NOTES

THE REGULATORY ARMS RACE: MOBILE-HEALTH APPLICATIONS AND AGENCY POSTURING

Daniel F. Schulke[*]

Mobile-health applications are largely unregulated by the federal government. These applications have tremendous potential to reduce the costs of caring for chronic disease patients. This is particularly true in rural communities where mobile-health applications could increase patient engagement and improve the quality of care. While these applications can be helpful in transforming and improving patient care, unregulated applications may harm patients or unintentionally release protected health information. The U.S. Food and Drug Administration (FDA) has asserted jurisdiction over some mobile-health applications as medical devices. FDA, however, lacks experience regulating the data security and interoperability of devices – an area in which the Office of the National Coordinator for Health Information Technology (ONC) has substantial experience. This Note explores several frameworks for regulating mobile-health applications as well as the advantages and disadvantages of each framework. This Note concludes by

[*] J.D. Candidate, 2014, Boston University School of Law. I would like to thank Susan Winckler and Kathy Kenyon for their invaluable assistance.

proposing two separate regulatory frameworks for mobile-health applications with different agencies responsible for each framework. Ultimately, FDA should use its authotity to regulate the clinical safety and effectiveness of mobile-health applications because of the substantial health risks that they pose to patients. While data security, and to a lesser extent interoperability, is an important consideration in safeguarding patients, private regulators operating under the supervision of ONC should have the ultimate responsibility for implementing protections in these areas.

INTRODUCTION

In recent years, the technological capabilities of mobile phones and mobile phone applications have advanced dramatically. As part of this expansion, both patients and physicians are increasingly utilizing healthcare-focused mobile-phone applications, or mobile-health (mHealth) applications, in clinical care. These applications serve a variety of functions. Some applications provide easy access to medical information like the symptoms and treatments for various diseases. Some applications are designed for patient use and track clinical measurements (like blood pressure readings or insulin levels), and a subset of these applications have the capability to calculate insulin doses or send the patient's clinical readings to a provider's electronic health record system (EHR). Not all applications are patient focused and providers can use applications on a tablet or phone to view and enter patient data into an EHR or send prescriptions through a computerized physician order entry system (CPOE).

Despite these attractive features, mHealth applications are largely unregulated and may pose substantial risks to the health and safety of consumers,[1] as well as to the privacy and security of consumer protected health information (PHI).[2] Medical devices are currently regulated by the Food and Drug Administration (FDA). MHealth applications, however, pose challenges that FDA's regulatory stucture is not yet capable of addressing. FDA has not regulated software for smartphones in the past and focused mainly on

[1] Health and safety refers to the physical health of a patient. For example, an mHealth applications could provide inaccurate information on how to treat a condition causing a negative impact on a patient's overall health.

[2] Patient privacy and security refers to safeguarding protected health information (PHI). *See* 45 C.F.R. § 160.103 (2012) (defining PHI). Privacy is an individual's right to control access to his PHI. *Protecting Your Privacy & Security*, HEALTHIT.GOV, http://www.healthit.gov/patients-families/your-health-information-privacy (last visited Sept. 5, 2013). Security is the device's or user's ability to protect PHI from unauthorized disclosure either when stored on the device or transmitted to another device. *Id.* Security requires technical safeguards, such as encryption, workstation security, and access controls, while privacy focuses more on an organization's policy and procedure for protecting PHI. While privacy and security overlap and have similar protections, this Note focuses on security standards for protecting data on mobile devices.

"software used as a component, or accessory of a medical device."[3] FDA has failed in the past to address security concerns present in approved medical devices.[4] Moreover, FDA's regulatory system is illsuited to regulate mHealth applications because the mHealth application industry is constantly innovating and responding to technological advances. FDA already takes a substantial amount of time to review and approve devices for safe and effective use.[5] Imposing FDA regulation on a market (like the mHealth application market) that responds quickly to technological change will significantly reduce innovation as the application developers adjust to the lengthy and rigorous FDA approval process. A potential regulatory partner for FDA, the Office of the National Coordinator for Health Information Technology (ONC), has some experience in developing privacy, security, and interoperability standards for software through its work with EHRs. ONC, however, lacks the regulatory authority to assist FDA in regulating mHealth applications.

FDA has asserted authority over mHealth applications that operate in a manner similar to medical devices and have the potential to cause substantial patient harm.[6] FDA will exercise enforcement discretion over mHealth applications that meet the definition of a device but pose a lower risk to the public health.[7] Despite FDA's claim of authority to regulate mHealth applications, Congress mandated that FDA, ONC, and the Federal Communications Commission (FCC) collaborate and draft a report on the most

[3] U.S. FDA, GENERAL PRINCIPLES OF SOFTWARE VALIDATION 2 (2002), http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm085281.htm (describing FDA's guidance for validating medical device software).

[4] *See* U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-12-816, MEDICAL DEVICES: FDA SHOULD EXPAND ITS CONSIDERATION OF INFORMATION SECURITY FOR CERTAIN TYPES OF DEVICES 16 (2012) (listing vulnerabilities present in active implantable medical devices). The popular show *Homeland* featured these device security vulnerabilities late in Season 2 when a hacker exploited an implantable medical device. *See* Tarun Wadhwa, *Potentially Perfect Crime: Assassination via Medical Device Hack*, MEDCITY NEWS (Dec. 6, 2012), http://medcitynews.com/2012/12/potentially-perfect-crime-assassination-via-medical-device-hack (describing a *Homeland* episode in which "the Vice President of the United States is assassinated by a group of terrorists that have hacked into the pacemaker controlling his heart").

[5] *See infra* notes 82-96 and accompanying text (describing the cumbersome FDA approval process).

[6] Mobile Medical Applications, 78 Fed. Reg. 59,038, 59,038 (Sept. 25, 2013) ("FDA intends to apply its regulatory oversight to only those 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."); *see also* U.S. FDA, GUIDANCE, MOBILE MEDICAL APPLICATIONS (2013), *available at* http://www.fda.gov/downloads/ MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM263366.pdf (providing more details on FDA's proposed regulatory approach to mHealth applications).

[7] *Id.* ("Some mobile apps may meet the definition of a medical device but because they pose a lower risk to the public, FDA intends to exercise enforcement discretion over these devices (meaning it will not enforce requirements under the FD&C Act).").

effective way to regulate including mHealth applications.[8] This Note analyzes several potential regulatory frameworks for FDA and ONC and evaluates the feasibility of these frameworks. in light of the dual goals of protecting consumers and encouraging developer innovation. This Note does not address *how* applications should be regulated (for example, through a risk-based regulatory framework), but rather *who* should regulate the devices between private regulators and the government, and between specific government agencies.

Part I of this Note reviews the background of mHealth applications and analyzes their potential to improve health care in rural areas and for those with chronic diseases. Part II analyzes the problems posed by unregulated mHealth applications. This Part focuses mainly on issues of data security, privacy, and interoperability, and also addresses patient safety concerns that arise from the malfunction or inappropriate use of mHealth applications. Part III then examines the existing regulatory structure and the authority of FDA and ONC to regulate mHealth applications. Part III also addresses existing initiatives by the agencies that may provide insight in the context of regulating mHealth applications. Part IV considers the existing regulatory structure, authority, and expertise examined in Part III and proposes three regulatory structures: private regulation, public regulation, and meta-regulation. This Note concludes that a regulatory model that combines public regulation with meta-regulation is the most ideal way to regulate mHealth applications based on current market realities, and on the expertise, authority, and current regulatory activities of FDA and ONC.

I. MOBILE-HEALTH APPLICATIONS AND THEIR POTENTIAL TO IMPROVE HEALTH CARE

As the United States has pushed to improve the quality and reduce the cost of health care, it has partially focused on incentivizing the development of a nationwide health information infrastructure that can improve the quality of patient care by harnessing the power of technology.[9] The United States is

[8] Food and Drug Administration Safety and Innovation Act, Pub. L. No. 112-144, § 618, 126 Stat. 993, 1063 (2012) (requiring these agencies to publish a report containing "a proposed strategy and recommendations on an appropriate, risk-based regulatory framework pertaining to health information technology, including mobile medical applications, that promotes innovation, protects patient safety, and avoids regulatory duplication"). This Note does not discuss FCC's role because this Note focuses on patient safety, and data standards on privacy, security, and interoperability. For information on FCC's role in regulating mHealth applications, see Keith Barritt, *Wireless Medical Devices: Navigating Government Regulation in the New Digital Age*, MED. DEVICES L. & INDUSTRY REP., Mar. 1, 2010, at 39 (discussing FCC's role in regulating medical devices that utilize "wireless communications technology").

[9] *See* American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, 123 Stat. 115, 226-79 (2009) (establishing grants to incentivize the adoption of electronic health records and altering the HIPAA breach notification requirements); Health Insurance

encouraging physicians to utilize computers in the form of a CPOE or EHR to improve the coordination of care between different providers, reduce medical errors, and improve medical records.[10] For the most part, these efforts have focused on the use of EHRs within physician practices and hospitals, but the development of mHealth applications has enabled patients to join in these efforts as well.

MHealth encompasses "any use of mobile technology to address healthcare challenges such as access, quality, affordability, matching of resources, and behavioral norms."[11] FDA's guidance defines a mobile application as a "software application that can be executed (run) on a mobile platform . . . , or a web-based software application that is tailored to a mobile platform but is executed on a server."[12] An mHealth application is a mobile application that is intended to "be used as an accessory to a regulated medical device; or to transform a mobile platform into a regulated medical device."[13] These applications are complex and utilize different technologies to transfer information.[14] The operating systems for mobile phones are just as diverse.[15] Mobile phones can capture information through image recognition, text recognition, and text-to-speech conversion programs.[16] Furthermore, mobile

Portability and Accountability Act (HIPAA) Privacy Rule, 45 C.F.R. §§ 160, 164.102-.106, 164.500-.534 (2012) (establishing requirements to protect the privacy of patients' protected health information); HIPAA Security Rule, 45 C.F.R. §§ 160, 164.102-.106, 164.302-.318 (2012) (establishing national standards to protect electronic personal health information).

[10] *See, e.g.*, U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-11-49, HEALTH CARE DELIVERY: FEATURES OF INTEGRATED SYSTEMS SUPPORT PATIENT CARE STRATEGIES AND ACCESS TO CARE, BUT SYSTEMS FACE CHALLENGES 9 (2010) ("[U]sing EHRs facilitates care coordination because EHRs make patient clinical information more readily available to providers and improve communication among providers, staff, and patients."); David C. Radley et al., *Reduction in Medication Errors in Hospitals Due to Adoption of Computerized Provider Order Entry Systems*, 20 J. AM. MED. INFORMATICS ASS'N 470, 473 (2013) ("At the rate of CPOE adoption and implementation in 2008, our findings suggest that medication errors were reduced by ~12.5% . . . . This equates to ~17.4 million . . . fewer medication errors over a 1-year period than would be expected without CPOE.").

[11] CHRISTINE ZHENWEI QIANG ET AL., WORLD BANK, MOBILE APPLICATIONS FOR THE HEALTH SECTOR 11 (2011), *available at* http://siteresources.worldbank.org/INFORMATIONANDCOMMUNICATIONANDTECHNOLOGIES/Resources/mHealth_report.pdf.

[12] U.S. FDA, *supra* note 6, at 7.

[13] *Id.* at 7-8 ("The intended use of a mobile app determines whether it meets the definition of a device.").

[14] *See* QIANG ET AL., *supra* note 11, at 12 (listing the technologies used to transmit mHealth information: "GSM, GPRS, 3G, and 4G-LTE mobile telephone networks; WiFi and WiMAX computer-based technologies; and Bluetooth for short-range communications").

[15] *See id.* (listing the software platforms supporting mHealth applications, ranging from "open-source operating systems like Linux, Google's Android, and Nokia's Symbian to proprietary ones like Apple's iOS and Microsoft's Windows 7 Mobile").

[16] *Id.* ("Overlaid with these operating systems are ways of capturing and processing data

phones can collect physiological data through device attachments.[17] The varied data technologies, operating system standards, and data capturing and processing methods utilized by mobile phone manufacturers creates a complex environment for regulation. When companies use different technologies to transfer data for each device they manufacture, regulators have difficulty developing universal standards for data transfer. Regulating these companies and application developers is even more burdensome if manufacturers develop their own data standards that require policing.

There are two broad categories of mHealth applications – provider-focused and patient-focused applications.[18] Provider-focused mHealth applications include clinical decision support systems that can run on mobile devices;[19] applications that allow providers to view MRI, x-ray, and CT imaging on their mobile devices;[20] electronic health record applications that link to a provider's EHR system;[21] applications that allow physicians to write electronic prescriptions;[22] applications used to scan drug barcodes to double-check the

such as image recognition, text recognition, and text-to-speech conversion.").

[17] Delphine Christin et al., *A Survey on Privacy in Mobile Participatory Sensing Applications*, 84 J. SYS. & SOFTWARE 1928, 1928 (2011) (describing the capabilities of mobile applications that utilize external sensors to measure, among other things, biometric data).

[18] For a description of the difference between patient- and provider-focused applications, see George Demiris et al., *Patient-Centered Applications: Use of Information Technology to Promote Disease Management and Wellness*, 15 J. AM. MED. INFORMATICS ASS'N 8, 8 (2008) (distinguishing between applications that focus on health care transactions, and "[p]atient-centered applications," which "enable a partnership among practitioners, patients, and their families . . . to ensure that procedures and decisions respect patients' needs and preferences"). For a different categorization of mHealth applications, see Amy J. Barton, Commentary, *The Regulation of Mobile Health Applications*, 10 BMC MED. 46, 46 (2012) (describing the Royal Tropical Institute's division of mHealth applications into eight different categories).

[19] *Technology Profile: Mobile Clinical Decision Support*, NEHI (June 12, 2012), http://www.nehi.net/publications/67/technology_profile_mobile_clinical_decision_support (linking to reports providing "technology profiles" for various types of mHealth applications including clinical support systems).

[20] *FDA Clears First Diagnostic Radiology Application for Mobile Devices*, U.S. FDA (Feb. 4, 2011), http://www.fda.gov/NewsEvents/Newsroom/PressAnnouncements/ucm242295.htm (describing FDA's approval of an application that will allow medical personnel to view images produced by CT, MRI, and nuclear medicine technology).

[21] *See, e.g.*, *Mobile Solutions: Put the Power of Care360 in the Palm of Your Hand*, CARE360, http://care360.questdiagnostics.com/EHR-Mobile-Health-Software.cfm (last visited Sept. 5, 2013) (describing a mobile application for Quest Diagnostics EHR system); *see also* Ken Terry, *Nine out of Ten Docs Recommend Mobile EHRs*, INFORMATIONWEEK HEALTHCARE (Aug. 16, 2012), http://www.informationweek.com/healthcare/electronic-medical-records/9-out-of-10-docs-recommend-mobile-ehrs/240005677 (describing the demand for mobile-EHR applications and one such application in particular).

[22] *See* Andrea Downing Peck, *One-Touch Access to a World of Resources*, MED. ECON.

drug, dose, and delivery methods against medication orders;[23] and applications with drug and clinical reference information.[24] Patient-focused mHealth applications include applications that allow patients to take glucose readings and send them to their providers;[25] applications that promote wellness programs;[26] applications that manage medications and alert providers when patients miss a dose;[27] and applications that monitor a patient's heart rate through a small patch worn on the patient's skin that transmits data from the patient's phone to the patient's providers.[28] Even with their incredible and constantly developing capabilities, these applications are little more than gadgets unless the health community and application developers can effectively integrate applications into the care system.[29] These applications must be able to communicate with EHRs and other health care technologies in order to be maximally effective.

(Sept. 10, 2011), http://medicaleconomics.modernmedicine.com/medical-economics/news/modernmedicine/modern-medicine-feature-articles/one-touch-access-world-medica (describing some of the most useful mHealth applications, including Rx-Writer, "an advertisement-based electronic prescription app that allows physicians to renew prescriptions in seconds rather than minutes").

[23] Jeni Williams, *The Value of Mobile Apps in Health Care*, HEALTHCARE FIN. MGMT., June 2012, at 96, 99 (describing an application implemented in an Oklahoma hospital that reduced adverse drug events and medication errors).

[24] *See* Peck, *supra* note 22 (describing useful mHealth applications like Epocrates Rx, which "allows doctors to banish their pocket drug reference to a bookshelf by providing up-to-date drug information, drug interactions, and pill identifiers").

[25] *See* JANE SARASOHN-KAHN, CAL. HEALTHCARE FOUND., PARTICIPATORY HEALTH: ONLINE AND MOBILE TOOLS HELP CHRONICALLY ILL MANAGE THEIR CARE 15-16 (2009), http://www.chcf.org/~/media/MEDIA%20LIBRARY%20Files/PDF/P/PDF%20ParticipatoryHealthTools.pdf (examining the potential of mHealth applications for diabetes management and examining several devices focused on diabetes medication management).

[26] Demiris et al., *supra* note 18, at 9.

[27] SARASOHN-KAHN, *supra* note 25, at 12 (stating that as many as sixty percent of patients do not adhere to their prescribed medication regimes and describing a mobile application, eMedMobile, which works with "smart labels" on prescription drugs to alert caregivers when patients skip a dose).

[28] Diana Manos, *New App Monitors Heart Rate, Respiration*, HEALTHCARE IT NEWS (Jan. 24, 2013), http://www.healthcareitnews.com/news/new-app-monitors-heart-rate-respiration ("SecuraFone offers 'real-time health monitoring' through a small patch worn on the chest, transferring the information to the cloud, and to any number of parties to whom the user wishes to give access – via email or smart phone.").

[29] INST. OF MED., THE ROLE OF TELEHEALTH IN AN EVOLVING HEALTH CARE ENVIRONMENT 84 (2012) ("The VA has demonstrated compelling data with a home telehealth program. They showed a 19 percent reduction in hospital readmissions for people within the program and, for the patients who are admitted, a 25 percent reduction in bed days. However, this is not just about technology. Rather, it is about the right payment model, the right culture, the standardization of process, the use of care coordinators, and then the right technology to help augment and accelerate all that.").

