONTROLS, https://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/Overview/GeneralandSpecialControls/ucm2005378.htm (last updated June 26, 2014).

[127] Allain, *supra* note 124, at 1070–71.

[128] *See* Simshaw et al., *supra* note 61, at 30–32.

[129] *See* Swanson, *supra* note 122, at 124–25.

[130] *Id.* at 125.

[131] *Id.* at 124.

[132] *See* Simshaw et al., *supra* note 61, at 28. Further, the FDA downgraded Medical Device Data Systems (MDDSs) in 2011 from Class III to Class I. Not only do these devices introduce high risk of data loss and confidentiality attacks, they may provide an infrastructure for other devices relying on MDDS data stores. *See* Wellington, *supra* note 12, at 173–74. These two circumstances evidence a lack of understanding of the complexity, structure, and potential risks associated with seemingly benign medical devices.

[133] *See Number of mHealth App Downloads Worldwide from 2013 to 2017 (in billions)*, STATISTA (2018), https://www.statista.com/statistics/625034/mobile-health-app-downloads/. The large volume of downloads does raise the question of why the FDA has

C. Primary Medical Device Oversight – E.U.

In contrast with the FDA, the E.U. organizes by class, yet requires manufacturers to comply with more clearance requirements. Manufacturers must complete clinical evaluations for all devices, regardless of class, including submission of a Clinician Evaluation Report (CER) evidencing clinical data collection procedures.[134] The requirement to conduct a clinical evaluation, submit a CER, and receive a CE Mark does evidence a comparatively stronger upfront obligation to ensure quality and anticipate impacts, at least for Class I and Class II devices.

Under the E.U. CE Mark model, manufacturers must select evaluators to review medical devices for the clinical evaluation prior to clearance.[135] The manufacturer should have a rationale and appropriately justify choice of evaluators in line with the device and engage evaluators with a reasonable amount of experience.[136] However, the E.U. does not specifically require evaluator independence or mandate a particular assessment approach and methodology for evaluating clinical protocols.

Similar to the U.S., the E.U. also permits manufacturers to establish equivalence to previously submitted devices. Under the MDD, however, manufacturers must purposefully consider and evaluate the degree of equivalence with respect to clinical application, technical functionality, and biological criteria.[137] Differences must not affect the overall performance and safety of the device, and data of both devices must illustrate comparative function.[138]

Although criteria may not explicitly include cybersecurity or artificial intelligence considerations, consideration of technical functionality, including deployment methods or principles of operation and critical performance requirements, could trigger additional inquiry rather than equivalence.[139] Additional clinical investigations should be conducted when, for example, there is a new use for technology or when new "design features" apply.[140] The commentary included in these guidelines appear to leave room for additional evaluation of technology architecture, including cybersecurity and AI reviews.[141]

In addition to E.U. regional requirements, some individual EEA countries have established specific cybersecurity requirements for medical device sales. In France, the ASIP Santé have established secondary clearance requirements

---

not established any standards for these applications given the potential for broad, if not individually acute patient or consumer injury, such as data loss.

[134] *See* Eur. Comm'n, *Guidance* (2010), *supra* note 114, at 5–6; European Commission: Health technology and Cosmetics, *Guidelines on Medical Devices*, MEDDEV 2.7/1 rev. 4, at 29–31 (2016) [hereinafter Eur. Comm'n, *Guidelines* (2016)].

[135] Eur. Comm'n, *Guidelines* (2016), *supra* note 134, at 11.

[136] *Id.* at 14–15.

[137] *Id.* at 32.

[138] *Id.* at 33.

[139] *Id.* at 34.

[140] *Id.* at 34–35.

[141] *See* Woods, *supra* note 66, at 443–44. The E.U. has also conducted a cybersecurity exercise, yet the EC has not issued additional guidelines.

beyond the CE Mark, including cybersecurity requirements, such as encryption of data in transmission and while stored in databases, two-factor authentication, and robust privacy procedures.[142] Although it is expected that countries will continue to establish these requirements broadly for medical devices and beyond, it is likely more efficient for the EC to develop guidelines that enable global organizations to meet most clearance requirements without managing a plethora of divergent country requirements.[143]

D. Risk Management Principles Governing Medical Device Clearance

Legal schemes in the U.S. and E.U., including clearance procedures, have evolved specifically to manage patient safety risk and adopt a "risk-based approach" to device clearance.[144] By establishing procedures that focus on manufacturer device quality, triage inherent device safety risk, requiring review and clearance by experienced medical device experts, and creating standards and guidelines for ongoing device safety management, regulators have, to date, minimized potential patient impacts. These procedures loosely reflect risk management concepts specific to each step in the standard medical device lifecycle: concept, prototype, preclinical, clinical, manufacturing, marketing, commercial use, and obsolescence (end-of-life).[145] Despite these widely accepted and established procedures; big data, cybersecurity, and AI patient risks ('new technology risks') require regulators to reconsider long-established principles enshrined in medical device legal frameworks and associated procedures.

