2016

Regulating Healthcare Robots in the Hospital and the Home: Considerations for Maximizing Opportunities and Minimizing Risks

Simshaw, Drew; Terry, Nicolas; Hauser, Kris; Cummings, M.L.

Drew Simshaw, Nicolas Terry, Kris Hauser & M.L. Cummings, Regulating Healthcare Robots: Maximizing Opportunities While Minimizing Risks, 22 Rich. J.L. & Tech 3 (2016).
http://hdl.handle.net/10945/61623

DRAFT
Regulating Healthcare Robots in the Hospital and the Home: Considerations for Maximizing Opportunities and Minimizing Risks

DREW SIMSHAW,*NICOLAS TERRY,** DR. KRIS HAUSER,*** DR. M.L. CUMMINGS****

ABSTRACT

Some of the most dynamic areas of robotics research and development today are healthcare applications. Demand for these robots will likely increase in the coming years due to their effectiveness and efficiency, an ageing population, the rising cost of healthcare, and the trend within the industry toward personalized medicine. But all-purpose "healthcare companions" and robotic "doctors" will not be available for purchase or be deployed in our hospitals any time soon. Rather, robots in healthcare will be an evolution in the coming decades. There are basic, pressing issues that need to be addressed in the nearer future in order to ensure that robots are able to maintain sustainable innovation with the confidence of providers, patients, consumers, and investors. We will only be able to maximize the potential of robots in healthcare through responsible design, deployment, and use, which must include taking into consideration potential issues 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 by resulting in overly restrictive reactionary regulation. In this paper, we 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, we examine the demand for robots in healthcare and assess the benefits that robots can provide. Second, we 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, including their increasing number of functions, complex data collection, processing, storing, and use practices, and increasing connectivity and potential for cloud usage, all resulting in an unprecedented expansion and centralization of patient data. Third, we examine the current regulatory framework within which these robots will operate, focusing on medical device regulation and data protection laws. 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. In order to maximize robots' potential and minimize risks to users, we will need to move towards some form of premarket review of robot "safety," which should include broad considerations of potential harms, including security. Furthermore, current sector-based limitations that lead to gaps between, for example, FTC and HHS-OCR oversight, should be eliminated so that privacy and security interests can be better protected in the "HIPAA-free" zone. A foundational regulatory framework for both medical devices and consumers which 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.

* Law & Policy Analyst, Indiana University Center for Law, Ethics, and Applied Research in Health Information, J.D., Indiana University Maurer School of Law, 2012, B.A., University of Washington, 2007.
** 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 and 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, 1998.

INTRODUCTION 2
I. ROBOTS IN HEALTHCARE: DEMAND AND BENEFITS 4
II. ROBOT TYPES AND CHARACTERISTICS 7
III. THE DISTINCTIVE FEATURES OF ROBOT DATA COLLECTION AND USE 11
IV. THE CURRENT REGULATORY FRAMEWORK 13
A. Device Regulation 13
B. Data Protection 18
CONCLUSION AND RECOMMENDATIONS 27

INTRODUCTION

Some of the most dynamic areas of robotics research and development today are healthcare applications.[1] From robot-assisted surgery,[2] to robotic nurses,[3] to in-home rehabilitation[4] and eldercare robots,[5] the possibilities and benefits seem endless. Demand for these robots will likely increase in response to rising healthcare labor costs and an aging population. Like many technologies though, robots are difficult to place within existing

[1] *See Healthcare Robotics: 2014*, Robotics Business Review, Industry Special Report, available at http://www.roboticsbusinessreview.com/research/report/healthcare_robotics_2014 (describing how, "[t]o 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").
[2] *See* John Markoff, *New Research Center Aims to Develop Second Generation of Surgical Robots*, The New York Times, October 23, 2014, http://www.nytimes.com/2014/10/23/science/new-research-center-aims-to-develop-second-generation-of-surgical-robots.html?_r=0 (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* Robotic Nurse Assistant project at Georgia Institute of Technology, http://www.hsi.gatech.edu/hrl/project_nurse.shtml (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* Stanford University's CHARM (Collaborative Haptics and Robotics in Medicine) Lab, http://charm.stanford.edu/Main/RehabilitationRobotics (describing rehabilitation robotics projects, including "Robotic Manipulation for Reaching" and "HAPI Bands: Haptic Augmented Posture Interface").
[5] *See* Will Knight, *Your Retirement May Include a Robot Helper*, MIT Technology Review, October 27, 2014, http://www.technologyreview.com/news/531941/your-retirement-may-include-a-robot-helper/.

regulatory frameworks and will cause regulatory turbulence. Near term, the areas of greatest turbulence will occur in (1) medical device regulation, (2) data protection regimes, and (3) licensure regulation of the "practice of medicine."

