REGULATING HEALTHCARE ROBOTS: MAXIMIZING OPPORTUNITIES WHILE MINIMIZING RISKS

Drew Simshaw,* Nicolas Terry,** Dr. Kris Hauser,*** Dr. M.L. Cummings****

Cite as: Drew Simshaw et al., *Regulating Healthcare Robots: Maximizing Opportunities While Minimizing Risks*, 22 RICH. J.L. & TECH. 3 (2016), http://jolt.richmond.edu/v22i2/article3.pdf.

I. INTRODUCTION

[1] Some of the most dynamic areas of robotics research and development today are healthcare applications.[1] Robot-assisted surgery,[2]

* Clinical Teaching Fellow, Georgetown Law, Institute for Public Representation—Communications & Technology section; J.D., Indiana University Maurer School of Law, 2012; B.A., University of Washington, 2007. The author thanks the participants of the We Robot 2015 conference, held on April 10, 2015 in Seattle, for their thoughtful comments on this paper.

** Hall Render Professor of Law & Executive Director, Hall Center for Law and Health Indiana University Robert H. McKinney School of Law; LL.M. University of Cambridge, 1977; B.A. (Hons. Law). Kingston University, 1975.

*** Associate Professor, Electrical & Computer Engineering, Duke University Pratt School of Engineering; Ph.D., Stanford University, 2008; B.A., University of California at Berkeley, 2003.

**** Associate Professor, Mechanical Engineering and Material Sciences, Duke University Pratt School of Engineering; Ph.D., University of Virginia, 2004; M.S., Naval Postgraduate School, 1994; B.S., U.S. Naval Academy, 1988.

[1] *See generally Healthcare Robotics: 2014*, ROBOTICS BUS. REV. (July 14, 2014), http://www.roboticsbusinessreview.com/research/report/healthcare_robotics_2014, *archived at* perma.cc/2XSV-JMXJ ("To support, enhance, and mitigate the healthcare burdens, our healthcare system is witnessing robotic medical technology entering hospital surgical suites, in-patient rooms, in-home patient care, and uses with emergency services and vehicles.").

robotic nurses,[3] in-home rehabilitation,[4] and eldercare robots[5] are all demonstrating rapidly iterating innovation. Rising healthcare labor costs and an aging population will increase demand for these human surrogates and enhancements. However, like many emerging technologies, robots are difficult to place within existing regulatory frameworks. For example, the federal Food, Drug, and Cosmetic Act (FD&C Act) seeks to ensure that medical devices (few of which are consumer devices) are safe, the HIPAA Privacy and Security Rules apply to data collected by health care providers (but not most consumer-facing hardware or software developers), and state licensing statutes oversee the conduct of doctors and nurses who, heretofore, have all been human beings.

[2] This paper will focus on the issues of patient and user safety, security, and privacy, and specifically the effect of medical device regulation and data protection laws on robots in healthcare. First, it will

[2] *See generally* John Markoff, *New Research Center Aims to Develop Second Generation of Surgical Robots*, N.Y. TIMES (Oct. 23, 2014), http://www.nytimes.com/2014/10/23/science/new-research-center-aims-to-develop-second-generation-of-surgical-robots.html?_r=0, *archived at* https://perma.cc/VT6V-L7KY (describing the University of California, Berkeley's new "research center intended to help develop medical robots that can perform low-level and repetitive surgical tasks, freeing doctors to concentrate on the most challenging and complex aspects of the operations they perform").

[3] *See generally Robotic Nurse Assistant*, HEALTHCARE ROBOTICS GA. INST. OF TECH. http://www.hsi.gatech.edu/hrl/project_nurse.shtml, *archived at* https://perma.cc/S3W2-23TG (last visited Nov. 24, 2015) (describing the ways in which "robotics can play a role in assisting nurses to complete their daily tasks in order to provide better healthcare," and the University's Healthcare Robotics Lab's "Direct Physical Interface" project).

[4] *See generally Rehabilitation Robotics*, CHARM LAB, http://charm.stanford.edu/Main/RehabilitationRobotics, *archived at* https://perma.cc/MHY5-A4FF (last visited Nov. 24, 2015) (describing rehabilitation robotics projects, including "Robotic Manipulation for Reaching" and "HAPI Bands: Haptic Augmented Posture Interface").

[5] *See generally* Will Knight, *Your Retirement May Include a Robot Helper*, MIT TECH. REV. (Oct. 27, 2014), http://www.technologyreview.com/news/531941/your-retirement-may-include-a-robot-helper/, *archived at* https://perma.cc/QJ36-ZQ8N (stating "robotics companies are eyeing elder care as a huge potential market").

examine the demand for robots in healthcare and assess the benefits that robots can provide. Second, it will look at the types of robots currently being used in healthcare, anticipate future innovation, and identify the key characteristics of these robots that will present regulatory issues. Third, it will examine the current regulatory framework within which these robots will operate, focusing on medical device regulation and data protection laws.

[3] A serious definitional problem confronts any such mapping of emerging technologies to existing regulatory systems. This is certainly the case with healthcare robots. For example, many interesting legal or policy issues arise surrounding the use of teleoperated robotics systems (e.g. surgical robots directly controlled by a surgeon). However, this paper focuses on existing and emerging robots with far greater levels of autonomy.[6] Such autonomy includes the supervisory control paradigm, in which certain functions are automated with a human supervising the system, all the way to fully autonomous robots.[7] Similarly, health care environments that are reliant on or dominated by all-purpose "healthcare companions" and robotic "doctors," utilizing artificial intelligence, will raise fascinating questions. However, these technologies will not be available for purchase or be deployed in our hospitals any time soon. Further, when they are, they will not have come out of nowhere, catching patients or consumers by surprise. Rather, this paper concentrates on near term issues. Even absent the stuff of science fiction, the first several generations of healthcare robots will themselves pose challenging issues. Robots in healthcare will be an evolution in the coming decades, and there are basic questions that need to be addressed in this nearer future in order to ensure that robots are able to maintain sustainable innovation with the

[6] Whereas most medical devices, and many currently deployed robots, represent automatic systems that act according to a preprogrammed script with defined entry and exit conditions for a task, this paper will focus on the unique implications of autonomous robots, which independently and dynamically determine if, when, and how to execute a task.

[7] By autonomous, we mean robots that have the ability to reason and take actions on their own without explicit approval from a human.

confidence of providers, patients, consumers, and investors. Only through such responsible design, deployment, and use will robots' potential be maximized in healthcare.

[4] Because we are likely to see health-related robots appearing in both conventional healthcare and consumer spaces, there will be regulatory disruption and the opportunity for regulatory arbitrage.[8] We argue the regulation of both spaces must change. In order to maximize robots' potential and minimize risks to users, regulation will need to move towards some form of premarket review of robot "safety." Such review, likely by the Food and Drug Administration (FDA), should include broad considerations of potential harms, including security. In the data protection sphere, existing sector-based limitations that lead to gaps between, for example, Federal Trade Commission (FTC) and Department of Health and Human Services' Office for Civil Rights (HHS-OCR) oversight, should be eliminated so that both patient and consumer privacy and security interests can be better protected. A foundational regulatory framework for both medical devices and consumers that is attuned to safety, security, and privacy will help foster innovation and confidence in robotics and ensure that we maximize robotic potential in healthcare.

II. ROBOTS IN HEALTHCARE: DEMAND AND BENEFITS

[5] Much of the demand for robots in healthcare stems from their ability to perform tasks that human beings either cannot do, do not wish to do, or cannot do as well or as efficiently. Efficiency is critical in both the hospital and home healthcare settings, as evidenced by strained hospital staffs[9] and a shortage of home caregivers.[10] An aging population logically

[8] *See infra* note 48 and accompanying text.

[9] *See, e.g.*, Christopher J. Gearon, *Staffing the Hospital of Tomorrow*, U.S. NEWS & WORLD REP. (Oct. 16, 2013, 12:15 PM), http://health.usnews.com/health-news/hospital-of-tomorrow/articles/2013/10/16/staffing-the-hospital-of-tomorrow, *archived at* https://perma.cc/G63A-5J8F ("Hospital staffing changes are driven by an aging population, a physician workforce shortage and health care reform.").

increases this demand. Worldwide, people are simply living longer. According to the United Nations, the world population over the age of 60 has tripled over the last 50 years, and is expected to triple again to 2 billion by 2050.[11] This trend will greatly impact the home care sector, as evidence demonstrates a desire among older populations to stay in the home, as opposed to living in a care facility.[12] But professional home care workers are in such high demand that their lack of qualifications and training are often overlooked.[13] Effectively designed robots could help meet this demand in a safer and more responsible, sustainable manner.

[6] Robots might also help meet demand for services created by the overall rising cost of healthcare, particularly its labor costs. Although there is some debate surrounding the long-term cost effectiveness of robots, the ability of robots to expand healthcare services outside the traditional healthcare setting could relieve current strains on hospital resources. In

[10] *See* Barbara Peters Smith, *Finding skilled elder home care workers not easy*, HERALD-TRIB. (May 26, 2013, 3:30 PM), http://www.heraldtribune.com/article/20130526/ARTICLE/130529745/-1/sports?Title=NEW-Finding-skilled-elder-home-care-employees-not-easy, *archived at* https://perma.cc/2B22-2YYZ [hereinafter *Finding skilled elder home care*].

