The Future of mHealth: Responding to a Changing Regulatory Landscape

Frank Pasquale and Melissa Goldstein

This paper was commissioned as part of the American Association for the Advancement of Science (AAAS) mHealth and Law workshops, which are supported by a grant from the Robert Wood Johnson Foundation.

Views and opinions expressed herein belong solely to the authors.
The Future of mHealth: Responding to a Changing Regulatory Landscape

Frank Pasquale and Melissa Goldstein

June 2014

I. Introduction
II. Current Policy Approaches to mHealth
   A. Privacy
      i. HIPAA-covered Entities
      ii. Other Entities
   B. Producer Innovation

III. Emerging Issues
   A. Baseline Guarantees of Privacy and Reliability
   B. The Limits of Self-Help
   C. Use Restrictions
   D. User Innovation

IV. Conclusion
I. Introduction

This paper will serve as a brief introduction to policy issues emerging in mHealth. The future of the field is likely to be shaped by increasing concern about finding the proper balance between fair data practices and innovation. Within each of these normative areas, there will be tensions as well. For example, is privacy more about accuracy (on the model of the Fair Credit Reporting Act (FCRA)), obscurity, or rights to permanently delete aspects of one’s past?\(^1\) Should innovation policy primarily take a consumer-directed angle, or should medical professionals and public health experts contribute more to the conversation?

We believe that the present conversation on mHealth has been too narrow, focusing on consumer-facing devices for relatively non-acute health issues (like sleep and food-intake tracking). There are diverse applications of mHealth in the US: they include connectors (of patients and providers), replicators (of extant technology), automators and customizers, informers and educators, administrators, and loggers and trackers.\(^2\) The diversity of normative goals for mHealth technology, in addition to the diversity of mHealth technology itself, merits a more nuanced discussion in the future. This briefing first outlines the extant policy framework, then moves to consider the types of issues presently neglected by policymakers.

II. Current Policy Approaches to mHealth

Section 618 of the Food and Drug Administration Safety and Innovation Act (FDASIA) required that the Food and Drug Administration (FDA), in consultation with the Office of the National Coordinator for Health Information Technology (ONC) and the Federal Communications Commission (FCC), develop a report that contains recommendations on a regulatory framework for health information technology.\(^3\) Previous to this report, health IT policies in the area of mHealth reflected the guidance provided by FDA regarding the regulation of medical devices.\(^4\) The FDA’s minimalist approach has largely rested on the assumption that broad

---

\(^1\) On the right to delete, see VIKTOR MAYER-SCHÖNBERGER, DELETE: THE VIRTUE of FORGETTING IN THE Digital AGE (Princeton Univ. Press, 2009).

\(^2\) We borrow this typology from Nathan Cortez, The MHealth Revolution, 47 U.C. DAVIS L. REV. 1173 (2014).


\(^4\) The FDA, through the use of a risk classification system, established guidance that distinguished between the types of health IT and only applied to technology that could be considered medical devices whose functionality could pose a risk to a patient’s safety. U.S. Department of Health and Human Services, Food and Drug Administration, Mobile Medical Applications: Guidance for Industry and Food and Drug Administration Staff (2013), available at http://www.fda.gov/downloads/MedicalDevices/.../UCM263366.pdf.
regulation could increase the cost and time associated with getting technology to market. The FDA has chosen to only regulate those mobile health, or mHealth, apps that (1) qualify as a mobile medical app that are “medical devices” under 201(h) of the Federal Food, Drug, and Cosmetic Act and (2) pose the “same or similar potential risks to the public health as currently regulated devices if they fail to function as intended.”

If an mHealth app can be classified as a mobile medical app, the Food and Drug Administration (FDA) classifies it as a Class I (requiring general controls because of low risk), Class II (medium risk), or Class III (high risk, requiring premarket testing) medical device. As part of its assessment of medical devices, the FDA follows quality systems standards according to ISO 9001 and ISO 13485. The Federal Trade Commission (FTC) also regulates mHealth apps to ensure that the products are not falsely advertised and that they properly protect patient’s privacy. Even though it is predicted there will be over 500 million mHealth app downloads by 2015, that the market should increase annually by 25% for the foreseeable future, and there are over 13,000 mHealth apps on Apple, the FDA has only approved approximately 100 mHealth apps.