Although many interesting law and policy issues arise surrounding the use of teleoperated robotics systems (e.g. surgical robots directly controlled by a surgeon), this paper focuses on existing and emerging robots with 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]

Many interesting legal and ethical questions surround the idea of healthcare someday being performed by robots utilizing artificial intelligence. However, all-purpose "healthcare companions" and robotic "doctors" 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, robots in healthcare will be an evolution in the coming decades, and there are basic, pressing issues that need to be addressed in the nearer future in order to ensure that robots are able to maintain sustainable innovation with the confidence of providers, patients, consumers, and investors. Only through such responsible design, deployment, and use will robots be able to maximize their potential in healthcare.

In this paper, we 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, we will examine the demand for robots in healthcare and assess the benefits

[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.

that robots can provide. Second, we 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, we will examine the current regulatory framework within which these robots will operate, focusing on medical device regulation and data protection laws.

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. In order to maximize robots' potential and minimize risks to users, we will need to move towards some form of premarket review of robot "safety." Such review, likely by the FDA, should include broad considerations of potential harms, including security. Furthermore, current sector-based limitations that lead to gaps between, for example, FTC and HHS-OCR oversight, should be eliminated so that privacy and security interests can be better protected in the "HIPAA-free" zone. A foundational regulatory framework for both medical devices and consumers which is attuned to safety, security, and privacy will help foster innovation and confidence in robotics and ensure that we maximize robotic potential in healthcare.

I. ROBOTS IN HEALTHCARE: DEMAND AND BENEFITS

Much of the demand for robots in healthcare stems from their ability to perform tasks that humans either cannot 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[8] and a shortage of

[8] *See e.g.*, Christopher J. Gearon, *Staffing the Hospital of Tomorrow*, U.S. News & World Report, October 16, 2013, http://health.usnews.com/health-news/hospital-of-tomorrow/articles/2013/10/16/staffing-the-hospital-of-tomorrow (explaining that "[h]ospital staffing changes are driven by an aging population, a physician workforce shortage and health care reform").

home caregivers.[9] This demand will continue to increase as one result of an aging population. 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.[10] This trend will have an especially great impact on 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.[11] But professional home care workers are in such high demand that their lack of qualifications and training are often overlooked.[12] Effectively designed robots could help meet this demand in a safer and more responsible, sustainable manner.

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 addition, homecare is often less expensive than institutionalization,[13] and many believe that robots may be preferable to humans in the home setting,[14] not only for their ability to outwork humans physically,[15] but also for their potential to provide emotional care and support.[16]

---

[9] *See* Barbara Peters Smith, *Finding skilled elder home care workers not easy*, Herald-Tribune, May 26, 2013, http://www.heraldtribune.com/article/20130526/ARTICLE/130529745/-1/sports?Title=NEW-Finding-skilled-elder-home-care-employees-not-easy.

[10] *See* United Nations, *World Population Ageing 1950-2050*, http://www.un.org/esa/population/publications/worldageing19502050/pdf/80chapterii.pdf.

[11] *See* Barbara Peters Smith, *Nation at crossroads in home care for elders*, Herald-Tribune, May 25, 2013, http://www.heraldtribune.com/article/20130525/ARTICLE/130529761 (describing how most older Americans prefer care in their own home to institutionalization).

[12] *See Finding skilled elder home care workers not easy*, supra n. 9 (describing "a fast-growing industry where many workers lack the training and skills needed for safe and reliable caregiving"). The rising demand for home nurses has caused many people to seek licenses who probably should not. *See id.* ("Paulina Testerman, an independent home health provider for 20 years in Sarasota, . . . says 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.").

[13] *See Nation at crossroads in home care for elders, supra* n. 11 ("Long-term care specialists agree that helping elders with care in their own homes could be more cost-effective than institutionalization — and it is what most older Americans prefer. But no one seems to know how the home care alternative would work on a larger scale.").