---

[142] *See* APPROVAL OF HEALTH DATA HOSTS: PUBLICATION OF THE CERTIFICATION REFERENCE FRAMEWORK FOR CONSULTATION, ASIP SANTÉ (Sept. 16, 2016), http://esante.gouv.fr/actus/services/agrement-des-hebergeurs-de-donnees-de-sante-publication-du-referentiel-de [hereinafter APPROVAL OF HEALTH DATA HOSTS].

[143] E.U. Directives, such as the Network and Information Security Directive (NIS) require individual countries to pass the directive as part of its own legal system. This often means that directives, in contrast with regulations, incorporate substantially more derogations, or deviations from the directive, when passed as country law. Although the General Data Protection Regulation (GDPR) operates as a regional law not requiring country law passage, the GDPR did reserve certain derogations for administrative and technical security measures, which might mean that individual countries still pass diverging requirements pertaining to personal information. In the E.U., the MDD, NIS, and GDPR combine as a co-governing regulatory framework, which means the EC should evaluate MDD guidelines with respect to country-specific guidelines affecting medical device clearance and SPI/personal information protection requirements. *See* Part II (D) and accompanying notes. Although not currently a topic of immediate discussion, existing legal challenges regarding FD&C Act preemption over state laws could pose similar challenges with states beginning to establish cybersecurity laws.

[144] Although the FDA does not explicitly identify these principles, one can assume that the medical device clearance procedures operationalize risk-management concepts.

[145] NAT'L INSTRUMENTS, *supra* note 18.

Principle 1: Triaging via device classification effectively balances manufacturer control and regulatory oversight.

Although on its face, classification appears to provide an efficient means to balance manufacturer design flexibility with government oversight, new technology risks may change the methodology for medical device classification.[146] The wide variance in U.S. classification oversight will likely lead to devices presenting substantially more cybersecurity or AI risk falling through the cracks.[147] Furthermore, classification based on previously cleared devices may prove inaccurate with more advanced technical infrastructure. In the U.S. manufacturers are encouraged to use previously cleared device classification to determine appropriate proposed classification for a new or substantially similar medical device. However, historical classification only accounts for part of the equation: the portion of the device that interacts with the human body or supports decision-making, rather than backend infrastructure. New technologies can dramatically affect the degree of decision-making support or introduce automated processes without human involvement that could hypothetically increase safety hazards to a patient, despite receiving minimal clearance due diligence under Class I or II review.[148]

Principle 2: Manufacturers are best positioned to plan for and identify potential safety issues in new technology.

In 1998, the FDA reiterated the importance of Quality Management Systems (QMS) in device manufacturing in relation to design controls.[149] Two independent studies in 1990 illustrated the criticality of design controls, rather than testing controls, in reducing downstream recalls and associated patient safety issues.[150] The purpose of such regulatory controls, such as pre-market submission criteria, is to reduce downstream issues.[151] It is faulty logic to contend that technology design issues would result in any fewer recall-related issues than existed with physical design flaws.[152] If the FDA relies on manufacturers to anticipate these issues without building appropriate controls into new technology design, the FDA will likely introduce the potential for costly recalls and patient safety issues.

Manufacturers with both robust research and compliance functions might be able to anticipate new technology risks, but well-resourced manufacturers are not

---

[146] *See* Wellington, *supra* note 12, at 186.

[147] *Id.*

[148] NAT'L INSTRUMENTS, *supra* note 18.

[149] 21 C.F.R. §§ 808, 812, 820 (2017) (describing two studies conducted in 1990 that demonstrated 44% of recall-related issues pertained to medical device design issues).

[150] *Id.*

[151] *Id.* The design control process may explicitly reference QMS programs, yet an essential portion of these programs, currently for Class II and Class III devices, includes reference to Guidelines. This process could be more effective with compulsory implementation of Pre-Market cybersecurity guidelines and future big data and AI guidelines, as well.

