CHEST™

Mobile Health
Assessing the Barriers

Nicolas P. Terry, LLM

Mobile health (mHealth) combines the decentralization of health care with patient centeredness. Mature mHealth applications (apps) and services could provide actionable information, coaching, or alerts at a fraction of the cost of conventional health care. Different categories of apps attract diverse safety and privacy regulation. It is too early to tell whether these apps can overcome questions about their use cases, business models, and regulation.

CHEST 2015; 147(5):1429-1434

ABBREVIATIONS: app = application; EMR = electronic medical record; FDA = US Food and Drug Administration; FTC = Federal Trade Commission; HIPAA = Health Insurance Portability and Accountability Act; mHealth = mobile health; PHR = personal health record

Mobile health (mHealth) promises to be a major force in US health care. Investments in mHealth companies and announcements or rumors of new products from market-leading technology companies continually raise expectations that health care will experience disruption as so many other brick-and-mortar industries have.

In 2013, 95 million Americans used their phones to access health information or use mHealth applications (apps), up 27% from 2012.[1] The US market for mHealth is estimated to reach $6.7 billion in 2014[2] and $49.1 billion in the global market by 2020.[3] As a product category, wearable technologies are expected to grow exponentially from 9.7 million units in 2013 to 135 million in 2018.[4] Not surprisingly, mHealth and wearable technologies businesses are attracting considerable amounts of venture capital interest,[5,6] with funding in the United States expected to grow from $3.5 billion to $6.5 billion from 2014 to the end of 2017.[7]

The mHealth ideal is very attractive. mHealth promises more personalized, timely interactions with patients. Patients may take more responsibility for their fitness and wellness and become more engaged in their health care. More health care will be delivered away from often inconvenient, centralized locations, and the sophisticated, yet friendly interfaces of mHealth apps should shame traditional health care into improving its processes. There is also some evidence that mHealth may reduce health disparities (or at least not worsen them) due to relative parity in smartphone ownership across black, Latino, and white populations,[8,9] although concerns about the role of socioeconomic status persist.[10,11]

Manuscript received October 3, 2014; revision accepted November 4, 2011.

AFFILIATIONS: From the Indiana University Robert H. McKinney School of Law, Indianapolis, IN.

CORRESPONDENCE TO: Nicolas P. Terry, LLM, Hall Center for Law and Health, Indiana University Robert H. McKinney School of Law, 530 W New York St, Indianapolis, IN 46202; e-mail: npterry@iupui.edu

DOI: 10.1378/chest.14-2459

However, any suggestion that mHealth will quickly disrupt traditional health care is naive. Although health care is overdue for a radical rethink, maybe even disruption,[12] mHealth itself faces considerable challenges. This article explains the mHealth landscape and identifies five categories of mHealth apps and discusses their use cases, likely regulation, and some of the financing hurdles they face.

The mHealth Landscape

The concept of digital health has been an increasing trend in health care from traditional health information technologies, such as electronic medical records (EMRs) and telemedicine, to more modern health-care innovations, such as social media interactions. Physicians have long used mobile devices to subscribe to drug interaction applications, and today, they are frequently granted EMR or computerized provider order entry mobile access. Some are even experimenting with innovative wearable technologies such as Google Glass. mHealth is a subset of digital health; its defining characteristic is that it is patient facing. That is, unlike most examples of digital health, patients interact directly with mHealth hardware and software, frequently without the direct involvement of conventional health-care providers.

Typically, mHealth is built on two core components: (1) a platform's hardware and operating system (eg, that found in a modern phone) and (2) the apps that provide fitness, wellness, or any number of other health-related services. In 2014, the number of mHealth apps available for the Apple iOS (Apple Inc) and Android (Google) platforms exceeded 100,000 (having doubled in 2.5 years).[13] Increasingly, the platform-app distinction will blur as platforms are equipped with aggregator apps, such as Apple Health, that pull together data from phone sensor arrays, external biosensors, and other apps.