[14] Even with humans, there is a "danger of the complete transformation of caregiving into labor, creating a situation where people's basic physical needs are efficiently provided for by 'workers,' but their deeper human and spiritual needs are largely ignored." Larry Polivka, quoted in Barbara Peters Smith, *Robots and more: Technology and the*

Finally, there may be increasing demand for robots resulting from the trend within the industry toward personalized healthcare.[17] Robots may prove to be especially helpful for patients requiring rehabilitation[18] and for those with special needs.[19] Research in this area is underway,[20] and will likely increase in the coming years.

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

---

future of elder care, Herald-Tribune, May 27, 2013, http://www.heraldtribune.com/article/20130527/ARTICLE/130529720. Relatives are currently being asked to do too much for their sick and aging loved ones, without the proper skills and training. *See* Susan C. Reinhard, *Home Alone: Family Caregivers Providing Complex Chronic Care*, AARP Public Policy Institute, October 2012, http://www.aarp.org/home-family/caregiving/info-10-2012/home-alone-family-caregivers-providing-complex-chronic-care.html (explaining how "the role of family caregivers has dramatically expanded to include performing medical/nursing tasks of the kind and complexity once only provided in hospitals). In addition to professional home care workers being undertrained, elderly home care patients are all-too-frequently victims of emotional or financial exploitation. *See Finding skilled elder home care workers not easy*, supra n. 9 (explaining that "the share of elders who depend on paid assistance is at 35 percent and rising — and the job opportunities in home health for workers with limited educations and little screening compound the possibilities for elder fraud").

[15] For instance, the robots recently deployed in a University of California San Francisco hospital can each carry up to 1,000 pounds and travel 12 miles per day. Staff writer, *New SF Hospital Feels Like the Jetsons*, Youth Health Magazine, February 1, 2015, http://www.youthhealthmag.com/articles/8602/20150201/ucsf-mission-bay-hospital-robots-in-healthcare-robots-in-hospitals-aethon-robots-aethon.htm.

[16] *See Robots and more: Technology and the future of elder care*, *supra* n. 14 (quoting Larry Polivka, executive director of the Claude Pepper Center at Florida State University, "A lot of people get kind of silly about robots . . . They 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"). Despite concerns that robots as caregivers will prevent patients' emotional needs from being met, therapeutic robots like Paro demonstrate that robots can actually do a tremendous amount of good on the emotional front. *See* Paro Therapeutic Robot, http://www.parorobots.com/; *Japan develops robotic seals to comfort sick and elderly*, BBC, October 2, 2010, http://www.bbc.com/news/health-11459745.

[17] *See Notice of Updates to the National Robotics Initiative (NRI)*, October 23, 2014, http://grants.nih.gov/grants/guide/notice-files/NOT-EB-14-008.html ("Affordable and accessible robotic technology can facilitate wellness and personalized healthcare.").

[18] *See A Research Roadmap for Medical and Healthcare Robotics*, at 7, http://bdml.stanford.edu/twiki/pub/Haptics/HapticsLiterature/CCC-medical-healthcare-v7.pdf ("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.").

[19] *See id*. at 8 ("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.").

[20] *See e.g., MIT scientists launch personalized robot project*, Phys.org, April 3, 2012, http://phys.org/news/2012-04-scientists-personalized-robot.html ("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.").

issues[21] 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 will entail an appreciation for the ways in which data are, and will be, utilized by robots in healthcare, and the regulatory landscape within which these robots will operate.

As Frank Tobe has said, "The 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."[22] Ensuring that safety, security, and privacy are promoted during the development, deployment, and use of robots in healthcare will help ensure the long-term ability of robots to help stakeholders meet these goals.

II. ROBOT TYPES AND CHARACTERISTICS

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 NSF runs a National Robotics Initiative with NIH participation in its Computer Science and Robotics Research program devoted to medical robots.[23] Last year, the EU launched SPARC, the world's largest civilian robotics program, which has a focus on healthcare.[24] But probably the most significant public and private investment in healthcare-specific robotics is taking place in Japan. Given its own baby boom

[21] *See infra* Sections II & III.
[22] Frank Tobe, *Where Are the Elder Care Robots?*, IEEE Spectrum, November 12, 2012, http://spectrum.ieee.org/automaton/robotics/home-robots/where-are-the-eldercare-robots.
[23] *See* Michael S. Young, *Artificial Intelligence, Telemedicine, and Robotics in Healthcare*, The SciTech Lawyer, Volume 6, Number 4, Spring 2010, http://www.fellerssnider.com/userfiles/file/MYoung%20AI%20article.pdf (citing http://officeofbudget.od.nih.gov/pdfs/FY10/Significant Items.pdf).
[24] *See* http://sparc-robotics.eu/.

generation with growing needs, demand has sparked several independent research initiatives and plans for government projects.[25]

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 to identify the regulatory issues that must be confronted.