[152] *Id.*

the only manufacturers developing cutting-edge medical devices. The new technology marketplace includes start-ups and small businesses, experts in innovative technology, but who may not have the resources to effectively implement standardized programmatic risk management functions. U.S. and E.U. regulatory authorities may need to scrutinize new technology implementations with greater diligence than established with comparatively well-understood technologies.

Principle 3: Experts in a medical specialty are best positioned to anticipate potential medical device harms.

U.S. and E.U. regulatory frameworks rely on subject matter experts in the medical field, either via regulatory panels or in clinical evaluations, to review submitted devices for potential safety issues.[153] Historically, this model worked well because the greatest patient risk related to medical functionality and relationship with the physical body. New technology, however, introduces patient safety risks connected to backend systems and infrastructure, rather than devices interacting with the physical body. These new types of risks either necessitate a new formula for panel or expertise selection or require complementary reviews from experts who understand new technology functionality.

Principle 4: Clinical trials reduce device risk and provide data to anticipate patient safety risks and side-effects.

New technology, such as AI, and new cyberattack vectors can dramatically change the risk landscape for patients outside clinical evaluation. AI functions by routinely reevaluating success, failure, and algorithmic "fit," altering instructions for operation based on new, continuously evaluated data. What were once separated algorithmic functions, research and predictive algorithms, now continuously reinforce and direct action as part of a live clinical trial: a machine learning utility reviews data, including how successful its data-created algorithms have been, then makes changes to the algorithms as needed and directs updates to the device, including algorithms used for diagnostic or predictive purposes. Cyberattackers could easily make use of AI utilities to create new methods and modalities of cyberattack, including new vulnerabilities and creative threat vectors. Both of these circumstances illustrate that using clinical trials to establish a baseline for patient risk cannot effectively anticipate or manage ongoing patient safety risks with respect to new technology.

Principle 5: Similar technology introduces a similar risk profile.

Both U.S. and E.U. regulatory frameworks rely heavily on substantial equivalence to make the medical device clearance process more efficient.[154] However, similar to classification, the concept of substantial equivalence primarily relies on the patient technology interface, the device module itself, to

[153] *See, e.g.*, U.S. FOOD & DRUG ADMIN., *supra* note 97; Council Directive 93/42/EEC, *supra* note 110.

[154] *See* Swanson, *supra* note 122; Eur. Comm'n, *Guidelines* (2016), *supra* note 134.

determine equivalence.[155] At present, new technology that connects and automates existing technology does not appear to introduce a "difference" that bars reliance on substantial similarity: a connected device likely will be classified as substantially similar to a static device if they perform the same function. However, both devices present different risk profiles.

Principle 6: Manufacturers are best positioned to evaluate products purchased from third parties.

Regulatory frameworks place responsibility on manufacturers to assume risk for purchased components or devices marketed and sold under the manufacturer's name. Historically, limited competition in the medical device manufacturing space might have previously positioned manufacturers as best able to evaluate potential risks within internal quality and testing procedures. Further, historically purchased components or devices might not have been as extensible as, for example, AI utilities or cloud infrastructures, which could introduce markedly different risk profiles when used on different peripheral medical devices (e.g. an insulin pump or a diet and exercise mobile app for cardiovascular patients after surgery). Components that provide broadly applicable services likely cannot be evaluated for all potential uses, and therefore would benefit from holistic review as part of a particular medical device infrastructure.[156]

These six principles support an efficient medical device regulatory scheme, yet challenging these principles from the new technology lens encourages appropriate changes needed to anticipate future patient safety issues. By challenging these principles, regulators will be better positioned to address regulatory gaps.

E. U.S. and E.U. Privacy and Cybersecurity Laws Fail to Fill Regulatory Gaps

Although the FDA has established a broad medical device definition, other laws and agencies may regulate cybersecurity and AI activities. In addition to the FDA in the U.S., the Office for Civil Rights (OCR) and the Federal Trade Commission (FTC) regulate cybersecurity activities, yet neither have developed models that considers AI impacts.[157] The OCR enforces the Health Insurance

---

[155] Eur. Comm'n, *Guidelines* (2016), *supra* note 134, at 32–35.

[156] It is widely accepted in products liability cases when physical components result in product failure, but historically software companies have not experienced potential exposure. *See* O'Brien, *supra* note 12, at 16. The FDA could require private contracting language in agreements between manufacturers related to FDA compliance obligations if the FDA finds itself unable to directly regulate component entities.

