HEALTHCARE BEGINS A MOBILE REVOLUTION

Michelle M. Ovanesian*

CITE AS: 1 GEO. L. TECH. REV. 170 (2016)
https://perma.cc/B3SU-Z59S

Healthcare is in the midst of a mobile revolution, and it will only be a matter of time before mobile healthcare applications ("apps") change how we deliver, consume, measure, and pay for healthcare.[1] The rapid pace of innovation and broad applicability of mobile healthcare applications have fueled this revolution. The healthcare mobile app market, currently estimated to be worth $4 billion, is expected to increase to $26 billion by 2017.[2]

In doctors' offices and hospitals, smartphones already are replacing stethoscopes and pagers as the most widely-used physician accessory.[3] Some federal agencies even have entire programs focused on the development and promotion of medical apps.[4] For example, the U.S. Department of Defense established a National Center for Telehealth and Technology evaluates mental health technologies for military personnel.[5] The program includes various smartphone apps, such as one that helps physicians diagnose and treat traumatic brain injuries and mental disorders by enabling users to track their emotional experiences over a certain period of time.[6] Ranging from the automation of simple tasks for healthcare providers to patient-specific analysis and diagnosis

* GLTR Staff Member; Georgetown Law, J.D. expected 2017; Georgetown University, M.S. (2013); University of California, Berkeley (2011).

[1] Nathan Cortez, *The Mobile Health Revolution?*, 47 U.C. DAVIS L. REV. 1173, 1190 (2014).

[2] Elizabeth A. Brown, *The Fitbit Fault Line: Two Proposals To Protect Health and Fitness Data At Work*, 16 YALE J. HEALTH POL'Y, L. & ETHICS 1, 9 (2016).

[3] Cortez, *supra* note 1, at 1177.

[4] *Id*. at 1214.

[5] *Id*. at 1215.

[6] *See id*.; *see also Smartphone Resiliency Apps*, U.S. ARMY (Feb. 28, 2013), https://www.army.mil/article/97390.

for consumers, mobile healthcare apps present numerous potential benefits and risks to consumers.[78]

Potential benefits include the reduction of medical errors, improvement of quality care, and prevention of more serious episodes of illness.[9] Mobile healthcare apps may also benefit consumers by shifting the locus of effective care away from medical facilities and professionals and toward digitally-empowered patients.[10] However, potential risks may outweigh the benefits and are greater for the poor, uninsured, and underinsured who may use an app lacking in clinical evidence for self-diagnosis and treatment rather than pay for a doctor's visit. The risks can range from relatively benign, such as an app claiming to relieve tooth pain that is actually clinically ineffective, to severe, such as an app storing personal health information that is hacked.

Today, a muddled assortment of different agencies—including the Food and Drug Administration (FDA), the Federal Trade Commission (FTC), and the Federal Communications Commission (FCC)—and regulations are involved in regulating the potential risks that mobile healthcare apps pose.[11] Unfortunately,

---

[7] *See, e.g.*, K Royal & Gretchen A. Johnson, *Cybersecurity And Medical Devices: Reality Bytes*, 32 NO. 8 ACC DOCKET 66, 80 (2014). ("The US Center for Disease Control has a vaccine application (CDC Vaccine Schedules 4) that helps medical professionals determine immunization schedules for their patients. On the other side, for parents or patients, the Children's Hospital of Philadelphia has launched Vaccines on the Go, which appears to be more informational than a tracking tool. However, VaxNation (created by a team of Baylor College of Medicine, University of Texas School of Public Health and Rice University students) is an online vaccination tracker. Once you enter your vaccination history and date of birth, you will see the age appropriate recommendations based on the Centers for Disease Control and Prevention's guidelines. Families can create an account, link to social media accounts and receive reminders.").

[8] Cortez, *supra* note 1, at 1182-83. ("For example, applications now enable clinicians to use their smartphones to view and manipulate medical images, analyze electroencephalograms ("EEGs") or electrocardiograms ("ECGs"), connect to bedside monitors, screen blood samples, or act as wireless remote controls for medical devices. In this latter category, several applications allow users to control FDA-regulated devices. Examples include apps that allow users to inflate and deflate blood pressure cuffs, perform portable ultrasounds, operate insulin pumps, and visually track whether wounds heal or regress. Other apps also display, analyze, or transmit patient data from an FDA-regulated device. For example, one app allows clinicians to use their phones to track patients' vital signs remotely, pulling data "from hundreds of different types of patient monitors." A related app allows obstetricians to monitor patients' contractions, fetal heartbeats, and other realtime waveform data. Yet another allows cardiologists to review and manipulate ECG results and histories.").

[9] Cortez, *supra* note 1, at 1177; Jamie Lynn Flaherty, *Digital Diagnosis: Privacy and The Regulation Of Mobile Phone Health Applications*, 40 AM. J.L. & MED. 416, 436 (2014).

[10] Cortez, *supra* note 1, at 1177.