[11] *See* U.N. DEP'T OF ECON. & SOC. AFFAIRS, POPULATION DIV., WORLD POPULATION AGEING 1950-2050, at 11, U.N. Doc. ST/ESA/SER.A/207, U.N. Sales No. E.02.XIII.3 (2002), https://web.archive.org/web/20150122071228/http://www.un.org/esa/population/publications/worldageing19502050/pdf/80chapterii.pdf, *archived at* https://perma.cc/474X-VTEA.

[12] *See* Barbara Peters Smith, *Nation at crossroads in home care for elders*, HERALD-TRIB. (May 25, 2013, 10:48 PM), http://www.heraldtribune.com/article/20130525/ARTICLE/130529761, *archived at* https://perma.cc/ECU9-ZQCC (describing how most older Americans prefer care in their own home to institutionalization) [hereinafter *Nation at crossroads*].

[13] *See Finding skilled elder home care*, *supra* note 10 (describing "a fast-growing industry where many workers lack the training and skills needed for safe and reliable caregiving" and the fact that "the rising demand for home health care has induced more people to obtain certified nurse assistant licenses when they are not suited for the work").

addition, homecare is often less expensive than institutionalization.[14] Many believe that robots are preferable to humans in the home setting,[15] not only for their ability to outwork humans physically,[16] but also for their potential to provide emotional care and support.[17]

[7] Finally, the industry trend toward personalized healthcare may increase demand for robots.[18] Robots may be especially helpful for patients requiring rehabilitation[19] and for those with special needs.[20]

[14] *See Nation at crossroads, supra* note 12.

[15] *See* Jason Maderer, *How Would You Like Your Assistant- Human or Robotic?*, GA. TECH. NEWS CENTER (Apr. 29, 2013), http://www.news.gatech.edu/2013/04/29/how-would-you-your-assistant-human-or-robotic, *archived at* https://perma.cc/C3D7-JW9E.

[16] *See e.g.*, *New SF Hospital Feels Like the Jetsons*, YOUTH HEALTH (Feb. 1, 2015), http://www.youthhealthmag.com/articles/8602/20150201/ucsf-mission-bay-hospital-robots-in-healthcare-robots-in-hospitals-aethon-robots-aethon.htm, *archived at* https://perma.cc/25GY-R3DK ("Each of the robots can also carry as much as 1,000 pounds of objects and travel for twelve miles a day.").

[17] *See* Barbara Peters Smith, *Robots and More: Technology and the Future of Elder Care*, HERALD-TRIB. (May 27, 2013), http://www.heraldtribune.com/article/20130527/ARTICLE/130529720?p=5&tc=pg, *archived at* https://perma.cc/5GQY-7SW6 ("[Robots] can in fact be of considerable assistance in providing physical aid, and might not be that bad as an emotional companion. People, with their imaginations, can create all kinds of characteristics that we might not believe possible."); *see e.g.* PARO THERAPEUTIC ROBOT, www.parorobots.com (last visited Jan. 29, 2016).

[18] *See Notice of Updates to the National Robotics Initiative, Notice no. NOT-EB-14-008*, NAT'L INST. OF HEALTH (Oct. 23, 2014), http://grants.nih.gov/grants/guide/notice-files/NOT-EB-14-008.html, *archived at* https://perma.cc/2W2X-65Y6 ("Affordable and accessible robotic technology can facilitate wellness and personalized healthcare.").

[19] *See A Research Roadmap for Medical and Healthcare Robotics*, STAN. UNIV. (2008), http://bdml.stanford.edu/twiki/pub/Haptics/HapticsLiterature/CCC-medical-healthcare-v7.pdf, *archived at* https://perma.cc/H85L-S7JW ("Socially assistive robotics focuses on using sensory data from wearable sensors, cameras, or other means of perceiving the user's activity in order to provide the robot with information about the user that allows the machine to appropriately encourage and motivate sustained recovery exercises.").

Research in this area is underway, and will likely increase in the coming years.[21]

[8] In order to realize and sustain these benefits, robots must be designed and deployed in the healthcare setting in a manner that maximizes their safety, security, and sensitivity to user privacy. Such deployment must include taking into consideration potential security and privacy issues[22] that could, if overlooked, manifest themselves in ways that harm patients and consumers, diminish the trust of key stakeholders of robots in healthcare, and stifle long-term innovation. Understanding these risks requires an appreciation for the ways in which data are, and will be, utilized by robots in healthcare, and the regulatory landscape within which robots will operate.

[9] As Frank Tobe has said, "[t]he many stakeholders in robotic healthcare (family members and caregivers, healthcare providers, technology providers, aging or disabled individuals) all have similar goals: To provide independence, preserve dignity, empower those with special needs and provide peace of mind to all of the stakeholders."[23] Ensuring that safety, security, and privacy are promoted during the development, deployment, and use of robots in healthcare will help guarantee the long-term ability of robots to help stakeholders meet these goals.

---

[20] *See id*. ("Socially assistive robots have been shown to have promise as therapeutic tool for children, the elderly, stroke patients, and other special-needs populations requiring personalized care.").

[21] *See e.g.*, *MIT Scientists Launch Personalized Robot Project*, PHYS.ORG (Apr. 3, 2012), http://phys.org/news/2012-04-scientists-personalized-robot.html, *archived at* https://perma.cc/5W3X-435L ("This project aims to dramatically reduce the development time for a variety of useful robots, opening the doors to potential applications in manufacturing, education, personalized healthcare, and even disaster relief.").

[22] *See infra* Parts III, IV.

[23] Frank Tobe, *Where Are the Elder Care Robots?*, IEEE SPECTRUM (Nov. 12, 2012, 4:25 PM), http://spectrum.ieee.org/automaton/robotics/home-robots/where-are-the-eldercare-robots, *archived at* https://perma.cc/WCW3-6UM9.

III. ROBOT TYPES AND CHARACTERISTICS

[10] To meet demand and seize the potential benefits of robots in healthcare, research is being conducted at companies and universities, and through national and international public and private initiatives. In the United States, the National Science Foundation (NSF) partnered with other organizations in a National Robotics Initiative with National Institutes of Health (NIH) participation in its Computer Science and Robotics Research program devoted to medical robots.[24] Last year, the European Union launched SPARC, the world's largest civilian robotics program, which has a focus on healthcare.[25] But probably the most significant public and private investment in healthcare-specific robotics is taking place in Japan.[26] Given its own baby boom generation with growing needs, demand has sparked several independent research initiatives and plans for government projects.[27]

---

[24] *See* Michael S. Young, *Artificial Intelligence, Telemedicine, and Robotics in Healthcare*, 6 SCITECH LAWYER 14 (Spring 2010), http://www.fellerssnider.com/userfiles/file/MYoung%20AI%20article.pdf, *archived at* https://perma.cc/WZA8-23RU.

[25] *See About SPARC*, SPARC ROBOTICS, http://sparc-robotics.eu/, *archived at* https://perma.cc/5KP8-23ZE (last visited Jan. 29, 2016).

[26] *See* Tim Maverick, *Japan's Tech Solution for Its Aging Population*, WALL ST. DAILY (July 11, 2015), http://www.wallstreetdaily.com/2015/07/11/japan-healthcare-robots/, *archived at* https://perma.cc/J2EN-7B5B.

[27] *See* Christian Crisotomo, *Robots: Japan's Future Elderly Care Workers*, VR WORLD (Jan. 22, 2015), http://www.vrworld.com/2015/01/22/robots-japans-future-elderly-care-workers/, *archived at* https://perma.cc/J4FM-DLHE ("Japan's elderly healthcare industry can be considered as a very important testbed that would help develop better robots in the future. . . . [R]obots may soon be Japan's future elderly care workers. Japan is the country with the highest number of elderly citizens. According to reports published a few years ago, it is estimated that at least more than 20% of the population in Japan comprise of elderly people aged 65 and above. Thus, there is more focus on elderly care in Japan than any other country. In fact so much, that the country is in constant need for caregivers and nurses who would look after their *dankai no sedai* (Japanese baby boomer) population.").

[11] These initiatives have led to the deployment of a variety of robots in healthcare, and more are being designed every day. Identifying the types and characteristics of different robots in healthcare will help identify the regulatory issues that must be confronted.

[12] Perhaps the most frequently discussed robots in healthcare today are "so-called surgical robots," such as the daVinci Surgical System.[28] These systems present a number of interesting legal issues, especially involving product and practice liability.[29] However, because doctors, at least for now, directly control surgical robots, these robots more closely resemble traditional medical devices than the sort of autonomous robots that will present unique safety, security, and privacy challenges. This could change, however, as surgical robots become increasingly autonomous.[30]

[13] Another emerging robot in the hospital setting is what can be described as a "routine task" robot, such as the kind recently introduced in

[28] *Berkeley's Autonomous Surgical Robotic System*, MEDGADGET (Oct. 30, 2014), http://www.medgadget.com/2014/10/berkeleys-autonomous-surgical-robotic-system.html, *archived at* https://perma.cc/JR5N-V5RY.

