Data Collection, Privacy, and the Role of Regulatory Agencies in Healthcare Robotics

Drew Simshaw
Indiana University
Center for Law, Ethics, and Applied
Research in Health Information
2719 E. 10th St., Suite 231
Bloomington, IN 47408
+1 (812) 856-1497
dsimshaw@indiana.edu

ABSTRACT
Healthcare is one of the most dynamic areas of robotics research and development today. From robot-assisted surgery, to robotic nurses, to in-home rehabilitation and eldercare robots, the possibilities and benefits seem endless. Demand for these robots will only continue to rise with traditional healthcare costs and an aging population. But as healthcare robots become more autonomous, we will continue to see significant changes in the way sensitive health data are collected, processed, and stored, magnifying existing privacy and security concerns, and creating new ones. As in many other sectors, healthcare technology is advancing faster than the laws designed to protect privacy and promote security. Robot manufacturers, healthcare professionals, patients, and law and policy makers must consider these implications now and in the coming years, when critical healthcare robot design will take place.

Challenge Theme & Submission Type
H: Healthcare **Q**: Question

General Terms
Design, Economics, Security, Human Factors, Security, Theory, Legal Aspects.

Keywords
Health, Healthcare, Law, Policy, Regulation, Security, Data Security, Information Security, Cybersecurity, Privacy.

1. INTRODUCTION
Two particular regulatory considerations for healthcare robots concerning privacy and security stem from two United States federal agencies: the Department of Health and Human Services, and its enforcement of HIPAA's Privacy and Security Rules, and the Food and Drug Administration's regulation of medical devices. Evaluating these agencies' roles requires examining current regulation within the context of larger legal, ethical, and social implications of robots in healthcare, and considering the best way to maximize opportunities and innovation, while minimizing privacy and security risks.

The Emerging Policy and Ethics of Human Robot Interaction, Mar 2, 2015, Portland, OR, USA.

2. U.S. REGULATORY AGENCIES

2.1 Department of Health & Human Services
First, certain health information generated, shared, and utilized by robots in healthcare will be subject to the Health Insurance Portability and Accountability Act (HIPAA), and specifically the law's Privacy and Security Rules. The HIPAA Privacy Rule [1] "provides federal protections for individually identifiable health information held by covered entities and their business associates and gives patients an array of rights with respect to that information" [2]. The HIPAA Security Rule [3] "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" [4].

Robots in healthcare greatly expand not only the sheer amount of personal health information that is collected, but also the ways in which those data are processed, stored, and used, and by whom. While many popular health technologies operate outside of HIPAA's domain (such as personal "wearables," e.g., Fitbit), certain robots could serve as a "vector" between the hospital and the home depending on who controls the robot and with whom the information is shared, greatly expanding the zone in which HIPAA applies. For example, Boston Children's Hospital's recent pilot program sent robots home with children following urological surgery in order to further monitor their health [5]. While HIPAA's applicability to a robot owned and operated by the patient's hospital (a covered entity) may be relatively straight forward, 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.

As personal robots continue to collect more information for a patient's own use, healthcare providers will understandably become increasingly inclined to gain access to and use the information as part of a patient's overall health management, creating an unprecedented expansion and centralization of patient data. Overall, the health data these robots generate, share, and rely on represent a far more complete, and therefore sensitive, account of a patient's health than is found in common medical and health records.

2.2 Food & Drug Administration
Second, robots in healthcare are regulated as "medical devices" by the United States Food and Drug Administration, 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" [6].

Even though the FDA has not offered specific guidance on medical robots, it has addressed other new healthcare technologies, including mobile medical applications. The FDA has explained that it "has a public health responsibility to oversee the safety and effectiveness of medical devices – including mobile medical apps," and that it "will apply the same risk-based approach the agency uses to assure safety and effectiveness for other medical devices" [7].

