American Journal of Law & Medicine, 40 (2014): 416-441

Digital Diagnosis: Privacy and the Regulation of Mobile Phone Health Applications

Jamie Lynn Flaherty[†]

A woman living in a remote part of Kenya cannot see vision is clouded and dark, and she is miles away from a hospital. Fortunately, a doctor visiting her community lifts up a smartphone and takes a picture of her eye. The Portable Eye Examination Kit ("PEEK") mobile application ("app") on the smartphone then conducts a vision test and reports her diagnosis of cataracts.[1]

With the proliferation of mobile health apps like Dr. Andrew Bastawrous's PEEK app, more people around the world, including those living in remote areas,

[†] J.D. Candidate 2015, Boston University School of Law; B.A. Lafayette College.

[1] *See* James Gallagher, *Optician's clinic that fits in a pocket*, BBC NEWS (Aug. 14, 2013), http://www.bbc.co.uk/news/health-22553730.

can access healthcare.[2] Approximately 85% of adults in the United States have a cell phone, and 53% of those phones are smartphones.[3]

As of 2012, one in five smartphone users in the United States had downloaded a health app.[4] Today, studies suggest users, physicians, app developers, and technology companies have developed over 97,000 mobile health apps.[5] From fertility scheduling apps like Glow[6] to MedXSafe[7]—an app that syncs sexually transmitted disease test results onto the user's personal mobile page—health-related applications for smartphones are becoming an increasingly prominent part of the healthcare market.[8]

These health apps, which often prompt users to input intimate personal information, pose a number of privacy concerns.[9] Health apps stand to improve doctor-patient communications,[10] increase access to healthcare,[11] reduce hospital readmissions,[12] and decrease healthcare costs.[13] However, many commercially available health apps also transmit unencrypted information to advertising and data analysis sites without the user's knowledge.[14] In a study by Privacy Rights Clearinghouse, approximately 39% of free apps and 30% of paid-for apps sent smartphone app user data to a third party; this data sharing was not disclosed by the developer in the app or in its privacy policy.[15] Due to these transmissions, the extent to which health apps are subject to Health Insurance Portability and Accountability Act of 1996 (HIPAA) compliance and U.S. Food and Drug Administration (FDA)

---

[2] *See* Robyn Whittaker, *Issues in mHealth: Findings From Key Informant Interviews*, J. MED. INTERNET RES. (Oct. 2, 2012), http://www.ncbi.nlm.nih.gov/pmc/articles/PMC3510768/.

[3] *See* SUSANNAH FOX & MAEVE DUGGAN, PEW RESEARCH CTR., MOBILE HEALTH 2012, 4 (2012), *available at* http://www.pewinternet.org/~/media/Files/Reports/2012/PIP_MobileHealth2012_FINAL.pdf.

[4] *Id.* at 11.

[5] *See* Peter McLaughlin & Melissa Crespo, *The Proliferation of Mobile Devices and Apps for Healthcare: Promises and Risks*, BLOOMBERG BNA (May 21, 2013), http://about.bloomberglaw.com/practitioner-contributions/the-proliferation-of-mobile-devices-and-apps-for-health-care-promises-and-risks/.

[6] *See* Colleen Taylor, *Backed With $6M, Max Levchin's Glow App For Tracking Female Fertility Debuts On The App Store*, TECHCRUNCH (Aug. 8, 2013), http://techcrunch.com/2013/08/08/glow-fertility-app/.

[7] *See* Ankita Rao, *Messaging Your Doctor? There's An App For That*, KHN BLOG (Feb. 27, 2013, 3:21 PM), http://capsules.kaiserhealthnews.org/index.php/2013/02/texting-your-doctor-theres-an-app-for-that/.

[8] *See* McLaughlin & Crespo, *supra* note 5.