[29] *See, e.g.,* Joe Carlson & Jaimy Lee, *Medical boon or bust? Suits raise allegations of defects in da Vinci robot*, MOD. HEALTHCARE (May 25, 2013), http://www.modernhealthcare.com/article/20130525/MAGAZINE/305259977, *archived at* https://perma.cc/2Y7K-ZGZU; *see also* Sulbha Sankhla, Robotic Surgery and Law in USA—a Critique, at 36–40 (June 1, 2013) (Unpublished Critique for LLM in IP Law and Policy, University of Washington), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2425046, *archived at* https://perma.cc/RZ5V-DVSP.

[30] *See Berkeley's Autonomous Surgical Robotic System*, *supra* note 28 ("While so-called surgical robots have been around for a few years now, they are really not robots at all, but rather remotely controlled machines that faithfully execute the commands of their masters. For robots to be real robots, they have to be autonomous and able to do tasks without much operator input. . . . Researchers at UC Berkeley have been working on getting a da Vinci surgical system to be smart enough to do some basic tasks on its own.").

a University of California San Francisco (UCSF) hospital.[31] The UCSF robots were deployed in order to "bring meals and medications to patients, transfer lab specimens, and carry linens," and each can "carry up to 1,000 pounds and travel twelve miles a day."[32] These essentially custodial robots are more autonomous and mobile, but not necessarily anthropomorphic or social. Their appeal lies in the fact that they can perform simple, routine tasks in order to free up human staff to perform the more "core functions" of healthcare.[33] Although these robots' tasks are "routine" now, they have the potential to begin taking on medical or caregiving tasks as their development advances.

[14] The most significant regulatory issues, though, could arise with "personal care" robots in the hospital and home healthcare settings. By their very nature, these robots will operate in increasingly autonomous and life-like ways, eventually performing actual care on patients and consumers. Someday, they may work alongside—or even replace—nurses, home care workers, and even doctors. There is already an emergence of rehabilitation robots in hospitals and general personal "assistant" or "care" robots in the home. As these robots begin to take on more medical tasks and caregiving functions, their potential to benefit society will depend in part on responsible design and use that accounts for safety, security, and privacy. Issues will arise in these areas as a result of several key characteristics of robots in healthcare.

[15] First, robots in the healthcare setting are performing an increasing number of functions, which will only continue to grow in number.[34] Such

[31] *See New SF Hospital Feels Like the Jetsons*, *supra* note 16.

[32] *Id.*

[33] *See id.*

[34] *See* Jessica Cocco, Note, *Smart Home Technology for the Elderly and the Need for Regulation*, 6 J. ENVTL. & PUB. HEALTH L. 85, 92–95 (2011), http://pjephl.law.pitt.edu/ojs/index.php/pjephl/article/view/56/44, *archived at* https://perma.cc/WRR3-4NGV (explaining the difference between passive and active-

functions include providing medication assistance, helping move patients, and communicating with doctors. As robots in healthcare access or connect with other devices, their functionality increases in complexity and variety.[35] With advancements in artificial intelligence and the ability to share and access vast amounts of data in the cloud, robots may someday be relied upon to make actual on-the-spot medical decisions, and be able to act on those decisions, such as administering medications. As a result, robots in healthcare are becoming increasingly autonomous in terms of both mobility and decision-making abilities.

[16] In addition, the data collection, processing, storing, and use of information by robots in healthcare are all vast compared to that of other medical devices.[36] When considering how best to handle data, it is important to consider both data that are *necessary* for the robot to function properly (including navigation, object recognition, etc.), and data that are *desirable* and will help robots maximize opportunities and fulfill specific medical and healthcare goals of doctors, patients, and consumers.

[17] Shifting from a general consumer setting to a healthcare-specific context, either in the hospital or the home, both especially unstructured environments, will increase the importance of a robot knowing and

intervention devices, and noting that robots resemble all three versions of active-intervention devices—sensors, reminder systems, and medication assistance).

[35] *See* ERICA PALMERINI ET AL., ROBOLAW: GUIDELINES ON REGULATING ROBOTICS 175 (Sept. 22, 2014), http://www.robolaw.eu/RoboLaw_files/documents/robolaw_d6.2_guidelinesregulatingrobotics_20140922.pdf, *archived at* https://perma.cc/783Z-YQ2U (explaining that personal care robots "will not be developed by implementing a single functioning (as in the case of robotic prosthesis)" and "could mutate function and form") [hereinafter ROBOLAW].

[36] *See generally* Christopher Prentice, *Technology in Healthcare Makes Evidence-based Medicine more Achievable with Automated Data Collection*, CIOREVIEW, http://robotics.cioreview.com/cxoinsight/new-technology-in-healthcare-makes-evidencebased-medicine-more-achievable-with-automated-data-collection-nid-6019-cid-75.html, *archived at* https://perma.cc/8ZKX-KFAZ (last visited Feb. 2, 2016).

possibly sharing the location of medication, objects, and people[37]—all especially critical to a robot's ability to effectively aid in treatment and care.

[18] In its 2014 *Guidelines on Regulating Robotics*, European research group RoboLaw acknowledged that the needs of the elderly have created demand for complex services that require networked robots, or "a group of autonomous mobile systems that exploit wireless communications with each other or with the environment and living systems in order to fulfill complex tasks."[38] Many of these features will necessitate complex data collection and use practices, which, given the uniqueness of robots and sensitivity of health-related information, will raise significant security and privacy issues.

IV. THE DISTINCTIVE FEATURES OF ROBOT DATA COLLECTION AND USE

[19] In light of their potential benefits, the complexity of robot data collection and use practices raise potential security and privacy issues in the healthcare setting.[39] The future healthcare robot will be able to monitor patients closely at all hours (one of their advantages over humans), and

[37] *See* Evan Ackerman, *Hoaloha Robotics Developing Socially Assistive Hardware Platform*, IEEE SPECTRUM (Sept. 4, 2013, 2:36 PM), http://spectrum.ieee.org/automaton/robotics/home-robots/hoaloha-robotics-developing-socially-assistive-hardware-platform, *archived at* https://perma.cc/B9MJ-4YFL (quoting Hoaloha Robotics: "Our robot has the benefit of knowing if a user is nearby and if the user is currently looking at the robot and for how long. It also tracks when the last conversation was, what it was about, and the history of other conversations with this user at this time of day.").

[38] ROBOLAW, *supra* note 35, at 169.

[39] *See, e.g.*, *id.* at 177 (Policy considerations include the fact that "[d]iagnostic, monitoring tools or any other device can be placed on board robots, thus gathering data on their environment and people." Further, "[t]hese data could be shared with other platforms even on a global basis . . . Thus, legal questions about data security and privacy issues need to be addressed.").

report information back to various health information technologies, other robots, and even human providers. Such data collection and use will increase in volume and complexity in both the hospital and home settings as medical devices begin taking on more autonomous functions and as personal consumer robots perform more healthcare tasks. These practices are distinguishable from other data actors because of the necessary access such robots will need to existing user information, the generation of new information, and the unprecedented resulting overall information they will possess about users.[40] Robots, even more than other technologies, will depend on connecting to other devices, including wearables and personal cell phones, for optimal information access and performance.[41] This is especially true in the healthcare context, where wearables and mobile applications increasingly collect health and wellness related information about users.[42] At the 2015 Consumer Electronics Show, Adam Thierer noted that "we can expect [personal care robots] to be fully networked, data-collecting machines that will know as much about us as any human caregiver, [and] possibly much more."[43]

---

[40] *See, e.g.*, *id.* at 189 (explaining that privacy risks with personal care robots "would be greater than the limitation of privacy caused by the 'Granny Cam' monitoring systems adopted in nursing homes" because "[t]he personal data are likely to be particularly sensitive as they pertain to the health of individuals, their life choices, political, philosophical and religious beliefs, sexual habits, etc. and this could eventually lead to a real 'death of privacy'").

[41] *See id.* at 169 ("In such systems, sensor networks and other intelligent agents, for example wearable and personal devices, extend the sensing range of the robots and improve their planning and cooperation capabilities.").

[42] *See* Harry Rhodes, *Accessing and Using Data from Wearable Fitness Devices*, 85 J. AHIMA 48 (Sept. 2014), http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_050743.hcsp?dDocName= bok1_050743, *archived at* https://perma.cc/K629-UX3A.

[43] Adam Thierer, *CES 2015 Dispatch: Challenges Multiply for Privacy Professionals, Part Two*, PRIVACY PERSPECTIVES (Jan. 14, 2015), https://iapp.org/news/a/ces-2015-dispatch-challenges-multiply-for-privacy-professionals-part-two/, *archived at* https://perma.cc/2U6B-GKCV (emphasis removed).

[20] Robots in healthcare will need to generate, use, and sometimes share a tremendous amount of data to function in the chaotic and unstructured hospital and home environments. Eventual ubiquity of robots in healthcare may lead to the use of cost effective "cloud robotics," outsourcing much of the robots' processing to remote servers where they can learn from the experiences of other robots and draw from databases for tasks such as object recognition.[44] The consumer setting may prove to be a catalyst for the development of cloud robotics and a consumer market for such technology.[45]

[21] Healthcare providers will not be alone in making sure robots function properly and perform desirably in the healthcare setting. Robot complexity will increasingly bring developers, technicians, and data service providers into physical healthcare settings. These actors each bring their own data use practices and potential vulnerabilities into the healthcare environment.