Thus mHealth policymakers are keeping track of several issues, and developers ignore them at their peril. Foremost are privacy and affirmative promotion of innovation.

---

7 U.S. Food & Drug Admin., Mobile Medical Applications, Guidance for Industry and Food and Drug Administration Staff (Sept. 25, 2013), available at http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM263366.pdf; FEDERAL FOOD, DRUG, AND COSMETIC ACT, Pub. L. No. 75-717, 52 Stat. 1040 (1938) (codified as amended at 21 U.S.C. § 301-99 (2012)) (defining device as “[...an instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, or other similar or related article, including any component, part, or accessory”, that is “intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease” or “[...intended to affect the structure or any function of the body”).
9 See id. at 38.
A. Privacy

There are many threats (both real and perceived) to personal information arising out of mHealth. With the passage of HITECH, Congress not only enhanced the privacy protections provided by the Health Insurance Portability and Accountability Act (HIPAA) by, for example, placing new limits on the sale of protected health information (PHI) but also created what is commonly referred to as the “meaningful use” program, whereby eligible providers can receive incentive payments for using electronic health records (EHR). In order to receive the incentive payments, providers must use EHRs in particular ways and must meet certain requirements, some of which also enhance privacy and security, such as the requirement to conduct a security risk analysis.

1. HIPAA-covered Entities

Providers, who qualify as HIPAA covered entities, must use certified technology that meets the criteria set by certification rules issued by ONC in order to achieve meaningful use. Under HITECH, ONC was charged with setting up a certification program to ensure that EHRs used by providers as part of the incentive program meet certain minimum requirements. These requirements also include a number of privacy and security specifications in addition to HIPAA’s requirements, for example the requirement to use authentication and access controls in order to be sure that individuals accessing health information electronically are who they claim to be.

2. Other Entities

There is growing activity at both the state and federal levels addressing the use of information technology in consumer products and services, including mobile health apps. The primary regulatory actors in this arena include the Federal Trade Commission (FTC), the FDA, the National Telecommunications and Information Administration (NTIA), the Federal Communications Commission (FCC), and some states. As noted in the recent White House Report on Big Data, the distinction between personal data and health care data is blurry, leading to regulation by different and sometimes conflicting federal and state law, including HIPAA, the Gramm-Leach-Bliley Act, and others.

Act, FCRA, and the Federal Trade Commission Act. Due to the complexity of complying with numerous laws when data is combined from various sources, the report suggests the potential need to carve out special data use authorities for the health care industry if it is to realize the potential health gains and cost reductions that could come from big data analytics.13

The various agencies involved have taken different approaches in the past few years as regulators have attempted to keep pace with rapid advances in technology. In general, however, these efforts have been guided by the Fair Information Practice Principles (FIPPS) and the Consumer Privacy Bill of Rights, with an emphasis on industry self-regulation and transparency. Key themes in agency approaches have emerged, such as enabling informed consumer choice through the provision of appropriate notice, expanding the definition of personally identifying information that should be protected, and focusing on the collection of consumer data by third parties, including the communication of such activity to consumers.

For purposes of this briefing, we will focus on the FTC, since it is exploring making policy on the data gathered by mHealth apps; Commissioners Brill and Ramirez have been thought leaders in the area.

Under Section 5 of the Federal Trade Commission Act, the FTC has the authority to prevent “unfair or deceptive” acts related to commercial activity. An act is considered “unfair” if it causes, or is likely to cause, substantial injury to a consumer that the consumer is not reasonably able to avoid, and which is not outweighed by benefits to the consumer. An act is considered “deceptive” if it involves a practice or representation that is likely to mislead a consumer acting reasonably and is also material to the consumer—that is, the practice or representation is likely to have kept the consumer from using the product had it not been misrepresented.

The HITECH Act requires the FTC to have a breach notification requirement rule as well.14 Entities not covered by HIPAA need to give notice to the FTC and to those whose personal health information was breached.