Two additional technologies feature in the present imagining of mHealth. The first is cloud computing. Mobile apps frequently will store mHealth data in the cloud, and cloud services increasingly will provide the data analytics back end for processing those data. The second is wearables. Currently, fitness bands and exercise monitoring apps dominate this category. They will be joined by more sophisticated biosensors, some of which will be included in watch-like devices.[14] Many phones are equipped with internal sensors, such as microphones, proximity sensors, accelerometers, ambient light sensors, barometers, and gyroscopes. Such phones are not only platforms but also, in a sense, wearables. In 2015, Apple will launch a new category of wearables called Watch that is equipped with several biosensors.[15] Unlike most wearables, Watch is relatively autonomous and itself a platform that app developers will be able to build out.

Careful attention to legal and, particularly, regulatory issues is recommended because of the complex interaction of state and federal law and the multiplicity of regulatory stakeholders. For example, although US Food and Drug Administration (FDA) regulation covers mHealth manufacturers but not health-care providers, health privacy regulation typically follows an opposite course, applying to health-care insiders but not those who provide mHealth apps and services. Currently, there are five core types of mHealth apps, a taxonomy that is loosely based on the patient-facing categories of mobile apps first published by the FDA in 2013[16]: (1) apps providing access to health records, (2) consumer versions of existing medical devices, (3) condition monitoring and management apps, (4) fitness trackers and wellness coaches, and (5) diagnosis or treatment apps.

Apps Providing Access to Health Records

Providers and health insurers increasingly have been giving patients access to their health records through, for example, web portals such as MyChart (Johns Hopkins Medicine). Many of those initiatives will migrate to apps. For example, health-care providers such as the Mayo Clinic and EMR developers such as Epic Systems Corporation are enabling patients to access their health records through Apple Health.[17]

In 2013, the FDA issued a nonbinding guidance detailing its current regulatory stance on mHealth apps, limiting its scrutiny to "only those mobile apps that are medical devices and whose functionality could pose a risk to a patient's safety if the mobile app were to not function as intended."[16] The FDA has indicated that apps that enable patient interaction with records will not face device regulation at this time.

In contrast, most records-accessing apps will be subject to health privacy regulation. The records are likely held by Health Insurance Portability and Accountability Act (HIPAA)-covered entities such as hospitals, physicians, and health insurers. App developers will be considered business associates.[18] In such cases, HIPAA's Privacy, Security, and Notification of Breach rules should be applicable. A more nuanced question arises regarding a health data aggregator app such as Apple Health: HIPAA may not apply if data are only stored on the device and the aggregator acts simply as a traffic cop directing the locally stored data to an authorized HIPAA-compliant app.[19]

Some apps will enable patients to curate their own health-care information in personal health records (PHRs). Recently, the market for PHRs has been dormant. However, the increase in mHealth platforms may lead to an increase in their popularity, particularly as programs such as Medicare's Blue Button facilitate records downloads.[20] PHRs are not subject to the full rigor of HIPAA privacy and security. However, the Federal Trade Commission (FTC) enforces a breach notification rule that applies to PHR vendors that are not covered entities.[21]

Consumer Versions of Existing Medical Devices

For several years, patients have been able to purchase phone-based consumer versions of some medical devices. For example, several businesses sell sphygmomanometer, glucometer, or spirometer accessories. Patients connect the hardware to their phone, and mHealth apps display and analyze the data.