Perhaps the most frequently discussed robots in healthcare today are so-called "surgical robots," such as the daVinci Surgical System.[26] These systems present a number of interesting legal issues, especially involving product and practice liability.[27] However, because surgical robots are, at least for now, directly controlled by doctors, they 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.[28]

Another emerging robot in the hospital setting is what can be described as a "routine task" robot, such as the kind recently introduced in a University of California San Francisco (UCSF) hospital.[29] The UCSF robots were deployed in order to "bring meals and medications to

[25] *See* Christian Crisotomo, *Robots: Japan's Future Elderly Care Workers*, VR World, January 22, 2015, http://www.vrworld.com/2015/01/22/robots-japans-future-elderly-care-workers/. "Japan's elderly healthcare industry can be considered as a very important testbed that would help develop better robots in the future." *Id.* "[R]obots may soon be Japan's future elderly care workers." *Id.* "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." *Id.*

[26] *See* http://www.davincisurgery.com/da-vinci-surgery/da-vinci-surgical-system/.

[27] *See, e.g.*, Joe Carlson and Jaimy Lee, *Medical boon or bust? Suits raise allegations of defects in da Vinci robot*, Modern Healthcare, May 25, 2013, http://www.modernhealthcare.com/article/20130525/MAGAZINE/305259977; Sulbha Sankhla, *Robotic Surgery and Law in USA—a Critique*, http://www.roboticsbusinessreview.com/pdfs/Robotic_Surgery_%281%29.pdf.

[28] *See Berkeley's Autonomous Surgical Robotic System*, *supra* n. 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.").

[29] *See New SF Hospital Feels Like the Jetsons*, *supra* n. 15.

patients, transfer lab specimens, and carry linens," and can each carry up to 1,000 pounds and travel 12 miles per day.[30] These 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.[31] Although these robots' tasks are "routine" now, they may begin taking on medical or caregiving tasks as their development advances.

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. We are currently seeing the 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.

First, robots in the healthcare setting are performing an increasing number of functions,[32] which will only continue to grow in number. Such functions include providing medication assistance, helping move patients, and communicating with doctors. Functions will increase in complexity and variety as robots in healthcare access or connect with other devices.[33] With

[30] *Id.*
[31] *Id.*
[32] *See* Jessica Cocco, *Smart Home Technology for the Elderly and the Need for Regulation*, 6 JOURNAL OF ENVIRONMENTAL AND PUBLIC HEALTH LAW 85 (2011), http://pjephl.law.pitt.edu/ojs/index.php/pjephl/article/view/56/44 (explaining the difference between passive and active-intervention devices, and noting that robots resemble all three versions of active-intervention devices—sensors, reminder systems, and medication assistance).
[33] *See* RoboLaw, *Guidelines on Regulating Robotics*, September 22, 2014, at 175, http://www.robolaw.eu/RoboLaw_files/documents/robolaw_d6.2_guidelinesregulatingrobotics_20140922.pdf

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.

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. 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 will help robots maximize opportunities and fulfill specific medical and healthcare goals of doctors, patients, and consumers.

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. The consumer setting may prove to be a catalyst for the development of cloud robotics and a consumer market for such technology.[34]

But moving 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

(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"].

[34] *See* Andrew A. Proia, Drew Simshaw, Kris Hauser, *Consumer Cloud Robotics and the Fair Information Practice Principles: Recognizing the Challenges and Opportunities Ahead*, MINNESOTA JOURNAL OF LAW, SCIENCE, & TECHNOLOGY (forthcoming 2015).

a robot knowing and possibly sharing the location of medication, objects, and people[35]—all especially critical to a robot's ability to effectively aid in treatment and care. 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."[36] 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 security and privacy issues that must be addressed.

III. THE DISTINCTIVE FEATURES OF ROBOT DATA COLLECTION AND USE

In light if their tremendous benefits, the complexity of robot data collection and use practices raise potential security and privacy issues in the healthcare setting.[37] The future healthcare robot will monitor patients closely at all hours (one of their advantages over humans), and 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

[35] *See* Evan Ackerman, *Hoaloha Robotics Developing Socially Assistive Hardware Platform*, IEEE Spectrum, September 4, 2013, http://spectrum.ieee.org/automaton/robotics/home-robots/hoaloha-robotics-developing-socially-assistive-hardware-platform (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").