[157] The Federal Communications Commission (FCC), for its part, had signaled a desire to regulate IoT devices generally, as all IoT devices must use Internet services regulated by the FCC, but this direction faltered with the 2016 change in administration. In addition to the FCC, multiple agencies have communicated a desire to regulate IoT. Unfortunately for medical device compliance, this mélange of regulatory interest is at best highly confusing for manufacturers, likely resulting in failure to follow any direction, especially when non-binding. *See* Woods, *supra* note 66, at 438–39.

Portability and Accountability Act (HIPAA), which applies to medical device manufacturers when manufacturers perform the role of a Covered Entity (CE) or Business Associate (BA).[158]

Medical device manufacturers may be designated a BA when performing activities that involve electronic Protected Health Information (ePHI) on behalf of a CE.[159] Although the definition of ePHI is broad, organizations may process ePHI if the data collected is de-identified. HIPAA requires CEs and BAs to consider data integrity issues, but the law is written from the perspective of patient privacy, which does not contemplate potential downstream device issues due to incorrect instructions or altered sensing data that might affect patient safety yet not include ePHI.

Congress updated HIPAA most recently in 2009 with the Health Information Technology for Economic and Clinical Health Act (HITECH Act).[160] HIPAA had established baseline privacy and security requirements, while the HITECH Act designated express authority for the Office for Civil Rights (OCR) to conduct audits on HIPAA compliance.[161] Despite HIPAA establishing one of the most restrictive federal laws for information security in the U.S., unfortunately most requirements do not address true cybersecurity risks.[162] Furthermore, HIPAA as currently drafted also does not anticipate new AI considerations and concerns.[163]

The Federal Trade Commission, pursuant to its broad rule-making authority and oversight for unfair and deceptive trade practices, has attempted to fill broad policy gaps in the digital technology space.[164] The *Wyndham* case reinforced the FTC's role in broadly regulating data protection activities, and several FTC cases involve both fallout from data breaches and allegedly unfair or deceptive privacy

---

[158] The designation as CE or BA critically determines whether HIPAA privacy and security rule requirements, as well as OCR audit activities apply to a given manufacturer or other entity. Importantly, many entities do not fit CE or BA designations. *See* Simshaw et al., *supra* note 61, at 27, 37 (describing a 'HIPAA-free zone' and the applicability of the security rule for ePHI).

[159] Many medical device manufacturers will not be regulated by the HIPAA security rule. *See* Wellington, *supra* note 12, at 158.

[160] U.S. DEPT. OF HEALTH & HUMAN SERV., HITECH ACT ENFORCEMENT INTERIM FINAL RULE (June 16, 2017), https://www.hhs.gov/hipaa/for-professionals/special-topics/HITECH-act-enforcement-interim-final-rule/index.html.

[161] *Id.*

[162] *See generally* Charlotte A. Tschider, *Enhancing Cybersecurity for the Digital Health Marketplace*, 26 ANNALS HEALTH L. 1 (2017) (identifying key gaps between FD&C Act and HIPAA cybersecurity requirements and advocating for enhanced FDA enforcement).

[163] This paper does not attempt to address all issues AI might pose in healthcare generally, but the serious lack of technical cybersecurity requirements does not anticipate big data stores and automation reliant on high levels of data integrity and accuracy. *Id.*

[164] *See* Simshaw et al., *supra* note 61, at 44–45 (describing the FTC's movement towards regulating IoT, big data, and other digital functions but highlighting limited FTC resources to fully regulate digital technologies); FEDERAL TRADE COMMISSION, MOBILE HEALTH APPS INTERACTIVE TOOL (Apr. 2016), https://www.ftc.gov/tips-advice/business-center/guidance/mobile-health-apps-interactive-tool (facilitating decision-making for FTC Health Apps).

practices.[165] The FTC has signaled a desire to broadly enforce fairness practices for IoT, responding to the FDA's reluctance to regulate general consumer health devices by publishing a report in 2015.[166] Thus far, the FTC has not also not independently established guidance for AI capabilities in IoT use broadly or specific to medical devices, and importantly the FTC's power is *post-facto*, imposing regulatory enforcement rather than preventing potential harms.[167]