The FDA guidance views these as substitutes for existing medical devices and therefore subject to formal device regulation. This is the case whether the app relies on a hardware accessory or smartphone internal sensors. In most cases, the hardware and apps will require only a 510(k), a premarket submission designed to establish the device's substantial equivalence to a legally marketed device.[22]

Although the safety of these apps will be scrutinized, the data they collect will be underprotected. Whether the data are stored locally on the device or on cloud services, they are unlikely to be subject to HIPAA privacy, security, or breach notification, although a few state health privacy statutes could apply.[23]

As with the other types of apps discussed next, other, less rigorous data protection may apply. For example, the FTC is more aggressively policing the health data space[24] and is paying particular attention to businesses that deviate from stated privacy policies.[25] Of course, such a regulatory model is less than effective if a business provides no privacy policy or only a weak one. Increasingly, therefore, meaningful privacy protection may depend on whether app stores will require developers to safeguard data privacy. For example, Apple Inc requires that apps using the Apple Health framework must provide a privacy policy and "may not use user data gathered from the HealthKit API [application program interface] for advertising or other use-based data mining purposes."[26] Although the HIPAA security rule will seldom be applicable, the FDA has issued a guidance requiring manufacturers to "develop a set of cybersecurity controls to assure medical device cybersecurity and maintain medical device functionality and safety."[27]

Condition Monitoring and Management Apps

These apps provide care that supplements conventional health care. Some simply monitor the patient's condition and record data. Others go farther and coach or prompt patients regarding compliance with healthy behaviors or medications. As Asch and colleagues[28] noted that

> patients with chronic illness might spend only a few hours a year with a doctor or nurse, but they spend 5000 waking hours each year engaged in everything else—including deciding whether to take prescribed medications or follow other medical advice, deciding what to eat and drink and whether to smoke, and making other choices about activities that can profoundly affect their health.

Early examples of such apps assist with the management of chronic conditions such as COPD, diabetes, or hypertension.[29] Some target particular cohorts such as children with diabetes, aiming to make tedious condition management more of a game. Studies suggest that monitoring and management apps will show some of the strongest market growth through the end of the decade.[3] One device recently approved by the FDA uses a wearable connected to an external device that monitors a patient with diabetes and then shares that data with chosen caregivers or family members.[30]

The FDA considers "apps that provide or facilitate supplemental clinical care, by coaching or prompting" or that "help patients document, show, or communicate to providers" as low risk and will not enforce traditional medical device regulation. Although this position is likely accurate at the present, some communication apps may start to blend in some of the diagnosis or treatment functionality seen in apps that, as discussed next, are already attracting device regulation. For example, a biosensor could monitor for heart rate variability against a baseline set by a physician and use a mobile app to both send an alarm and open a video communication chat between the patient and physician.[31] Use of such advanced capabilities would require a preexisting physician-patient relationship and adequate informed consent.

Other species of legal exposure may depend on how the patient comes to use monitoring and similar apps. For example, some large or highly specialized providers (or their business associates) might have developed the app in question. If so, patient data created or stored by the app likely would be protected by HIPAA.

In contrast, if the app was developed independently but a physician either recommended the app or endorsed the patient's choice, HIPAA is unlikely to apply (although, as already discussed, the FTC might be able to leverage an app developer's privacy policy). However, such recommendation or endorsement by a physician should concern privacy officers and other risk managers at health-care institutions because of potential liability exposure if, for example, the app leaked patient information or provided the patient injury-causing advice.

Fitness Trackers and Wellness Coaches

Fitness wristbands and their individual tracker apps were the predecessors of emerging wellness and other mHealth applications. Trackers collect data from phone sensors, wearables, and biosensors and provide data and coaching as varied as steps taken or elapsed time between periods of standing rather than sitting. Regulations made under the Affordable Care Act permit employers to use nondiscriminatory wellness plans, including those with incentives or penalties to modify employee lifestyles.[32] One-half of US employers with ≥ 50 employees offer wellness programs, but available data do not support the requirement that such programs successfully lower health-care costs.[33-35] Eager to find programs that do work, employers are turning to trackers. One study estimates that 13 million fitness devices with embedded wireless connectivity will be used by employers over the next 5 years.[36]

The FDA considers these apps and their biosensors as low risk, and at present, it does not intend to regulate them as devices. Of course, some hardware may turn out to be flawed, opening up exposure to a regulatory action as exemplified by the recall of some fitness wristbands that caused rashes.[37] Accessories, wearables, and even apps that cause harm also may face state common law products liability actions or claims brought under state consumer protection statutes.