Once classified as "medical devices," such robots are subject to the FDA's recent cybersecurity guidance for medical device manufacturers [8], 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" [9]. With their autonomous, mobile, and interactive abilities, the complexities of medical robots are quickly and starkly surpassing those of traditional medical devices. Although the FDA's recent emphasis on cybersecurity is important, it is only focused on threats as they relate to device functionality and physical safety, and not necessarily potential harm to a patient's privacy and psychological wellbeing. Marginalized under this guidance is attention to data security vulnerabilities that do not necessarily affect a patient's physical safety, but nevertheless lead to unauthorized access to and use of valuable and sensitive health information, of which robots will have an unprecedented amount.

3. PROACTIVE CONSIDERATIONS

Ensuring that privacy and security risks are effectively managed is essential to realizing the benefits robots bring to healthcare. It is important that these risks are not overlooked by doctors, hospital patients, and users of at-home medical robots, in light of the unprecedented benefits these life-like caregivers will provide in the face of ever-growing demand. Many of these risks can be anticipated and appreciated today with an understanding of the types of data collected, how they are stored and used, and by whom. Under current regulation, the FDA proactively addresses the need for advanced consideration of security, but only as it relates to physical safety, and HIPAA protects only certain data in certain hands after those data are created and stored. Robot exceptionalism requires expanding our notion of patient "safety" to include larger privacy and ethics considerations among those that must be proactively accounted for, subject to oversight by an existing or entirely new health or robotics agency.

Healthcare is not an area that can afford to be reactive in its approach to robotics law and policy. Effective mitigation will require prospective appreciation of existing and anticipated risks to privacy and security, which should be accounted for throughout a robot's design, deployment, and use in the healthcare setting. Increased proactive commitment from policymakers, healthcare providers, and roboticists to effective risk management practices and certain "privacy by design" principles will help maximize opportunities for robotics in the healthcare setting, while minimizing risks to privacy and security. Such proactive policy will better facilitate robot innovation and deployment than waves of reactionary restrictions that would result from high profile breaches or privacy violations in the future, ultimately stifling long term innovation.

4. INTERDISCIPLINARY SOLUTIONS

Such proactive solutions will require the involvement of medical robot engineers, designers, and manufacturers, as well as healthcare providers who are currently utilizing, or planning to utilize, robots in their practice. It will also be useful to third parties, such as cloud service providers, who will be storing and processing the massive amounts of data necessary for advanced robots to function, as these providers now constitute HIPAA "covered entities" as business associates of healthcare providers. Such interdisciplinary collaboration will help lawyers, policy analysts, privacy and cybersecurity professionals, and law and policy makers charged with the difficult but imperative task of crafting a regulatory environment that maximizes these robots' potential, while minimizing the associated privacy and security risks. This interdisciplinary collaboration is essential if healthcare robots are to continue have a smooth, secure, and responsible deployment into the healthcare arena.

5. ACKNOWLEDGMENTS

Thanks to Kris Hauser, Nicolas Terry, and Missy Cummings for providing valuable insight into the development of this topic, and to the HRI 2015 Workshop on The Emerging Policy and Ethics of Human-Robot Interaction for the opportunity to discuss it. Thanks also to the directors and staff of Indiana University's Center for Applied Cybersecurity Research (CACR) and Center for Law, Ethics, and Applied Research in Health Information (CLEAR) for their support and guidance. Final thanks to Andrew Proia for his prior collaboration that inspired this topic.

6. REFERENCES

[1] 45 CFR 160, 164 A, E.

[2] *Understanding Health Information Privacy*, U.S. Department of Health & Human Services, http://www.hhs.gov/ocr/privacy/hipaa/understanding/.

[3] 45 CFR 160, 164 A, C.

[4] *Understanding Health Information Privacy , supra* note 2.

[5] *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.

[6] The Federal Food Drug & Cosmetic (FD&C) Act, Section 201(h).

[7] FDA 2013 Mobile Medical Applications guidance, available at http://www.fda.gov/MedicalDevices/ProductsandMedicalProcedures/ConnectedHealth/MobileMedicalApplications/ucm255978.htm.

[8] *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.

[9] 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.