MHealth applications, when appropriately utilized, possess tremendous potential for improving the quality and affordability of health care, especially in rural areas of the United States.[30] There are large disparities between health care access in rural areas and urban areas. In rural areas, there are 57 generalist physicians per 100,000 residents, compared with 78 per 100,000 in urban areas.[31] MHealth applications may be a useful tool to equalize this disparity[32] because they have the potential to provide higher quality care at a low cost in rural areas where physician access is limited. This is particularly important because rural areas have "a higher prevalence of chronic diseases."[33] MHealth applications can reduce the cost and improve the quality of health care by improving a patient's ability to manage his condition outside of the doctor's office. Furthermore, mHealth applications may allow for more frequent clinical visits without the inconvenience of traveling to a doctor because the applications, when coupled with telehealth technology, can serve the function of a check-up appointment by transferring clinical data to a patient's physician.[34] Low-cost mHealth applications can allow patients to safely and

[30] MHealth applications are primed to benefit more than just the rural United States; numerous studies have hypothesized and analyzed the benefits of mHealth applications in developing countries. *See, e.g.*, James G. Kahn et al., *'Mobile' Health Needs and Opportunities in Developing Countries*, 29 HEALTH AFF. 254, 254 (2010) (finding that there is some evidence that mHealth technology may improve health care in the developing world, but calling for the structured evaluation of this potential); Warren A. Kaplan, *Can the Ubiquitous Power of Mobile Phones Be Used to Improve Health Outcomes in Developing Countries?*, GLOBALIZATION & HEALTH (May 23, 2006), http://www.globalizationandhealth.com/content/2/1/9 (finding that current evidence both supports and refutes the idea that mHealth technology will improve healthcare outcomes in the developing world).

[31] Eric H. Larson & Thomas E. Norris, *Rural Demography and the Health Workforce: Interstate Comparisons*, *in* STATE OF THE HEALTH WORKFORCE IN RURAL AMERICA: PROFILES AND COMPARISONS 23, 27 (Eric H. Larson et al. eds., 2003).

[32] There are disparities that need to be overcome in order for mHealth applications to be effectively utilized by individuals in rural areas. FCC has recognized these disparities and is developing programs to address these disparities in access to broadband. *See* FED. COMMS. COMM'N, CONNECTING AMERICA: THE NATIONAL BROADBAND PLAN 136-39, 146 (2010) (discussing the broadband availability gap problem and proposing solutions).

[33] LARRY GAMM ET AL., RURAL HEALTHY PEOPLE 2010: A COMPANION DOCUMENT TO HEALTHY PEOPLE 2010, at 91 (2003) ("The disproportionate prevalence of chronic disease is reflected in the higher crude all-causes mortality rates reported for rural areas.").

[34] *See* Ateev Mehrotra et al., *A Comparison of Care at E-Visits and Physician Office Visits for Sinusitis and Urinary Tract Infection*, 173 JAMA INTERNAL MED. 72, 73 (2013) (finding that e-visits have the potential to lower healthcare spending); Darrell West, *How Mobile Devices Are Transforming Healthcare*, CTR. FOR TECH. INNOVATION 3-4 (2012), *available at* http://www.brookings.edu/research/papers/2012/05/22-mobile-health-west (describing the potential benefits of mHealth applications to reduce costs, improve the quality of care, and reduce the need for visits to the physician for chronic condition patients).

securely manage their conditions and communicate with their health care providers.[35]

MHealth applications, however, pose a safety risk to patients as they become an increasingly common tool in the clinical care arsenal. The use of mHealth applications has exploded in recent years with over 40,000 applications currently on the market, up from 17,000 available in November 2011.[36] Market analysts project that by 2015, 500 million smart phone users will use a medical app.[37] A recent survey by the Pew Internet & American Life Project found that 31% of cell phone owners use their phone to look for health or medical information online, an increase from 17% in 2010.[38] Young to middle-aged cell phone owners, ages 18 to 29 and 30 to 49, use their cell phones to look up health or medical information more than any other age groups.[39] This trend is understandable given the propensity for younger generations to utilize new emerging technologies. Though this trend is promising for future elderly populations, current mobile phone users over the age of sixty-five are much less likely to use mHealth applications.[40] The population as a whole could benefit from increasing the sixty-five-and-older population's use of mHealth applications and other telehealth technology because this particular population is more afflicted by chronic conditions.[41] On

[35] *See, e.g.*, INST. OF MED., *supra* note 29, at 77-80 (describing the success of Vidant Health in rural eastern North Carolina, where it implemented a remote monitoring plan for patients with cardiovascular and pulmonary disease in ten hospitals, reducing the number of hospitalizations and hospital bed days by at least eighty percent); *cf.* QIANG ET AL., *supra* note 11, at 21 ("Cardiovascular disease, diabetes, cancer, and chronic respiratory diseases account for 35 million deaths a year worldwide – 80 percent of them in developing countries. Again, m-health applications can extend the reach of the health system and help patients being treated for these diseases. Because these chronic diseases often require lifelong support and management, they are well-suited for remote supporting using m-health applications.").

[36] Howard Larkin, *mHealth*, HOSP. & HEALTH NETWORKS MAG., Apr. 2011, at 22 ("As of November, there were more than 17,000 medical applications available for download from major app stores.").

[37] Jenny Gold, *Lawmaker Pitches New FDA Office of Mobile Health*, KAISER HEALTH NEWS (Sept. 26, 2012), http://www.kaiserhealthnews.org/stories/2012/September/27/FDA-Mobile-apps.aspx ("By 2015, 500 million smartphone users are expected to be using medical apps.").

[38] SUSANNAH FOX & MAEVE DUGGAN, PEW INTERNET & AM. LIFE PROJECT, MOBILE HEALTH 2012, at 2 (2012), *available at* http://www.pewinternet.org/~/media/Files/Reports/2012/PIP_MobileHealth2012.pdf ("One in three cell phone owners (31%) have used their phone to look for health information. In a comparable, national survey conducted two years ago, 17% of cell phone users had used their phones to look for health advice.").

[39] *Id.* at 4-5 ("Among all cell phone owners, some demographic groups are more likely than others to look for health information on their phones: Latinos, African Americans, those between the ages of 18 and 49, and college graduates.").

[40] *Id.*

[41] *See* NAT'L CTR. FOR HEALTH STATS., U.S. DEP'T OF HEALTH & HUMAN SERVS., PUB.

the other side of the provider-patient relationship, providers are increasingly utilizing smart phones that are capable of operating mHealth applications and EHR adoption rates have been quickly increasing as a result of the meaningful use (MU) incentive program.[42]

MHealth applications are still in their infancy with considerable untapped potential, as a large percentage of popular applications focus on diet and exercise management, rather than interoperable, integrated disease-management tools.[43] Such fitness applications, however, can provide useful tools for individuals looking to stay healthy and enjoy the proven benefits of controlling diet and exercise.[44] Because controlling diet and exercise is fundamental to the management of most chronic diseases, these technologies are valuable to a patient's overall health and their further development should be encouraged. Managing chronic diseases is one way to tame the cost crisis in the American healthcare system.[45] MHealth applications can also help patients manage chronic conditions[46] by promoting self-management and providing

NO. 2012-1232, HEALTH, UNITED STATES, 2011 WITH SPECIAL FEATURE ON SOCIOECONOMIC STATUS AND HEALTH 12 (2012), *available at* http://www.cdc.gov/nchs/data/hus/hus11.pdf (finding that the prevalence of heart disease increases with age); *id.* at 185 tbl.49 (finding that heart disease, cancer, and stroke all occur at substantially higher rates in individuals sixty-five and over); *id.* at 188 tbl.50 (finding that diabetes occurs at substantially higher rates in individuals sixty-five and over); *id.* at 40 (finding the percent of individuals with two or more chronic conditions increased from 1999-2000 to 2009-2010).

[42] The meaningful use incentive program provides incentive payments to eligible providers and hospitals if they can adopt and use electronic health records in a meaningful way as defined by the Centers for Medicare and Medicaid Services. *See infra* notes 144-51 and accompanying text; *see also* Catherine M. DesRoches et al., *Adoption of Electronic Health Records Grows Rapidly, but Fewer than Half of US Hospitals Had at Least a Basic System in 2012*, HEALTH AFF. WEB FIRST, July 2013, at 3-4; Chun-Ju Hsiao et al., *Office-Based Physicians Are Responding to Incentives and Assistance by Adopting and Using Electronic Health Records*, HEALTH AFF. WEB FIRST, July 2013, at 3.

[43] FOX & DUGGAN, *supra* note 38, at 14 (finding that eighty-one percent of health application users use applications to track exercise, diet, and/or weight, compared to nine percent who use applications for blood pressure, blood sugar or diabetes, and/or medication management).

[44] *See* Bonnie Spring et al., *Integrating Technology into Standard Weight Loss Treatment*, 173 JAMA INTERNAL MED. 105, 107-08 (2013) (finding that individuals assigned to a weight loss program involving a mobile application lost a mean of 3.9 kilograms more than participants without the mobile application).

[45] Partnership for Solutions, *Making the Case for Ongoing Care: September 2004 Update*, ROBERT WOOD JOHNSON FOUND. (Sept. 1, 2004), http://www.rwjf.org/en/research-publications/find-rwjf-research/2004/09/chronic-conditions-.html ("People with chronic conditions account for 83 percent of health care spending and those with five or more chronic conditions have an average of almost fifteen physicians visits and fill over 50 prescriptions in a year.").

[46] *See, e.g.*, M. CHRISTOPHER GIBBONS ET AL., AGENCY FOR HEALTHCARE RES. & QUALITY, PUB. NO. 09(10)-E019, IMPACT OF CONSUMER HEALTH INFORMATICS

tools to help patients manage their conditions[47] and medications.[48] MHealth applications may also enable patients to provide more accurate clinical histories to their physicians based on objective data in addition to subjective feelings about their health.[49] Some applications even transfer this data directly to a provider's EHR system.[50] This capability allows physicians to monitor a patient's condition remotely, thus reducing the necessity of in-person check-up visits.[51]

APPLICATIONS 3-5 (2009) (discussing studies showing that consumer health informatics applications can have a significant impact on personal habits related to diet, exercise, and substance abuse, but they also have the potential to impact chronic diseases and mental health conditions); JOHN D. PIETTE, CAL. HEALTHCARE FOUND., USING TELEPHONE SUPPORT TO MANAGE CHRONIC DISEASE 18 (2005), *available at* http://www.chcf.org/topics/chronicdisease/index.cfm?itemID=111784 (describing the types of patients who are most likely to benefit from access to telephone care); Adam Darkins et al., *Care Coordination/Home Telehealth: The Systematic Implementation of Health Informatics, Home Telehealth, and Disease Management to Support the Care of Veteran Patients with Chronic Conditions*, 14 TELEMEDICINE & E-HEALTH 1118, 1118-20 (2008) (describing the potential benefits of Care Coordination/Home Telehealth (CCHT) for veterans with chronic conditions, and particularly those veterans living in rural areas).

[47] *See, e.g.*, Tammy R. Toscos et al., *Integrating an Automated Diabetes Management System into the Family Management of Children with Type 1 Diabetes: Results from a 12-Month Randomized Controlled Technology Trial*, 35 DIABETES CARE 498, 498 (2012) (finding that patients with a wireless device that monitors and reports blood glucose levels were better able to manage their diabetes care and had significantly better glycemic control compared to those without the technology).

[48] SARASOHN-KAHN, *supra* note 25, at 12 (stating that as many as sixty percent of patients do not adhere to their prescribed medication regimes and describing a mobile application, eMedMobile, which reads "smart labels" on prescription drugs and alerts caregivers when a patient misses a dose).

[49] *Id.* at 15-16 (describing a diabetes application that turns an iPhone into a "combined glucose meter and insulin pump" and another application that is capable of interfacing with a glucose meter, charting the results within the application and providing calculations for sugar intake during meals).

[50] *See* Demiris et al., *supra* note 18, at 10 ("Patient-centered applications often require the secure exchange of clinical data via electronic messages from different patient record systems to consolidate the disparate data required for disease management."); *see also* QIANG ET AL., *supra* note 11, at 17-20 (categorizing the potential benefits of mHealth applications for providers and patients); Peter Wayner, *Monitoring Your Health with Mobile Devices*, N.Y. TIMES, Feb. 23, 2012, at B7, *available at* http://www.nytimes.com/2012/02/23/technology/personaltech/monitoring-your-health-with-mobile-devices.html ("When patients are dealing with chronic conditions, you might see a doctor every six weeks or two months . . . . For people to have real command over these diseases, we need to close the feedback loop and give people the information they need to make smarter decisions in real time." (internal quotation marks omitted)).

[51] MATTHEW NEWMAN ET AL., CTR. FOR CONNECTED HEALTH POL'Y, FISCAL IMPACT OF AB 415: POTENTIAL COST SAVINGS FROM EXPANSION OF TELEHEALTH 7-9 (2011), *available at* http://cchpca.org/sites/default/files/Fiscal%20Impact%20of%20AB%20415%20Potential

II. BARRIERS TO SUCCESSFULLY UTILIZING THE POWER OF MOBILE-HEALTH APPLICATIONS

A. *Privacy, Security, and Interoperability*

While mHealth applications possess great potential for improving the quality and reducing the cost of health care, storing PHI on mobile phones and transferring that data over unsecured networks raises a number of concerns. The Health Insurance Portability and Accountability Act (HIPAA) governs the regulation of security and privacy standards for electronically transmitted PHI.[52] HIPAA established rules for viewing electronic PHI, including standardized data transmission requirements.[53] Unfortunately, these standards are inadequate within the changing landscape of the health IT environment. For example, HIPAA likely does not cover third-party developers whose applications may not have stringent data protection standards for transmission or storage in compliance with HIPAA.[54]

The Federal Trade Commission's health breach notification rule is another federal enforcement mechanism that governs the privacy and security of mHealth applications.[55] This rule operates like HIPAA, but it applies to a

%20Cost%20Savings%20from%20Expansion%20of%20Telehealth_0_0.pdf (reviewing literature studying the efficiency, effectiveness, and access to care associated with the use of telehealth); Laurence C. Baker et al., *Integrated Telehealth and Care Management Program for Medicare Beneficiaries with Chronic Disease Linked to Savings*, 30 HEALTH AFF. 1689, 1689 (2011) (finding that spending decreased substantially for chronic care Medicare patients enrolled in a telehealth intervention program). *But see* Catherine Henderson et al., *Cost Effectiveness of Telehealth for Patients with Long Term Conditions (Whole Systems Demonstrator Telehealth Questionnaire Study)*, BRIT. MED. J., Apr. 6, 2013, at 13, 13 (finding that a telehealth intervention was not a cost effective addition to a standard treatment regimen over a twelve-month period).

[52] HIPAA delegates authority to HHS to issue regulations on privacy and security standards. *See* 42 U.S.C. §§ 1320d to 1320d-8 (2006) (defining the Secretary's power to issue rules concerning the establishment of standards and requirements for transmitting electronic health information); HIPAA Privacy Rule, 45 C.F.R. §§ 160, 164.102-.106, 164.500-.534 (2012); HIPAA Security Rule, 45 C.F.R. §§ 160, 164.102-.106, 164.302-.318 (2012) (establishing national standards to protect electronic personal health information).

[53] 45 C.F.R. §§ 164.302-.318 (establishing security requirements for PHI for electronic and physical access).

[54] HIPAA only applies to covered entities and their business associates. Covered entities are health plans, healthcare clearinghouses, and healthcare providers who electronically transmit health information. 45 C.F.R. §160.103. MHealth application developers will need to determine whether their applications will be used by a covered entity and involve the transmission or storage of PHI. Adam H. Greene, *When HIPAA Applies to Mobile Applications*, MOBIHEALTHNEWS (June 16, 2011), http://mobihealthnews.com/11261/when-hipaa-applies-to-mobile-applications. Applications used by patients, however, are not covered by HIPAA unless a covered entity is involved. *Id.*

[55] 16 C.F.R. pt. 318 (2013) (requiring companies to notify consumers when the security of their PHI has been breached).

separate list of covered entities, including personal health record (PHR) related entities, third-party services providers, and vendors of PHR.[56]

The first privacy and security concern is the actual storage of PHI on mobile devices. Providers may store sensitive data on mobile devices such as notes taken during a patient visit or EHR records. If this information is not encrypted, it may be easily accessible if a provider's device is lost or stolen,[57] hacked,[58] or simply displayed in an inappropriate location, such as on public transportation. Furthermore, if a mobile device has malware or spyware, which is increasingly common, then the storage of unencrypted PHI on the mobile device poses a substantial security risk.[59]

MHealth applications that transmit PHI to providers' EHR systems also pose risks to patient privacy. If the transfer of PHI is not secured, then third parties with the appropriate tools can intercept PHI transmitted by cell phones and use the information to commit medical identity theft or healthcare fraud.[60] Currently, most health and wellness mHealth applications send unencrypted private information.[61] Not only are the mHealth applications themselves using inadequate protections for private information, but providers are still learning how to securely utilize mobile devices in clinical care, compounding the security threat. Just a few years ago, providers were using text messages to communicate with patients. The Joint Commission on Accreditation of Healthcare Organizations (The Joint Commission) deemed this practice

[56] 16 C.F.R. § 318.2(f) (defining PHR related entities); § 318.2(h) (defining third-party service providers); § 318.2(j) (defining vendor of personal health records); § 318.3 (establishing the breach notification requirement for PHR-related entities, third-party service providers and vendors of PHR).

[57] *See* CHRIS HOURIHAN & BRYAN CLINE, HEALTH INFO. TRUST ALLIANCE, A LOOK BACK: U.S. HEALTHCARE DATA BREACH TRENDS 13, 38-42 (2012), *available at* http://hitrustalliance.net/breachreport/HITRUST%20Report%20-%20U.S.%20Healthcare%20Data%20Breach%20Trends.pdf (finding that theft and loss are the most likely causes of breached electronic records and recommending security measures such as encryption to protect data on all endpoint platforms).

[58] *See id.* at 32-35 (discussing the threat of cybercrime to large hospital systems and the lack of data on PHI breaches due to cybercrime).

[59] *Mobile Device Security: The Insider's Guide. Opinions and Tips from the World-Leading Experts*, MOBITHINKING, http://mobithinking.com/mobile-device-security (last visited Sept. 5, 2013) (interviewing three experts on the security risks posed by the storage of PHI on mobile phones).