[22] Privacy and security challenges will be further magnified if, instead of just accessing *information* from other devices, robots actually physically merge with other devices. RoboLaw explains that personal care robots "could mutate function and form by inserting or removing other electronic devices (smart phones, tablets, etc.) and various ambient-assisted living tools (including equipment for diagnostics, monitoring and control). This thus involves a mass of personal information that should be protected."[46]

[23] The pace at which robots are being developed and adopted could risk marginalizing certain security and privacy considerations if proper attention is not paid at all stages of design, deployment, and use. As

[44] *See* Andrew Proia, Drew Simshaw & Kris Hauser, *Consumer Cloud Robotics and the Fair Information Practice Principles: Recognizing the Challenges and Opportunities Ahead*, 16 MINN. J.L. SCI. & TECH. 145, 153 (2015).

[45] *See id.* at 149.

[46] ROBOLAW, *supra* note 35, at 175.

robotics in healthcare advances, it will be important to constantly reexamine existing and emerging data practices, to evaluate the ways and by whom data will be collected, processed, stored, and used, and to gauge the awareness of roboticists and manufacturers when it comes to the resulting regulatory challenges, outlined below.

V. THE CURRENT REGULATORY FRAMEWORK

[24] Indeterminacy as to the application of regulatory models, or just unsubtle gaps in regulation, causes regulatory turbulence. In the short term, a lack of effective regulation can lead to harms, be they physical or informational. Indeterminacy can also cause markets to fail with manufacturers or consumers electing to "sit out" in light of the confusion. In the medium or longer term, real or perceived harms may lead to regulatory "patches," which may under-regulate out of fear of stifling innovation.[47] Regulators may also under-regulate by making a category error, regulating with inapt rules or the "wrong" agency. The most serious episodes of turbulence can lead to regulatory disruption (and considerable consumer or patient harms) or regulatory arbitrage whereby providers or sellers migrate to the least regulated domains.[48] Likely the most pressing issues involving the regulation of robots in healthcare will be device regulation and data protection.

A. Device Regulation

[25] There is no doubt that some current and future health care robots are or will be subject to regulation by the FDA as "medical devices."

[47] *See* Joe Harpaz, *How Regulation Stifles Technological Innovation,* DAILY RECKONING (May 6, 2014), http://dailyreckoning.com/how-regulation-stifles-technological-innovation/, *archived at* https://perma.cc/NRC4-M9WQ.

[48] *See generally* Nicolas P. Terry, Chad S. Priest & Paul P. Szotek, *Google Glass and Health Care: Initial Legal and Ethical Questions*, 8 J. HEALTH & LIFE SCI. L. 93, 93 (2015) (discussing the legal issues, such as privacy and the necessary compliance with the Health Insurance Portability and Accountability Act, with the use of Google Glass in the healthcare setting).

Devices subject to such regulation are broadly defined as any

> instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, or other similar or related article, including any 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, in man or other animals, or . . . intended to affect the structure or any function of the body of man or other animals.[49]

These medical devices are subject to safety regulations enforced by the Center for Devices and Radiological Health.[50] Crucially, such devices are subject to premarket review if they are being marketed for the first time, if a new intended use is proposed, or if changes are made to the devices that could significantly affect safety or effectiveness.

[26] Some currently regulated medical devices may begin to display autonomous or semi-autonomous characteristics. For example, robotic surgical systems designed to perform independently of physicians[51] or the semi-autonomous Sedasys anesthesiology machine.[52] These systems will likely continue to be regulated as medical devices as they evolve. Less

[49] Federal Food, Drug, and Cosmetic Act § 201(h), 21 U.S.C. § 321 (2014).

[50] *See About the Center for Devices and Radiological Health*, U.S. FOOD & DRUG ADMIN., http://www.fda.gov/AboutFDA/CentersOffices/OfficeofMedicalProductsandTobacco/CDRH/, *archived at* https://perma.cc/3B4N-MHZY (last visited Feb. 2, 2015).

[51] *See Berkeley's Autonomous Surgical Robotic System*, *supra* note 28 ("Researchers at UC Berkeley have been working on getting a da Vinci surgical system to be smart enough to do some basic tasks on its own.").

[52] *See* Todd C. Frankel, *New machine could one day replace anesthesiologists*, WASH. POST (May 11, 2015), http://www.washingtonpost.com/business/economy/new-machine-could-one-day-replace-anesthesiologists/2015/05/11/92e8a42c-f424-11e4-b2f3-af5479e6bbdd_story.html, *archived at* https://perma.cc/X6TW-Y7U6.

clear, however, is how the FDA will treat more custodial robots that initially perform only "routine tasks," but slowly begin taking on more or ministerial healthcare tasks. Similar questions will arise as personal consumer robots in the home perform an increasing number of tasks that could be considered medical.

[27] Robotics is not the only emerging healthcare technology. Similar issues of regulatory turbulence, even disruption, are posed by the growth of mobile platforms, medical apps, and wearables.[53] Overlapping questions arise between these technologies and robotics, including the migration of "professional" medical technologies such as sensors and analytical software into consumer space, the shock to consumer or patient expectations as their medical information leaves the safety of the HIPAA-policed domain to a HIPAA-free zone, and the likelihood that medical apps will become increasingly smarter until their diagnostic prowess begins to look suspiciously like the "practice of medicine."

[28] Therefore, to understand which robots will be regulated as medical devices, it is helpful to examine the FDA's guidance on its regulation of mobile medical applications.[54] First released in 2013, this nonbinding guidance on "mHealth apps" took a risk-based approach to regulation of these emerging technologies.[55] The agency limited its scrutiny to "only those mobile apps that are medical devices and whose functionality could pose a risk to a patient's safety if the mobile app were to not function as intended."[56] Accordingly, the FDA will not regulate low risk apps that

[53] *See generally* Nicolas Terry, *Mobile Health: Assessing the Barriers*, 147 CHEST J. 1429–34 (May 2015).

[54] *See generally Mobile Medical Applications: Guidance for Industry and Food and Drug Administration Staff*, U.S. FOOD & DRUG ADMIN. (Feb. 9, 2015), http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM263366.pdf), *archived at* https://perma.cc/2LUN-KWQA (expressing the FDA's current thinking on regulation of mobile medical applications and devices).

[55] *See id.* at 4.

[56] *Id.* at 4.

only coach, prompt, or help patients communicate with providers, nor will it regulate apps that serve as "fitness trackers" or "wellness coaches."[57] The agency will regulate apps that act as substitutes for existing medical devices, but these apps will likely only require a premarket submission establishing substantial equivalence to an existing legally marketed device.[58] Finally, device regulation will apply to apps performing patient-specific analysis or providing patient-specific diagnosis or treatment recommendations.[59] Like mobile apps, robots may adopt many of these functions. Unlike apps, however, robots will be able to go further and physically and socially interact with the user, creating additional concerns.[60] In the end, there may be a potential merger between mobile apps and robots as mobile assistants, such as Apple's Siri,[61] continue to develop on mobile platforms.

[29] If the FDA takes a similar approach to robot regulation, we could expect that a robot's specific functions would determine whether it is subject to device regulation. Device regulation should continue to apply for robots that are developed as increasingly autonomous versions of existing medical devices. For new devices, the level of autonomy and amount of doctor supervision might determine whether the FDA considers a robot safe enough. For example, the Sedasys system, a "computer-assisted personalized sedation machine," was initially rejected by the FDA

[57] *See id.* at 15–16.

[58] As later sections will demonstrate, data associated with robots that resemble these apps will still face protection issues because in many cases HIPAA will not apply, and the FTC will only get involved if the robot deviated from its privacy policy. *See infra* Section IV.B.

[59] *See Mobile Medical Applications: Guidance for Industry and Food and Drug Administration Staff*, *supra* note 56, at 13–15.

[60] *See* M. Ryan Calo, *Robots and Privacy, in* ROBOT ETHICS: THE ETHICAL AND SOCIAL IMPLICATIONS OF ROBOTICS 187–90 (Patrick Lin et al. eds., 2012).

[61] *See* Siri, APPLE, http://www.apple.com/ios/siri/, *archived at* https://perma.cc/HH2M-PEUX (last visited Feb. 2, 2016).

in 2010 over safety concerns, and was approved in 2013 only after Johnson & Johnson agreed to only use the system for simple procedures, like colonoscopies, and to require an anesthesiologist to be on-call to handle any emergencies.[62] For robots that begin by performing routine or non-medical tasks, but evolve into what we might consider "healthcare" or "medical" robots, their qualification as "medical devices" may depend on the specific functions adopted. FDA clearly believes that most mobile health apps are benign, ranging from the recreational to very low risk. Given the agency's experience with surgical robots,[63] it is unlikely that FDA will take a hands-off or regulation-lite approach to any robots that have significant interactions with patients.

[30] To the extent that certain robots will be regulated as medical devices, two additional FDA guidance documents produced in recent years are particularly relevant to robots in healthcare. First, the FDA has acknowledged that "[c]hanges in health care have moved care from the hospital environment to the home environment," and that "[a]s patients move to the use of home health care services for recuperation or long-term care, the medical devices necessary for their care have followed them."[64] Accordingly, the FDA offers special guidance for home use devices,[65]

[62] *See* Frankel, *supra* note 52.