[9] *See, e.g.*, Ann Carrns, *Free Apps for Nearly Every Health Problem, but What About Privacy?*, N.Y. TIMES, Sept. 11, 2013, http://www.nytimes.com/2013/09/12/your-money/free-apps-for-nearly-every-health-problem-but-what-about-privacy.html ("Health apps collect all sorts of personal information . . . [a]nd, they often transmit unencrypted information over insecure network connections.").

[10] *See* Rao, *supra* note 7.

[11] *See* Whittaker, *supra* note 2.

[12] Timothy Aungst, *Implementing mobile technology to reduce hospital readmissions*, IMEDICALAPPS (Aug. 22, 2013), http://www.imedicalapps.com/2013/08/mobile-technology-hospital-readmissions/.

[13] *See, e.g.*, ERNST & YOUNG, MHEALTH: MOBILE TECHNOLOGY POISED TO ENABLE A NEW ERA IN HEALTHCARE 47 (2012), *available at* http://www.ey.com/Publication/vwLUAssets/mHealth/$FILE/mHealth%20Report_Final_19%20Nov%2012.pdf (discussing how physicians' use of mobile devices can reduce costs).

[14] *See* Carrns, *supra* note 9.

[15] LINDA ACKERMAN, PRIVACY RIGHTS CLEARINGHOUSE, MOBILE HEALTH AND FITNESS APPLICATIONS AND INFORMATION PRIVACY: REPORT TO CALIFORNIA CONSUMER PROTECTION FOUNDATION 5 (2013), *available at* https://www.privacyrights.org/mobile-medical-apps-privacy-consumer-report.pdf.

regulation has become a topical issue.[16] On September 23, 2013, the FDA released its final mobile health app guidance, which revealed that the FDA would regulate only those apps that constitute medical devices and/or pose significant risks to patients.[17] This guidance has left some questions unanswered, particularly regarding which types of apps "pose significant risks." In addition to following FDA regulation, health apps that distribute protected health information among covered entities or business associates of covered entities must be HIPAA compliant.[18] However, because only a limited subset of health apps falls under either of these two categories, many commercially available apps escape regulation under either the FDA or HIPAA, many apps still expose users' health information to various third parties.[19]

Part I of this note summarizes the current regulation of health apps. Part II analyzes the interactions between health apps and HIPAA, focusing on three specific apps that pose varying levels of privacy risks. The first is a healthcare-messaging app that is clearly within the scope of HIPAA regulation. The second app is an informational, fitness-related app that safely falls outside of HIPAA's reach. The third health app falls between the first two—it does more than merely provide information but falls short of explicitly diagnosing or directly communicating with a physician about protected health information. The main focus will be on this third app, which is commercially available and currently escapes HIPAA regulation. Part II thus illustrates that although health apps help consumers as well as physicians, many commercially available apps currently fall outside of HIPAA's scope, leaving users' private health information unprotected. Part III describes the various ways smartphone apps threaten personal privacy and lays out the tension between innovation and regulation. Part IV suggests that instead of expanding HIPAA protection, there ought to be a broad privacy-based approach to regulating health apps and legislation that requires all apps to have clear, complete privacy policies.

I. THE REGULATION OF MOBILE HEALTH APPLICATIONS

A. BENEFITS OF MOBILE HEALTH APPS

As mobile phones have become an increasingly prevalent part of modern society, people have begun developing mobile apps for smartphones that provide a number of services.[20] A mobile app is a piece of information-access software designed to run on a mobile device.[21] Mobile apps are sold through online stores, such as the Apple App store[22] or the Google Play Android store.[23] While early apps

---

[16] *See, e.g.*, Y. Tony Yang & Ross D. Silverman, *Mobile Health Applications: The Patchwork of Legal and Liability Issues Suggests Strategies yo Improve Oversight*, 33 HEALTH AFF. 222, 226 (2014) (discussing current regulation of health apps and how "the uncertainty of whether and how mHealth affects existing legal regime").

[17] *See* Kendra Casey Plank, *FDA Releases Final Mobile App Guidance, Reserves Oversight for High-Risk Products*, BLOOMBERG BNA (Sept. 23, 2013), www.bloombergbna.com.