[60] Many cell phones do not have security measures in place to defend against third party attacks. *Id.*; *see also* Don Van Natta Jr. et al., *Tabloid Hack Attack on Royals, and Beyond*, N.Y. TIMES, Sept. 5, 2010, at MM30 (describing the Murdoch phone-hacking scandal).

[61] Linda Ackerman, *Mobile Health and Fitness Applications and Information Privacy*, PRIVACY RIGHTS CLEARINGHOUSE 18 (July 15, 2013), https://www.privacyrights.org/mobile-medical-apps-privacy-consumer-report.pdf (finding that only thirteen percent of free and ten percent of paid mHealth and fitness applications encrypt all connections to the applications developer).

unsecure and unacceptable because text message data can easily be intercepted.[62] The Joint Commission instead recommended that providers switch to mobile applications with the appropriate protections in place, so providers can communicate in a "truly secure mobile conversation" with patients.[63]

In addition to privacy and security concerns, an EHR's ability to interpret data sent from a mobile device depends on "interoperability," or how PHI is actually transferred from a mobile device to an EHR system. Mobile devices use a variety of technologies to transfer data.[64] One of the more important functionalities of mHealth applications is transferring clinical data to a provider's EHR system, where a physician can read it and eventually add it to a patient's electronic record.[65] In order for an EHR to receive and interpret PHI, the PHI needs to be in a standardized data format that is compatible with EHR systems. The Institute of Medicine (IOM) defines data standards as the "methods, protocols, terminologies, and specifications for the collection, exchange, storage and retrieval of information associated with health care applications."[66] IOM states that standardizing health care data involves standardizing the definition of data elements,[67] data interchange formats,[68] terminologies,[69] and knowledge representation.[70] Failure to comply with these

[62] Justin Montgomery, *JCAHO Issues Ban on Physician Texting, Signifies Importance of Secure Mobile Communication Outside SMS*, MHEALTHWATCH (Nov. 29, 2011), http://mhealthwatch.com/jcaho-issues-ban-on-physician-texting-signifies-importance-of-secure-mobile-communication-outside-sms-18266 ("The Joint Commission on Accreditation of Healthcare Organizations (JCAHO) recently issued a so-called 'ban' on physician texting, saying it's 'not acceptable' for medical professionals to communicate patient information via SMS.").

[63] *Id.*

[64] *See* QIANG ET AL., *supra* note 11, at 12 (listing the main technologies used to transmit mHealth data).

[65] *See Interoperability: An Essential Component for Scalable mHealth*, MHEALTH INSIGHTS (Mar. 2013), http://www.pwc.com/en_GX/gx/healthcare/mhealth/mhealth-insights/assets/pwc-mhealth-insights-interoperability-an-essential-component-for-scalable-mhealth-pdf.pdf (stating that only fifty-three percent of doctors report that the mHealth applications they use work with their EHR and the "lack of interoperability between technologies is often to blame").

[66] INST. OF MED., PATIENT SAFETY: ACHIEVING A NEW STANDARD FOR CARE 128 (Philip Aspden et al. eds., 2004).

[67] *Id.* ("*Definition of data elements*—determination of the data content to be collected and exchanged.").

[68] *Id.* at 128-29 ("*Data interchange formats*—standard formats for electronically encoding the data elements . . . . Interchange standards can also include document architectures for structuring data elements as they are exchanged and information models that define the relationships among data elements in a message.").

[69] *Id.* at 129 ("*Terminologies*—the medical terms and concepts used to describe, classify, and code the data elements and data expression languages and syntax that describe the relationships among the terms/concepts.").

standards substantially limits the potential benefits of mHealth applications. For example, if an mHealth application did not use a widely accepted data standard, such as Health Level 7 (HL7), then the beneficial impact of the application would be significantly limited, as the data would not be truly available for the care provider to utilize because his EHR system may not understand the data standard used by the application.[71] It would be as if the patient was providing an oral history recorded on paper rather than an objective data-driven history that can be interpreted by an EHR and added to a patient's health record. In order to maximize the beneficial impact of mHealth applications, it is imperative that the above-mentioned data standards are harmonized. Without standard harmonization, mobile applications will fail to offer the main benefit of having the ability to transfer clinical data almost instantaneously, securely, and frequently.

B. *Patient Safety Concerns*

MHealth applications also pose patient safety concerns.[72] For example, an application that supplies incorrect information on how to treat a particular condition could be harmful to patients who do not have the expertise to distinguish clinically appropriate and inappropriate treatment options. MHealth applications that provide incorrect medical advice can be harmful when patients (or providers) rely on the application to treat a condition. This is problematic with applications such as interactive clinical decision support systems (CDSS),[73] which can use specific patient data to come up with a clinical diagnosis, or medical reference tools that are not interactive, but provide information on certain conditions similar to a medical dictionary.[74]

---

[70] *Id.* ("*Knowledge Representation*—standard methods for electronically representing medical literature, clinical guidelines, and the like for decision support.").

[71] *See, e.g.*, Standards, Implementation Specifications, and Certification Criteria for Electronic Health Record Technology, 77 Fed. Reg. 54,163, 54,284 (Sept. 4, 2012) (to be codified at 45 C.F.R. pt. 170) (defining standards required for certification of EHRs for various code sets including HL7).

[72] *See, e.g.*, U.S. FDA, *supra* note 6, at 13-15 (listing types of applications subject to regulation, including: applications that display, store, analyze, or transmit patient-specific medical device data; applications that "transform the mobile platform into a medical device by using attachments, display screens, or sensors or by including functionalities similar to those of currently regulated medical devices;" and applications that "perform[] patient-specific analysis and provid[e] patient-specific diagnosis, or treatment recommendations").

[73] *Clinical Decision Support*, HEALTHIT.GOV, http://www.healthit.gov/policy-researchers-implementers/clinical-decision-support-cds (last visited Sept. 5, 2013) ("Clinical decision support (CDS) provides clinicians, staff, patients or other individuals with knowledge and person-specific information, intelligently filtered or presented at appropriate times, to enhance health and health care. . . . These tools include computerized alerts and reminders to care providers and patients; clinical guidelines; condition-specific order sets; [and] focused patient data reports and summaries . . . .").

[74] *See, e.g.*, *Standards of Medical Care in Diabetes – 2012: Mobile App Information*,

When patients fail to understand information contained in an application, or the application has incorrect information to start with, there is a substantial risk of patient harm. Patients generally do not have the education and experience to judge a treatment plan proposed by a CDSS application or reference guide. When a provider-focused application, such as a CPOE functioning within an EHR, provides incorrect information, it is more likely that an appropriately educated individual (such as a pharmacist, nurse, or physician) will catch and correct the error.[75] Such patient-focused clinical decision support tools can empower patients by informing them about their conditions and potential treatment options, which they can then discuss with their doctors.[76] Reference tools that describe clinical conditions, as opposed to interactively diagnosing a patient, can pose a problem because they may provide incorrect information about clinical conditions. While medical-reference applications can threaten patient safety, government agencies are unlikely to regulate them because they aggregate publicly available information. Conversely, CDSS applications are likely to be regulated by a government agency because they offer diagnoses based on patient-specific information.[77]

Applications that monitor a patient's key vital signs can also cause patient-safety problems when they provide incorrect data, which prevents accurate tracking of a condition's progress. As discussed above, mHealth applications provide tremendous benefits to patients with chronic conditions[78] who need to track health indicators. Applications that provide false clinical measurements, however, can lead to unnecessary care because patients may think they are sicker than they actually are. Additionally, false measurements may cause a delay in obtaining necessary care because the results can appear more positive

AM. DIABETES ASS'N, http://care.diabetesjournals.org/content/35/Supplement_1/S11/suppl/DC3 (last visited Sept. 5, 2013) ("The Standards of Care app . . . features quick and easy access to the American Diabetes Association standards, recommendations, and guidelines for diagnosing and treating diabetes and its complications in various settings.").

[75] *See, e.g.*, *Remote CPOE Error—A Situation That's More than Remotely Possible*, INST. FOR SAFE MED. PRACTICES (May 31, 2007), http://www.ismp.org/newsletters/acutecare/articles/20070531.asp.

[76] *See* Neil Versel, *Mobile Supports "Patient Activation" of Clinical Decision Support*, MOBIHEALTHNEWS (Nov. 23, 2011), http://mobihealthnews.com/14871/mobile-supports-patient-activation-of-clinical-decision-support (explaining that clinical decision support tools can empower patients to "activate themselves" by helping determine their own treatment, monitoring their conditions, deciding whether to comply with their physician's instructions, and making educated decisions about when to seek care).

[77] FDA's guidance classifies applications that "perform[] patient-specific analysis and provid[e] patient-specific diagnosis, or treatment recommendations" as regulated mHealth applications. U.S. FDA, *supra* note 6, at 11.

[78] *See supra* Part I (describing the potential of mHealth applications to improve the quality and cost-effectiveness of patient care, particularly for patients with chronic conditions or those living in rural areas).

than the actual indicators.[79] For example, a patient could suffer severe health consequences if his blood sugar level is displayed incorrectly on an mHealth application and he adjusts his insulin or diet accordingly.

A related problem may arise when an mHealth application that is linked to a clinician's EHR provides that clinician with incorrect clinical parameters on the patient, like serum lipids, HbA1c levels, or blood pressure. The incorrect clinical parameters mask potential problems and limit the clinician's opportunity to offer an appropriate clinical judgment to the patient. Ultimately, those mHealth applications that focus on collecting data from patients and providing health professionals with clinically actionable information are the most appropriate targets for government regulation. Such applications are most likely to harm patients if they are poorly designed or malfunction. The justification for regulating these applications is that patients need to be protected from potential harms that patients, due to their relative lack of medical expertise, are likely unable to prevent. Devices that merely provide information to patients are no more deserving of regulation than any other inaccurate information found in a publication or on a website. Nonpatient-specific information provided by mHealth applications to clinicians is even less in need of regulation because physicians and other health professionals have the appropriate training necessary to compensate for any problems caused by malfunctioning or incorrect mHealth applications. The idea of whether FDA's proposed risk-based system of regulation is appropriate is outside the scope of this Note, but the point that there are patient-safety risks to using mHealth applications is critically important to determining which agency, if any, should regulate mHealth applications.

III. A COMPLEX WEB OF REGULATORY AUTHORITY

The complexity of the regulatory environment makes the regulation of mHealth applications particularly challenging. MHealth applications provide guidance on how to safely and effectively manage a patient's medical condition, an area typically regulated by FDA. The applications could also very well fall within the purview of the meaningful use (MU) incentive program and the future use of EHR systems and health information exchanges, an area influenced by incentive payments for compliance with certification standards issued by ONC. Furthermore, these applications often involve highly complex technological specifications that require expertise by a regulating body, and no singular regulatory authority has the requisite expertise to effectively regulate these applications.[80] Despite this, both FDA and ONC are

[79] *See, e.g.*, Joel A. Wolf et al., *Diagnostic Inaccuracy of Smartphone Applications for Melanoma Detection*, 149 JAMA DERMATOLOGY 422, 424 (2013) (finding that three applications that do not involve a physician evaluation misdiagnosed thirty percent of melanomas as benign).

[80] *Compare* U.S. FDA, DRAFT GUIDANCE, CONTENT OF PREMARKET SUBMISSIONS FOR MANAGEMENT OF CYBERSECURITY IN MEDICAL DEVICES (2013), *available at* http://www.fda.

locked in a regulatory arms race of sorts, issuing plans and regulations to demonstrate that each understands the requirements of the other's regulatory domain in order to obtain regulatory authority over mHealth applications and health information technology in general.

A. *Food and Drug Administration (FDA)*

FDA's authority to regulate medical devices stems from the Federal Food, Drug, and Cosmetic Act (FDCA), which defines a device as:

> An 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 . . . which does not achieve its primary intended purposes through chemical action within or on the body of man or other animals and which is not being metabolized for the achievement of its primary intended purposes.[81]

Accessories or components of medical devices are thus regulated as medical devices under FDA's authority.[82] The level of regulation depends on the class of the regulated parent device.[83] FDA classifies devices into Class I, II, or III devices based on the risk they pose to human users.[84] Class I, II, and III devices are all subject to regulation under FDA's "general controls."[85] Most Class I devices are exempt from premarket-clearance requirements because

gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm356186.htm, *and FDA Safety Communication: Cybersecurity for Medical Devices and Hospital Networks*, U.S. FDA (June 13, 2013), http://www.fda.gov/MedicalDevices/Safety/Alertsand Notices/ucm356423.htm, *with* OFFICE OF THE NAT'L COORDINATOR FOR HEALTH INFO. TECH., HEALTH INFORMATION TECHNOLOGY PATIENT SAFETY ACTION & SURVEILLANCE PLAN 10-16 (2012), http://www.healthit.gov/sites/default/files/safetyplanhhspubliccomment.pdf.

[81] 21 U.S.C. § 321(h) (2012). For a more thorough analysis of FDA's device approval process, see INST. OF MED., MEDICAL DEVICES AND THE PUBLIC'S HEALTH: THE FDA 510(K) CLEARANCE PROCESS AT 35 YEARS 41-60 (2011).

[82] An accessory can be defined as "an article intended for use in or with a finished medical device, intended for use by the end user." Bradley Merrill Thompson, *FDA Regulation of Mobile Health*, MOBIHEALTHNEWS 4 fig.1 (2010), http://mobihealthnews.com /research/fda-regulation-of-mobile-health. A component is "an article intended for use in or with a finished medical device, intended for use by a manufacturer." *Id.*

[83] U.S. FDA, *supra* note 6, at 13 ("Mobile medical apps [that are an extension of one or more medical devices] are considered an accessory to the connected device and are required to comply with the controls applicable to that connected device.").

[84] 21 U.S.C. § 360c(a) (defining various classes of medical devices).

[85] *General Controls for Medical Devices*, U.S. FDA, http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/Overview/GeneralandSpecialControls/ucm055910.htm (last updated May 31, 2009) (describing FDA's general controls).

they pose the lowest risk to users.[86] However, Class II devices, because of their heightened risk, are subject to "special controls" because FDA's general controls are insufficient to provide "reasonable assurance of the safety and effectiveness of the device."[87] The highest risk devices – Class III – require, in addition to FDA's general controls, premarket approval (PMA), which is the most stringent type of review conducted by FDA.[88] FDA conducts two types of PMAs – expedited and original PMAs.[89] Expedited PMAs are necessary for devices that are "intended to (a) treat or diagnose a life-threatening or irreversibly debilitating disease or condition and (b) address an unmet medical need."[90]

FDA also has a premarket-notification requirement under 21 U.S.C. § 360(k) that requires device manufacturers to disclose the class of a device, clinical trial data for the device, actions taken to secure premarket clearance under 21 U.S.C. § 360e, and performance data that reasonably assures safe and effective performance of the device under 21 U.S.C. § 360d.[91] Class I device manufacturers can be exempt from this requirement if a device "is not intended for a use which is of substantial importance in preventing impairment of human health," or if a device does not "present[] a potential unreasonable risk of illness or injury."[92]

Another approval method that FDA uses for devices is the 510(k) clearance process. This allows manufacturers to avoid the premarket approval process if they can demonstrate their product is substantially equivalent[93] to an already

[86] 21 U.S.C. § 360c(a)(C) (requiring class III premarket approval for class I devices if "insufficient information exists to determine that the application of general controls are sufficient to provide reasonable assurance of the safety and effectiveness of the device" and "is represented to be for a use in supporting or sustaining human life or for a use which is of substantial importance in preventing impairment of human health, or presents a potential unreasonable risk of illness or injury").

[87] *General Controls for Medical Devices*, *supra* note 85.

[88] 21 U.S.C. § 360c(a).

[89] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-12-418, MEDICAL DEVICES: FDA HAS MET MOST PERFORMANCE GOALS BUT DEVICE REVIEWS ARE TAKING LONGER 8 (2012) (clarifying the distinction between types of PMA processes).

[90] *Id.* at 8-9.

[91] 21 U.S.C. §§ 360(k), 360e, 360d (mandating performance standards for medical devices).

[92] *Id.* § 360(*l*) (covering "exemption[s] from reporting requirements").

[93] The FDCA defines substantially equivalent as:

> [W]ith respect to a device being compared to a predicate device, that the device has the same intended use as the predicate device and that the Secretary by order has found that the device – (i) has the same technological characteristics as the predicate device, or (ii)(I) has different technological characteristics and the information submitted that the device is substantially equivalent . . . that demonstrates that the device is as safe and effective as a legally marketed device, and (II) does not raise different questions of safety and effectiveness than the predicate device.

Id. § 360c(i).

approved Class II or III device.[94] Despite being "generally more economical, faster[,] and less burdensome to industry and the FDA,"[95] the 510(k) device clearance process has been criticized for failing to effectively approve devices based on safety and effectiveness.[96]

In the past, FDA has "not issued an overarching software policy" to regulate all medical devices containing software.[97] Instead, FDA has classified certain types of software as devices.[98] FDA's final guidance states that they intend solely to regulate mHealth applications that satisfy the statutory definition of a device[99] and either "are used as an accessory to a regulated medical device; or transform a mobile platform into a regulated device."[100] Applications of several categories are thus excluded from FDA's intended regulatory scope, including general health and wellness applications, applications that act as EHRs, applications that serve as reference guides, and applications that automate office operations.[101]

FDA uses three key examples to represent which mobile applications it considers medical devices subject to regulation:

> Mobile apps that are an extension of one or more medical devices by connecting to such device(s) for purposes of controlling the device(s) or displaying, storing, analyzing, or transmitting patient-specific medical data. . . . Mobile apps that transform the mobile platform into a regulated medical device by using attachments, display screens, or sensors or by including functionalities similar to those of currently regulated medical devices. . . . [Finally,] [m]obile apps that become a regulated medical device (software) by performing patient-specific analysis and providing patient-specific diagnosis, or treatment recommendations.[102]

---

[94] *See* CTR. FOR DEVICES & RADIOLOGICAL HEALTH, U.S. DEP'T OF HEALTH & HUMAN SERVS., THE NEW 510(K) PARADIGM 1-2 (1998) ("The FDAMA [Food and Drug Administration Modernization Act] also gave FDA the authority to directly exempt certain Class II devices rather than first down-classifying them to Class I before they become eligible for exemption.").