[63] Letter from Elizabeth A. Kage, Acting Dist. Dir. Pub. Health Servs., Food & Drug Admin., to Gary S. Guthart, President and CEO, Intuitive Surgical, Inc. (July 16, 2013) (on file with FDA), http://www.fda.gov/ICECI/EnforcementActions/WarningLetters/2013/ucm363260.htm, *archived at* https://perma.cc/B6YH-GA43.

[64] *See Home Use Devices*, U.S. FOOD & DRUG ADMIN., http://www.fda.gov/MedicalDevices/ProductsandMedicalProcedures/HomeHealthandConsumer/HomeUseDevices/default.htm, *archived at* https://perma.cc/H69V-KSN9 (accessed by searching for page in archive.org).

[65] *See, e.g.*, *Design Considerations for Devices Intended for Home Use: Guidance for Industry and Food and Drug Administration Staff*, U.S. FOOD & DRUG ADMIN. 1 (Nov. 24, 2014), http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm331675.htm, *archived at* https://perma.cc/4H4Q-TQFF; *Medical Device Home Use Initiative*, U.S. FOOD & DRUG ADMIN. 7 (Apr. 2010),

which outline some of the unique safety challenges presented in the home, including "risks result[ing] from interactions among the user, the use environment, and the device, [which] can greatly affect user and patient safety."[66] Aimed at manufacturers, the guidance stresses that "[t]hese risks are best addressed at the design stage."[67] Many of the safety challenges described will be the same—or, more likely, magnified—with robots. This includes reliance on wireless signals that may be unavailable in certain parts of the home,[68] and the need to recognize certain "human factors" which require "[u]nderstanding and optimizing how people use and interact with technology."[69] This guidance indicates the FDA's awareness and appreciation of the changing healthcare landscape, and the unstructured environment in which healthcare robots will be operating in the coming years.

[31] However, the challenges presented by personal care robots, specifically, will differ from both medical devices and other robots. RoboLaw has explained, for instance, that personal care robots "greatly change the concept of 'safety' because, unlike industrial robots: (i) they need to be used for a wide range of requirements in environments that are not well defined; (ii) they are used by non-specialist users; and (iii) they share work space with humans."[70] Premarket review of "safety" for robots must account for these unique considerations.

---

http://www.fda.gov/downloads/MedicalDevices/ProductsandMedicalProcedures/HomeHealthandConsumer/HomeUseDevices/UCM209056.pdf, *archived at* https://perma.cc/56N8-XB4L.

[66] *Design Considerations for Devices Intended for Home Use: Guidance for Industry and Food and Drug Administration Staff*, *supra* note 65, at 2.

[67] *Id.*

[68] *See id.* at 4.

[69] *Id.* at 13.

[70] ROBOLAW, *supra* note 35, at 174.

[32] The FDA's recent cybersecurity guidance for medical device manufacturers is also especially relevant to robots in healthcare—particularly those connected to the Internet in the hospital or the home.[71] This guidance recommends that manufacturers "consider cybersecurity risks as part of the design and development of a medical device, and submit documentation to the FDA about the risks identified and controls in place to mitigate those risks."[72] In addition, the FDA released a "safety communication" to manufacturers and healthcare organizations that listed recommendations designed to mitigate cybersecurity risks to medical devices.[73] The FDA has also opened a cybersecurity lab to test medical devices.[74]

[33] Robot designers and manufacturers should be aware of the FDA's emphasis on cybersecurity to ensure successful deployment, because even

[71] *See Content of Premarket Submissions for Management of Cybersecurity in Medical Devices: Guidance for Industry and Food and Drug Administration Staff*, U.S. FOOD & DRUG ADMIN. 4 (Oct. 2, 2014), http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM356190.pdf, *archived at* https://perma.cc/M3WH-5V5W.

[72] Press Release, Food & Drug Admin., The FDA takes steps to strengthen cybersecurity of medical devices (Oct. 1, 2014), http://www.fda.gov/NewsEvents/Newsroom/PressAnnouncements/ucm416809.htm, *archived at* https://perma.cc/JB5H-746P (The FDA recently held a public forum "to discuss how government, medical device developers, hospitals, cybersecurity professionals, and other stakeholders can collaborate to improve the cybersecurity of medical devices and protect the public health.").

[73] *See Cybersecurity for Medical Devices and Hospital Networks: FDA Safety Communication*, U.S. FOOD & DRUG ADMIN. (June 13, 2013), http://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm356423.htm, *archived at* https://perma.cc/J6UQ-6K55 [hereinafter *FDA Safety Communication*].

[74] *See* Emily Wasserman, *FDA beefs up cybersecurity efforts to ensure safety standards*, FIERCEMEDICAL DEVICES (June 6, 2014), http://www.fiercemedicaldevices.com/story/fda-beefs-cybersecurity-efforts-ensure-safety-standards/2014-06-06, *archived at* https://perma.cc/2HHQ-8G3T ("The agency . . . created a 'cybersecurity laboratory,' which stages deliberate cybersecurity attacks to sniff out any defects that could leave a device open to attack.").

though the current guidelines are merely recommendations, they may become *de facto* requirements in the future.[75] Hospital networks are notoriously insecure.[76] Subjecting robots to this environment only magnifies vulnerabilities already posed to regular medical devices and electronic health records. Indeed, the threats to physical safety caused by insecure medical devices of all kinds are real, leaving pacemakers, defibrillators, insulin pumps, and other devices vulnerable to hacks.[77] These threats may be magnified with robots due to their ability to manipulate their surroundings. Robots used in the home may encounter even more vulnerable environments with less physical and cyber security and even less sophisticated users.

[34] Although the FDA's recent emphasis on cybersecurity may ultimately result in more secure robots, its review is only focused on threats as they relate to device functionality and the resulting effect on

[75] *See* Philip Desjardins, *FDA Scrutinizes Networked Medical Device Security*, INFORMATIONWEEK (Dec. 1, 2014), http://www.informationweek.com/healthcare/security-and-privacy/fda-scrutinizes-networked-medical-device-security/a/d-id/1317758, *archived at* https://perma.cc/6P8R-HCXG ("By outlining cyber security premarket submission content recommendations, the FDA could lay the groundwork for a new category of *de facto* required information that will be needed for the agency to adequately review premarket submissions for connected devices.").

[76] *See, e.g.*, *FDA Safety Communication*, *supra* note 73 ("Recently, the FDA has become aware of cybersecurity vulnerabilities and incidents that could directly impact medical devices or hospital network operations."); Chad Garland, *Hackers stole 4.5 million patients' data in hospital breach*, L.A. TIMES (Aug. 18, 2014, 1:18 PM), http://www.latimes.com/business/technology/la-fi-tn-community-health-hacked-20140818-story.html, *archived at* https://perma.cc/5WXR-8VCT.

[77] *See, e.g.*, David F. Carr, *Hackers Outsmart Pacemakers, Fitbits: Worried Yet?*, INFORMATIONWEEK (Dec. 12, 2013), http://www.informationweek.com/healthcare/security-and-privacy/hackers-outsmart-pacemakers-fitbits-worried-yet/d/d-id/1113000, *archived at* https://perma.cc/LH8S-GDYP (describing how "cybersecurity researchers have demonstrated the potential to hack[] pacemakers, defibrillators, insulin pumps, and other devices that could have life-or-death consequences").

physical safety, and not necessarily potential broader harms. Device functionality is important, but should not cause stakeholders to overlook the notion that the data associated with devices are often a more valuable target than the devices themselves.[78] Attention to certain security vulnerabilities is marginalized under current device regulation, specifically those security vulnerabilities that do not necessarily affect a patient's physical safety, but may nevertheless lead to unauthorized access to and use of valuable and sensitive health information, of which robots will have an unprecedented amount.

[35] The natural inclination in response to this apparent shortcoming is to look to HIPAA as the widely accepted health information privacy law. Indeed, users of traditional medical devices controlled by covered entities have HIPAA to rely on for some health information disclosure protections. But, as the following section describes, this is not the case with certain private consumer robots operating outside of HIPAA's domain. After these robots are made available to the public, users will rely heavily on the FTC for security and privacy protection.[79] Even robots that are regulated by the FDA and subject to HIPAA, though, are developed without mandated proactive consideration of information security and privacy by design. Current devices with limited functions, and correspondingly limited safety, privacy, and security concerns, might be adequately served by current regulation schemes; but robots might prove to be the technology that brings to light the need for more or restructured security and privacy oversight, especially by the FTC.

B. Data Protection

[36] Healthcare data challenges are well known. For example, hospitals and medical devices have been identified in recent years as being

[78] *See* Klint Finley, *Hacked Fridges Aren't the Internet of Things' Biggest Worry*, WIRED (Mar. 12, 2015), http://www.wired.com/2015/03/hacked-fridges-arent-internet-things-biggest-worry/, *archived at* https://perma.cc/Y45F-HY6P ("[I]n the business of hacking, it's not the device that's valuable. It's the data they generate.").