A notification titled “Privacy Policy” that does not actually protect privacy,

---

14 16 C.F.R. § 318.3.
could be a deceptive practice. Consumers should be able to rely on some basic protections. Failing that, unfairness authority may be relevant here. Inadequate security practices could be unfair to consumers because they expect their information to be adequately protected.

The FTC has also issued suggestions to rising app developers encouraging best practices. The document stresses that app developers need to be truthful in describing the capabilities of the app and disclosing key app information clearly and conspicuously. The document also encourages privacy by suggesting to app developers privacy by design, transparency regarding data practices, offering choices that are easy to find and use, protecting kids’ privacy, requiring consent to collect sensitive information, and establishing policies to keep user data secure.

---

15 Center for Democracy & Technology, Comments of the Center for Democracy & Technology to the office of the National Coordinator’s PHR Roundtable, Dec. 2, 2010, p. 12 (hereinafter CDT) (saying that “privacy policy” doesn’t necessarily mean that an entity will not collect and use private health information).
17 Solove explication of Wyndham decision. This needs some explanation. Many readers will not know Solove or Wyndham.
19 Id. (“Whether it’s what you say on a website, in an app store, or within the app itself, you have to tell the truth. False or misleading claims, as well as the omission of certain important information, can tick off users and land you in legal hot water.”)
20 Id. (“Generally, the law doesn’t dictate a specific font or type size, but the FTC has taken action against companies that have buried important terms and conditions in long licensing agreements, in dense blocks of legal mumbo jumbo, or behind vague hyperlinks.”)
21 Id. (“[Privacy by design means…] Incorporating privacy protections into your practices, limiting the information you collect, securely storing what you hold on to, and safely disposing of what you no longer need.”)
22 Id. (“Even if you need to collect or share data so your app can operate, be clear to users about your practices. Explain what information your app collects from users or their devices and what you do with their data.”)
23 Id. (“Give your users tools that offer choices in how to use your app – like privacy settings, opt-outs, or other ways for users to control how their personal information is collected and shared. ”)
24 Federal Trade Commission, Marketing Your Mobile App: Get It Right from the Start (2013), (“Chances are you make assurances to users about the security standards you apply or what you do with their personal information. At minimum, app developers — like all other marketers — have to live up to those promises. The FTC has taken action against dozens of companies that claimed to safeguard the privacy or security of users’ information, but didn’t live up to their promises in the day-to-day operation of their business. The FTC also has taken action against businesses that made broad statements about their privacy practices, but then failed to disclose the extent to which they collected or shared information with others – like advertisers or other app developers. What if you decide down the road to change your privacy practices? You’ll need to get users’ affirmative permission for material changes. Just editing the language in your privacy policy isn’t enough in those circumstances. ”)
25 Id. (“If your app is designed for children under 13 and collects personal information, you have additional requirements under the Children’s Online Privacy Protection Act (COPPA) and the FTC’s COPPA Rule… Under COPPA, you have to clearly explain your information practices, provide direct notice to parents about those practices, and get parental consent before collecting personal information from kids. These obligations apply to you when third parties (like ad networks or plug-ins) collect personal information through your app. COPPA also requires that you keep “personal information” collected from children confidential and secure. The rule defines that term to include a first and last name, an address, a telephone number, online contact information, a screen name or
B. Producer Innovation

The FDA and other agencies have released some preliminary guidance on mHealth, which present certain minimal guidance as to what mHealth firms should do to maintain safe, effective, and privacy-protecting apps. In addition, the FDASIA Health IT report outlines a risk based framework for health IT governance. The report highlights some general principles for future federal oversight of health IT including the need to promote innovation, protect patient safety, and avoid regulatory duplication. The report separates health IT functions into three categories: administrative, health management, and medical devices. It asserts that only medical device health IT functions should be the focus of FDA oversight because they generally pose greater risks to patient safety than the other two classifications; FDA oversight is better suited to provide assurance of safety and effectiveness for these functionalities.