[95] INST. OF MED., *supra* note 81, at 73.

[96] *See id.* (concluding that FDA's 510(k) clearance process fails to effectively screen devices for safety and effectiveness and ultimately recommends that FDA eliminate the 510(k) clearance process).

[97] U.S. FDA, *supra* note 6, at 6.

[98] *Id.*

[99] *See supra* note 81 and accompanying text.

[100] U.S. FDA, *supra* note 6, at 12. For more information on this topic, and for a condensed summary of the proposed categories of regulated devices, see Barton, *supra* note 18, at 2 tbl.1.

[101] U.S. FDA, *supra* note 6, at 23-24.

[102] *Id.* at 14-15 (listing mHealth applications that will be subject to FDA's regulatory oversight).

Once FDA determines an mHealth application falls within FDA's intended regulatory scope, the next step is to appropriately classify the applications.[103] An application that functions as a medical device is regulated under the device definitions outlined in the FDCA based on the risk associated with the application and its potential for causing harm to a patient.[104] An application that serves as an accessory to a medical device is categorized in the same class as the primary device.[105]

FDA's final guidance does not contemplate the privacy and security concerns associated with the transmission of data from mHealth applications. These issues are likely missing from the final guidance because FDA has not typically regulated devices for information security issues.[106] FDA has instead focused predominantly on protecting patient safety.[107] For example, when FDA issued regulations on implantable medical devices that could transmit data wirelessly, it failed to consider the threat of intentional unauthorized access to implantable medical devices.[108] With similar concerns for mHealth applications, FDA likely has not developed the expertise to regulate privacy and security concerns from intentional hacking threats to mHealth applications over the past year.

Yet data security poses a substantial threat to the effectiveness of another area of FDA regulation of mHealth applications – the possibility of 510(k) clearance.[109] The problem is that some medical devices used in hospitals have substantially different usage requirements than devices that are attachments to

[103] *See* Thompson, *supra* note 82, at 14 (providing a list of factors which can aid a manufacturer in determining an application's likely classification, including "the seriousness of the particular disease or condition" targeted, and "whether the software is intended or designed to provide any real time, active or online patient monitoring functions").

[104] *See supra* notes 81-90 and accompanying text.

[105] *See supra* note 83 and accompanying text.

[106] U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 4, at 24.

[107] *See* Daniel B. Kramer et al., *Security and Privacy Qualities of Medical Devices: An Analysis of FDA Postmarket Surveillance*, 7 PLOS ONE, July 20, 2012, at 4, *available at* http://www.plosone.org/article/info%3Adoi%2F10.1371%2Fjournal.pone.0040200#references (finding that in a nine-year period of analysis, FDA issued no recalls related to patient security or privacy); *CDRH Mission, Vision and Shared Values*, CENTER FOR DEVICES & RADIOLOGICAL HEALTH, U.S. FDA, http://www.fda.gov/AboutFDA/CentersOffices/OfficeofMedicalProductsandTobacco/CDRH/ucm300639.htm (last updated Apr. 17, 2012) ("The mission of the Center for Devices and Radiological Health (CDRH) is to protect and promote the public health. We assure that patients and providers have timely and continued access to *safe*, *effective*, and *high-quality* medical devices . . . ." (emphasis added)).

[108] U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 4, at 22 ("For the two medical devices that have known vulnerabilities, FDA considered information security risks from unintentional threats, but not risks from intentional threats during its premarket review of the related supplements. FDA stated that it did not generally consider intentional information security threats in its review process at the time these devices were reviewed.").

[109] *See supra* note 94 and accompanying text.

mobile devices. Glucose meters in hospitals, for example, generally do not have the same intentional hacking concerns that glucose meters attached to mobile devices do. Using a substantially similar certification process for mobile devices as traditional medical devices will ignore the need for higher privacy and security regulations on mobile versions. Furthermore, mobile applications approved for use on some platforms may have different security requirements on other platforms, yet the device could be approved despite these additional potential security threats. Therefore, under current regulations and FDA's current approach, any mobile application that is substantially equivalent to an already approved medical device will likely be approved under 510(k) clearance without regard for any additional privacy and security concerns posed by the difference between mobile and hospital use of these applications.

Finally, the draft guidance does not suggest how FDA will handle postmarket surveillance efforts for mHealth applications, how to ascertain when an application causes a patient harm, or how to determine whether an application breaches a patient's PHI security. While the HHS Office of Civil Rights (OCR) is responsible for enforcing rules against HIPAA violations by healthcare providers,[110] and FTC is responsible for enforcing rules governing violations of patient privacy in other businesses,[111] no regulatory agency is responsible for preventing breaches of patient PHI by mHealth applications. FDA could fill this regulatory gap, but may not be the ideal regulator because FDA is largely unfamiliar with HIPAA violations and lacks the expertise to sanction HIPAA offenders. Alternatively, FDA could ask OCR to monitor certain applications that have a high risk of HIPAA violations. FDA could also inform OCR of any potential privacy and security concerns that OCR could then address. Even though under these circumstances FDA would not directly regulate mHealth applications for HIPAA violations, FDA could have an important cooperative role protecting patients against mobile applications that consistently breach patient PHI. However, without a robust reporting system for mHealth applications, concerns about patient PHI security will likely be under addressed.

FDA could have a substantial role in conducting postmarket surveillance for mHealth applications that it has chosen to regulate as medical devices for patient safety and effectiveness. FDA already has several postmarket surveillance efforts under way.[112] For example, Manufacturer and User Facility Device Experience (MAUDE) is an adverse event reporting system that requires manufacturers, hospitals, and health care providers to submit

[110] U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 4, at 48 ("OCR is responsible for developing, interpreting, and enforcing the Privacy and Security Rules called for in the Health Insurance Portability and Accountability Act of 1996 (HIPAA).").

[111] 16 C.F.R. § 318 (2013) (granting FTC the authority to punish businesses for breaches of patient privacy and requiring business to report breaches of privacy).

[112] CTR. FOR DEVICES & RADIOLOGICAL HEALTH, *supra* note 94, at 5-6.

information on adverse events.[113] FDA, in addition to MAUDE reporting, can examine the safety of a device by requiring the manufacturer to conduct a postmarket surveillance study, but the focus of these reviews is usually on clinical outcomes rather than data security risks.[114] FDA can also order a study by the device manufacturer after the approval of a device certified through a premarket approval order. These reports focus on "assess[ing] device safety, effectiveness, and/or reliability including longer-term, real-world device performance"[115] in larger and more diverse patient populations. The problem with voluntary postmarket surveillance systems like MAUDE is the heightened susceptibility to underreporting.[116] Mobile applications might thus require a faster and more stringent reporting system, especially when privacy- and security-related problems arise when PHI is stored on a mobile application or device. FDA is planning to replace MAUDE with the FDA Adverse Event Reporting System (FAERS).[117] FAERS will still focus on passive surveillance and predominantly on clinical effectiveness and safety risks rather than information security.[118] Yet FDA officials state that FAERS reports will be able to identify information security problems.[119]

These systems are only as good as the data they contain. It would be difficult to associate a specific mHealth application with similar adverse healthcare events across the country without a way to identify the application. That is, it would be hard to tie numerous adverse healthcare events across the country to one malfunctioning application without an easy-to-use identification system that relates directly to the application. In order to solve the problem of attributing an adverse event to a device, FDA started a Unique Device Identification (UDI) initiative.[120] This initiative is just one part of FDA's overall framework for national postmarket surveillance, working in tandem with some of the systems discussed previously for monitoring medical devices. The goal of the UDI initiative is to create a surveillance system that provides near real-time clinical performance and safety data for all medical devices.[121]

---

[113] *See* U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 4, at 28-29 (finding that the MAUDE system, although it does not require reporting from providers and consumers, is capable of identifying information security problems with devices).

[114] *See id.* at 30 (discussing security controls to mitigate informational security risks); CTR. FOR DEVICES & RADIOLOGICAL HEALTH, U.S. DEP'T OF HEALTH & HUMAN SERVS., STRENGTHENING OUR NATIONAL SYSTEM FOR MEDICAL DEVICE POSTMARKET SURVEILLANCE 5 (2012), *available at* http://www.fda.gov/downloads/AboutFDA/CentersOffices/CDRH/CDRHReports/UCM301924.pdf.

[115] CTR. FOR DEVICES & RADIOLOGICAL HEALTH, *supra* note 114, at 6.

[116] *See* Kramer et al., *supra* note 107, at 4 (concluding that clinicians are often unable to identify potential security problems, and therefore may not report every incident).

[117] U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 4, at 34.

[118] *Id.*

[119] *Id.*

[120] Unique Device Identification System, 78 Fed. Reg. 58,687 (Sept. 24, 2013).

[121] *Id.* at 58,787 ("[T]his information will contribute to the rapid identification of risks

The UDI system would create a unique numeric or alphanumeric code for each device model that could then be scanned by a barcode reader and logged into an EHR.[122] Then instead of conducting lengthy postmarket surveillance studies, FDA could benefit from private health care system EHRs that associate patient records with specific devices or software. This system could also be applied to mHealth applications; rather than using an actual barcode on the label for the device, the UDI could be located somewhere within the software.[123] Software updates, however, may make this process difficult as an update could change the software substantially and essentially create a new device. FDA has solved this problem by requiring new unique device identifiers when a software update results in a new version or model of the sofrware. It would be useful for adverse event reporting to separate pre- and post-update patients into different groups to determine if a software update has solved existing adverse event or privacy issues.[124]

Despite these new reporting systems, FDA's current processes, particularly the premarket approval process, are slow and cumbersome and would likely inhibit innovation in the "explosively dynamic" mHealth industry.[125] A report from the U.S. Government Accountability Office (GAO) compared the time it takes for an FDA review under the 510(k) process and the full premarket approval (PMA) process. The report found that while the length of 510(k) reviews decreased from 2003 to 2010, the waiting time for a final decision (including off time waiting for responses from the sponsor) increased from 100 to 161 days.[126] For PMAs, original PMA time to final decision (again,

and benefits associated with a device within specific subpopulations. By linking clinical detail and information regarding device use, more effective device safety surveillance and evaluation studies could be conducted, contributing to a more complete safety and effectiveness profile for devices, and enabling more appropriate and timely remedies when potential safety concerns are identified.").

[122] *Id.* ("[W]hile not required, FDA anticipates that providers will include the UDIs of a wide variety of devices in patients' Electronic Health Records (EHRs) and Personal Health Records (PHRs).").

[123] *Id.* at 58,820 ("[S]tand-alone software regulated as a medical device must provide its unique device identifier through either or both of the following: (1) An easily readable plain-text statement displayed whenever the software is started; (2) An easily readable plain-text statement displayed through a menu command . . . .").

[124] *Id.* at 58,826. This should make it easier for FDA to track whether device updates resolve any issues leading to adverse events. Furthermore, one FDA official told the U.S. Government Accountability Office that "although this effort was not specifically designed to help FDA identify information security problems involving medical devices, it will help FDA identify specific device models that could encounter information security problems." U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 4, at 33.

[125] Gold, *supra* note 37.

[126] U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 89, at 15-16 (explaining that FDA officials stated this increase can be accounted for by FDA asking the sponsors for further information rather than rejecting the submission).

including off time) increased from 462 days in 2003 to 627 days in 2008.[127] Expedited PMA time (including off time) decreased from 704 days to 545 days from 2003 to 2009.[128] Regardless of the review process used, FDA approval is a lengthy process. FDA's review processes are prolonged because FDA does not adequately communicate "the regulatory standards [FDA] uses to evaluate submissions" to device sponsors.[129]

Furthermore, FDA regulations governing the level of review for mHealth applications can be quite confusing for developers of mobile applications who are unfamiliar with the FDA device-approval process. A Member of Congress proposed one way to pick up the pace of FDA approvals for mHealth application developers – establishing an "Office of Wireless Health Technology" within FDA to speed communications with application developers, help alleviate this informational gap, and decrease the negative impact of regulatory approval on innovation.[130] This new office would help mHealth application developers better understand the effect of existing regulations, and strike a better balance between the salutary and negative effects of the regulatory process. The bill has not left the Health Subcommitee of the House of Represenatives' Energy and Commerce Committee.[131]

Despite these challenges, FDA is a suitable candidate for regulating mHealth applications because it has existing regulatory authority over medical devices and the infrastructure to support both premarket approval and postmarket surveillance. Moreover, FDA's expertise in monitoring adverse-event reports to protect patient safety and device quality would be valuable components in regulating mHealth applications. FDA's lengthy and confusing approval process will reduce innovation in the mHealth application market, and slow the rate at which mHealth applications can incorporate new technologies. Furthermore, FDA only recently started to consider privacy and security concerns with medical devices. FDA's inexperience may cause substantial economic harm to patients.

[127] *Id.* at 29.

[128] *Id.* at 31. GAO states that "the average time to final decision for expedited PMAs was highly variable" due to the small number expedited PMA submissions, an average of seven per year. *Id.*

[129] *Id.* at 34 ("The most commonly mentioned issue raised by industry and consumer advocacy stakeholder groups was insufficient communication between FDA and stakeholders throughout the review process.").

[130] Health Care Innovation and Marketplace Technologies Act of 2012, H.R. 6626, 112th Cong. § 1013 (2012) (requiring the Office of Mobile Health to, among other things, conduct meetings, publish annual reports, and establish an educational website detailing the effect of regulations on wireless health technologies).

[131] *H.R.6626 – Health Care Innovation and Marketplace Technologies Act of 2012*, CONGRESS, http://beta.congress.gov/bill/112th/house-bill/6626 (last visited Sept. 5, 2013).

B. *The Office of the National Coordinator for Health Information Technology (ONC)*

ONC was created in section 3001 of the Health Information Technology for Economic and Clinical Health (HITECH) Act within the American Recovery and Reinvestment Act of 2009 to promote:

> [D]evelopment of a nationwide health information technology infrastructure that allows for the electronic use and exchange of information and that (1) ensures that each patient's health information is secure and protected, in accordance with applicable law; (2) improves health care quality, reduces medical errors, reduces health disparities, and advances the delivery of patient-centered medical care . . . .[132]

The HITECH Act gave ONC the authority to create standards for establishing MU under the Medicare and Medicaid Electronic Health Records Incentive Programs (the EHR Incentive Programs). HITECH tasks ONC with reviewing and endorsing "standard[s], implementation specification[s], and certification criteri[a] for the electronic exchange and use of health information."[133] These standards – as stated in ONC's final certification criteria rule – are in place to "test and certify [that] a Complete EHR[134] or EHR Module[135] provides certain capabilities, and where applicable, to require that those capabilities be implemented in accordance with adopted standards and implementation specifications."[136] ONC's only role in promulgating standards and implementing specifications is to ensure that EHRs have certain capabilities, not to govern how or when a provider uses those capabilities.[137]

In 2011, ONC implemented the ONC HIT Certification Program (the Certification Program) to certify Complete EHRs and EHR Modules.[138] This Certification Program establishes an ONC approved accreditor (ONC-AA)

---

[132] American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, § 3001(b), 123 Stat. 115, 230.

[133] *Id.* § 3001(c)(1)(A).

[134] A "Complete EHR" is defined as "EHR technology that has been developed to meet, at a minimum, all applicable certification criteria adopted by the Secretary." 45 C.F.R. § 170.102 (2012).

[135] An "EHR Module" is defined as "any service, component, or combination thereof that can meet the requirements of at least one certification criterion adopted by the Secretary." *Id*.

[136] Initial Set of Standards, Implementation Specifications, and Certification Criteria for Electronic Health Record Technology; Final Rule, 75 Fed. Reg. 44,590, 44,592 (July 28, 2010).

[137] *Id.* For example, ONC's certification criterion for the meaningful use Stage 1 objective of "maintain active medication list" requires that an EHR "enable a user to electronically record, modify, and retrieve a patient's active medication list . . . ." *Id.* at 44,604.

[138] 45 C.F.R. § 170.500 (establishing the ONC HIT Certification Program to replace the Temporary Certification Program).

which accredits ONC-Authorized Certification Bodies (ONC-ACB).[139] The ONC-ACB certifies EHRs and EHR modules using ONC's certification criteria for privacy and security, MU requirements,[140] and interoperability standards.[141] The Certification Program also requires the ONC-ACBs to conduct surveillance on certified devices to confirm that the devices continue to conform to the certification standards.[142] Unfortunately, these standards are used as part of ONC's *voluntary* certification process.[143] Unlike FDA's review process for medical devices and drugs, ONC has no authority to mandate certification of electronic health record systems or modules. The power behind ONC's certification authority is that hospitals and healthcare providers must use Complete EHRs and EHR Modules that are ONC-certified in order to qualify for MU and incentive payments under the EHR Incentive Programs.

Enacted under the HITECH Act, the EHR Incentive Programs allow eligible professionals (EPs)[144] and hospitals[145] to qualify for incentive payments beginning in 2011[146] and ending in 2016.[147] There are both Medicaid and Medicare versions of the EHR Incentive Program, with slightly different maximum incentives, administrative structures, and MU requirements.[148]

---

[139] For more information, see *id.* §§ 170.500-.599; *ONC HIT Certification Program*, HEALTHIT.GOV, http://www.healthit.gov/policy-researchers-implementers/onc-hit-certification-program (last visited Sept. 5, 2013).

[140] 45 C.F.R. § 170.302 (2012).

[141] *Id.* § 170.205.

[142] *See id.* § 170.523(i); 76 Fed. Reg. 1262, 1281-85 (Jan. 7, 2011).

[143] American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, § 3001(c)(5)(A), 123 Stat. 115, 232 (describing the ONC certification program as "voluntary"). The ARRA explicitly states that nothing in the Act should be construed "(1) to require a private entity to adopt or comply with a standard or implementation specification adopted under section 3004; or (2) to provide a Federal agency authority, other than the authority such agency may have under other provisions of law, to require a private entity to comply with such a standard or implementation specification." *Id.* § 3006(a), 123 Stat. at 241. Section 13112 is a slight exception to this rule whereby agencies will require in contracts with healthcare plans, providers, or insurers that the plan, provider, or insurer when it upgrades, implements, or acquires health information technology (HIT) systems, that they only utilize ONC-certified technology systems. *Id.* § 13112, 123 Stat. at 243.

[144] An eligible professional is a physician, as defined in 42 U.S.C. § 1395x(r) (2006).