[79] *See infra* Section IV.B.

notoriously insecure.[80] There is also a dichotomy, albeit frequently a false one, between strong privacy protections and provider, researcher, and policymaker calls for unfettered data collection, liquidity, and (secondary) use. Robots in healthcare will magnify these challenges. Overall, as described in previous sections, data that are necessary and desirable to enable effective use of robots in healthcare will represent an unprecedented generation and centralization of health and other sensitive information, much of which is inadequately considered under current regulation.[81] AI-based devices pose a particular challenge to data protection principles because they thrive on the collection and analysis of vast amounts of data. While Fair Information Practice Principles (such as data minimization and respect for context) make sense in human-human interactions, it may be too early to articulate any limits on data collection by robots.[82]

1. Robot-Carried PHI in HIPAA-Protected Space

[37] Most personal health information generated, shared, and utilized by robots in the traditional healthcare setting will be subject to the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules. The HIPAA Privacy Rule "provides federal protections for individually identifiable health information held by covered entities and their business associates," on whom the rule places duties, which are enforced by the U.S. Department of Health and Human Services (HHS) Office of Civil Rights (OCR).[83] The HIPAA Security Rule, also enforced

[80] *See, e.g.*, *FDA Safety Communication*, *supra* note 73; Garland, *supra* note 76.

[81] *See, e.g.*, Thierer, *supra* note 43.

[82] *See* NAT'L INST. OF STANDARDS AND TECH., APPENDIX A-FAIR INFORMATION PRACTICE PRINCIPLES (FIPPS), http://www.nist.gov/nstic/NSTIC-FIPPs.pdf, *archived at* https://perma.cc/Q2BU-UGGS.

[83] *See* 45 C.F.R. § 160 (2014); 45 C.F.R. § 164(A, E) (2014); *see also Understanding Health Information Privacy*, U.S. DEP'T OF HEALTH & HUMAN SERVS., http://www.hhs.gov/ocr/privacy/hipaa/understanding/, *archived at* https://perma.cc/27C9-DRR3.

by OCR, "specifies a series of administrative, physical, and technical safeguards for covered entities and their business associates to use to assure the confidentiality, integrity, and availability of electronic protected health information."[84] A covered entity is defined as a health plan, a health care clearinghouse, or a health care provider who electronically transmits any health information in connection with transactions for which HHS has adopted standards.[85] A business associate is "a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity."[86] It is important to note that, to the extent that HIPAA applies to certain robots in healthcare, it only accounts for disclosures of information after that information is collected.[87] Missing from current regulation is a proactive, pre-deployment mandate to incorporate security and privacy protections of information into the design of robotic systems, similar to the way the FDA proactively regulates physical safety.[88]

[84] *See* 45 C.F.R. § 160 (2014); 45 C.F.R. § 164(A, C) (2014); *see also Understanding Health Information Privacy*, *supra* note 83.

[85] *See* 45 C.F.R. § 160.103 (2014); *see also To Whom Does the Privacy Rule Apply and Whom Will It Affect?*, NAT'L INST. HEALTH, http://privacyruleandresearch.nih.gov/pr_06.asp, *archived at* https://perma.cc/2U3Z-2A7B.

[86] *Health Information Privacy*, U.S. DEP'T OF HEALTH & HUMAN SERVS., http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/businessassociates.html, *archived at* https://perma.cc/YCE3-QLSB; 45 C.F.R. § 160.103 (2014) (definition of "business associate").

[87] *See* Nicolas P. Terry, *Protecting Patient Privacy in the Age of Big Data*, 81 UMKC L. REV. 385, 386–87 (2012) ("[W]hile HIPAA/HITECH provide increasingly robust protections against unauthorized uses of health information by a relatively narrow set of traditional health care provider data stewards, it does almost nothing to regulate the collection of health data. This is because the HIPAA Privacy Rule is a misnomer. It is not a privacy rule because it only protects against data disclosure not against data collection. It is therefore more appropriately described as a confidentiality rule.").

[88] *See supra* Part IV.A.

[38] Because the vast majority of hospitals are HIPAA covered entities, identifiable health information collected by robots under the control of hospitals or their business associates will be subject to the Privacy and Security Rules. HIPAA thoroughly accounts for disclosure practices of identifiable health information held by covered entities, but these practices will become increasingly complex as robots in healthcare utilize more third parties on a regular basis, such as cloud service providers.[89] Robots in healthcare will highlight the fact that these essential and highly involved "business associates" are now directly liable for their violations under the HIPAA final omnibus rule, as opposed to only being accountable under their mandated contracts with covered entities.[90] Overall, and as previous sections have described, robots in healthcare greatly expand not only the sheer amount of personal health information that is collected, but also the ways in which data are processed, stored, and used, and by whom, complicating privacy and security compliance efforts in the hospital setting.

2. Robot-Carried PHI outside HIPAA-Protected Space

[39] While most data collected and used by healthcare robots operating within a hospital environment will be subject to the HIPAA rules, the same cannot be said for many other robots involved in healthcare. Overall, far more difficult data protection questions arise outside of conventional healthcare. If robots are being deployed for medical purposes, healthcare, or comfort by persons who are *not* covered entities or their business associates, the HIPAA Privacy and Security Rules do not apply.

[40] Issues will arise as the healthcare setting expands to the home, where many popular health technologies currently operate outside of

[89] *See supra* Part II.

[90] *See* Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules, 78 Fed. Reg. 5,566 (Jan. 25, 2013) (to be codified at 45 C.F.R. pts. 160 & 164).

HIPAA's domain, including personal "wearables" such as Fitbit[91] and the aforementioned mobile medical apps.[92] But even those robots in the home that are subject to HIPAA will encounter a wide range of data protection challenges. For example, a recent Boston Children's Hospital pilot programs sent monitoring robots home with children who had urological surgery.[93] In situations like these, and especially as robot functions become more complex, challenges may stem from the fact that robots in the home need to collect vast amounts of information about users and their environment,[94] even beyond the health information protected under HIPAA.[95]

[41] Less complicated, but also less satisfying, is the privacy-security regulation of home robots that are not supplied by HIPAA entities. As previous sections have described, some of these robots may be regulated for physical safety by the FDA, including cybersecurity to the extent that

[91] *See Fitbit*, http://www.fitbit.com, *archived at* https://perma.cc/CG7A-6CT3 (last visited Feb. 2, 2016).

[92] *See supra* Part IV.A.

[93] *See* Erin McCann, *Health IT Promises New Paradigm of Patient Care*, HEALTHCARE IT NEWS (Sept. 12, 2012, 3:49 PM), http://www.healthcareitnews.com/news/health-it-promises-new-paradigm-patient-care, *archived at* https://perma.cc/Y88C-42WB.

[94] *See* Proia, Simshaw & Hauser, *supra* note 44, at 157 (describing the data collection practices of household robots, including the "detailed mapping of buildings and rooms, as well as particular data on objects within that environment, including data that will help determine what the object is and where the object is located").

[95] *See, e.g.*, Cocco, *supra* note 34, at 104 (noting that this is the case with smart home technology for the elderly, as, "[t]he kinds of information collected and transmitted by smart home technology go beyond the scope of the definition [of protected health information]. While the information pertaining to a resident's heart rate, respiration, and medication intake will most likely be protected, information about his or her location in the home over time would most likely not be. To consider information regarding whether someone missed a television show or used the sink 'protected health information' would be a stretch of the definition.").

it affects device functionality, but not broader privacy-security harms.[96] In addition, HIPAA will govern the disclosure of certain protected health information, but only if that information is collected and controlled by covered entities, which might not always be the case in the home setting.

[42] Examples of these household robots may emerge if domestic consumer "personal assistant" robots (such as Jibo[97] and Pepper[98]), unaffiliated with any covered entity, begin taking on healthcare-related tasks such as monitoring an individual's daily activity, issuing medication reminders, and suggesting when to seek medical assistance if it senses something wrong. Because these robots are unaffiliated with any covered entity, they will not be subject to the HIPAA Privacy and Security Rules.

[43] It does not follow, though, that these robots will be completely unregulated. Indeed, some oversight such as FDA device, and hence cybersecurity, regulation likely would still apply.[99] However, the data protection model is more complicated and ultimately less satisfactory. In the case of mobile medical apps that fall outside of HIPAA protection, it is still possible that some state privacy laws may apply, but by their terms even the most pro-privacy of these[100] would not currently apply to "consumer" robots operating in a "HIPAA-free zone."[101]

---

[96] *See supra* Part IV.A.

[97] *See* JIBO, http://www.jibo.com, *archived at* https://perma.cc/62TM-3QSL (last visited Jan. 29, 2016).

[98] *See Who Is Pepper?*, ALDEBARAN, https://www.aldebaran.com/en/a-robots/who-is-pepper, *archived at* https://perma.cc/HM3B-EX5U (last visited Jan. 17, 2016).

[99] *See supra* Part IV.A.

[100] *See generally* California Confidentiality of Medical Information Act (CMIA), CAL. CIV. CODE § 56.06 (Deering 2015) (demonstrating California state privacy law may apply to mobile medical apps).

[101] *See* Terry, *supra* note 87, at 387 ("The health care sector and its stakeholders constitute an area considerably larger than the HIPAA-regulated zone. As a result, some traditional health information circulates in what may be termed a HIPAA-free zone.").