[18] *See* Adam H. Greene, *When HIPAA applies to mobile applications,* MOBIHEALTHNEWS (June 16, 2011), http://mobihealthnews.com/11261/when-hipaa-applies-to-mobile-applications/.

[19] *See id.*

[20] *See* Alex Krouse, Note, *iPads, iPhones, Androids, and Smartphones: FDA Regulation of Mobile Phone Applications as Medical Devices*, 9 IND. HEALTH L. REV. 731, 741 (2012).

[21] *See id.* at 733.

[22] *See App Store*, APPLE, https://itunes.apple.com/us/genre/ios/id36?mt=8 (last visited Nov. 2, 2014).

were limited in number and mainly consisted of a simple calendar or task list, today, anyone with a smartphone can browse through over one million apps with a wide array of functions.[24] These apps range from the simple, such as those that allow users to access the internet, to the complex, such as those that allow users to check in for flights[25] or control their home's thermostats from across town.[26]

As smartphones and apps become more popular, developers strive to produce new creative and convenient apps that bring the abundant resources of the computer into one's mobile device.[27] Smartphones pervade everyday personal life, and they are becoming increasingly ubiquitous in professional life as well. "Bring Your Own Device" (BYOD) programs are a new trend where employers allow—and arguably encourage—employees to use their personal smartphones for work purposes.[28] As a result of such initiatives, employees—especially healthcare employees—increasingly opt to use their personal smartphones at work.[29] According to a survey conducted by Cisco mConcierge, 89% of healthcare workers use their personal smartphones for work purposes.[30] Apps related to health and medicine are therefore becoming increasingly common, and they are dramatically changing the nature of the healthcare industry.[31]

The intersection between mobile technologies and healthcare, now termed "mHealth," is an increasingly important area due to health apps' many benefits.[32] For example, physicians have found mobile apps useful in numerous health interventions, such as helping people to stop smoking and to better manage their diabetes.[33] Many also praise health apps for increasing access to healthcare and improving communication between physicians and patients.[34] Simply by having a smartphone with a health app, users can reach out to their physicians and share diagnostic information wherever they may be.[35] Accordingly, as mHealth continues to expand, doctors can not only improve their care for their own patients, but they can also better reach and serve those in remote, underserved communities, as

---

[23] *See App Store*, GOOGLE PLAY, https://play.google.com/store/apps?hl=en (last visited Nov. 2, 2014).

[24] *See* Sarah Perez, *An Upper Limit For Apps? New Data Suggests Consumers Only Use Around Two Dozen Apps Per Month*, TECHCRUNCH (Jul. 1, 2014), http://techcrunch.com/2014/07/01/an-upper-limit-for-apps-new-data-suggests-consumers-only-use-around-two-dozen-apps-per-month/.

[25] *See* Susan Stellin, *Yes! Download That Airline App*, N.Y. TIMES, Feb. 29, 2012, http://www.nytimes.com/2012/03/04/travel/airline-apps-that-check-you-in-map-airports-and-follow-luggage.html?_r=0.

[26] Nest allows users to change their thermostat in their home from their smartphone. *See* Megan Wollerton, *Nest app 4.0 improves thermostat, makes room for smoke detector*, CNET (Nov. 15, 2013, 9:15 AM), http://reviews.cnet.com/8301-17889_7-57612537/nest-app-4.0-improves-thermostat-makes-room-for-smoke-detector/.

[27] *See* Krouse, *supra* note 20, at 737.

[28] Cory Fox, *Personal Smartphones: A Ticking HIPAA/HITECH Time Bomb?*, JD SUPRA (Apr.10, 2013), http://www.jdsupra.com/legalnews/personal-smartphones-a-ticking-hipaahi-00665/.

[29] *Id.*

[30] *Id.*

[31] *See* McLaughlin & Crespo, *supra* note 5.