[145] 42 U.S.C. § 1395ww(a) (Supp. V 2011) (governing "payments to hospitals for inpatient hospital services").

[146] *Id.* § 1395w-4(o)(1)(E)(i) (Supp. V 2011) (defining the first payment year as 2011).

[147] *Id.* § 1395w-4(o)(1)(A) (Supp. V 2011) (ending incentive payments after the year 2016).

[148] For more information, see *Choosing a Program: Medicare or Medicaid?*, CTR. FOR MEDICARE & MEDICAID SERV. (May 22, 2013), https://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/index.html?redirect=/EHRIncentivePrograms/30_Meaningful_Use.asp#TopOfPage (contrasting Medicare and Medicaid EHR Incentive Programs).

These programs were structured to encourage the quick and widespread adoption of EHRs by prohibiting EPs from joining the EHR Incentive Programs after 2014.[149] EPs or hospitals that are not meaningful users by 2015 will receive reduced incentive payments.[150] The first requirement for an EP to become a meaningful EHR user is to use "certified EHR technology in a meaningful way."[151]

To reiterate, ONC's authority is tied substantially to the MU incentive payments. These payments are substantial for early adopters, while EPs who are not meaningful users by 2015 will be penalized until they meet the MU requirements set by CMS. ONC's authority to develop and continuously adjust standards and certification criteria is not, however, entirely voluntary because the statutory penalties never end and only grow indefinitely over time. EPs who are meaningful users in 2013 will not receive a payment reduction in October 2014, while EPs who cannot demonstrate MU by July 1, 2014 will receive a one percent payment reduction.[152] CMS and ONC plan to release three stages of MU. These stages will incentivize EPs and hospitals to implement and use their EHRs in accordance with the MU requirements. Despite slow progress implementing the Stage 2 requirements, released in September 2012, ONC began to collect comments on Stage 3 of MU in November 2012.[153]

---

[149] 42 U.S.C. § 1395w-4(o)(1)(B)(v) (Supp. V 2011) (establishing 2014 as the last year a provider can join the EHR Incentive Programs). Furthermore, starting in 2013, eligible professionals who first adopt EHRs after 2013 receive a reduced incentive payment. *Id.* § 1395w-4(o)(1)(B)(ii) to (iii). Providers who adopted in 2011 or 2012 received $3000 more than providers adopting in 2013, and are able to participate for all five years. *Id.*

[150] *Id.* § 1395w-4(a)(7)(A) (Supp. V 2011) (determining percentages of fees applicable to professionals who are not meaningful EHR users by 2015). A similar provision exists for payment to hospitals. *See id.* § 1395ww(b)(3)(B)(ix)(I) (reducing incentive payments for hospitals who are not meaningful EHR users by specified years).

[151] *Id.* § 1395w-4(o)(2)(A)(i).

[152] Medicare and Medicaid Programs; Electronic Health Record Incentive Program—Stage 2, 77 Fed. Reg. 53,968, 53,972 (Sept. 4, 2012).

[153] *See* HIT Policy Committee: Request for Comment Regarding the Stage 3 Definition of Meaningful Use of Electronic Health Records (EHRs), 77 Fed. Reg. 70,444, 70,444 (Nov. 26, 2012); Jodi G. Daniel, *Comment Period Now Open: Help Set the Stage for Meaningful Use Stage 3*, HEALTHIT BUZZ (Nov. 27, 2012, 12:30 PM), http://www.healthit.gov/buzz-blog/meaningful-use/set-stage-meaningful-stage-3 (inviting comments on the Stage 3 MU requirements). Some groups like the American Medical Association (AMA) and American Hospital Association (AHA) have objected to ONC's pace in developing and planning Stage 3 of MU. AMA argues "we believe that it is a serious mistake to keep adding stages and requirements to the meaningful use program without evaluating Stage 1 of the program." Letter from James L. Madara, Exec. Vice President, Am. Med. Ass'n, to Farzad Mostashari, Nat'l Coordinator, Office of the Nat'l Coordinator for Health Info. Tech. 4 (Jan. 14, 2013), *available at* http://www.ama-assn.org/resources/doc/washington/stage-3-meaningful-use-electronic-health-records-comment-letter-14jan2013.pdf. AHA similarly argues that "[a]s of September 2012, fewer than one-third of hospitals had met the Stage 1 requirements

Another substantial part of ONC's duties is to ensure patient health information is securely transferred in a nationwide health information technology infrastructure. In order to do so, ONC must develop consistent standards across all HIT users to accomplish the secure transfer and storage of private health information.[154] ONC has several initiatives that focus on this task. One such initiative is the eHealth Exchange, a nonprofit public-private consortium that replaced an ONC-run project known as the Nationwide Health Information Network (NHIN) in October 2012.[155] ONC defined the goal of the NHIN as a "set of standards, services, and policies that enable the secure exchange of health information over the Internet."[156] NHIN completed the transfer to the eHealth Exchange in late 2012, and will provide a health information exchange infrastructure that is more efficient to operate, less burdensome to test, and capable of reaching a wider consumer base.[157]

The Standards and Interoperability Framework (S&I Framework) is another ONC initiative that could change the way health information is transferred between EHRs. The S&I Framework is a collaborative effort between public and private sector participants that focuses on "providing the tools, services and guidance to facilitate the functional exchange of health information."[158] There are a number of initiatives within the S&I Framework that concentrate on mHealth-related issues, such as harmonizing data standards for interoperability,[159] automatically "pushing" data (as opposed to "pulling" data),[160] and designing a mobile interface for securely accessing and transferring health information.[161]

---

and received a Medicare incentive payment." Letter from Linda E. Fishman, Senior Vice President, Am. Hosp. Ass'n, to Farzad Mostashari, Nat'l Coordinator, Office of the Nat'l Coordinator for Health Info. Tech. 1 (Jan. 14, 2013), *available at* http://www.aha.org/advocacy-issues/letter/2013/130114-cl-hhs-os-2012-0007.pdf. AHA also argues that if ONC addresses "the current limits to interoperability [ONC] will bring far greater benefits than rushing into a definition for Stage 3 that is not built on lessons learned from Stage 1, let alone Stage 2 [which was released September 2012]." *Id.* at 2.

[154] *See* American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, § 3001(b)-(b)(1), 123 Stat. 115, 230 (defining the duties of ONC).

[155] *eHealth Exchange Brief History*, HEALTHEWAY, http://www.healthewayinc.org/index.php/exchange (last visited Sept. 5, 2013).

[156] *Nationwide Health Information Network*, HEALTHIT.GOV, http://www.healthit.gov/policy-researchers-implementers/nationwide-health-information-network-nwhin (last visited Sept. 5, 2013).

[157] *eHealth Exchange*, HEALTHEWAY, http://healthewayinc.org/index.php/exchange (last visited Sept. 5, 2013).

[158] *What Is the S&I Framework?*, S&I FRAMEWORK, http://wiki.siframework.org/Introduction+and+Overview (last visited Sept. 5, 2013).

[159] *See, e.g.*, *S&I Framework Newsletter*, S&I FRAMEWORK (Feb. 2013), http://wiki.siframework.org/file/view/SI+Framework+Newsletter_Feb+2013.pdf/409799872/SI%20Framework%20Newsletter_Feb%202013.pdf.

[160] *See A HIMSS Guide to Participating in a Health Information Exchange*, HIMSS 9

Another intriguing ONC initiative relevant to mHealth applications is ONC's Direct Project. The goal of the Direct Project is to specify a "simple, secure, scalable, standards-based way for participants to send authenticated, encrypted health information directly to known, trusted recipients over the Internet."[162] The Direct Project is directly relevant to the transfer of data from an mHealth application to an EHR in a secure format to be viewed by a care provider. The decision to adopt the Direct Project's standards is left to the discretion of the developers.

ONC held a 2012 Mobile Device Roundtable to examine the implementation of a "national, multi-prong privacy and security educational initiative targeted at health care providers" in December 2012. ONC also created online tools that "encourage health care providers and professionals to know the risks and take the steps to protect and secure health information when using mobile devices."[163] Though ONC has made strides in creating initiatives to address interoperability between healthcare devices, it has not directed much attention to general IT security controls. In May 2011, the Health and Human Services Office of the Inspector General (OIG) issued a report on this lack of focus.[164] OIG ultimately suggested that ONC broaden its focus to develop

(Nov. 2009), http://www.himss.org/files/HIMSSorg/Content/files/HIE/HIE_GuideWhitePaper.pdf (describing the difference between "pushing" and "pulling" data); *Automate Blue Button Interface Push Workgroup*, S&I FRAMEWORK, http://wiki.siframework.org/ABBI+Push+Workgroup (last visited Sept. 5, 2013) (explaining a proposal to meet the "goal of 'automating transmission of personal health data to a specific location, using the Blue Button'").

[161] *RESTful Health Exchange (RHEX)*, S&I FRAMEWORK, http://wiki.siframework.org/RHEx (last visited Sept. 5, 2013) (describing RHEX as "open-source, exploratory project to pilot proven web technologies that support simple, secure, standards-based health information exchange").

[162] *Direct Project Overview*, THE DIRECT PROJECT 4 (Oct. 11, 2010), http://wiki.directproject.org/file/view/DirectProjectOverview.pdf.

[163] *Health Information Technologies: Administration Perspectives on Innovation and Regulation: Hearing Before the Subcomm. on Oversight & Investigations of the H. Comm. on Energy & Commerce*, 113th Cong. 12-13 (2013) (statement of Farzad Mostashari, National Coordinator, Office of the Nat'l Coordinator for Health Info. Tech.), *available at* http://docs.house.gov/meetings/IF/IF02/20130321/100544/HHRG-113-IF02-Wstate-MostashariF-20130321-SD002.pdf.

[164] OFFICE OF THE INSPECTOR GEN., DEP'T OF HEALTH & HUMAN SERVS., PUB. NO. A-18-09-30160, AUDIT OF INFORMATION TECHNOLOGY SECURITY INCLUDED IN HEALTH INFORMATION TECHNOLOGY STANDARDS (2011), *available at* https://oig.hhs.gov/oas/reports/other/180930160.pdf. OIG defines general IT security controls as the "structure, policies, and procedures that apply to an entity's overall computer operations, ensure the proper operation of information systems, and create a secure environment for application systems and controls." *Id.* at 3. In the report, OIG found that ONC's lack of focus on general IT security controls included "encrypting data stored on mobile devices, using two-factor authentication, and updating (patching) the OSs that process and store sensitive health-related information." *Id.* at 6.

standards to protect data storage, rather than just the transmission of health data.[165] In order to fully secure the use of health data from hackers, OIG recommended that ONC adapt ONC's regulatory strategy to encompass general IT security standards that can protect data outside of the interoperability context.[166]

ONC's 2014 Edition EHR Certification Criteria addresses some of the flaws highlighted by the OIG May 2011 Report. The 2014 Edition includes section 170.314(d)(7). This section identifies the need for securing health information "created or maintained by the Certified EHR Technology" by implementing end-user device encryption.[167] It also requires information to be encrypted if electronic health information remains on the end-user device.[168] Alternatively, under § 170.313(d)(7), EHR systems could be programmed to not store data on an end-user device, such as a tablet with an application that allows a physician to enter information into an EHR from the tablet.[169] This is a step in the right direction for securing private health data on end-user devices. ONC, however, specifies within the comment and response section following the criterion that this certification criterion "is generally not intended to apply to personally owned end-user devices, unless an EHR developer supported technology is loaded/installed on such a device."[170] This means that ONC's requirement to prevent storing PHI on an end-user device does not apply to devices used by patients or personally owned devices used by providers (aside from using an EHR developer's supported application).[171]

Currently, MU and the ONC Certification Criterion standards do not address the applicability or use of mHealth applications as part of the definition for MU. Because of this, ONC has no certification criteria for mHealth

---

[165] *Id.* at 9.

[166] The HIT Policy Committee (HITPC), in proposing recommendations for Stage 3 of MU, included two-factor authentication for remote access as one potential requirement. OFFICE OF THE NAT'L COORDINATOR FOR HEALTH INFO. TECH, DEP'T OF HEALTH & HUMAN SERVS., HEALTH INFORMATION TECHNOLOGY; HIT POLICY COMMITTEE: REQUEST FOR COMMENT REGARDING THE STAGE 3 DEFINITION OF MEANINGFUL USE OF ELECTRONIC HEALTH RECORDS 36 (2012), *available at* http://www.healthit.gov/sites/default/files/hitpc_stage3_rfc_final.pdf.

[167] Standards, Implementation Specifications, and Certification Criteria for Electronic Health Record Technology, 2014 Edition, 77 Fed. Reg. 54,163, 54,236 (Sept. 4, 2012).

[168] *Id.* ("EHR technology presented for certification must be able to encrypt the electronic health information that remains on end-user devices.").

[169] *Id.*

[170] *Id.* at 54,238.

[171] This comes at a time when an increasing number of healthcare workers use their personal phones for work purposes. *BYOD Insights 2013: A Cisco Partner Network Study*, CISCO 6, http://www.ciscomcon.com/sw/swchannel/registration/internet/registration.cfm?SWAPPID=91&RegPageID=350200&SWTHEMEID=12949 (last visited Sept. 5, 2013) (finding that 88.6% of surveyed workers in the healthcare industry use their smartphone for work purposes).

applications that could help a provider attain an MU requirement and the incentive payments that come with it. Therefore, in order for ONC to have certification authority over mHealth applications, mHealth applications would need to be considered EHR modules and be added to MU regulations by CMS.[172] Without being included in MU, providers have no direct incentive to use mHealth applications. [173]

Despite ONC's various initiatives on standards and interoperability, its authority is mostly limited to creating standards for an interoperable health exchange. However, the power to regulate EHRs and health information exchange has not been vested in any agency yet.[174] Currently, the EHR Incentive Programs are the driving force behind ONC's regulatory authority. The stages of MU have thus far failed to include the use of mHealth applications as an option or requirement for receiving an incentive payment or avoiding penalties. If MU Stage 3 were to include mHealth applications in some form, ONC presumably would have to develop certification criteria for these mHealth applications and then assess which ones provide the capabilities for privacy, security, and interoperability that meet the goals and objectives of the MU program.

IV. REGULATORY SYSTEM SOLUTIONS

Regulation is a response to a market failure. With mHealth applications, the market has failed to create applications that are safe, effective, and interoperable.[175] The cost of implementing privacy and security safeguards and interoperability standards is excessive compared to the relatively low cost of applications in a saturated market. This market failure could result in applications that are incapable of communicating with EHR systems, bodily injury to consumers who rely on applications, or unwanted disclosure of private health information. This part of the Note will outline various theories of

[172] ONC could indirectly regulate mHealth applications as EHR modules as they did in the latest edition of the Certification Criteria for EHRs. *See* Standards, Implementation Specifications, and Certification Criteria for Electronic Health Record Technology, 2014 Edition, 77 Fed. Reg. 54,163 (Sept. 4, 2012).

[173] Hospitals and hospitalists in particular have an indirect incentive to adopt mHealth applications as part of CMS' Hospital Readmissions Reduction Program. CMS has started penalizing hospitals for readmissions and mHealth applications may help hospitals keep high-risk patients healthy through medication management or tracking the progression of a condition through clinical measurements. *See* 77 Fed. Reg. 53,258, 53,675-76 (Aug. 31, 2012) (establishing the Hospital Readmissions Reduction Program).

[174] This is an interesting area of development that is outside of the scope of this Note. It seems likely that the power to regulate electronic health records will be vested in ONC, rather than FDA.

[175] *See* Francis M. Bator, *The Anatomy of Market Failure*, 72 Q.J. ECON. 351, 351 (1958) (defining market failure as "the failure of a more or less idealized system of price-market institutions to sustain 'desirable' activities or to estop 'undesirable' activities").

regulation that could be applied to mHealth applications, their strengths and weaknesses, and how the theories would work in practice.

Before analyzing the pros and cons of the various ways to regulate mHealth applications, it is important to delineate the requirements for effective regulation. First, practical regulatory standards must be created for data storage, transission, and interoperability, and clinical safety and effectiveness. Second, some form of verification is necessary to identify mHealth applications that meet the requirements for each of these areas. Third, some form of recognition, such as certification, is needed to label applications as having met the applicable requirements. Verification marks may depend on a regulatory authority's expertise. For example, one regulator's mark may indicate compliance with clinical safety and effectiveness requirements, while another regulator's mark may indicate compliance with data security, privacy, and interoperability requirements. Fourth, once an mHealth application is on the market, it should be tested for continuing compliance, and both the applications and complaints regarding them should be monitored for security, clinical effectiveness, and patient-safety concerns.

A. *Pure Private Regulation*

One approach to regulating mHealth applications is private regulation where a private organization serves as the regulatory body. This Section will analyze one potential private regulatory approach to regulating mHealth applications.

Pure private regulation entails a private entity establishing regulations for its own industry without significant government intervention. This type of private regulation typically consists of a free-market system for regulation with an entity (or competing entities) conducting some sort of regulatory function for an industry without a government mandate.[176] Private regulation is based in part on the theory that, in a free market, participants choose products based on information concerning the safety, quality, and price of the product.[177] Private regulation seeks to inform the marketplace by having incentive-based regulation by industries and other private entities, as opposed to coercive regulation by the government.[178] The main difference between public and

[176] David Vogel, *The Private Regulation of Global Corporate Conduct*, *in* THE POLITICS OF GLOBAL REGULATION 151, 153-55 (Walter Mattli & Ngaire Woods eds., 2009) ("A defining feature of civil regulation is that its legitimacy, governance, and implementation are not rooted in public authority. . . . The market-based regulatory mechanisms [that are] typically employed by civil regulations, namely, producer certification, product labeling, third-party auditing, and information disclosure . . . .").

[177] *See* Yesim Yilmaz, *Private Regulation: A Real Alternative for Regulatory Reform* 1, 3 (Cato Institute, Policy Analysis No. 303, Apr. 20, 1998), http://www.cato.org/sites/cato.org/files/pubs/pdf/pa-303.pdf (arguing that private regulation is both more efficient and better suited to protect customers than government regulation).

[178] *Id.* at 2 ("The regulatory system should be able to deliver positive incentives so that people will 'voluntarily modify their behavior.'").

private regulation is that in private regulation there is no power for private entities to forcefully remove products from the market, and therefore it is the consumer's prerogative to choose products based on informed decisions.