[36] RoboLaw, *supra* n. 33, at 169 (citation omitted).

[37] *See, e.g.*, *id.* at 177 ("Diagnostic, monitoring tools or any other device can be placed on board robots, thus gathering data on their environment and people. These 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.").

unprecedented resulting overall information they will possess about users.[38] 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.[39] This is especially true in the healthcare context, where wearables and mobile applications increasingly collect health and wellness related information about users. 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."[40]

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.

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."[41]

---

[38] For example, RoboLaw has explained 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.'" *Id*. at 189 (citations omitted).

[39] *See id*. ("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.").

[40] Adam Thierer, *CES 2015 Dispatch: Challenges Multiply for Privacy Professionals, Part Two*, IAPP Privacy Perspectives, January 14, 2015, https://privacyassociation.org/news/a/ces-2015-dispatch-challenges-multiply-for-privacy-professionals-part-two/

[41] RoboLaw, *supra* n. 33, at 175.

The pace at which robots are being developed and adopted, in light of their tremendous potential benefit, could risk marginalizing certain security and privacy considerations if proper attention is not paid at all stages of design, deployment, and use. As robotics in healthcare advances, it will be important to constantly reexamine existing and emerging data practices and evaluate the ways in which data will be collected, processed, stored, and used, and by whom, and to gauge the awareness of roboticists and manufacturers when it comes to the resulting regulatory challenges, outlined below.

IV. THE CURRENT REGULATORY FRAMEWORK

A. Device Regulation

Certain robots in healthcare are subject to regulation by the Food and Drug Administration (FDA) as "medical devices." Devices subject to such regulation are broadly defined as "an instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, 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, in man or other animals, or . . . intended to affect the structure or any function of the body of man or other animals."[42] These medical devices are subject to safety regulations enforced by the Center for Devices and Radiological Health,[43] and specifically the Federal Food Drug & Cosmetic Act's premarket review whenever a device is being marketed for the first time, proposing a new intended use, or making changes that could significantly affect safety or effectiveness.

[42] Section 201(h) of the Federal Food Drug & Cosmetic (FD&C) Act.
[43] *See* http://www.fda.gov/AboutFDA/CentersOffices/OfficeofMedicalProductsandTobacco/CDRH/.

As certain medical devices which are currently regulated begin to take on increasingly autonomous functions (such as a robotic surgical system beginning to perform without doctor assistance),[44] they will likely continue to be regulated as medical devices. Less clear, however, is how the FDA will treat robots that initially perform only "routine tasks," but eventually begin taking on certain healthcare tasks. These questions will also arise as personal consumer robots in the home perform an increasing number of tasks that could be considered medical.

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.[45] First released in 2013, this nonbinding guidance on "mHealth apps" took a risk-based approach to regulation of these emerging technologies. 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."[46] Accordingly, the FDA will not regulate low risk apps that only coach, prompt, or help patients communicate with providers, nor will it regulate apps that serve as "fitness trackers" or "wellness coaches." 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.[47] Finally, device regulation will apply to apps performing patient-specific analysis or providing patient-specific diagnosis or treatment recommendations. Like mobile apps, robots may adopt

[44] *See Berkeley's Autonomous Surgical Robotic System*, *supra n. 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.").
[45] *See Mobile Medical Applications Guidance for Industry and Food and Drug Administration Staff*, February 9, 2015, available at http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM263366.pdf
[46] *Id*. at 4.
[47] 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.

many of these functions. Unlike other technologies, though, robots will be able to go further and physically and socially interact with the user.

If the FDA were to take a similar approach to robot regulation, we could expect that a robot's specific functions would determine whether it is subject to device regulation. For robots that are developed in the form of increasingly autonomous versions of existing medical devices, device regulation should continue to apply. 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" will depend on the specific functions adopted.

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."[48] Accordingly, the FDA offers special guidance for home use devices,[49] which outline some of the unique safety challenges presented in the home. Although it does not mention robots, 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. However, the challenges presented by personal care robots will differ from both medical devices and other robots. RoboLaw has explained, for instance,

[48] Food and Drug Administration, *Home Use Devices*, http://www.fda.gov/MedicalDevices/ProductsandMedicalProcedures/HomeHealthandConsumer/HomeUseDevices/default.htm.