In the E.U., omnibus privacy and cybersecurity laws have established a baseline for personal information management, such as health-related data, and these laws apply to medical device manufacturers and consumer manufacturers equally. The General Data Protection Regulation (GDPR) has succeeded the Data Protection Directive, promising enhanced data privacy rights and increased obligations for organizations to report data breaches.[168] The GDPR requires reasonable administrative and technical security measures when handling personal information of natural persons, such as device consumers or patients, including special attention to ongoing confidentiality, integrity, and availability of personal information.[169] Although the GDPR does not specify, in detail, these measures, manufacturers selling devices in the E.U. must implement reasonable measures to address these risks.[170]

Similarly, the Network and Information Security Directive (NIS Directive) requires cybersecurity incident reporting and other network and system resiliency efforts to ensure critical infrastructure providers, such as health care providers, provide reliable and reasonably protected patient services.[171] The NIS Directive has granted the European Network and Information Security Agency (ENISA) authority to develop cybersecurity guidelines, but it is not yet clear whether such guidelines will directly apply to medical device or health device manufacturers.[172]

The E.U. has, thus far, not specified what reasonable administrative and technical cybersecurity controls might apply under the GDPR, through guidelines or other specific requirements. It is unclear, as well, whether the NIS Directive will apply to general manufacturing capabilities or medical device manufacturers, as well as direct health care providers.[173] However, it seems likely that these

---

[165] *See* F.T.C. v. Wyndham Worldwide Co., 10 F. Supp. 3d 602 (D.N.J. 2014). The Third Circuit has upheld the FTC's enforcement role with respect to data security enforcement.

[166] *See* Poudel, *supra* note 30, at 1016–17.

[167] *See* Simshaw et al., *supra* note 61, at 45.

[168] Commission Regulation 2016/679, 2016 O.J. (L 119) 1.

[169] *Id.* at (32).

[170] *Id.* The GDPR has been drafted in an intentionally broad manner, to ensure that all organizations handling the personal information of E.U. residents protect the personal information in a manner consistent with internal E.U. law. The U.S. Privacy Shield established adequacy in the E.U., permitting data export from the E.U. to the U.S. under modified standards. Commission Implementing Decision 2016/1250, 2016 O.J. (L 207) 1. However, the Privacy Shield does not eliminate GDPR compliance obligations for U.S. companies doing business with E.U. organizations or consumers.

[171] Council Directive 2016/1148, 2016 O.J. (L 194) 1.

[172] *Id.* at Preamble, 36–42.

[173] Many countries around the world have established laws that apply to "Critical Infrastructure" providers, including the U.S. *See, e.g.*, *Cybersecurity Law of the People's*

regulations will be applied coextensively as they solve different problems, similar to the FD&C Act and HIPAA in the U.S.: medical device safety (MDD), data protection as a civil right (GDPR), and critical infrastructure protection (NIS Directive).

III: Regulating Medical Device Cybersecurity for Artificial Intelligence

The U.S. and the E.U. have both established broad oversight responsibility for medical devices.[174] According to this approach, it is likely, if not probable, that consumer health devices might also be considered medical devices under these definitions.

If the U.S. and the E.U. intend to regulate these devices, as well as medical devices, it is critically important to understand potential gaps with respect to cybersecurity and artificial intelligence safety concerns. Both regions must consider new technology safety concerns holistically, including how classification to post-market obligations must adapt and change to adequately address these challenges. If the U.S. and E.U. do not intend to fully regulate medical devices, broadly speaking, each country may consider narrowing definitions or otherwise collaborating with other government agencies to ensure some oversight applies to these devices.

A. Classification and Clearance

The first step required by the U.S. and E.U. involves classifying medical devices in collaboration with panel experts, external experts, and by previously classified devices. To ensure appropriate classification considering new risks, regulatory bodies should effectively consider new types of patient safety issues introduced by artificial intelligence and cybersecurity concerns in the classification process.

Although historically classification relies on the degree of connectivity with the human body and device placement location, classification should also consider whether patient relies on a particular device in critical medical decision-making.[175] For example, a self-service insulin monitoring system may give inaccurate or intentionally wrong dose information to a patient relying on the device. This type of directed activity, although not automatically delivering insulin via an insulin

---

Republic of China (Draft), AMCHAM CHINA, https://www.amchamchina.org/uploads/media/default/0001/05/b78e2db2b147c09b8430b6bd55f81bc8299ea50f.pdf (establishing broad cybersecurity requirements to critical infrastructure operators including health care). It is still unclear under what circumstances these requirements could apply to health or medical device manufacturers.

[174] *See supra* Part II and accompanying notes (describing medical device definitions and classifications under both legal frameworks).