Two examples of private regulation of health information technology are the Certification Commission for Health Information Technology (CCHIT)[179] and Happtique's development of standards for mHealth applications.[180] CCHIT is an industry-run regulating body that certifies EHRs. Some have criticized CCHIT's certification criteria as "being excessively favorable to vendors."[181] While CCHIT is not a potential candidate to regulate mHealth applications, the criticism of an industry-run regulatory body is still applicable. Happtique, on the other hand, is not an industry-run certification body, and instead has a board comprised of individuals with expertise in mHealth, technology, and patient advocacy. In developing its mHealth application standards, Happtique received input from federal agencies and private organizations to help guide its approach.[182] Happtique is free from the target industry's influence because it is not an application-developer-focused organization. Happtique was founded to represent a group of health care organizations and clinicians and to help them identify "technically and substantively valid apps."[183] This distinguishes Happtique as a potentially unbiased private certification body for regulating mHealth applications. Happtique aims to fill the gap between applications that will be regulated by FDA and the large majority of those that will not with its

[179] *About CCHIT*, CCHIT, https://www.cchit.org/about (last visited Sept. 5, 2013) (detailing CCHIT's history of certifying EHRs beginning in 2006 to the present where CCHIT is an Authorized Certification Body for ONC certification of EHR technology).

[180] *See Health App Certification Program: Certification Standards*, HAPPTIQUE (Feb. 27, 2013), http://cdn1.hubspot.com/hub/219577/HACP_Standards_FINAL_2.pdf (describing Happtique's standards for mHealth applications including standards for operability, privacy, security, and content). Happtique describes these standards as "not only complement[ing] the objectives of key federal agencies involved in the regulation of mobile health apps, but also rais[ing] the bar for a growing segment of apps that are currently not subject to heightened regulatory oversight." Brian T. Horowitz, *Happtique Publishes Final Standards for Mobile Health App Certification*, EWEEK (Mar. 4, 2013), http://www.eweek.com/mobile/happtique-publishes-final-standards-for-mobile-health-app-certification.

[181] Sharona Hoffman & Andy Podgurski, *Finding a Cure: The Case for Regulation and Oversight of Electronic Health Record Systems*, 22 HARV. J.L. & TECH. 103, 132-34 (2008) (listing several reasons why CCHIT certification is inadequate to safely test EHRs).

[182] *Happtique Health App Certification Program*, HAPPTIQUE, http://www.happtique.com/app-certification (last visited Sept. 5, 2013) (describing the certification standards, who conducts the certification, and how to apply for certification).

[183] CEO Benjamin Chodor stated that Happtique is "well suited" to serve as a "private sector-based app certification program." *Health Information Technologies: Harnessing Wireless Innovation: Hearing Before the Subcomm. on Commc'ns & Tech. of the H. Comm. on Energy & Commerce*, 113th Cong. 7 (2013) (statement of Benjamin M. Chodor, Chief Exec. Officer, Happtique, Inc.), *available at* http://docs.house.gov/meetings/IF/IF16/20130319/100525/HHRG-113-IF16-Wstate-ChodorB-20130319.pdf.

private certification system for mHealth applications.[184] Happtique Chief Executive Officer Benjamin Chodor, however, agreed that for the higher-risk applications "FDA is the best suited and most appropriate agency to regulate those apps that fall under their purview . . . ."[185]

CCHIT is likely an unsuitable regulator of the higher-risk mobile applications over which FDA has asserted authority because CCHIT focuses on EHR devices. Furthermore, CCHIT is an industry-run regulator and thus potentially biased. Happtique is ultimately an unsuitable regulator for the higher-risk mobile applications because the CEO of Happtique has publicly testified that FDA should regulate the higher-risk devices. With CCHIT and Happtique as unsuitable regulators, this Note examines a potentially more appropriate private regulator of various health devices. Perhaps one of the most widely known modern examples of private regulation is Underwriters Laboratories (UL). UL is an independent company that "certifies, validates, tests, inspects, audits, and advises and trains" in a variety of fields, but most relevant to this Note is their work in the "Life & Health" field.[186] The services of UL are voluntary and not mandated by the U.S. government (though a private entity may ask UL to certify a product for compliance with government-mandated regulations).[187]

Despite being a voluntary certification body, UL evaluated over 20,000 types of products in 2012 alone.[188] UL also has relevant experience with regulating mHealth applications. Currently, UL tests devices such as infusion pumps and "human factors engineering" for medical devices to support requests for FDA approval.[189] Furthermore, UL is already working on standards for interoperability for mHealth applications and electronic health records.[190] UL has an enforcement mechanism to ensure certified products

[184] *Id.* at 7.

[185] *Id.* at 11.

[186] *What We Do*, UNDERWRITERS LABORATORIES, http://www.ul.com/global/eng/pages/aboutul/whatwedo (last visited Sept. 6, 2013).

[187] *UL Background and Facts FAQ*, UNDERWRITERS LABORATORIES, http://www.ul.com/global/eng/pages/corporate/contactus/faq/general/background (last visited Sept. 6, 2013) ("There are no laws specifying that a UL Mark must be used.").

[188] *By the Numbers*, UNDERWRITERS LABORATORIES, http://www.ul.com/global/eng/pages/aboutul/whatwedo/bythenumbers (last visited Sept. 6, 2013) (stating that "20,104 types of products were evaluated by UL" in 2012).

[189] *Medical and In-Vitro Diagnostic Devices*, UNDERWRITERS LABORATORIES, http://www.ul.com/global/eng/pages/offerings/industries/healthsciences/medicaldevices (last visited Sept. 6, 2013) (describing UL's medical diagnostic device capabilities).

[190] *eHealth, mHealth, EHR, EMR, HIT and Medical Device Interoperability*, UNDERWRITERS LABORATORIES, http://www.ul.com/global/eng/pages/offerings/industries/healthsciences/services/ehealth (last visited Sept. 6, 2013) ("It is UL's intention to lead/support the development of interoperability standards in conjunction with other standards development organizations (SDO) and regulatory bodies for the interoperability testing and verification of eHealth devices (both medical devices and eHealth products).").

continue to meet certain standards and can take action against manufacturers whose previously certified products fall out of compliance. UL conducts follow-up certification visits to the manufacturer and if a product or the manufacturer is out of compliance with UL standards, then UL may revoke the certification and force the manufacturer to remove UL markings from the product.[191] UL, however, is not a lone force in private certification. In fact, when it comes to industries with "well-defined, widely accepted, and easy to understand standards[,]" many private regulators are expected to "assume a certification role and face competition."[192]

Private regulation offers several benefits over its public counterpart. Proponents argue that private regulation "takes much less time, consumes fewer resources, [] costs less . . . [and] independent parties are responsive and flexible, evolutionary, and can avoid 'one-size-fits-all' regulation."[193] With mHealth applications, flexibility is critical. The regulator's ability to react quickly to changes in the industry provides application developers opportunities to innovate concurrently with technological advances, rather than be subjected to a lengthy review process that slowly adapts to technological changes.[194] For example, since cell phone technology changes every year, it is imperative for application developers to be able to respond to innovation in the marketplace quickly. Therefore, the lengthy FDA approval process will likely restrict the ability of developers to keep pace with the technology.[195] Alternatively, private regulation has the potential to move faster than FDA device regulation due to the fact that multiple private entities can certify devices simultaneously using commonly adopted certification standards.

There are also disadvantages to private regulation. First, because private regulation is voluntary, market availability ceases to indicate safety or reliability. Consumers must rely on the presence or absence of a privately created, and hopefully recognizable, symbol to indicate compliance with some set of standards. A symbol of certification can put the consumer at ease – like the symbol used by UL to certify thousands of everyday devices.[196] This

[191] *UL Variation Notice and Corrective Action Requirements: UL/C-UL/ULC Mark Follow-Up Services*, UNDERWRITERS LABORATORIES, http://www.ul.com/global/documents/offerings/services/fus/globalfieldservices/variation.pdf (last visited Sept. 6, 2013) (detailing the UL options after a product is determined to be nonconforming).

[192] Yilmaz, *supra* note 177, at 10.

[193] *Id.* at 3.

[194] *See* U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 89, at 15, 29 (examining FDA's review process time and finding a time to market of up to 161 days for nonpremarket approval submissions and up to 627 days for premarket approval submissions).

[195] *See* Gold, *supra* note 37 ("The FDA began regulating a handful of medical apps last year . . . . [B]ut some developers have complained that the approval process will be too slow. Medical devices, which the FDA regulates in a similar way, wait six to 20 months for approval . . . .").

[196] *Marks for North America*, UNDERWRITERS LABORATORIES, http://www.ul.com/global/eng/pages/corporate/aboutul/ulmarks/mark/marks-for-north-america (last visited Sept. 6,

symbol is capable of assuring consumers that they have purchased a product that was certified by a company that stakes its reputation on the label. However, despite the benefit of quicker regulation due to multiple private regulators,[197] having several companies certifying various mHealth applications under varying standards could make it difficult for consumers to determine which symbols indicate the highest quality. Furthermore, given the sheer volume of applications that need to be certified, consumers may find it difficult to shop around and make informed decisions.[198] The business model of private regulators is also a source of concern. If an application developer is financing the review, verification, and monitoring of its products, it is likely to prefer the task go to private regulators that provide the appearance of safety, security, and effectiveness without the reality of it. This marketer-financed business model is more vulnerable to conflicts of interest than a consumer-financed (for example, by subscription) or government-financed regulatory model.[199]

2013) ("If a product carries [the UL Listing Mark], it means UL found that representative product samples met UL's safety requirements. These requirements are primarily based on UL's own published standards for safety. This type of Mark is seen commonly on appliances and computer equipment, furnaces and heaters, fuses, electrical panel boards, smoke and carbon monoxide alarms, fire extinguishers and sprinkler systems, personal flotation devices, bullet resistant glass, and thousands of other products."); *see* David Leo Weimer, *Safe—and Available—Drugs*, *in* INSTEAD OF REGULATION 239, 266 (Robert W. Poole, Jr. ed., 1982) ("Firms offering certification services might arise to help the more-reputable manufacturers distinguish themselves from the rest of the industry. These independent firms might be hired to certify quality control in manufacturing, validity of clinical studies, and truthfulness of therapeutic claims. If the certification firms were successful in establishing their credibility with physicians and consumers, the entire pharmaceutical industry would be forced to seek their services.").

[197] *See* Peter Grindley, *Regulation and Standards Policy: Setting Standards by Committees and Markets*, *in* THE REGULATORY CHALLENGE 210, 218 (Matthew Bishop et al. eds., 1995) (comparing the benefits of regulation by public committee and standards set by the private market).

[198] There are estimated to be at least 40,000 mHealth applications on the market with the number of applications increasing by 23,000 in just one year. *See supra* note 36 and accompanying text (discussing the recent, dramatic increase in the number of applications). This may be one reason why private regulation is better suited than government regulation, as agencies such as FDA do not have the flexibility to increase their regulatory capacity in response to unexpected, dramatic increases in the market.

[199] Though government funds finance a majority of FDA's regulation system, industry user fees contribute to this funding as well. *See* News Release, U.S. FDA, FDA Seeks $4.5 Billion to Support Medical Product Development, Protect Patients and Ensure Safety of the Food Supply (Feb. 13, 2012), http://www.fda.gov/newsevents/newsroom/pressannouncements/ucm291691.htm. The conflict of interest is less present because presumably FDA regulators are impartial. Furthermore, FDA is the only avenue for medical devices and drugs to get to the market and there are no competing regulators with potentially less stringent or less protective regulatory standards.

Another drawback with this system is that private regulation is typically voluntary and industry run, and thus the incentive to remove products from the market is constrained by contractual terms and opportunistic behavior.[200] Private regulators have no inherent authority to take products off of the market, and developers are not obligated to comply with penalties imposed by private regulators. Some private regulatory bodies do not remove products from the marketplace, but rather ecertify the product and wait for the market to react.[201] The effectiveness of private regulation primarily hinges on informed consumers knowing which private regulators are trustworthy and which products are safe based on the presence of marks of certification, attributes that can be difficult for consumers to discern.

In practice, it is likely that more than one competitor will regulate any given mHealth application.[202] It may be that no single private regulator has the experience necessary to regulate all types of devices and related applications for clinical effectiveness and safety, as well as data privacy, security, and interoperability. Given that private regulators will themselves be competing for certification business revenue, the potential for the least effective private regulator to become the most sought after and best financed by its device-industry and application-developer customers would be a constant cause for concern.

A remaining question in determining how private regulators would address mHealth applications is whether one or more private regulators will even be interested in certifying devices for privacy, security, and interoperability. For the sake of argument, this Note will assume that private regulators will want to certify mHealth applications.[203] As far as the first stage of regulation outlined

[200] Andrew A. King & Michael J. Lenox, *Industry Self-Regulation Without Sanctions: The Chemical Industry's Responsible Care Program*, 43 ACAD. MGMT. J. 698, 700, 713-14 (2000) (finding that, without explicit contractual sanctions, self-regulatory bodies fall victim to opportunism – that is, without an "iron fist of explicit sanctions" opportunistic behavior of firms will "lead to 'adverse selection' and 'moral hazard'"); Yilmaz, *supra* note 177, at 9 ("Private regulation also has effective enforcement mechanisms. Independent third parties use legally enforceable contracts; sanctions including revoking of approvals, fines, and pulling products off the market; and public announcements.").

[201] Yilmaz, *supra* note 177, at 13 ("UL conducts annual and unannounced on-site monitoring and product inspection. If a company fails the inspection, UL can revoke its certification of the product.").

[202] *See id.* ("Although it is the dominant standard-setting body in the United States, UL has many competitors in testing and certification.").

[203] In a world where private regulators choose not to certify devices for privacy, security, and interoperability, it is possible that the free market could still, in the absence of identifiable certification symbols, effectively lead to the most efficient results. After all, patients likely will want to integrate their data with their EHR, either through their own initiative or that of their care provider, and the market may respond to this demand if profitable. As for privacy and security standards, mHealth application developers are subject to FTC enforcement of the breach notification rule if their applications send PHI to a

above, setting standards would be straightforward for UL or any other private entity to design. UL could design interoperability and safety standards based on the work that ONC has already completed in the area, or UL could develop its own standards based on its experience and industry input. Certification of these standards would again be straightforward for private regulators to implement. Once standards are developed, private regulators could emerge, and many would be capable of certifying mHealth applications.[204] While there is, again, no authority – aside from contractual – for the private regulators to mandate that mHealth application developers certify their product according to these standards, informed consumers will likely want to purchase products that are certified or have some guarantee of privacy, security, and interoperability.[205] Furthermore, providers can help steer patients towards

personal health record. BUREAU OF CONSUMER PROT., FTC, COMPLYING WITH THE FTC'S HEALTH BREACH NOTIFICATION RULE 1-2 (Apr. 2010), *available at* http://business.ftc.gov/sites/default/files/pdf/bus56-complying-ftcs-health-breach-notification-rule.pdf (detailing who and what is subject to the Health Breach Notification Rule, including vendors of personal health records). FTC enforcement may be inadequate, though, as the Breach Notification Rule only requires covered entities to notify affected consumers and FTC. If a developer fails to notify FTC and affected consumers within a certain timeframe the developer may be subject to fines by FTC, up to $16,000 per violation. 16 C.F.R. § 318.7 (2013); BUREAU OF CONSUMER PROT., *supra*, at 7. The threat of enforcement may not deter a developer from using unsecured data storage and transmission standards in its applications if the only threat is they must notify the public and FTC with no threat of pecuniary damage. FTC recently stepped up enforcement and issued guidelines for mobile application developers on how to avoid privacy violations. *See* FTC, MOBILE PRIVACY DISCLOSURES: BUILDING TRUST THROUGH TRANSPARENCY (Feb. 2013), *available at* http://www.ftc.gov/os/2013/02/130201mobileprivacyreport.pdf (suggesting best practices for mobile application developers to improve disclosures of privacy violations); Edward Wyatt, *F.T.C. Suggests Privacy Guidelines for Mobile Apps*, N.Y. TIMES, Feb. 2, 2013, at B1, *available at* http://www.nytimes.com/2013/02/02/technology/ftc-suggests-do-not-track-feature-for-mobile-software-and-apps.html ("In a strong move to protect the privacy of Americans as they use the Internet on their smartphones and tablets, the Federal Trade Commission on Friday said the mobile industry should include a do-not-track feature in software and apps and take other steps to safeguard personal information.").

[204] This parallels ONC's certification system wherein ONC developed the standards for certification and subsequently authorized six certification bodies to carry out ONC's work. *See Authorized Testing and Certification Bodies*, HEALTHIT.GOV, http://www.healthit.gov/policy-researchers-implementers/authorized-testing-and-certifications-bodies (last visited Sept. 6, 2013) ("EHR certification by an [Authorized Testing and Certification Body] will signify to eligible professionals, hospitals, and critical access hospitals that the EHR technology has the capabilities necessary to support their efforts to meet the goals and objectives of meaningful use.").

[205] *See* HENRY I. MILLER, TO AMERICA'S HEALTH: A PROPOSAL TO REFORM THE FOOD AND DRUG ADMINISTRATION 78 (2000) ("[M]any retailers are reluctant to carry products lacking UL (or equivalent) approval, and, occasionally, insurers deny liability coverage for products without it."); Sebastien Houde, How Consumers Respond to Product Certification: A Welfare Analysis of the Energy Star Program 36-37 (Oct. 30, 2012) (unpublished

privately certified applications. Finally, private regulators are capable of performing postmarket surveillance to guarantee that certified products continue to meet the regulator's certification standards. A private (or public) regulator's reputation depends on effective postmarket surveillance. As just one example, UL performs postmarket surveillance in its continuous certification process.[206] If an application fails, it loses the UL seal of approval.[207] This system could easily work with mHealth applications with regards to privacy, security, and interoperability. Many competitors likely would be willing to conduct the same continuing certification to help accommodate the vast and increasing quantity of mHealth applications available on the market.