That may well be true presently, but in the future many people may begin using mHealth apps as disintermediated health care providers. For instance, the ACA includes many “narrow network” and high deductible plans—so it’s possible that those buying insurance on the exchanges may choose a dermatology app to examine a potentially cancerous mole rather than waiting for (or paying a great deal for) an appointment with a dermatologist. The app marketplace could easily

---

26 Id. (“…it’s important to get users’ affirmative OK before you collect any sensitive data from them, like medical, financial, or precise geolocation information.”)

27 Id. (“Under the law, you… have to take reasonable steps to keep sensitive data secure. One way to make that task easier: If you don’t have a specific need for the information, don’t collect it in the first place. The wisest policy is to: collect only the data you need; secure the data you keep by taking reasonable precautions against well-known security risks; limit access to a need-to-know basis; and safely dispose of data you no longer need.”)

28 FDASIA Health IT Report, April, 2014, at 32 (“[I]n June 2012, the FCC worked with an independent mHealth83 Task Force, which collaborated on several policy recommendations to the FCC, other Federal agencies, and to industry, with the goal of making mHealth a routine medical best practice by 2017. To date, FCC has acted on nearly all of the mHealth Task Force’s recommendations including actions to increase interagency collaboration and information sharing, expand on existing programs to encourage mHealth adoption, and build on government and industry efforts to increase capacity, reliability, interoperability, and safety of mHealth technologies. The FCC has recently established a health subcommittee for its Consumer Advisory Committee (a federal advisory committee), chaired by the leaders of the mHealth Task Force and has held an mHealth Innovation Expo at its headquarters.”).


30 Food, Drug, and Cosmetic Act, 21 U.S.C. § 321(h) (2012) (”...an instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, or other similar or related article, including any component, part, or accessory”, that 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 “... intended to affect the structure or any function of the body of man or other animals.”)
become subject to a Gresham’s dynamic, where bad and cheap apps outcompete quality ones. Moreover, given that some US populations are categorically excluded from ACA protection (think, for instance, of undocumented immigrants), mHealth may take on a role for them that it appears to be assuming in poor, less developed countries. Stratification of health opportunities may pose extraordinary new challenges for policymakers.

Many members of the US Congress, however, are presently pressing for affirmative deregulation of this space. The ostensible rationale here is to encourage investment in the field by assuring entrepreneurs that law will not unduly interfere with their ability to turn a profit. But absent clear evidence that intervention will unduly distort or impede the market, some basic health policy standards should still inform policy here. The classic “triple aim” of increasing access, reducing cost, and improving quality should be the lodestar for policymakers in the mHealth space, as it is in the rest of health care.

III. Emerging Issues

A. Baseline Guarantees of Privacy and Reliability

A growing technical literature has pointed out the flaws in efforts to shift responsibility onto consumers to “control” their health data. As Narayanan et al. argue, “more control over personal data almost inevitably translates to more decisions, which leads to cognitive overload. . . . Since users lack expertise in software configuration, security vulnerabilities may result. A related point is that users may be unable to meaningfully verify privacy guarantees provided through cryptography.” Privacy policymakers need to invest in better governance structures here. Moreover, when medical devices have the potential to cause irremediable harm, tort and contract are not enough to appropriately deter defects. Regulation may be needed.

One model for assuring baseline levels of quality in mHealth may be the strategy pursued under HITECH (and implemented by ONC) to deputize certifications to third parties called Authorized Testing and Certification Bodies (ATCBs). The FDASIA report specifically addresses the importance of accreditation to improve

---

health of patients through HIT. If the ATCBs adopted a rating system, medical providers could also more easily determine which mHealth app to purchase, especially if the ratings included different specialized uses.

B. The Limits of Self-Help

We should also note that “control solutions” may require significant alteration of the ways in which data collectors maintain their databases. We can only solve problems like “runaway data” for medical reputations if data controllers are required to attach an identifiable symbol (such as “+H+” for health) into metadata for observations recording or predicting health information. That would allow the data controllers to filter out health information in reports and calculations performed in response to sensitive queries in the employment and insurance contexts. In other words, we need to develop a basic infrastructure of annotation and filtering before we can begin to do the monitoring necessary to prevent many forms of data misuse.