[44] Rather, most responsibility in such cases would fall on the FTC. The FTC has become increasingly active in consumer privacy matters related to the Internet of Things,[102] big data, [103] and data brokers,[104] all of which have had significant impact on health information in recent years. The agency is likely to play a critical role in any attempt to regulate consumer robots, which may become more widespread in the near future.[105] The FTC does not differentiate between health data protection in conventional and emerging healthcare spaces.[106] Rather, it protects data somewhat indirectly, by enforcing privacy policies or otherwise characterizing bad data practices as unfair or misleading.[107] This agency's role may expand in the coming years, as robots might prove to be the

[102] *See, e.g.*, FED. TRADE COMM'N, INTERNET OF THINGS: PRIVACY & SECURITY IN A CONNECTED WORLD i (2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf, *archived at* https://perma.cc/BK9Y-XUEN [hereinafter FTC IoT Report].

[103] *See, e.g.*, *Big Data: A Tool for Inclusion or Exclusion?*, FED. TRADE COMM'N (Sept. 15, 2014), https://www.ftc.gov/news-events/events-calendar/2014/09/big-data-tool-inclusion-or-exclusion, *archived at* https://perma.cc/SK5G-PJX5.

[104] *See, e.g.*, FED. TRADE COMM'N, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY i (May 2014), https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf, *archived at* https://perma.cc/B2Q5-7FM2.

[105] *See generally* Proia, Simshaw & Hauser, *supra* note 44, at 161–63 (explaining that "privacy advocates and policymakers will likely look to the . . . [FTC framework] to determine the adequacy of cloud robotics companies' data practices").

[106] *See In re LabMD, Inc.: Case Summary*, FED. TRADE COMM'N, https://www.ftc.gov/enforcement/cases-proceedings/102-3099/labmd-inc-matter, *archived at* https://perma.cc/P7RM-UZG2 (last updated Dec. 18, 2015).

[107] *See* Julie Brill, Comm'r, Fed. Trade Comm'n, Keynote Address at EuroForum European Data Protection Days: Data Protection and the Internet of Things 6 (May 4, 2015), https://www.ftc.gov/system/files/documents/public_statements/640741/2015-05-04_euroforum_iot_brill_final.pdf, *archived at* https://perma.cc/3SWK-X599.

technology that brings to light the need for more or restructured security and privacy oversight.

[45] However, the FTC is limited both in its powers and its resources. Section 5 of the Federal Trade Commission Act (FTC Act) generally authorizes the FTC to investigate and prevent deceptive trade practices.[108] It should be noted, however, that FTC jurisdiction is almost entirely ex post facto. That is, unlike the FDA's intervention with regard to some classes of medical devices, the FTC does not perform pre-marketing scrutiny or approval.[109]

[46] There are three areas where it is likely that the FTC would become involved in regulating robots in the home. First, as with any other consumer product, the FTC will intervene if the product is deceptively advertised. For example in the "mole app cases," the defendants' apps used smartphone images to calculate the risk of skin imperfections being pre-cancerous or cancerous.[110] Personal assistant robots in the home may very well attempt to perform similar diagnostic functions, and if they do, may be subject to FTC enforcement.

[47] Second, the FTC may argue that, as in the Wyndham Hotels litigation, providing a product or service (including, presumably, home

[108] *See* 15 U.S.C. § 45(a)(1) (2012) ("[U]nfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful.").

[109] *See* Resp't LabMd, Inc.'s Mot. to Dismiss Compl. with Prejudice & to Stay Admin. Proceedings at 22, *In re* LabMD, Inc., No. 9357 (F.T.C. Nov. 12, 2013), https://www.ftc.gov/sites/default/files/documents/cases/131112respondlabmdmodiscomplaintdatyadminproceed.pdf, *archived at* https://perma.cc/M474-GTTY.

[110] *See In re* Health Discovery Corp., No. C-4516, at 2 (F.T.C. Apr. 13, 2015), https://www.ftc.gov/system/files/documents/cases/150413hdcmelappdo.pdf, *archived at* https://perma.cc/CPT2-GLWV; Fed. Trade Comm'n v. Lasarow, et al., No. 15-cv-1614, at 2, 4 (N.D. Ill. 2015), https://www.ftc.gov/system/files/documents/cases/150223avromorder.pdf, *archived at* https://perma.cc/TE29-RNM4.

monitoring and robotic services) with inadequate data security by itself constitutes an "unfair practice."[111]

[48] Third, and where the FTC has placed most of its energy in privacy cases, it may argue that the supply of a product or service with an inaccurate privacy policy, or where the supplier fails to comply with its own announced privacy or security policies, is a deceptive or misleading practice.[112]

[49] Traditionally, the FTC's consumer protections have only applied to health information to the extent that it represents one of the many kinds of "sensitive" information with which the agency is concerned.[113] However, recent proposals by the White House and the FTC itself indicate that the role of the FTC in protecting health information, both with HIPAA covered entities and in the HIPAA-free zone, may be expanding. The security and privacy issues arising with robots in healthcare, currently marginalized under existing regulatory frameworks, demonstrate why the FTC may play a critical role in encouraging concepts such as privacy and

[111] *See* Fed. Trade Comm'n v. Wyndham Worldwide Corp., 799 F.3d 236, 240 (3rd Cir. 2015) [hereinafter *Wyndham*]; *see also* Compl. at 4–5, *In re* LabMD, Inc., No. 9357 (F.T.C. Aug. 28, 2013), https://www.ftc.gov/sites/default/files/documents/cases/2013/08/130829labmdpart3.pdf, *archived at* https://perma.cc/H3XD-CBNT (redacted public version) (showing that the FTC is again using the 'unfair practices' argument in breached consumer data cases).

[112] *See* Press Release, Fed. Trade Comm'n, Medical Billing Provider and its Former CEO Settle FTC Charges That They Misled Consumers About Collection of Personal Health Data (Dec. 3, 2014), https://www.ftc.gov/news-events/press-releases/2014/12/medical-billing-provider-its-former-ceo-settle-ftc-charges-they, *archived at* https://perma.cc/658N-TJHN; Press Release, Fed. Trade Comm'n, Fandango, Credit Karma Settle FTC Charges that They Deceived Consumers By Failing to Securely Transmit Sensitive Personal Information (Mar. 28, 2014), https://www.ftc.gov/news-events/press-releases/2014/03/fandango-credit-karma-settle-ftc-charges-they-deceived-consumers, *archived at* https://perma.cc/JUD6-9AWL.

[113] *See generally* Proia, Simshaw, & Hauser, *supra* note 44, at 181, 183 (explaining the heightened focus on certain Fair Information Practice Principles necessary when sensitive information is involved).

security by design, which will help maintain responsible design and deployment of robots in the coming years and enable further innovation in this critical area.

[50] As recently as 2012, the FTC's report "Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers" implied that HIPAA's Privacy and Security Rules adequately protect health information.[114]

[51] However, in the years since, smartphone platforms, wearables, and big data brokers operating in the HIPAA-free zone have caused what appears to be a shift in policy.[115] The White House's 2015 draft consumer privacy bill seemed to indicate support for a significant extension of FTC oversight into healthcare with its inclusion of certain medical data in the categories that are to be protected.[116] Such dual regulation may seem

[114] *See* FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS 16–17 (March 2012), https://www.ftc.gov/reports/protecting-consumer-privacy-era-rapid-change-recommendations-businesses-policymakers, *archived at* https://perma.cc/PU2L-BFGR; *see also* Nicolas Terry, *Should Health Lawyers Pay Attention To The Administration's Privacy Bill?*, HEALTH AFF. BLOG (Mar. 13, 2015), http://healthaffairs.org/blog/2015/03/13/should-health-lawyers-pay-attention-to-the-administrations-privacy-bill/, *archived at* https://perma.cc/N9FK-Q67F ("The conventional wisdom implicit in the 2012 [FTC] reported was that health information was adequately protected by the domain-specific HIPAA Privacy and Security Rules, hence the HIPAA-entity exception in the framework and a similar provision in the FTC's 2012 offering.").

[115] *See* Terry, *supra* note 114.

[116] *See Administration Discussion Draft: Consumer Privacy Bill of Rights Act of 2015*, at 20, https://www.whitehouse.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf, *archived at* https://perma.cc/5BKV-ATSZ; Terry, *supra* note 114 ("[M]edical data clearly fall within the bill's purview. The definition of personal data is quite broad (albeit likely not broad enough for many privacy advocates), includes non-exclusive examples such as a 'health care account number,' and 'any data that are collected, created, processed, used, disclosed, stored, or otherwise maintained and linked, or as a practical matter linkable by the covered entity' to that numerical identifier.").

duplicative, but in fact, such an approach could produce a successful regulatory scheme in which the FTC oversees the initial collection of health information, while HIPPA governs subsequent disclosure practices. In other words, the FTC will focus on general privacy and use of health and other sensitive information, and HIPPA will focus on sector-based confidentiality and disclosure of protected health information.[117]

[52] One way to enable such a regulatory scheme is to remove the sector-based limitations currently limiting the FTC's influence in healthcare. Such an approach would "allow[] for true collection regulation, leaving HIPAA/HITECH to regulate the disclosure practices of covered entities. New privacy rules common to all sectors and limiting data collection would then sit upstream of existing health care regulation that would continue to deal with unauthorized information disclosure."[118]

[53] Privacy and security issues associated with robots in healthcare could be an area where the FTC is quite comfortable regulating, as many of the issues associated with such robots, and particularly with those that will provide care in the home, align with areas of focus of the agency. For one, robots in the home in general, and those performing healthcare tasks specifically, will be collecting data on a person's most private matters, which, like smart home technology generally, has led to calls for increased regulation of such practices.[119] These concerns mirror those expressed at

[117] *See* Terry, *supra* note 87, at 406 ("[C]oncerns about duplicate burdens are unwarranted in the case of health care regulation. . . . HIPAA/HITECH employs a sector-based confidentiality (disclosure-centric) model. The White House and to an extent the FTC proposals are primarily privacy (collection-centric) endorse models.").