Of course, private regulation does not have an inherent enforcement mechanism apart from contractual obligations signed by voluntary actors, which poses problems in this context. For example, if an application loses certification for interoperability, no one will be harmed. But, people may stop using the application – a strong incentive for the developer to maintain interoperability. If, however, an application fails privacy and security standards, the private regulator's inability to remove the application from the market becomes a larger issue because it could cause actual harm. The regulator can only decertify a product and let the market react by ceasing to purchase the product. It seems entirely possible that if a developer's application fails a private regulator's certification standards, the developer could drop out of the contract with the private regulator and continue marketing the product – albeit without the potential value of a private regulator's certification. Furthermore, developers are not bound to choose a specific certification body. In the event there are multiple certification bodies, developers could pick and choose a certification body with less rigorous enforcement and still obtain a certificate of compliance. The enforcement presence of FTC is a potential solution to this problem, with developers correcting privacy and security concerns for applications that fall under FTC's jurisdiction.[208] When an application is not subject to FTC's health breach

manuscript), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2175436 (concluding that the Energy Star label indicating certification "could increase sales of a particular refrigerator model in a range of 7 to 15%").

[206] *Inspection*, UNDERWRITERS LABORATORIES, http://www.ul.com/global/eng/pages/solutions/services/inspection (last visited Sept. 6, 2013) (providing links to the various inspection services offered by UL to ensure compliance with certification standards).

[207] *Id.*; *NOM Certifications Directory*, UNDERWRITERS LABORATORIES, http://www.ul.com/global/eng/pages/corporate/certifications/nommarkpcoportal/nomcertificationsdirectory (last visited Sept. 6, 2013) (listing the various types of certification, including "cancelled certificate: revoked compliance statement mainly due to product or contract non-compliance [with certification specifications]").

[208] *See* BUREAU OF CONSUMER PROT., *supra* note 203, at 7 (providing tips for businesses to comply with the HIPAA breach notification rule and alerting businesses they may be subject to a "civil penalty of up to $16,000 per violation").

notification rule, though, it may be more difficult to rely on the free market to police these actions. Patients will often be unaware that any personal health information was stolen, and if they do find out, uncovering an mHealth application as the source of the breach would be highly unlikely.

MHealth applications are complex and require more than just the regulation of data standards to make them truly safe and effective. For many consumers and developers, a more important inquiry may be how safe and effective the applications are and whether the applications contribute to any serious adverse healthcare events. First, private regulators must develop standards to certify mHealth applications for safety and effectiveness, essentially acting in the role of FDA. UL, along with other potential private regulators, should be more than capable of developing these standards as it often helps manufacturers certify their products and speeds up FDA approval.[209] UL has developed more than 1000 standards[210] in use today and has even developed a standard specifically for software.[211] Furthermore, since the regulator may be more familiar and responsive to the industry, the standards-development process should be faster and custom-tailored to mHealth applications.

With respect to certification, UL has extensive experience certifying devices for safety and even has some experience certifying medical devices such as infusion pumps.[212] Again, however, UL lacks authority to mandate certification for mHealth applications generally.[213] Whether voluntary

[209] *See Human Factors Engineering for Medical Devices*, UNDERWRITERS LABS., http://www.ul.com/global/eng/pages/offerings/industries/healthsciences/medicaldevices/usability (last visited Sept. 6, 2013) ("UL provides full life-cycle human factors engineering services to meet regulatory, standards certifications and marketing requirements which allows manufacturers to use an independent third party to assess their products, design processes, and improve their in-house knowledge[.]"); *Services for Infusion Pump Manufacturers*, UNDERWRITERS LABORATORIES, http://www.ul.com/global/eng/pages/offerings/industries/healthsciences/medicaldevices/ul60601/infusionpump (last visited Sept. 6, 2013) ("UL's full service laboratories . . . have the test equipment and trained technical staff to provide a full suite of services to help infusion pump manufacturers apply to global regulatory markets.").

[210] *Catalog of Standards*, UNDERWRITERS LABORATORIES, http://www.ul.com/global/eng/pages/solutions/standards/accessstandards/catalogofstandards (last visited Sept. 6, 2013) (listing UL's more than 1000 standards for safety).

[211] *See, e.g.*, *UL 1998 Standard for Software in Programmable Components*, UNDERWRITERS LABORATORIES CATALOG STANDARDS (May 29, 1998), http://www.ul.com/global/eng/pages/solutions/standards/accessstandards/catalogofstandards/standard/?id=1998_2 (listing the UL standard for "Software in Programmable Components").

[212] *See Medical and In-Vitro Diagnostic Devices*, *supra* note 189 (detailing the standard setting ability of UL including in the area of infusion pumps).

[213] One potential private regulation alternative would be for Google and Apple to require that all mHealth applications sold on their respective markets be privately certified for patient safety and device security concerns. Considering Google's and Apple's combined share of the smartphone market, this approach would effectively create a requirement of private certification. *See* Don Reisinger, *Android Nabs Record 80 Percent Market Share in Q2*, CNET (Aug. 1, 2013, 9:16 AM), http://news.cnet.com/8301-1035_3-57596548-94/andr

certification systems will work to preserve the health and safety of patients who are using the applications will depend on the free market's demand for safe and effective certified applications over uncertified applications. This gives freedom and flexibility to manufacturers without imposing stringent certification criteria and a lengthy process similar to what would be imposed by FDA. The trade off is that consumers mostly have to determine which applications – within the class of potentially harmful applications – are safe, with the assistance of a private regulator's certification, rather than relying on the assumption that because these applications have made it to the market they are safe.[214]

UL also has experience monitoring manufacturers and inspecting their facilities after they release certified devices to the market to ensure that manufacturers are continuing to meet the certification standards.[215] If a manufacturer fails these mandatory inspections, UL will remove their trusted certification label from the product.[216] After UL removes their certification from an mHealth application, ideally the market will notice that the product is no longer certified. Consumers may still use the products if they are unaware of (or indifferent to) the fact that the product has lost its certification. Eventually tort litigation may force the product off the market,[217] but, until that time, consumers may continue to use the product and risk unnecessary harm.[218]

oid-nabs-record-80-percent-market-share-in-q2 (reporting an eighty percent worldwide smartphone market share for Googles Android and a 13.6% market share for Apple's iOS).

[214] FDA-approved devices are not always safe, however, and sometimes approved devices are recalled for causing harm or for lack of clinical effectiveness. *See Medical Devices: List of Device Recalls*, U.S. FDA, http://www.fda.gov/MedicalDevices/Safety/ListofRecalls/default.htm (last updated May 24, 2013) (listing the recent medical device recalls).

[215] *Inspection*, *supra* note 206 (providing links to the various inspection services offered by UL to ensure compliance with certification standards).

[216] Yilmaz, *supra* note 177, at 13 ("UL conducts annual and unannounced on-site monitoring and product inspection. If a company fails the inspection, UL can revoke its certification of the product."); *NOM Certifications Directory*, *supra* note 207 (listing the various types of certification).

[217] Tort litigation for injuries caused by approved medical devices, however, has become substantially more difficult in recent years. *See* Riegel v. Medtronic, Inc., 552 U.S. 312, 330 (2008) (holding that state tort claims are preempted under the Medical Device Amendments of 1976 "to the extent they are 'different from, or in addition to' the requirements imposed by federal law"). Some have proposed reforms to the tort system as a way to deregulate the prescription drug market. *See* Weimer, *supra* note 196, at 267-77 ("[S]trengthening the strict liability laws, abolishing the community-standard provision, encouraging no-fault insurance, and promoting a bounty system would improve incentives for manufacturers and physicians to promote and develop effective and safe drugs.").

[218] Doctors may be able to react to some extent to certification revocations, but it is unlikely that doctors will know which applications each patient is using and be able to inform the patient that said application is no longer safe. A doctor can more easily alert patients to decertification if the doctor uses the same certified applications for all patients.

In sum, private regulation offers several advantages over costly, time-consuming public regulation – mainly flexibility, speed, and responsiveness to the industry being regulated.[219] Ultimately the decision of whether to trust private regulation with mHealth applications depends on faith in the free market and in consumers' ability to become and remain informed about product safety and certification. One of the fundamental distinctions between private and public regulation – apart from the regulating body – is the reaction to unsafe products. With respect to mHealth applications, the risk of applications malfunctioning or providing incorrect data is too grave to leave to private regulation without a powerful enforcement mechanism. Leaving products on the market is unacceptable when the products concern the health of unaware or uncaring consumers relying on these devices to manage a health condition.

B. *Public Regulation*

The counterpoint to private regulation is conventional command-and-control public regulation. In this system a public agency or entity pronounces standards and certifies devices accordingly. Once a device fails certification or proves to be hazardous to the public health, then the agency can recall the product and mandate its removal from the market.

The theory of conventional regulation stems from the idea that private companies are incapable of effectively self-regulating because of the potential for bias in enforcement and rulemaking. The free market fails to account for harm to individuals, either because of the costs of accommodating for that harm or because the public has difficulty making decisions that further their best interests on such a highly technical issue.[220] The theory of public regulation needs to be modified in this context, as neither FDA nor ONC has both the expertise and authority to successfully regulate mHealth applications. One way to apply conventional regulation to mHealth applications would be to have FDA and ONC work cooperatively, with FDA exercising general authority and ONC acting as a subject-matter expert on data standards to help inform FDA's regulatory.[221] This regulatory model is best positioned to ensure

Regardless, it would be difficult for the doctor to discover if the application was decertified.

[219] *See* Neil Gunningham & Joseph Rees, *Industry Self-Regulation: An Institutional Perspective*, 19 L. & POL'Y 363, 366 (1997) ("According to proponents, the benefits of industry self-regulation are apparent: speed, flexibility, sensitivity to market circumstances and lower costs."); Yilmaz, *supra* note 177, at 9-10 (arguing that private regulation is flexible and responsive to industry change, and cheaper than federal regulation).

[220] *See* Lori Qingyuan Yue et al., *The Failure of Private Regulation: Elite Control and Market Crises in the Manhattan Banking Industry*, 58 ADMIN. SCI. Q. 37, 37-39 (2013) (examining the effects of private regulation on industry).

[221] An alternative way to apply public regulation with multiple agencies would be to allow the agencies to exercise independent jurisdictional authority wherein FDA regulates mHealth applications, but ONC concurrently continues to operate its certification program for EHR modules – a category that may include some mHealth applications.

the safety, interoperability, and security of mHealth applications while allowing the applications to reach their full clinical potential.

A modern example of this type of regulatory framework is ONC's certification of EHRs. ONC was given statutory authority to certify EHRs capable of meeting the requirements for MU.[222] The American Recovery and Reinvestment Act of 2009 mandated that ONC consult with the Director of the National Institute of Standards and Technology (NIST) when developing a certification program.[223] NIST served in an advisory role for ONC, filling in ONC's informational gaps with NIST's own expertise.[224] NIST was instrumental in providing the expertise necessary to develop and test health IT tools as part of a certification program.

When examining the jurisdictional authority to regulate mHealth applications, it is clear that FDA has the authority in this arena, or is at least asserting its authority, to regulate *some* mHealth applications as medical devices.[225] On the other hand, ONC lacks any real authority to regulate mHealth applications. ONC only has the authority to develop standards for data interoperability, privacy, and security, as well as authority to incentivize EHR manufacturers to adopt ONC standards in order for providers to implement these technologies for MU incentive payments.[226] Despite this certification power, ONC does not have a meaningful punitive mechanism to implement these standards. By contrast, FDA has the ability to mandate the removal of products from the market when the products prove to be unsafe or ineffective.[227]

---

[222] American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, § 3001(c)(5), 123 Stat. 230, 232 ("The National Coordinator . . . shall keep or recognize a program or programs for the voluntary certification of health information technology as being in compliance with applicable certification criteria adopted under this subtitle. Such program shall include, as appropriate, testing of the technology . . . .").

[223] *Id.* ("The National Coordinator, in consultation with the Director of the National Institute of Standards and Technology, shall keep or recognize a program or programs for the voluntary certification of health information technology as being in compliance with applicable certification criteria under this subtitle.").

[224] *Test Method for Health Information Technology*, NIST, http://healthcare.nist.gov/use_testing (last updated Feb. 7, 2011) (describing NIST's collaboration with ONC in developing test procedures for the ONC EHR certification program).

[225] *See* U.S. FDA, *supra* note 6, at 10 (describing FDA's intention to regulate only a subset of mHealth applications that meet the definition of a device while exercising enforcement discretion with respect to low-risk devices).

[226] *See supra* Part III.B (discussing ONC and MU).

[227] 21 U.S.C. § 360h(e) (2012) (defining FDA's authority to recall devices if "there is a reasonable probability that a device intended for human use would cause serious, adverse health consequences or death"). FDA has no statutory authority to recall a device for privacy, security, or interoperability concerns. Congress would need to amend the FDCA to allow FDA to recall devices for privacy, security, and interoparability concerns.

While FDA has the jurisdictional authority to regulate mHealth applications and the ability to mandate their removal them from the market in the event they are unsafe, it does not have the requisite expertise to holistically regulate these applications. FDA's expertise and infrastructure is limited to approving devices for patient-safety concerns and conducting postmarket surveillance.[228] FDA has yet to adapt its device-approval processes to regulate data privacy and security and has little experience certifying theinteroperability of data from medical devices to EHRs. ONC has almost a decade of experience working on data privacy, security, and interoperability with EHRs and seems very well suited to be instrumentally involved in regulating mHealth applications.

Because of the interplay between the two agencies' authority and expertise, a public regulatory system would function with FDA as the chief regulator and ONC as an ancillary advisor. ONC's expertise on data privacy, security, and interoperability could be successfully integrated into FDA's well-developed regulatory system. This cooperative system ensures that, together, the public agencies have both the authority and the expertise to regulate mHealth applications in the most effective way.

This framework provides several advantages. An agency without enforcement power but with expertise is capable of providing valuable input to the one agency that has the enforcement power. Furthermore, application developers would need to only clear one regulatory approval process before their applications could hit the market. By incorporating standards into FDA's device approval process, this framework would also effectively mandate privacy and security controls as well as interoperability standards.[229] This mandate would be a boon for patients and providers as they reap the benefits, but it may also hamper innovation and the number of applications available.[230]

This regulatory framework is not without flaws. MHealth applications that are categorized as Class I[231] (or no Class) in FDA's device approval process may still pose risks to patient privacy and security. However, these applications are exempt from a stringent FDA approval process, thereby eliminating any opportunity to utilize ONC's expertise on privacy and security issues.[232] Applications that are not regulated by FDA because they pose no

[228] *See supra* Part III.A (discussing the statutory authority of FDA to regulate medical devices and the institutional capacity of the agency).

[229] It may be wise for future regulatory bodies to mandate security and interoperability standards for all electronic health devices, but, at the current stage of regulation, this is a voluntary certification process run by ONC.

[230] Fewer applications on the market may not be a terrible thing. Given the astonishing and still growing number of medical applications for mobile phones, consumers may soon become overwhelmed by the sheer number available.

[231] A few examples of Class I medical devices are examination gloves, wheelchair parts, and various test reagents. *Product Classification Database*, U.S. FDA, http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfpcd/classification.cfm (last updated Aug. 5, 2013).

[232] *See supra* notes 91-94 and accompanying text (discussing the mandatory premarket approval of certain devices and the exemption of the premarket approval process for other

risks to patient safety would need to be regulated by ONC as part of ONC's existing certification process or by a private regulator, such as Happtique. In order to certify these applications, FDA would need to create another class that applies to devices that transmit health data but pose no risk to privacy and security. Creating another device class would likely confuse manufacturers and application developers even further given the already intense uncertainty over what FDA classification applies, despite numerous guides. One solution to this problem might be to allow ONC to certify applications of all Classes while FDA approves devices based on safety. However, this would require ONC to act outside of its advisor role and become a joint regulator with FDA, which ONC does not have the statutory authority to do. Joint regulation, with authority truly shared between two agencies, can be problematic because of agency conflict over how the product should be regulated.[233] Another issue is that FDA's approval process is lengthy and slow for manufacturers.[234] Some have already expressed a fear that applying this process to mobile applications would stifle innovation and the number of applications available.[235]

Because of these problems, public command-and-control regulation is neither the ideal nor likely solution for the regulation of mHealth applications. While protective of patient safety, a public regulation framework is too burdensome and inflexible for application developers because applications are not only regulated for clinical effectiveness and safety but also for data standards. Public regulation by FDA is necessary to some extent on the issue of safety and effectiveness of mHealth applications. Moreover, ONC could (and should) continue to utilize its experience and resources to develop standards and certifications requirements for mHealth applications and other devices. However, it seems that regulating mHealth applications for privacy, security, and interoperability concerns would best be left to the market to incentivize adoption of the most appropriate standards.[236] Ultimately, the

devices).

[233] *See, e.g.*, Lars Noah, *Challenges in the Federal Regulation of Pain Management Technologies*, 31 J.L. MED. & ETHICS 55 (2003) (describing the challenges posed by joint-regulation of pain management drugs by FDA and DEA).

[234] *See supra* notes 126-29 and accompanying text (documenting the delay in FDA approval).

[235] *See, e.g.*, *Health Information Technologies: Harnessing Wireless Innovation: Hearing Before the Subcomm. on Commc'ns & Tech. of the H. Comm. on Energy & Commerce*, 113th Cong. 3 (2013) (statement of George S. Ford, Ph.D., Chief Economist, Phoenix Ctr. for Advanced Legal & Econ. Pub. Policy Studies), *available at* http://docs.house.gov/meetings/IF/IF16/20130319/100525/HHRG-113-IF16-Wstate-FordG-20130319.pdf ("Given the nature of regulation, the costs to innovation and competition may not be offset by improvements in safety and efficacy."). Fewer applications on the market may not be a terrible thing. Given the astonishing and still growing number of medical applications for mobile phones, consumers may soon become overwhelmed by the sheer number available.

[236] *Contra* INST. OF MED., *supra* note 81, at 163 (arguing that data standards are too important to leave with a self-certification mechanism and calling for the "establishment of

benefits of prescribing these standards can be achieved without public regulation.