The applicability of HIPAA and HITECH to mHealth depends as a first matter on whether the mHealth app is created by a HIPAA-covered entity, or is part of the non-covered sphere, delegated in the case of personal health records to the FTC for supervision. However, as the recent White House Report on Big Data notes, the privacy frameworks that currently cover health information may not be well suited to address developments in predictive medicine or genomics or facilitate the research that drives them. As a result, some health care leaders have voiced the need for a broader trust framework to grant all health information, regardless of its source, some level of privacy protection. Such a framework may need to focus more on the use, rather than the collection and analysis, of data.

---

34 U.S. Food & Drug Admin., et. al. FDASIA Health IT Report: Proposed Strategy and Recommendations for a Risk-Based Framework (April 2014),16, 21-22 (reasoning that accreditation can be applied to health IT in a “risk-based manner to distinguish high quality products, developers, vendors and organizations from those that fail to meet a specified level of quality, safety, or performance”)


36 Perhaps E-discovery and deduplication software may be tweaked to remove health data without the need of annotation. Computer science researchers are already investigating similar projects, such as removing social security numbers and certain names from court records due to be digitized and made available online. But I believe such innovation could be a long time in coming.

37 Covered entities mean health plans, health care clearinghouses, and health care providers who transmit electronic health information. 45 C.F.R. § 160.103.

C. Use Restrictions

As Nicolas Terry has shown, a threat scenario not adequately covered in the extant literature is the rise of data brokers outside the HIPAA-protected zone who can project health reputations onto identifiable individuals, even without access to records from entities covered by HIPAA. 39 Scott Peppet has further confirmed that many Internet of Things companies have not implemented even basic “privacy by design” principles.40

Given documented problems with current consumer-focused privacy laws, we need to go beyond “notice and consent” models. Rather than “empowering” consumers to block certain collection or analysis of data, policymakers need to focus on prohibiting the use of certain types of data in certain situations. In employment or basic banking services, for instance, health data should not even enter the calculus of decision. If society committed to this model, individuals wouldn’t fear mentioning that they had cancer on Facebook, or worry that a condition mentioned on PatientsLikeMe might somehow lead to a higher interest rate.

“De-regulationists” will characterize such rules as an assault on knowledge itself and burdensome regulation. But if the Internet can “route around” damage, it can route around the putative distortions of regulation, too. Moreover, some argue that regulation is a required facilitator for industry change.41 Specifically, proponents of health IT regulation argue that, instead of hindering growth, providing a regulatory structure helps to establish an infrastructure that encourages interoperability.42 In addition, regulations can support the consistent evolution of existing markets instead of allowing disruptive new markets to displace older technologies.43

Health-inflected information from entities not covered under HIPAA can be a critical source of correlations, profiles, and attributions. They have already started to enter into the world of credit cards. Lenders are moving beyond credit

42 Id.
43 Id.
scoring to “credit analytics,” which tracks a consumer’s every transaction. As FTC Commissioner Julie Brill noted, a major retailer like Target can “know” a customer is pregnant before even other family members do, simply by crunching the numbers on a sufficiently large data set of purchases and doing pattern recognition. Not surprisingly, some customers have found it creepy to start receiving pregnancy-related ads simply on the basis of big data analysis of their purchases of large bags, bright blue rugs, and zinc supplements. Do individuals have similar aversions to collection, aggregation, or use of mHealth-related data? Initial research indicates concerns here.

Target responded, not by explaining to customers how it came to its conclusions, but by mixing more non-pregnancy-related ads into the circulars targeting expectant mothers. Target also does not appear particularly adept at protecting its data trove: in 2013, hackers stole “mailing and email addresses, phone numbers or names, [and] the kind of data routinely collected from customers during interactions like shopping online.” We do not know how that information will circulate. That emerging threat scenario is one key reason for requiring all data brokers, and those using their services, to document exactly where they get (and where they send) their data. Otherwise, data from breaches could easily be laundered.