Data protection regulation is more problematic. Absent interaction with conventional providers, HIPAA regulation will be inapplicable. As already discussed, FTC regulation likely will turn on whether the app developer has a robust privacy policy (and that may turn on whether the relevant app store rules require one).

More generally (and this applies to most of the app categories discussed here), the barrier that the initial generations of mHealth must scale is a product of the very data the apps will access or create. This is already true of fitness and wellness apps and eventually will be an issue for the diagnostic apps discussed next. Biometric data will stream from numerous external biosensors, in addition to those already built into smartphones, into both silo and data-aggregating apps. Conventional health-care providers will provide still more data by providing access to patient records and care plans.

However, without context, data are not particularly useful, which is at least one of the reasons why we employ health-care professionals: to interpret medical data. For apps to generate useful information from collected data, they will need to establish useful baselines despite a broadly heterogeneous user base. The sheer quantity of data being collected by continually monitoring mHealth apps compounds the problem. Apps will need to deemphasize the trivial (eg, How many steps did I take today?) and sensitize users to critical information. This data-sorting-costs challenge has other characteristics. For example, mHealth apps will include alarms, and as physicians already know from their experience with clinical decision support systems, those may raise questions of alarm fatigue.[38]

Diagnosis or Treatment Apps

This final category of apps is the least developed but long term, may be the most interesting (and controversial). As already discussed, without context, data are not particularly useful, and a major challenge for mHealth is to produce usable information. Certainly, doubts exist about whether physicians will be willing consumers of yet another stream of biometric data, however proud their patients are of their daily step counts.[39] And, how useful will patients find their data? "Information is useful only if it's actionable,"[40] and that requires that the apps (or their cloud servers) process the data and provide a decision or recommend a course of action, functions that may expose app developers to physician pushback, regulation, or even liability.

The FDA has indicated that device regulation will apply to apps that perform patient-specific analysis and provide patient-specific diagnosis or treatment recommendations. Thus, mHealth apps that are ambitious (and possibly much more useful) or even potentially disruptive of conventional health-care delivery may face serious regulatory barriers. These barriers may start with FDA regulation, but looking ahead, mHealth app developers may even find themselves in conflict with state regulators who police the practice of medicine.[41] In contrast, these apps likely will operate outside the HIPAA-regulated domain and only occasionally will attract the attention of the FTC or state privacy regulators.

For developers of all types of mHealth apps, a major barrier to the creation of a sustainable business is regulatory indeterminacy. The FDA guidance on safety regulation has reduced that indeterminacy, although some commentators argue that far more regulatory specificity is necessary.[42] For responsible actors, there is far more uncertainty about which privacy laws apply or what regulatory agencies must be navigated. Bad actors will simply exploit regulatory gaps at the expense of patients.

Potential Business-Side Barriers for mHealth

Regulatory considerations aside, whether mHealth can become a sustainable business remains unclear. The conventional US health-care industry dwarfs its potential disruptors with an annual revenue of almost $1.7 trillion. In contrast, the current mobile handset business is worth approximately $60 billion, with mobile apps contributing another $25 billion. For some categories of apps and services, monetization is a relatively straightforward answer. For example, hospitals and their EMR vendors and health insurers usually provide free or inexpensive apps designed to increase satisfaction or convenience (and so customer loyalty) and, increasingly, to promote and execute wellness plans. Similarly, manufacturers of smartphone platforms will provide aggregator apps and continually improve internal sensors to promote platform loyalty and competitive customer experiences. Manufacturers of fitness bracelets, biosensors, or substitutes for traditional devices, such as BP cuffs, will offer free apps but can charge for the necessary hardware accessories.