C. *Meta-Regulation*

Meta-regulation combines the benefits of both private regulation and public regulation, creating a system that accommodates the power expertise imbalance between FDA and ONC and the complexity of mHealth applications themselves. Meta-regulation coordinates private regulation with federal agency oversight. This is not the first time that meta-regulation has been proposed for regulating medical devices, and likely not the last.[237] This section will examine meta-regulation in the context of mHealth applications. Meta-regulation is a step between conventional agency regulation and the self-correcting free market.[238] Gunningham and Rees outlined two types of meta-regulation – "mandated full self-regulation" where the private organization is in charge of rulemaking and enforcement[239] and "mandated partial self-regulation" where the government either makes the rules for enforcement by the private entity or enforces rules made by a private entity.[240]

One current example of meta-regulation is the Financial Industry Regulatory Authority (FINRA). FINRA was created in 2006 when the National Association of Securities Dealers, Inc. (NASD) and the New York Stock Exchange Group, Inc. (NYSE Group) merged their regulatory authority into a singule self-regulatory organization.[241] This new organization was "responsible for regulatory oversight of all securities firms that do business with the public;

an oversight organization . . . [and] a mechanism for assessing conformance with the data standards").

[237] *See* MILLER, *supra* note 205, at 76-81 (proposing a system of certification by a private entity overseen by a public regulator for medical device regulation). The European Union utilizes "Notified Bodies" for certifying medical devices for the Members States. *See Need for Notified Body?*, EUROPEAN COMM'N, http://ec.europa.eu/enterprise/policies/single-market-goods/cemarking/professionals/manufacturers/notified-body/index_en.htm?filter=14 (last visited Sept. 6, 2013) (detailing what products need to go before a Notified Body to be compliant).

[238] Cary Coglianese & Evan Mendelson, *Meta-Regulation and Self-Regulation*, *in* THE OXFORD HANDBOOK OF REGULATION 146, 149-50 (Robert Baldwin et al. eds., 2010) ("[M]eta-regulation focuses very much on outside regulators but also incorporates the insight from self-regulation that targets themselves can be sources of their own constraint.").

[239] Gunningham & Rees, *supra* note 219, at 365 (defining "mandated full self-regulation" as "privatiz[ing] both rulemaking and enforcement").

[240] *Id.* (defining "mandated partial self-regulation" as "limit[ing] privatization to either regulatory function, but not both"). Gunningham and Rees acknowledge a third type: pure self-regulation whereby the private group takes the initiative to create rules and enforce them with no government mandate. *Id.* (defining "'pure' self-regulation" as regulation "without any form of external intervention").

[241] Order Approving Proposed Rule Change to Amend the By-Laws of NASD to Implement Governance and Related Changes, 72 Fed. Reg. 42,169 (Aug. 1, 2007).

professional training, testing and licensing of registered persons; arbitration and mediation; market regulation by contract . . . and industry utilities . . . ."[242] This is a form of mandated full self-regulation where FINRA both creates the rules for enforcement and then enforces those rules. FINRA's ability to create rules is somewhat tempered by SEC's oversight and ability to directly regulate the industry. This government oversight can help temper the threat of agency capture by the regulated industry.

The benefits of a meta-regulatory system are that the regulating group is close to the industry itself and therefore responsive to changes in the market, flexible, faster than a federal regulatory agency, and knowledgeable where perhaps the regulating agency is lacking.[243] All of these benefits are critical in a fast-paced industry like mHealth, where innovation is critical. Furthermore, mHealth application developers operate in a highly technical environment that regulators like FDA are unlikely to understand.

Some critics of meta-regulation models assert that the private groups who regulate the industry are subject to agency capture and this impedes their ability to regulate primarily for the general public's interest.[244] Critics also claim that private regulators are "frequently an attempt to deceive the public into believing in the responsibility of an irresponsible industry"[245] and that "self-regulatory standards are usually weak, enforcement is ineffective and punishment is secret[ive] and mild."[246] With meta-regulation, the customer is the developer rather than the public. If the self-regulatory organization is incentivized only to regulate in its own best interest and sufficient controls are not in place, then the organization will act in its own, and not the public's, best interest. On the other hand, if the incentives are for the self-regulatory organization to regulate in the public's interest, then there is no need for a regulatory solution structure since the free market will sufficiently police the industry.[247]

With mHealth development, one inventive might be the government chartering private organizations to regulate mHealth applications. If a private regulator of mHealth applications were to do a poor job, then the government

[242] *Id.* at 42,170.

[243] *See* Coglianese & Mendelson, *supra* note 238, at 152 ("As Gunningham and Rees note, proponents argue that, 'the benefits of industry self-regulation are apparent: speed, flexibility, sensitivity to market circumstances and lower costs.'" (quoting Gunningham & Rees, *supra* note 219, at 366)).

[244] Gunningham & Rees, *supra* note 219, at 366 ("[S]elf-regulation has an extremely tarnished image, and is often reviled . . . for being a charade.").

[245] *Id.* at 370 (quoting John Braithwaite, *Responsive Regulation in Australia*, *in* BUSINESS REGULATION AND AUSTRALIA'S FUTURE 81, 93 (Peter Grabowsky & Johan Braithwaite eds., 1993)).

[246] *Id.*

[247] Coglianese & Mendelson, *supra* note 238, at 153 ("The primary problem with self- and meta-regulation is that even though businesses have better information to find solutions to public problems, they do not necessarily have better incentives to do so.").

could either revoke the regulator's charter, or even step in to regulate mHealth applications directly. The threat of revocation of a private regulator's charter would be both credible and effective if the government were to charter multiple private regulatory entities and continuously compare their performance both publicly and privately. Thus, a poorly performing private regulator would have an incentive to balance its interest in satisfying client developers with the public's interest in effective oversight, as the government would have a ready supply of competitors available to step in if revocation became necessary. A variation on this approach would be to have the government contract with private regulators.[248] In this situation, the cost of paying for contractors to regulate would be borne by taxpayers, financed by user fees assessed on developers, or both.

Meta-regulation could apply in a variety of ways to the mHealth arena. In one model, FDA may claim total authority to regulate mHealth applications. FDA would then authorize several external regulators to conduct the safety and efficacy reviews – without explicit review from FDA – for the mHealth applications. By taking the applications out of the regular FDA approval process, the applications are likely to be approved faster, thus helping the developers stay up to date with innovation in the market. Yet this model addresses only a portion of the potential issues surrounding mHealth applications because of FDA's unfamiliarity with privacy, security, and interoperability standards. Under a second related model, FDA would have approval authority, but ONC would serve as a critical regulatory advisor that provides FDA with recommended strategies to regulate mHealth applications. A third model would have both FDA and ONC authorize private regulators to regulate the applications under the supervision of each respective agency. As discussed above, however, ONC lacks the authority to require application developers to adopt ONC certification standards. Only FDA's private regulators would be backed by a credible threat that the government will take action against a mobile developer who flouts a private regulator's request to recall unsafe or ineffective applications.

Under any of these models, FDA and ONC might find it easiest to recognize a single consortium certification body created by mobile application developers in lieu of an approach built on a series of competing federally certified private regulators. FDA could certify a consortium trained in regulating mHealth applications for clinical effectiveness and safety. While this does not seem likely, it is a strong possibility with a meta-regulation framework for mHealth applications. ONC could certify a consortium to

[248] Both FDA and ONC have utilized this approach to regulating products. ONC selects a private accreditation body which then approves several private certification organizations to certify health IT devices. *See supra* notes 138-43 and accompanying text. FDA also uses contracts with a private accreditation organization to accredit third-party auditors to audit and certify foreign facilities to prevent food safety problems. *See* 78 Fed. Reg. 45,782 (July 29, 2013).

regulate mHealth applications for compatibility with ONC's recognized standards for interoperability as well as privacy and security standards for transferring and storing data.[249] ONC would likely develop both the interoperability and privacy and security standards required for mHealth applications to achieve certification under this scheme.[250] Because of ONC's current lack of enfocement power for these standards, this consortium of developers could only enforce the certification standards through revoking the certification seal that demonstrates ONC compliance.[251]

Ideally, this seal would encourage market participants to inform themselves before purchasing products and would serve as a guide for choosing only certified mHealth applications.[252] Because the consortium could determine how to enforce the standards, this model would qualify as mandated partial self-regulation.[253] In this situation, ONC would develop certification requirements (for example, data standards) and leave enforcement of those certification requirements to the private regulators – here, the certifying bodies that have adopted ONC's standards for certification. The term "mandated" is misleading because ONC is not mandating compliance in the same way FDA can mandate compliance with its device-approval process, but is rather directly involved in the rulemaking through the agreement with the private regulators. Allowing private regulation of ONC's standards is a satisfactory solution because the industry should have leeway in how it applies standards rather than being subject to a more stringent government certification process.

[249] Using ONC's standards makes sense given that they have been researched and developed for years. Starting a new process to develop standards would be costly and damage the ultimate goal of interoperability with EHRs.

[250] This is not to say that competing standards could not or would not be developed by private organizations to compete with ONC's certification process, in fact such an outcome is likely. It seems likely that ONC's standards – even without any real regulatory authority – will be adopted for certification because of its expertise in developing national standards for EHR certification. *See, e.g.*, Standards, Implementation Specifications, and Certification Criteria for Electronic Health Record Technology, 2014 Edition, 77 Fed. Reg. 54,163 (Sept. 4, 2012).

[251] ONC has no real enforcement authority over the certification of mHealth applications unless they are considered EHR modules for purposes of MU, in which case providers will seek to use ONC certified devices in order to receive MU payments. *See supra* Part III.B (discussing the regulatory efforts in regards to privacy, security, and interoperability).

[252] ONC released a certification mark to help consumers identify health IT devices certified under ONC's certification program. This certification mark assures consumers that these devices can achieve "interoperability, functionality and security." *See* Press Release, U.S. Dep't of Health and Human Servs., New Certified Health IT Mark Announced (July 10, 2013), *available at* http://www.hhs.gov/news/press/2013pres/07/20130710b.html.

[253] JOSEPH V. REES, REFORMING THE WORKPLACE: A STUDY OF SELF-REGULATION IN OCCUPATIONAL SAFETY 11 (1988) ("[There are] two basic approaches to mandated partial self-regulation: public enforcement of privately written rules, and governmentally monitored internal enforcement of publicly written rules.").

Furthermore, mHealth applications that utilize ONC-developed standards would likely be interoperable with EHR technology that is also certified by ONC. Most application malfunctions under this system would likely not physically harm patients, but instead be related to privacy, security, and interoperability. These concerns are less of a problem because – at least as far as developers that fall under FTC's definition of a covered entity – developers will be incentivized to protect patient data from security breaches, for fear of being fined by FTC, and consumers will be incentivized to purchase applications bearing ONC's certification label for purposes of interoperability. The market is capable of managing these concerns.

The main benefit of the meta-regulation system is that it allows for private regulation that is responsive to the market and quicker than conventional regulation. Meta-regulation could also be considered as safe as conventional regulation if public agencies were authorized to act if a market failure lead to cases of patient harm associated with mHealth applications. FDA is well suited to this role because their safety and effectiveness approval process for devices has been in practice for years.[254] Although FDA only recently adopted a set of standards for certifying software as part of a medical device and is not as experienced in regulating this style of medical device,[255] its experience with hardware, effectiveness, and safety standards makes it a strong contender for regulating mHealth application software.

FDA's existing processes are notably slow and could severely hinder innovation in the field, as well as cost developers large amounts of money in the form of device user fees. FDA's slow approval process would hold back the fast-paced mobile application market. Furthermore, application developers often operate on low budgets with low profit margins. Applying FDA's device user fees to application developers could significantly restrict the market for mHealth applications that provide assistance to patients with severe medical conditions.[256]

Allowing a private regulator to assume the responsibilities for mHealth applications under FDA's supervision might ease the burden on both FDA and

[254] Some suggest that FDA's approval process needs further refining. *See, e.g.*, INST. OF MED., *supra* note 81, at 196-204 (recommending various modifications to FDA's device approval process, focusing on the 510(k) procedures).

[255] U.S. FDA, *supra* note 6, at 6-7 (outlining FDA's history of regulating devices but recognizing a gap in official software policy).

[256] *Compare* Scott Austin, *The Surprising Numbers Behind Apps*, WALL ST. J. (Mar. 11, 2013), http://blogs.wsj.com/digits/2013/03/11/the-surprising-numbers-behind-apps ("According to a survey of app developers . . . 34% of application developers made less than $15,000 in income . . . 65% make less than $35,000[,] [a]nd just 12% make more than $100,000."), *with* 77 Fed. Reg. 45,359, 45,360 (July 31, 2012) (establishing FDA device user fees for premarket applications at a standard fee of $248,000 ($62,000 for small businesses with gross receipts less than $100 million) and 510(k) approvals at a standard fee of $4960 ($2480 for small businesses)). A potential solution would be to apply a different device fee rate for application developers.

mobile application developers. The private regulators, or a single consortium regulator operating under FDA authority, would need to conduct their own postmarket surveillance for mHealth application safety and effectiveness. Any harm the devices cause could easily be attributed to any number of factors – such as an individual not taking proper care of himself or catching a transient illness. Without regulation it would be difficult to track data trends on mHealth applications and discover when the devices are indeed at fault. FDA's postmarket surveillance efforts are moving towards this capability, and may help inform private regulators of mHealth application postmarket issues.[257] In the event that an application is unsafe, the private regulator would need to inform FDA, so FDA can review the private regulator's rationale for removing the application from the market, and then FDA can remove the application if appropriate.

Both FDA's and ONC's meta-regulation systems would be mandated partial self-regulation and each agency would establish its respective requirements for regulating mHealth applications while the private regulators enforce those requirements on the agency's behalf.[258] "Conventional regulation's weaknesses stem from the demands that it places on regulators' capacities – and the costs and other negative consequences when those demands cannot be met."[259] By delegating these burdens to private regulators operating with revocable public authority, the agencies can remove some of the burden associated with mHealth applications while retaining the same regulatory standards for patient safety, clinical effectiveness and data standards for privacy, security, and interoperability.

Meta-regulation takes into account some of the best aspects of public and private regulation and forms a framework that meets a common ground in the interests of both patients and developers. Ultimately, meta-regulation can flexibly respond to market change on technical issues, such as the privacy, security, and interoperability standards, while also ensuring that the applications patients are using are safe and effective.[260]

CONCLUSION

MHealth applications have enormous potential for expanding access to health care services for the underserved and improving quality of care for patients with a wide variety of medical conditions. These applications come with substantial risk too, both to an individual's privacy and health. MHealth

[257] *See supra* notes 112-24 and accompanying text (discussing FDA postmarket surveillance systems).

[258] *See* Gunningham & Rees, *supra* note 219 and accompanying text.

[259] Coglianese & Mendelson, *supra* note 238, at 163.

[260] Some have proposed that industry-wide standards – guidance – as opposed to regulation may be all that is necessary to promote the use of data standards. *See* David Collins, *Industry-Wide Standards Can Influence Innovation*, MHIMSS (Mar. 26, 2013), http://www.mhimss.org/blog/industry-wide-standards-can-influence-innovation.

applications are particularly difficult to regulate because they intersect the jurisdiction and expertise of several agencies. Among private regulation, meta-regulation, and public regulation, the system that offers the most potential for protecting patients while also allowing necessary flexibility for innovation required by the industry is public regulation. Ultimately, even though FDA approval is slow, given a simple choice between no regulation and regulation, patient safety should triumph over innovation in an industry. Innovation may produce new, more clinically effective applications that can improve the health of patients, but the potential harm to innovation caused by FDA regulation is a necessary evil. The marginal benefit created by applications being quicker to market is not worth the potentially severe and irreparable harm caused to the health of patients by error-ridden applications. No patient should suffer harm simply to allow an industry to be free to react faster to market changes. It is unlikely anyone will perish because a more methodical and accountable regulatory system slows the pace of innovation for mHealth applications.

On the other hand, public regulation is less appropriate for privacy, security, and interoperability standards where the risk of patient harm is greatly reduced. While ONC has the expertise to create privacy, security, and interoperability standards, it lacks the authority, capacity, and experience to effectively regulate mHealth applications for privacy, security, and interoperability. Furthermore, regulation of privacy, security, and interoperability does very little to encourage appropriate use of the technologies. Only the individuals using applications can ensure they are used in a way that secures data or works with other devices. FDA has the authority to issue regulations requiring manufacturers to comply with these kinds of standards during the premarket approval process, but such an exercise of government power could prove onerous for developers to implement with little additional net benefit above what can be realized through a meta-regulation approach.

The cleanest solution would be for Congress to authorize ONC to regulate mHealth applications for privacy, security, and interoperability standards in a similar way to how FDA regulates medical devices for safety and effectiveness. Under that approach, ONC could remove applications from the market that did not meet ONC's standards. Given industry and potential consumer opposition to such a solution, however, a solution based on the meta-regulation and public regulation joint model proposed below may be more likely to garner the support necessary for implementation.

This Note proposes a solution that is a mix between public and meta-regulation. With regard to device safety and clinical effectiveness, mHealth applications should be regulated by FDA following a traditional regulatory construct linked to the level of risk associated with the device-application combination. This builds on FDA's vast experience regulating devices for safety and effectiveness and its existing procedures and postmarket surveillance systems. Despite the drawbacks associated with the pace of FDA's approval process, it is best positioned among the current pool of potential regulators to balance the pace of innovation with the need to keep patients safe

and to ensure that applications continue to be safe after they are on the market. On the other side of the equation, mHealth applications should be subject to a meta-regulation system for privacy, security, and interoperability standards, which are much less likely to affect patient health and safety. Such a system of regulation fits with ONC's existing regulatory structure for EHRs through ONC-authorized private regulators. Furthermore, even though ONC has no authority to mandate application developers' compliance with ONC's certification standards, the market will likely encourage developers to achieve ONC certification.

While this approach would require developers to go through both public and private regulatory bodies to assure their applications are ONC certified and FDA approved, the burden is offset by the fact that having both agencies regulate the areas of their expertise is likely more efficient than placing one agency in charge of all mHealth application concerns, irrespective of its capabilities. The proposed approach is also superior to an approach that would regulate only health and safety *or* privacy, security, and interoperability, as would be likely if mHealth applications were regulated under the auspices of only one agency. In such a case where only one agency has the authority to regulate mHealth applications, one area would be effectively regulated, but the other area would be ineffectively regulated depending on the expertise of the agency.

Ultimately, regulating mHealth applications is an interesting problem that likely will – and should – result in a mixture of meta-regulation for privacy, security, and interoperability standards coupled with public regulation to ensure the applications are safe and effective for patients.