[175] *See* Price 2, supra note 11, at 450 (describing how devices are classified as a default Class II as a matter of law and medical algorithms might likely be classified higher than average consumer health algorithms). Higher classification would, no doubt, force more focused attention on AI-enabled devices. However, the reliance on substantial equivalence (and deferential classification as such by the FDA) might avoid these higher classifications.

pump, might cause a similar patient injury risk as a device that automatically delivers insulin. Similarly, a medical navigation system partially or fully automating cardiovascular mapping with AI could provide inaccurate information leading to downstream surgical complications. Lower classification devices can and likely will "do substantial mischief" without interfacing directly with the body.[176] Considering a more adaptive approach to classification could prevent potential serious safety issues with less invasive devices.

The device clearance process must evolve to meet changing cybersecurity and AI safety concerns. In the U.S., it is fair to assume that panel review has improved reviews by concentrating scientific knowledge for a particular set of devices. However, with increased reliance on technological innovation, panel reviews will not likely address specific cybersecurity or AI risks introduced through backend infrastructures. Regulators should consider alternative checkpoints or reviews to ensure infrastructure receives the same or similar review as the primary medical device attachment interfacing with the patient directly. The National Institute of Standards and Technology (NIST) has established multiple standards that the FDA could leverage for reviewing medical device cybersecurity and AI safety, such as NIST Cybersecurity Framework and future outcomes from the National Science and Technology Council's National Artificial Intelligence Research and Development Strategic Plan.[177]

The FDA's current Pre-Market Guidelines on cybersecurity could be tremendously useful with validation and enforcement, and further development on additional guidelines (with associated compulsory implementation) could improve results.[178] Although Type II 510(k) submissions should consider the cybersecurity guidelines, reviewing bodies should require additional evidence of program implementation and validate guideline implementation, absent specific requirements. Similarly, the PMA process should fully evaluate design plans, testing procedures, and clinical outcomes specific to cybersecurity activities, such as requiring completion of quarterly independent penetration testing and

---

[176] *Id.* at 460.

[177] NAT'L INST. FOR STANDARDS & TECH., FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY (Feb. 12, 2014), https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf; NAT'L SCI. & TECH. COUNCIL, EXEC. OFFICE OF THE PRESIDENT, THE NATIONAL ARTIFICIAL INTELLIGENCE RESEARCH AND DEVELOPMENT STRATEGIC PLAN (Oct. 2016), https://www.nitrd.gov/PUBS/national_ai_rd_strategic_plan.pdf. *See generally* NAT'L INST. FOR STANDARDS & TECH., SECURITY AND PRIVACY CONTROLS FOR FEDERAL INFORMATION SYSTEMS AND ORGANIZATIONS, (Apr. 2013), http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf (explaining industry standard cybersecurity requirements).

[178] Pre-market guidelines could be enhanced further with specific medical device cybersecurity requirements. *See, e.g.*, Browning, *supra* note 17, at 650–54 (describing various technologies that reduce cyberattack risk); Simshaw et al., *supra* note 61, at 58 (positing an expansion of 'premarket review or other proactive process' for robotics application). It should be noted that the FDA developed the Pre-Market Guidelines after a U.S. Government Accountability Office (GAO) report identifying substantial FDA gaps regarding known cybersecurity issues. *See* Wellington, *supra* note 12.

submitting these records prior to acceptance. The PMA process could also appoint a machine learning or AI expert, in lieu of formal pre-market guidelines on AI, to validate unsupervised or supervised learning environments used in medical device production environments.[179]

The E.U. has set the stage for these reviews by directly addressing the movement towards software and has an opportunity to build on this recognition through explicit software reviews. Further, the applicability of the clinical evaluation to all device classes provides an opportunity to address latent cybersecurity and artificial intelligence safety issues in all devices. However, the lack of specific evaluator requirements in the CE Mark process may reduce the efficacy of this process.[180] The E.U. has an opportunity to establish required qualifications for evaluators reviewing software, including evaluation based on the ISO 27001 information security framework and future ISO AI developments.[181] The EC might also consider developing Guidelines associated with the MDD and consistent with the Network and Information Security Directive to streamline compliance for manufacturers.[182]

B. Substantial Equivalence

Manufacturers rely on substantial equivalence heavily for device clearance, and with good reason. When substantial equivalence reduces disclosure, testing, and clinical obligations, especially for newly marketing products, there is built-in incentive for manufacturers to describe medical devices as merely improvements on previously submitted devices.[183] The E.U. appears to have anticipated that manufacturers may attempt to "game the system" and has therefore established more granular considerations for conducting additional clinical evaluations.