[32] "mHealth" is a term describing "medical and public health practice supported by mobile devices, such as mobile phones, patient monitoring devices, tablets, personal digital assistants (PDAs), and other wireless devices." *See* Whittaker, *supra* note 2; *see also* Morgan Reed, *Apps Showcase the Bright Future of Mobile Health*, HUFFINGTON POST (Oct. 10, 2013, 11:33 AM), http://www.huffingtonpost.com/morgan-reed/apps-showcase-the-bright-_b_4078221.html (discussing the various benefits of health apps and how they "will revolutionize the way patients monitor their health and interact with healthcare providers").

[33] Whittaker, *supra* note 2.

[34] *Id.*; *see also* Gallagher, *supra* note 1.

[35] *See* Reed, *supra* note 32.

illustrated by the PEEK app diagnosing cataracts in Kenya.[36] An additional example of the global reach of mHealth initiatives is Text to Change—an organization that led an HIV/AIDS-related text messaging initiative in Uganda that approximately doubled the number of Ugandans counseled and tested for HIV/AIDS.[37]

The benefits of health apps extend beyond increasing access and quality of communication; commercially available apps can also improve the general wellbeing of users. A Pew Research poll suggests that 19% of smartphone users have downloaded an app specifically to track or manage their health.[38] For example, there are health apps that can record a user's heart rate,[39] diagnose depression,[40] and conduct urine analysis.[41] These health apps can also save lives; for example, a doctor flying cross-country diagnosed a fellow passenger as having a heart attack and helped save her life by using a mobile health app called AliveCor ECG.[42] In addition, after the 2010 earthquake in Haiti, a man trapped under rubble used a first aid app on his mobile phone to learn how to control his own bleeding.[43] As these examples illustrate, health apps are ushering in a new world of healthcare with increased access, improved communication, and prolonged personal wellness.

Many argue that mHealth initiatives will also cut healthcare costs by encouraging good health habits, such as exercise and healthy eating, and by enabling users to better manage chronic conditions.[44] According to the Organisation for Economic Co-operation and Development, the United States spends approximately 17.9% of its GDP on healthcare.[45] As this oft-cited statistic poignantly reveals, the United States is in desperate need of efficient solutions to reduce healthcare costs, and many point to mHealth as such a solution.[46] One way that mHealth can promote efficiency and decrease healthcare costs is by reducing hospital readmissions.[47] Under the Affordable Care Act's (ACA) Hospital Readmissions Reduction Program, Centers for Medicare and Medicaid Services (CMS) will reduce payments to certain

---

[36] *Id.*

[37] *Our History,* TTC MOBILE SOLUTIONS FOR SOCIAL CHANGE, http://www.ttcmobile.com/about-us/ (last visited Nov. 2, 2014).

[38] FOX & DUGGAN, *supra* note 3, at 11.

[39] *See* Amy Rabinovitz, *Azumio's 'Instant Heart Rate App' passes the 10 million download mark*, EXAMINER.COM (Nov. 17, 2011), http://www.examiner.com/article/azumio-s-instant-heart-rate-app-passes-the-10-million-download-mark.

[40] *See* Gallagher, *supra* note 1.

[41] Biosense Technologies's app, uChek, allows users to take images of their urine and send them off to be tested for key chemicals. *See* Michael V. Copeland, *New App Turns Your iPhone Into a Mobile Urine Lab*, WIRED (Feb. 26, 2013), http://www.wired.com/2013/02/smartphone-becomes-smart-lab/.

[42] Jonah Comstock, *Airplane rescue, Colbert booking round out Topol's HIMSS week*, MOBIHEALTHNEWS (Mar. 11, 2013), http://mobihealthnews.com/20745/airplane-rescue-colbert-booking-round-out-topols-himss-week/.

[43] Josh Levs, *Trapped father survives with help of phone app*, CNN (Jan. 24, 2010, 6:15 PM), http://www.cnn.com/2010/WORLD/americas/01/24/haiti.survivor.phone.app/.