Other categories of mHealth apps and services may find it harder to generate revenue. No current conventional health-care business model has similar properties. Indeed, the contrasts to the conventional business of health care are striking. Unlike mHealth, our health-care system is primarily reactive, and that is reflected in its financing system. Only with the Affordable Care Act have we begun the pivot from curing sickness to promoting wellness. Furthermore, most mHealth apps and services seek revenue directly from patients, eschewing the third-party reimbursement model that underpins conventional health care.

If mHealth apps are sold at commodity prices yet have to provide complex server-side or cloud services, the sustainability of patient-facing mHealth may be called into question. The alternative is the widely used "freemium" model. That model unlocks additional features following a user's in-app purchase.[43] However, selling health apps with deliberately disabled features until the payment of a premium seems regressive. The alternative freemium model is the subsequent removal of advertising. However, having advertising (much-criticized default approach of web services)[44] in mHealth apps in the first place would be controversial. Ads could be distracting and the privacy implications serious. At the very least, ad-supported mHealth apps should expect heightened scrutiny from app stores and the FTC.

Conclusions

The mHealth narrative combines the decentralization of health care with patient centeredness. Because it is patient facing, mHealth is consistent with contemporary calls to reform health care from a push model to one where patients pull only necessary resources.[45] Operationally, mHealth places "tools for monitoring health and medical diagnosis…increasingly…in the hands of consumers" together with "online services for them to report and analyze data."[46] Mature mHealth apps and services could provide actionable information, coaching, or alerts at a fraction of the cost of conventional health care. It is too early to tell whether they can overcome questions about their use cases, business models, and regulation. Fully realized, mHealth could deliver a compliant, better-informed, continually monitored, and self-regulating patient.

Acknowledgments

Financial/nonfinancial disclosures: The author has reported to *CHEST* the following conflicts: Mr Terry serves on the Consumer Workgroup of the Health IT Policy Committee (US Department of Health and Human Services). The views expressed here are his alone.

References

1. US mobile health audience jumps to 95 million adults – new research highlights mobile opportunities for pharma marketers. October 24, 2013. Manhattan Research website. http://manhattanresearch.com/News-and-Events/Press-Releases/mobile-health-95-million. Accessed December 23, 2014.
2. 'The mHealth market is still in its infancy, but mobile operators, software developers, data management providers, and indeed the majority of healthcare practitioners are preparing themselves for a tidal industry shift,' says latest Visiongain report. Visiongain website. https://www.visiongain.com/Press_Release/660/%E2%80%98The-mHealth-market-is-still-in-its-infancy-but-mobile-operators-software-developers-data-management-providers-and-indeed-the-majority-of-healthcare-practitioners-are-preparing-themselves-for-a-tidal-industry-shift-'-says-latest-Visiongain-report. Accessed December 23, 2014.
3. Grand View Research, Inc: global mHealth market expected to reach USD 49,119.2 million by 2020. March 2014. Grand View Research website. http://www.grandviewresearch.com/press-release/global-mHealth-market. Accessed December 23, 2014.
4. Smartwatches and smart bands dominate fast-growing wearables market. CCS Insight website. http://www.ccsinsight.com/press/company-news/1944-smartwatches-and-smart-bands-dominate-fast-growing-wearables-market. Accessed December 23, 2014.
5. Quittner J. Why the 'Internet of things' nabbed $1 billion in VC in 2013. March 20, 2014. Inc. website. http://www.inc.com/jeremy-quittner/

venture-capital-flows-to-gadget-and-hardware.html. Accessed December 23, 2014.