[49] *See, e.g.*, *Design Considerations for Devices Intended for Home Use - Guidance for Industry and Food and Drug Administration Staff*, November 24, 2014, available at http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm331675.htm; *Medical Device Home Use Initiative*, white paper, April 2010, http://www.fda.gov/downloads/MedicalDevices/ProductsandMedicalProcedures/HomeHealthandConsumer/HomeUseDevices/UCM209056.pdf.

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; (2) they are used by non-specialist users; and (iii) they share work space with humans."[50] Premarket review of "safety" for robots must take these unique considerations into account.

Second, and even more relevant to all robots in healthcare, whether in the hospital or the home, is the FDA's recent cybersecurity guidance for medical device manufacturers,[51] recommending that they "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."[52] In addition, the FDA released a "safety communication" to manufacturers and healthcare organizations, listing steps they should consider taking to mitigate cybersecurity risks to medical devices.[53] The FDA also opened a cybersecurity lab to test medical devices.[54]

Robot designers and manufacturers must be aware of the FDA's emphasis on cybersecurity to ensure successful deployment, because even though the current guidelines are

[50] RoboLaw, *supra* n. 33, at 174.
[51] *Content of Premarket Submissions for Management of Cybersecurity in Medical Devices*, U.S. Department of Health and Human Services, Food and Drug Administration, issued on October 2, 2014, available at http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM356190.pdf.
[52] FDA News Release, *The FDA takes steps to strengthen cybersecurity of medical devices*, October 1, 2014, available at http://www.fda.gov/NewsEvents/Newsroom/PressAnnouncements/ucm416809.htm. 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." *Id*.
[53] Food and Drug Administration, *Cybersecurity for Medical Devices and Hospital Networks: FDA Safety Communication*, issued June 13, 2013, available at http://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm356423.htm [hereinafter "FDA Safety Communication"].
[54] *See* Emily Wasserman, *FDA beefs up cybersecurity efforts to ensure safety standards*, Fierce Medical Devices, June 6, 2014, http://www.fiercemedicaldevices.com/story/fda-beefs-cybersecurity-efforts-ensure-safety-standards/2014-06-06 ("The agency also created a 'cybersecurity laboratory,' which stages deliberate cybersecurity attacks to sniff out any defects that could leave a device open to attack.").

merely recommendations, they may become *de facto* requirements in the future.[55] Because hospital networks are notoriously insecure,[56] subjecting robots to this environment only magnifies vulnerabilities already posed to regular medical devices and health records. Indeed, the threats to physical safety caused by insecure medical devices of all kinds are real,[57] and may be magnified with robots due to their ability to manipulate their surroundings. FDA regulation is an important part of ensuring that devices, including robots, are safe and secure.

But with their autonomous, mobile, and interactive abilities, the technical and social complexities of robots in healthcare are quickly and starkly surpassing those of traditional medical devices, which increase the risk of harms beyond just physical safety. 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 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.[58] Marginalized under current device regulation is attention to security vulnerabilities that do not necessarily affect a patient's physical

[55] Philip Desjardins, *FDA Scrutinizes Networked Medical Device Security*, InformationWeek, December 1, 2014, http://www.informationweek.com/healthcare/security-and-privacy/fda-scrutinizes-networked-medical-device-security/a/d-id/1317758 ("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.").

[56] *See, e.g.*, FDA Safety Communication, *supra* n. 53 ("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*, LA Times, August 18, 2014, http://www.latimes.com/business/technology/la-fi-tn-community-health-hacked-20140818-story.html.

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

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

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.

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, after the devices have been approved by the FDA and are in use. But, as the following section will describe, this is not the case with certain private consumer robots operating outside of HIPAA's domain. After these robots are determined to be physically safe and are released to the public, users will rely heavily on the FTC for subsequent security and privacy protection.[59] 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

Healthcare data challenges are well known. For example, hospitals and medical devices have been identified in recent years as being notoriously insecure.[60] 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

[59] *See infra* Section IV.B.
[60] *See*, *e.g.*, FDA Safety Communication, *supra* n. 53; Garland, *supra* n. 56.