---

[179] The FDA has begun to anticipate AI challenges, but has not yet established formal procedures for evaluating AI technologies. One important step, creating guidance on clinical decisional applications using algorithms, unfortunately does not anticipate how machine learning applications will actually be used and does not address how cybersecurity plays into decisional support. *See* Brian Edwards, *FDA Guidance on Clinical Decision Support: Peering Inside the Black Box of Algorithmic Intelligence*, CHILMARK RESEARCH (Dec. 19, 2017), https://www.chilmarkresearch.com/fda-guidance-clinical-decision-support/. For example, requiring a manufacturer to disclose the inputs used to generate the recommendation may be impossible if a machine learning utility created the algorithm from vast data sets and the algorithm is too complex for a human to ascertain.

[180] *See* Eur. Comm'n, *Guidance* (2010), *supra* note 114.

[181] *See generally* APPROVAL OF HEALTH DATA HOSTS, *supra* note 142 (describing new certification requirements for health services operating in France, including ISO 27001 certification). This same certification process could be extended to lab environments or operators. *See* Price 2, supra note 11 at 461.

[182] *See infra*, Part III (E) and accompanying notes. The EC should make explicit whether the MDD and Network and Information Security Directive both apply to medical device manufacturers as critical infrastructure operators.

[183] It is remarkable that many of these improvements will independently merit new patents for utility improvements, but pass as substantially equivalent as medical devices. Although the Author does not expect a radical shift in legal interpretation, she urges regulators to consider how substantial changes in technical infrastructure might dramatically affect patient safety and closely scrutinize substantial equivalence proposals.

However, the E.U. could build on these considerations by more explicitly using infrastructure, cybersecurity, or AI examples in their Guidelines. The U.S., for its part, could require disclosure of information on changes to backend infrastructure in the 510(k) for substantial equivalence submissions.

In the U.S., the FDA should consider proposed models that more effectively manage device safety and efficacy throughout its lifecycle. The Committee on Public Health Effectiveness of the FDA 510(k) Clearance Process (CPHE) previously recommended opportunities for 510(k) improvements, including greater reliance on scientific research and more robust pre- and post-market regulation.[184] A greater focus on scientific research and post-market regulation could improve monitoring of device changes due to AI utility evolution and device performance. The inherent nature of AI functionality always changing would likely enhance post-market regulation activities and efforts by improving functionality and avoiding safety issues, so long as data used has not been subject to unauthorized change or cyberattack.

C. Component Review and Device Integration

In the U.S. and E.U., components require previously established clearance, or the manufacturer must include components in their submission processes. In the E.U., as in the U.S., manufacturers can submit components as standalone devices, which likely results in a Class III device evaluated without backend system components while backend system components are likely evaluated under Class I requirements.[185] Unfortunately, this model of component management fails to provide holistic device review that should anticipate AI risks.

The FDA has established cybersecurity and software guidelines for components and off-the-shelf software, which encourages manufacturers to review components from this perspective.[186] However, cybersecurity measures only protect systems as-implemented. Manufacturers, therefore, cannot ascertain the rigor of controls in a vacuum and must evaluate the system holistically.

Regulators should consider requiring holistic evaluation of medical devices that include digital connectivity components: internet connectivity, backend infrastructure, and AI utilities. This type of new evaluation would certainly

---

[184] *See* Swanson, *supra* note 122, at 152–53, 155. The CPHE emphasized focus on post-market activities. Another model includes Comparative Effectiveness Research (CER), which includes comparing alternative treatments against one another. *Id.* at 160–61. For AI-enabled devices, this could entail performance considerations, such as speed to decision, learning rate, or program adaptability.

[185] *See* Eur. Comm'n, *Guidance* (2010), *supra* note 114.

[186] *See* U.S. Food & Drug Admin., Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices (May 11, 2005), https://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm089543.htm; U.S. Food & Drug Admin., Guidance for Industry—Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software (Jan. 14, 2005), https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm077823.pdf.

identify more upfront engineering and configuration issues and ensure design, as implemented, reduces potential patient safety issues.