[118] *Id.* at 407 (explaining that "HIPAA's weakness . . . []the fact that it provides only a confidentiality model of protection[,] can be cast as a strength when it comes to compatibility with the White House and FTC collection-centric models of protection").

[119] *See, e.g.*, Cocco, *supra* note 34, at 106 ("The data at issue with smart homes could concern almost every detail of a person's life, including bathroom visits, interactions with other people, food intake, medications, sleep cycles, and physiological data. Thus, it is necessary to institute proper regulations to reconcile the interest in privacy protection in the home with this kind of pervasive technology.").

the FTC's 2013 workshop on the Internet of Things.[120] In addition, the FTC has acknowledged the significance of the sheer volume of data that will be generated by home-connected devices.[121] As with other home connected devices, health-related data gathered by a robot not affiliated with a HIPAA-covered entity could be used in the future for purposes not anticipated at the time of collection.[122] These uses would present challenging questions, even beyond privacy and security.[123] Perhaps most significantly, the FTC has acknowledged the increasing problem of the "HIPAA-free zone," and believes consumers should have transparency and choices over their sensitive information, regardless of who collects

[120] *See* Fed. Trade Comm'n, Transcript, Internet of Things Workshop 67–68, 70–72 (Nov. 19, 2013), http://www.ftc.gov/sites/default/files/documents/public_events/internet-things-privacy-security-connected-world/final_transcript.pdf, *archived at* https://perma.cc/LYA6-AAUG [hereinafter IoT Workshop Transcript]; *see also* FTC IoT Report, *supra* note 102, at 14 ("Some of these risks involve the direct collection of sensitive personal information, such as precise geolocation, financial account numbers, or health information—risks already presented by traditional Internet and mobile commerce. Others arise from the collection of personal information, habits, locations, and physical conditions over time, which may allow an entity that has not directly collected sensitive information to infer it.") (footnotes omitted).

[121] *See* FTC IoT Report, *supra* note 102, at 14 ("The sheer volume of data that even a small number of devices can generate is stunning: one participant indicated that fewer than 10,000 households using the company's IoT home-automation product can 'generate 150 million discrete data points a day' or approximately one data point every six seconds for each household.") (footnotes omitted).

[122] *See id.* at 16 ("[O]ne researcher has hypothesized that although a consumer may today use a fitness tracker solely for wellness-related purposes, the data gathered by the device could be used in the future to price health or life insurance or to infer the user's suitability for credit or employment (*e.g.*, a conscientious exerciser is a good credit risk or will make a good employee). According to one commenter, it would be of particular concern if this type of decision-making were to systematically bias companies against certain groups that do not or cannot engage in the favorable conduct as much as others or lead to discriminatory practices against protected classes.") (footnotes omitted).

[123] *See, e.g.*, *id.* at 17 (implying a question of whether we want insurance companies to offer lower premiums to people who share data from their healthcare robot).

it.[124]

[54] Because robots in healthcare are so difficult to place within existing regulatory frameworks, they demonstrate, perhaps even more than other emerging technologies and robots in general, how close some of these frameworks must come to each other in order to close gaps in protections for things like safety, security, and privacy. The previously described dual (but not overlapping) FTC and HIPAA regulatory scheme is one example. The FTC has also expressed in its call for general data protection legislation an apparent willingness to align its goals with the FDA's concern of physical safety: "General data security legislation should protect against unauthorized access to both personal information *and device functionality itself*. For example, if a pacemaker is not properly secured, the concern is not merely that health information could be compromised, but also that a person wearing it could be seriously harmed."[125] So whereas OCR and the FDA may be unable or unwilling to expand their roles to account for the gaps in security and privacy protections that will be exposed by robots in healthcare, the FTC appears both able and willing to do so.

[124] *See id.* at 51–52 ("HIPAA protects sensitive health information, such as medical diagnoses, names of medications, and health conditions, but only if it is collected by certain entities, such as a doctor's office or insurance company. Increasingly, however, health apps are collecting this same information through consumer-facing products, to which HIPAA protections do not apply. Commission staff believes that consumers should have transparency and choices over their sensitive health information, regardless of who collects it."); *see also* Susan D. Hall, *FTC Report on IoT Calls for Update to HIPAA Standards*, FIERCEHEALTHIT (Jan. 28, 2015), http://www.fiercehealthit.com/story/ftc-report-internet-things-calls-updated-hipaa-standards/2015-01-28, *archived at* https://perma.cc/Z487-K9N9 ("[The Report] also calls for more updated and consistent HIPAA standards. The report points out the healthcare applications increasingly are collecting the same sensitive information from patients as doctors' offices and insurance companies through consumer-facing products not covered by HIPAA. . . . 'Consumers should have transparency and choices over their sensitive health information, regardless of who collects it,' according to the report's authors.").

[125] FTC IoT Report, *supra* note 102, at vii–viii (emphasis added).

[55] Overall, regardless of what law applies, or which regulatory agency has the lead, robots will have a significant impact on the data protection environment. The health data these increasingly autonomous robots will generate, share, and rely on represent a far more complete, and therefore sensitive, account of a patient's health than is found in current medical and health records.

VI. CONCLUSION AND RECOMMENDATIONS

[56] Robots have tremendous potential to have a profoundly positive effect on healthcare, both in the hospital and home environments. Confronting regulatory challenges involves not only anticipating eventual "healthcare companions" or "robotic doctors," but also understanding the characteristics of emerging robots in the coming years. From a legal standpoint, it is important to acknowledge the ways in which robots will evolve, including (1) from increasingly autonomous robotic functions of medical devices (e.g., *autonomous* robot surgery), and (2) from increasing healthcare functions being performed by general personal robots (e.g., Jibo[126] and Pepper[127]). Current medical device regulation and data protection laws will present legal challenges for the emergence of these robots that must be addressed in the very near future if innovation is going to continue to thrive. Accordingly, this paper has focused on the issues of patient and user safety, security, and privacy, and identified gaps in such protections that are likely to emerge as robots in healthcare continue to advance.

[57] The FDA will regulate many robots as medical devices, including increasingly autonomous devices and personal robots that perform certain tasks. Because these robots will be subject to premarket review, safety will be evaluated before these robots are deployed. However, the FDA's current review is only concerned with device functionality and security as they relate to *physical* safety. Unaccounted for during current premarket review are potential non-physical harms that are magnified by autonomous

[126] *See* JIBO, *supra* note 97.

[127] *See Who is Pepper?*, *supra* note 98.

robots in the healthcare setting. Robots in healthcare will present an unprecedented expansion and centralization of patient data. HIPAA provides some health information disclosure protections of information associated with devices after they are already in use, but will not apply to certain private consumer robots operating outside of HIPAA's domain.

[58] As a result, robots warrant an expansion of what is considered during premarket review, or through some other similar proactive process. Proper design must include taking into consideration these broader potential harms that could, if overlooked, manifest themselves in ways that harm patients and consumers, diminish the trust of the public in robots, and stifle long-term innovation by resulting in overly restrictive reactionary regulation. Because not all robots in healthcare will constitute "medical devices," review might be most appropriately conducted by an agency that examines all robots with medical and healthcare-related functions.[128]

[59] Homecare robots may or may not be considered "medical devices," depending on their functions, and may or may not be subject to HIPAA, depending on who controls and has access to the robot's information. As a result, FTC oversight of data practices will be needed in order to better protect patient and consumer privacy, especially as robots become more prominent in the HIPAA-free zone. A successful scheme could be one in which the FTC oversees a robot's initial collection of health information, while HIPAA continues to govern subsequent disclosure practices. One way to enable such a regulatory scheme is to remove the sector-based limitations currently limiting the FTC's influence in healthcare.

[60] Both pre-deployment review of security and privacy considerations and post-deployment enforcement of proper data practices should encourage the principles of security and privacy by design. However, robotic technology is rapidly advancing and dynamic, so regular review of policies and practices by healthcare institutions will also be critical. In

[128] *See, e.g.*, Ryan Calo, *The Case for a Federal Robotics Commission,* BROOKINGS INST. (Sept. 2014), http://www.brookings.edu/research/reports2/2014/09/case-for-federal-robotics-commission, *archived at* https://perma.cc/C4H8-BVZQ.

addition, agencies should consider developing emerging technology divisions to address these and related issues as automated and robotic technologies become ubiquitous.

[61] Because we are likely to see health-related robots appearing in both conventional healthcare and consumer spaces, there will be regulatory disruption and the opportunity for regulatory arbitrage. We argue the regulation of both must change. A foundational regulatory framework for both medical devices and data protection that is attuned to safety, security, and privacy will help foster innovation and confidence in robotics and ensure that we maximize the potential of robots in healthcare.