Credit card companies have not ignored the lesson; indeed, they may have pioneered it. As the New York Times reported, some “companies started cutting cardholders’ credit lines when charges appeared for . . . marriage therapy because data indicated [it was a sign] of desperation or depression that might lead to job loss.” What about people who pay cash for such counseling (a right guaranteed by HITECH, if inadequately implemented)? Data broker Acxiom appears to be using proxy data for health status when it markets “intimate details like whether a person is a ‘potential inheritor’ or an ‘adult with senior parent,’ or whether a

---

45 Heather Patterson, Fellow, Information Law Institute, Department of Media, Culture and Communications, New York University, http://law.fordham.edu/center-on-law-and-information-policy/32700.htm.
D. User Innovation

We increasingly find ourselves needing to consider knowledge systems, ecologies built over time and space, rather than the efficiency or fairness of single transactions in the knowledge economy. Apps may now thrive on the basis of a dyadic trade of 99 cents and vast information collection for access. However, if invasive profiling develops (along with manipulative tactics to gain more revenue), individuals may start withdrawing from app marketplaces. Far from menacing app providers, the FTC’s nudges of mobile apps toward fair data practices are a way of preserving a “grand bargain” among all participants to preserve cooperative and mutually beneficial relationships that market exchange ideally presupposes. That common set of standards and commitments is the foundation for mutually advantageous contracts between consumers, producers, and the “prosumers” whose data is increasingly valuable to innovators. Policymakers need to consider how rules and incentives can encourage the growth of user communities who can build on and adapt apps.

IV. Conclusion

Carnegie Mellon professor Jesse Schell gave the following example at a Silicon Valley confab, explaining the fun and games possible in a pervasively monitored world of mHealth:

Well, I think it'll be like this: You get up in the morning to brush your teeth and the

---


51 Neil M. Richards & Jonathan H. King, *Three Paradoxes of Big Data*, 66 Stan. L. Rev. Online 41, 42 (2013) (“While big data pervasively collects all manner of private information, the operations of big data itself are almost entirely shrouded in legal and commercial secrecy. We call this the Transparency Paradox.”).

52 Christian Fuchs, *Class and Exploitation on the Internet*, in *Digital Labor: The Internet as Playground and Factory* 211, 217 (Trebor Scholz ed., 2013) (quoting Alvin Toffler, *The Third Wave* 267 (1980) (defining the notion of a “prosumer” as the “progressive blurring of the line that separates producer from consumer”)).
toothbrush can sense that you’re brushing your teeth, and so, hey, good job for you! Ten points for brushing your teeth. And it can measure how long, and you’re supposed to brush ‘em for three minutes, and you did. And so you get a bonus for that. Hey, you brushed your teeth every day this week, another bonus. All right, and who cares? The toothpaste company, the toothbrush company; the more you brush, the more toothpaste you use. They have a vested financial interest.53

So too do corporate leaders in charge of wellness programs. Employers will want to know if workers are getting regular exercise, eating well, and flossing, and can discount up to 30% of health insurance premiums for well-behaved health maximizers. Beyond employers, however, are the wellness program data vendors, who might act in similar ways to the data brokers studied by the FTC. How long such vendors may contractually keep employees’ wellness data and what analytics they are allowed to perform for what (and whose) purposes, are questions that we cannot answer.

Policymakers need to go beyond vague notions of “privacy” or “innovation” to address broader social consequences of such health information collection, aggregation, and use. We must resist solutionism: an orientation to problems that tends to “reach[] for the answer before the questions have been fully asked.”54 Is the goal really technologically and legally enabling fine-grained data control, or do we need to address something deeper in the way our society distributes rewards and opportunities based on (factors related to) health status?

Health data solutionism tends to prioritize issues that widely accessible technology can address: small, algorithmically decomposable bits of wicked problems. It will continue to employ a small army of lawyers and computer scientists (who will, not coincidentally, be poised to take advantage of “Control Solutions” far more effectively than the rest of the population). We must be willing to delve far deeper into actual business and employment practices with substantive, verifiable, auditable standards of nondiscrimination. Our present “health information games” focus on optimal mixes of self-disclosure and concealment. Rather than helping individuals play those games better, we should focus our energies on creating a society where their stakes are radically reduced, or, ideally, they do not have to play at all.

54 EVGENY MOROZOV, TO SAVE EVERYTHING, CLICK HERE: THE FOLLY OF TECHNOLOGICAL SOLUTIONISM: 6 (2013) (internal marks omitted).