D. Ongoing Management[187]

Despite upfront due diligence and enhanced clearance processes, cybersecurity and AI safety concerns will likely arise for marketed devices. The FDA issued the Postmarket Management of Cybersecurity in Medical Devices Guidelines in 2016, which describe ongoing obligations (in non-binding form) to anticipate ongoing cybersecurity threats, evaluate vulnerabilities, appropriately patch systems, and effectively anticipate patient safety risks.[188] Although these guidelines do not include independent AI considerations, the model could be leveraged to establish ongoing manufacturer responsibilities, assuming the guidelines incentive model effectively changes manufacturer behavior.[189] The FDA should consider approaches to encourage adherence or otherwise validate the existence of programmatic capabilities for post-market management in the submission process. The E.U. could also benefit from a similar set of Guidelines for post-market activities.

Devices leveraging AI capabilities will likely require a new model for clinical testing and ongoing management. Regulators should consider requiring ongoing QMS activities outside standard cybersecurity monitoring activities specifically related to AI functionality, similar to how the FDA has approached its Expedited Access Pathway (EAP) program to some extent.[190] In EAP, the FDA accepts less stringent upfront testing while requiring more postmarket controls. Although for AI it is critically important to have properly configured infrastructure to ensure accuracy in algorithmic calculation, a pre-classification followed by more rigorous postmarket controls could work for AI-enabled devices. Examples of postmarket controls could include self-monitoring AI utilities to identify unauthorized

[187] Although not explored within this Article, instructions for use may become increasingly important for both healthcare customers and patients, as well as disclaimers, warnings, and other instruction-like communications. Cybersecurity requirements rely in part on network connectivity, such as a hospital network, an individual's home wireless network, or a cellular connection. *See* Browning & Tuma, *supra* note 17, at 643. Regulatory agencies may consider requiring instructions when safety depends heavily on installation, regardless of classification. In the E.U., Class I and Class II devices do not require instructions for use, if they can be used "safely without any . . . instructions," though today safety determination does not generally include network installation considerations. *See* Eur. Comm'n, *Guidance* (2010), *supra* note 114, at 6.

[188] *See* Browning & Tuma, *supra* note 17, at 676–77. The FDA has attempted to create incentives for complying with post-market guidance by relaxing urgent reporting requirements. However, after one year in use, questions still remain as to whether an incentive-based model sufficiently generates compliant activity. The FDA repeatedly acknowledges that the direction given in post-market guidance is non-binding. *See* Woods, *supra* note 66, at 433. Non-binding guidance, however, leaves manufacturers questioning compulsory activities and allows the FDA to establish an indefinite position. *See* Swanson, *supra* note 122, at 133.

[189] Browning & Tuma, *supra* note 17, at 676–77; *see* Swanson, *supra* note 122, at 133–34.

[190] *See* Price 2, supra note 11, at 463.

changes or routinely validating previously established range values to ensure AI utilities do not change previously established tested "safe" operation ranges.

Postmarket surveillance should be compulsory for AI-enabled devices, specifically due to the frequent changes to these devices and the substantial risks associated with cyberattacks on connected devices. Ongoing, manufacturers should also ensure that the device, as cleared, has not changed so substantially it no longer performs within approved operating standards and reapply for clearance when a device exceeds these standards.

E. Collaborative Efforts and Omnibus Laws

At the time of writing, the U.S. has not established any broad, omnibus baseline requirements for operating or protecting new technologies, although Congress has specifically tasked NIST to develop standards for cybersecurity and emerging technologies.[191] The FDA could explicitly reference NIST standards in future AI guidelines, review adherence to NIST cybersecurity standards in the clearance process, collaborate with NIST to develop medical device-specific requirements, or leverage NIST expertise in device clearance reviews until such expertise resides in the FDA.

The E.U. has established omnibus laws, but these laws also pose more questions for manufacturer compliance. It is unclear, for example, whether the NIS critical infrastructure, by definition, applies to health device manufacturers or mainly health care providers. The European Commission should clarify regulatory application with respect to the GDPR, NIS, and MDD, and collaborate to develop medical device guidelines that also meet GDPR and NIS requirements while addressing AI considerations.

Conclusion

Manufacturers are already using big data infrastructures and AI utilities to develop revolutionary medical devices. Without more attention to medical device clearance and ongoing management, patients will likely suffer the consequences. Although the FDA's FD&C Act and the E.U.'s MDD legal frameworks have historically managed device safety risks, new technologies pose new challenges for existing risk principles. By embracing change and developing effective frameworks, the U.S. and E.U. will enable the use of transformative technologies while simultaneously protecting patients of the future.

[191] E-Government Act of 2002, P.L. 107–347 (2002), 116 Stat. 2900.