6. Miliard M. Health IT attracting huge investments. July 16, 2014. Healthcare IT News website. http://www.healthcareitnews.com/news/health-it-attracting-huge-investments. Accessed December 23, 2014.
7. Healthcare IT start-up funding fueling digital disruption. September 2014. Accenture website. http://www.accenture.com/us-en/Pages/insight-healthcare-it-start-up-funding-fueling-digital-disruption.aspx. Accessed December 23, 2014.
8. Lopez MH, Gonzalez-Barrera A, Patten E. Closing the digital divide: Latinos and technology adoption. March 7, 2013. PewResearch Hispanic Trends Project website. http://www.pewhispanic.org/2013/03/07/closing-the-digital-divide-latinos-and-technology-adoption. Accessed December 23, 2014.
9. Smith A. African Americans and technology use. January 6, 2014. PewResearch Internet Project website. http://www.pewinternet.org/2014/01/06/african-americans-and-technology-use. Accessed December 23, 2014.
10. Kontos E, Blake KD, Chou WYS, Prestin A. Predictors of eHealth usage: insights on the digital divide from the Health Information National Trends Survey 2012. *J Med Internet Res*. 2014;16(7):e172.
11. Viswanath K. An unhealthy digital divide. January 28, 2014. Harvard School of Public Health website. http://www.hsph.harvard.edu/news/features/unhealthy-digital-divide. Accessed December 23, 2014.
12. Terry N. Information technology's failure to disrupt healthcare. Social Science Research Network website. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2118653. Accessed December 23, 2014.
13. *mHealth App Developer Economics 2014*. May 6, 2014. research-2guidance website. http://research2guidance.com/r2g/mHealth-App-Developer-Economics-2014.pdf. Accessed December 23, 2014.
14. Basis website. http://www.mybasis.com. Accessed December 23, 2014.
15. Apple Watch website. http://www.apple.com/watch. Accessed December 23, 2014.
16. Mobile medical applications: guidance for industry and Food and Drug Administration staff. February 9, 2015. Food and Drug Administration website. http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM263366.pdf. Accessed December 23, 2014.
17. Comstock J. Apple reveals tracking app HealthKit and partners with Mayo Clinic, Epic. mobihealthnews website. http://mobihealthnews.com/33728/apple-reveals-tracking-app-healthkit-and-partners-with-mayo-clinic-epic. Accessed December 23, 2014.
18. Applicability. 45CFR §160.102.
19. Sullivan M. EHR giant Epic explains how it will bring Apple HealthKit data to doctors. September 17, 2014. VentureBeat website. http://venturebeat.com/2014/09/17/ehr-giant-epic-explains-how-it-will-bring-apple-healthkit-data-to-doctors. Accessed December 23, 2014.
20. Download claims with Medicare's Blue Button. Medicare.gov website. http://www.medicare.gov/manage-your-health/blue-button/medicare-blue-button.html. Accessed December 23, 2014.
21. Complying with the FTC's health breach notification rule. Bureau of Consumer Protection Business Center website. http://www.business.ftc.gov/documents/bus56-complying-ftcs-health-breach-notification-rule. Accessed December 23, 2014.
22. Premarket notification (510k). Food and Drug Administration website. http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/HowtoMarketYourDevice/PremarketSubmissions/PremarketNotification510k/default.htm. Accessed December 23, 2014.
23. Confidentiality of Medical Information Act. Cal Civ Code §56.06(b).
24. LabMD, Inc., in the matter of. Federal Trade Commission website. http://www.ftc.gov/enforcement/cases-proceedings/102-3099/labmd-inc-matter. Accessed December 23, 2014.
25. Enforcing privacy promises: making sure companies keep their privacy promises to consumers. Federal Trade Commission website. www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/enforcing-privacy-promises. Accessed December 23, 2014.
26. HealthKit. Apple App Store Review Guidelines website. https://developer.apple.com/app-store/review/guidelines/#healthkit. Accessed December 23, 2014.