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.[61]

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[62] "provides federal protections for individually identifiable health information held by covered entities and their business associates,"[63] 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). The HIPAA Security Rule,[64] also enforced 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."[65] 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.[66] "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."[67]

[61] *See, e.g.*, Thierer, *supra* n. 40.
[62] 45 CFR 160, 164 A, E
[63] *Understanding Health Information Privacy*, U.S. Department of Health & Human Services, http://www.hhs.gov/ocr/privacy/hipaa/understanding/.
[64] 45 CFR 160, 164 A, C
[65] *Understanding Health Information Privacy*, *supra* n. 63.
[66] 45 CFR 160.103; *See also, To Whom Does the Privacy Rule Apply and Whom Will It Affect?*, U.S. Department of Health and Human Services, National Institutes of Health, http://privacyruleandresearch.nih.gov/pr_06.asp.
[67] Health Information Privacy, U.S. Department of Health & Human Services, http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/businessassociates.html. *See also* definition of "business associate" at 45 CFR 160.103.

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.[68] 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.[69]

Because the vast majority of hospitals are HIPAA covered entities, identifiable health information collected by robots which are controlled by hospitals or their business associates will be subject to the Privacy and Security Rules. 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.

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. Issues will arise as the healthcare setting expands to the home, where many popular health technologies operate outside of HIPAA's domain, including personal "wearables" such as Fitbit[70] and the aforementioned mobile medical apps.[71] But even those robots in the home that are subject to HIPAA will encounter data protection challenges. For example, Boston Children's Hospital's recent pilot program sent robots home with children

[68] *See* Nicolas P. Terry, *Protecting Patient Privacy in the Age of Big Data*, 81 UMKC LAW REVIEW 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.") [hereinafter "Protecting Patient Privacy"].
[69] *See supra* Section IV.A.
[70] *See* http://www.fitbit.com/.
[71] *See supra* Section IV.A.

following urological surgery in order to further monitor their health.[72] 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, not all of which would necessarily be protected health information under HIPAA,[73] a law constructed for the traditional healthcare setting.

Even less clear is how the law applies to independent at-home personal care robots which might not be directly affiliated with a traditional covered entity, but whose information is just as, if not more, sensitive. This may become a realistic scenario as domestic consumer "personal assistant" robots (such as Jibo[74] and Pepper[75]), 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.

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. 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

[72] *See* Erin McCann, *Health IT promises new paradigm of patient care*, Healthcare IT News, September 12, 2012, http://www.vgocom.com/health-it-promises-new-paradigm-patient-care.

[73] This has been described as the case with smart home technology for the elderly, as well. "The 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." Cocco, *supra* n. 32 at 104 (footnote omitted).

[74] *See* http://www.jibo.com/.

[75] *See* https://www.aldebaran.com/en/a-robots/who-is-pepper.

providers.[76] Robots in healthcare will highlight the fact that these essential and highly involved "business associates" are now directly liable under the HIPAA final omnibus rule.[77]

It does not follow, though, that these robots will be completely unregulated. Indeed, some oversight such as FDA device regulation[78] likely would still apply. However, the data protection model is more complicated. It is possible that some state privacy laws may apply, but even the most pro-privacy of these[79] would not currently apply to "consumer" robots operating in a "HIPAA-free zone."[80]

Rather, most responsibility in such cases would fall on the Federal Trade Commission (FTC). This agency does not differentiate between health data protection in conventional and emerging healthcare spaces.[81] Rather, it protects data somewhat indirectly by enforcing privacy policies or otherwise characterizing bad data practices as unfair or misleading. This agency's role may expand in the coming years, as 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.

The FTC has become increasingly active in consumer privacy matters related to the Internet of Things[82], big data, [83] and data brokers[84], all of which have had significant impact on

[76] *See supra* Section II.
[77] *See* Department of Health and Human Services, *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; Final Rule*, February 25, 2013, http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf.
[78] *See supra* Section IV.A.
[79] California Confidentiality of Medical Information Act (CMIA), Civil Code, Section 56-56.07, available at http://www.leginfo.ca.gov/cgi-bin/displaycode?section=civ&group=00001-01000&file=56-56.07.
[80] *See* Protecting Patient Privacy, *supra* n. 68 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.").
[81] *See In re LabMD*, available at https://www.ftc.gov/enforcement/cases-proceedings/102-3099/labmd-inc-matter.
[82] *See, e.g, Internet of Things: Privacy and Security in a Connected World*, FTC Staff Report, https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf [hereinafter "FTC IoT Report"].
[83] *See, e.g., Big Data: A Tool for Inclusion or Exclusion?*, FTC Events, September 15, 2014, https://www.ftc.gov/news-events/events-calendar/2014/09/big-data-tool-inclusion-or-exclusion.

health information in recent years. The agency will also likely play a critical role in any attempt to regulate consumer robots, which may become more widespread in the near future.[85] In light of rising demand for home healthcare services, healthcare-related functions will likely be performed by both general "personal assistant" robots and, eventually, by robots designed specifically to provide healthcare. As previous sections have described, some of these robots will be regulated for physical safety by the FDA, including cybersecurity to the extent that it affects device functionality, but not broader security harms. 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.