[11] Flaherty, *supra* note 9, at 436; Cortez, *supra* note 1, at 1179.

most agencies "have adopted a posture of facilitating rather than regulating mobile health."[12]

For example, the FDA recently issued a non-binding guidance document delineating the types of apps that it will and will not regulate.[13] In the guidance document, the FDA clarifies that it will regulate those apps that meet the statutory definition of "device."[14] The term "device" means "an instrument, apparatus, implement, machine, contrivance, implant…..which is….intended to affect the structure or any function of the body of man or other animals."[15]

While some apps clearly do or do not meet the definition of "device," most apps lie in a "gray" area where FDA regulation is uncertain.[16] Thus, apps like Apple's Health App, which allows users to store and track all of their fitness and health data and even asks for information about sexual history and partners, fall into the "gray" area of unregulated apps.

Despite the scores of federal agencies and regulations overseeing mobile healthcare apps, no current law or regulation clearly protects the health data that apps might collect, and there are few restrictions on app developers as to the type of data they can collect and how they can monetize the data collected.[17]

For example, the FCC has the authority to enforce consumer information privacy provisions and establish regulations on consumer proprietary network information ("CPNI") or "information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a

---

[12] Cortez, *supra* note 1, at 1211.
[13] *Id*. at 1203-04.
[14] *Id*.
[15] Cortez, *supra* note 1, at 1209-12; J. Wasserman and LaToya C. Sutton, *What's in This Stuff? An Update on FDA's Policies and Enforcement Actions Concerning Novel Ingredients in Food and Dietary Supplements*, FOOD SAFETY MAG. (June 12, 2016), http://www.foodsafetymagazine.com/magazine-archive1/junejuly2016/whate28099s-in-this-stuff-an-update-on-fdae28099s-policies-and-enforcement-actions-concerning-novel-ingredients-in-food-and-dietary-supplements/.
[16] Cortez, *supra* note 1, at 1209-12.
[17] Brown, *supra* note 2, at 24, 34; Flaherty, *supra* note 8, at 424. Some healthcare apps may fall under the Health Insurance Portability and Accountability Act. "To fall under HIPAA's scope, "protected health information" (PHI) must be communicated between covered entities, including "business associates." PHI includes individually identifiable health information, meaning information collected from an individual that either "identifies the individual" or reasonably "can be used to identify the individual." "Covered entities" include health plans, healthcare clearinghouses, and healthcare providers who transmit health information in electronic form. If an entity does not meet the definition of a covered entity or business associate, or does not transmit PHI, it need not comply with HIPAA's requirements."

telecommunications carrier."[18] Although the CPNI regulations seem to protect location information and to prevent telecommunications companies from marketing user information, they to do not apply to third party app developers and "there are no clear rules for the disclosure of this data and often no way for consumers to control the data they reveal" when a consumer uses an app that is separate from the telecommunications carrier.[19]

In addition to a lack of protective federal laws and regulations, many mobile healthcare apps lack transparent privacy policies, and it is unclear whether a consumer will be able to sue a developer for a privacy violation.[20]

As of now, a malicious acquaintance or employer may be able to legally use and indefinitely store, without your consent, the personal health information stored in an app in your phone.[21][22][23]

Smartphones are only becoming more and more commonplace, and the FDA estimates that 500 million smartphone users now use or will soon use at least one health care app.[24] The development of healthcare apps is progressing exponentially, but privacy regulations in this field have been left behind. A robust dialogue about privacy and mobile healthcare apps among universities, civic organizations, and citizens is needed. Additionally, federal interagency

---

[18] Flaherty, *supra* note 8, at 434-35.

[19] *Id.*

[20] Flaherty, *supra* note 8, at 437; Brown *supra* note 2, at 36. "If an app developer were to violate these terms, however, it is not clear that the consumer whose data were sold would have a right of action against either Apple or the developer. Consumers may be incidental beneficiaries of these terms, but it is unlikely that a court would find that they had standing to sue either a developer for failing to follow them or Apple for failing to insist on them."

[21] Brown, *supra* note 2, at 34. "The potential profit from collecting, analyzing, repackaging, and selling health-related data to employers and/or marketers is barely limited by law. As it stands, app and device makers can now access a wide range of users' health-related data without those users' consent."

[22] Flaherty, *supra* note 8, at 437. Analogizing to Fourth Amendment doctrine, one could cogently argue that people do not have a reasonable expectation of privacy if they voluntarily choose to input private, personal information on the Internet or on a smartphone. As the Supreme Court stated in *Katz v. United States*, "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection." Thus there are reduced privacy protections when people input information into apps because they are essentially putting that information out into the public."

[23] *See also Smith v. Maryland*, 442 U.S. 735 (1979). "The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government. . . . This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed."

[24] Brown, *supra* note 2, at 9.

cooperation is necessary in order to provide consistent and meaningful regulatory oversight. Finally, at a minimum, app developers should be required to create accessible privacy policies, obtain informed consent to use consumers' information, and inform users of holes and breaches in app cybersecurity.