27. Center for Devices and Radiological Health. *Content of Premarket Submissions for Management of Cybersecurity in Medical Devices: Guidance for Industry and Food and Drug Administration Staff*. Rockville, MD: Food and Drug Administration; 2014.
28. Asch DA, Muller RW, Volpp KG. Automated hovering in health care—watching over the 5000 hours. *N Engl J Med*. 2012;367(1):1-3.
29. Farr C. Exclusive: two Apple medical trials shed light on how HealthKit will work. September 15, 2014. Reuters website. http://www.reuters.com/article/2014/09/15/us-apple-health-idUSKBN0HA0Y720140915. Accessed December 23, 2014.
30. FDA approves Dexcom SHARE™, the first remote mobile communications device used for continuous glucose monitoring (CGM). October 20, 2014. Dexcom, Inc, website. http://www.dexcom.com/news/fda-approves-dexcom-share. Accessed December 23, 2014.
31. Introducing the HealthPatch® family of biosensors. Vital Connect website. http://www.vitalconnect.com. Accessed December 23, 2014.
32. Fact sheet: the Affordable Care Act and wellness programs. US Department of Labor website. http://www.dol.gov/ebsa/newsroom/fswellnessprogram.html. Accessed December 23, 2014.
33. Mattke S, Liu H, Caloyeras J, et al. Workplace wellness programs study: final report, 2013. RAND Corporation website. http://www.rand.org/pubs/research_reports/RR254.html. Accessed December 23, 2014.
34. Munro D. RAND Corporation (briefly) publishes sobering report on workplace wellness programs. May 28, 2013. Forbes website. http://www.forbes.com/sites/danmunro/2013/05/28/rand-corporation-briefly-publishes-sobering-report-on-workplace-wellness-programs. Accessed December 23, 2014.
35. Frakt A, Carroll AE. Do workplace wellness programs work? Usually not. September 11, 2014. *The New York Times* website. http://www.nytimes.com/2014/09/12/upshot/do-workplace-wellness-programs-work-usually-not.html. Accessed December 23, 2014.
36. Corporate wellness is a 13 Million unit wearable wireless device opportunity. September 25 2013. Allied Business Intelligence, Inc, Research website. https://www.abiresearch.com/press/corporate-wellness-is-a-13-million-unit-wearable-w. Accessed December 23, 2014.
37. Fitbit recalls force activity-tracking wristband due to risk of skin irritation. US Consumer Product Safety Commission website. https://www.cpsc.gov/en/Recalls/2014/Fitbit-Recalls-Force-Activity-Tracking-Wristband. Accessed December 23, 2014.
38. Szczerba RJ. Understanding healthcare's top technology hazard. August 25, 2014. Forbes website. http://www.forbes.com/sites/robertszczerba/2014/08/25/understanding-healthcares-top-technology-hazard. Accessed December 23, 2014.
39. Sullivan M. Guess what? Doctors don't care about your Fitbit data. August 15, 2014. VentureBeat website. http://venturebeat.com/2014/08/15/guess-what-doctors-dont-care-about-your-fitbit-data. Accessed December 23, 2014.
40. Honan M. The next big health app needs to do more than just track our numbers. March 21, 2014. Wired website. http://archive.wired.com/gadgetlab/2014/03/heres-hoping-healthbook-puts-pretty-face-numbers. Accessed.
41. Medical licensure. American Medical Association website. http://www.ama-assn.org/ama/pub/education-careers/becoming-physician/medical-licensure.page. Accessed December 23, 2014.
42. Cortez N. The mobile health revolution? *UC Davis Law Rev*. 2014;47:1173-1230.
43. Koetsier J. Mobile app monetization: freemium is king, but in-app ads are growing fast. March 27, 2014. VentureBeat website. http://venturebeat.com/2014/03/27/mobile-app-monetization-freemium-is-king-but-in-app-ads-are-growing-fast. Accessed December 23, 2014.
44. Zuckerman E. The Internet's original sin. August 14, 2014. *The Atlantic* website. http://www.theatlantic.com/technology/archive/2014/08/advertising-is-the-internets-original-sin/376041. Accessed December 23, 2014.
45. Berwick DM, Nolan TW, Whittington J. The triple aim: care, health, and cost. *Health Aff (Millwood)*. 2008;27(3):759-769.
46. Digital life in 2025: the Internet of things will thrive by 2025. May 14, 2014. PewResearch Internet Project website. http://www.pewinternet.org/files/2014/05/PIP_Internet-of-things_0514142.pdf. Accessed December 23, 2014.