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.[86] In most cases, HIPAA covered entities are exempt from FTC oversight in light of their existing HIPAA obligations. But 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 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.

---

[84] *See, e.g., Data Brokers: A Call for Transparency and Accountability*, Federal Trade Commission, May 2014, https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.

[85] *See generally*, Proia et. al. *supra* n. 34.

[86] *See id*. (explaining the heightened focus on certain Fair Information Practice Principles necessary when sensitive information is involved).

As recently as 2012, the FTC's report "Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers"[87] implied that HIPAA's Privacy and Security Rules adequately protect health information.[88] 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.[89] The White House's 2015 draft consumer privacy bill[90] seems 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.[91] Such dual regulation may seem 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.[92]

One way to enable such a regulatory scheme would be 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

[87] *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers*, FTC Report, March 2012, https://www.ftc.gov/reports/protecting-consumer-privacy-era-rapid-change-recommendations-businesses-policymakers.
[88] Nicolas Terry, *Should Health Lawyers Pay Attention To The Administration's Privacy Bill?*, HealthAffairs Blog, March 13, 2015, http://healthaffairs.org/blog/2015/03/13/should-health-lawyers-pay-attention-to-the-administrations-privacy-bill/.
[89] *Id.*
[90] *Administration Discussion Draft: Consumer Privacy Bill of Rights Act of 2015*, https://www.whitehouse.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf.
[91] *See* Terry, *supra* n. 88 ("[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.").
[92] *See* Protecting Patient Privacy, *supra* n. 68 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.").

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."[93]

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.[94] These concerns mirror those expressed at the FTC's 2013 workshop on the Internet of Things.[95] In addition, the FTC has acknowledged the significance of the sheer volume of data that will be generated by home connected devices.[96] 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.[97] These uses would present challenging questions, even

[93] *Id*. at 407. In this sense, "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." *Id*.

[94] *See, e.g.*, Cocco, *supra* n. 32 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.").

[95] *See Transcript of 2013 FTC IoT Workshop*, at 14, http://www.ftc.gov/sites/default/files/documents/public_events/internet-things-privacy-security-connected-world/final_transcript.pdf ("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)) [hereinafter "IoT Workshop Transcript"]. *See also*, FTC IoT Report, *supra* n. 82.

[96] IoT Workshop Transcript, *supra* n. 95, 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)).

[97] *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

beyond privacy and security.[98] 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 it.[99]

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."[100] So whereas OCR and the FDA may be unable or unwilling to expand their roles to

---

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)).

[98] E.g., "Do we want insurance companies to offer lower premiums to people who share data from their healthcare robot?" *See id*. at 17.

[99] "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." FTC IoT Report, *supra* n. 82. *See also*, Susan D. Hall, FTC report on IoT calls for update to HIPAA standards, FierceHealthIT, January 28, 2015, http://www.fiercehealthit.com/story/ftc-report-internet-things-calls-updated-hipaa-standards/2015-01-28 ("[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.").

[100] FTC IoT Report, *supra* n. 82, at vii-viii (emphasis added).

account for the gaps in security and privacy protections that will be exposed by robots in healthcare, the FTC appears both willing and able to do so.

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.

CONCLUSION AND RECOMMENDATIONS

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 and Pepper). 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.

Many robots will be regulated by the FDA as medical devices, including increasingly autonomous existing 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 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.

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 which 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 may be appropriately conducted by an agency that examines all robots with medical and healthcare-related functions.[101]

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 could be to remove the sector-based limitations currently limiting the FTC's influence in healthcare.

[101] *See, e.g.*, Ryan Calo, The Case for a Federal Robotics Commission, The Brookings Institution, September 2014, http://www.brookings.edu/research/reports2/2014/09/case-for-federal-robotics-commission.

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

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 which 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.