[44] *See* Peggy McShane & Christina Cavoli, *How Mobile Healthcare Apps Can Help Reduce Healthcare Costs*, SEGUETECHNOLOGIES.COM (Nov. 6, 2013), http://www.seguetech.com/blog/2013/11/06/how-mobile-healthcare%20apps-reduce-costs.

[45] *Health expenditure, total (% of GDP),* WORLD BANK, http://data.worldbank.org/indicator/SH.XPD.TOTL.ZS (last visited Nov. 2, 2014)*; see also* Jason Kane, *Health Costs: How the U.S. Compares With Other Countries*, PBS NEWSHOUR (Oct. 22, 2012, 10:30 AM), http://www.pbs.org/newshour/rundown/2012/10/health-costs-how-the-us-compares-with-other-countries.html (describing how the United States spends "more than two-and-a-half times more than most developed nations in the world").

[46] *See* McShane & Cavoli*, supra* note 44.

[47] Aungst, *supra* note 12.

hospitals with excess readmissions.[48] Health apps that allow patients to better communicate with their doctors and remind patients to take their prescriptions may help reduce hospital readmissions and thereby play an increasingly important role post-ACA.[49] A physician panel member at the mHealth and Telehealth World Congress in Boston suggested that using mobile phones is a relatively easy way for patients, even those with limited exposure to the technology, to track their symptoms and avoid being readmitted to the hospital.[50] This physician found that "[p]atients were able to use the devices for educational points, measurement of vitals, and to answer questions . . . in order to assess for possible interventions by caregivers."[51]

Health apps also may help reduce administrative costs. The Deloitte Center for Health Solutions released a report suggesting that mHealth could save approximately $305 billion in administrative costs by reducing travel time and improving communication of medical decisions.[52]

B. FDA REGULATION OF MOBILE HEALTH APPS

While health apps have innumerable benefits, they also pose regulatory concerns. Ease and convenience aside, health apps present countless privacy, security, and legal challenges.[53] When users input (sometimes very personal) information into a health app, it is not clear where this information goes and what the app developer or phone manufacturer does with it. Moreover, as these health apps become increasingly prevalent and subsequently increase access to healthcare, there is a risk that consumers, as well as physicians, will rely too heavily on these apps as a means of diagnosis and treatment.[54] Thus an additional justification for the regulation of health apps is to address the concern that consumers might begin replacing doctor appointments with health apps.[55] The fact that large corporations are becoming increasingly invested and involved in mobile health apps further suggests a need for regulation.[56] Companies like Apple, AT&T, and Verizon Wireless have begun developing and promoting various health-related apps, and it is unclear how and to what extent people will use and rely on these apps, and what these large companies will do with user information they gather through these apps.[57]

---

[48] *Readmissions Reduction Program*, CENTERS FOR MEDICARE & MEDICAID SERVICES, http://www.cms.gov/Medicare/Medicare-Fee-for-Service-Payment/AcuteInpatientPPS/Readmissions-Reduction-Program.html (last updated Aug. 4, 2014); *see also* 42 C.F.R. §§ 412.150-.154 (2013).

[49] *See, e.g.*, *Caremerge App 'ReThink ReAdmissions' Launches On AllScripts.com And Reduces 30-Day Readmission To Hospitals*, HEALTH IT OUTCOMES (Sept. 17, 2013), http://www.healthcaretechnologyonline.com/doc/caremerge-app-readmissions-allscripts-and-reduces-0001.

[50] Aungst, *supra* note 12.

[51] *Id.*

[52] DELOITTE, MHEALTH IN AN MWORLD: HOW MOBILE TECHNOLOGY IS TRANSFORMING HEALTH CARE 12 (2012), *available at* http://www.deloitte.com/assets/Dcom-UnitedStates/Local%20Assets/Documents/us_chs_2012_mhealth_HowMobileTechnologyIsTransformingHealthCare_032213.pdf.

[53] Deborah Runkle, *The mHealth revolution,* SCITECH LAWYER (Winter-Spring 2013), http://go.galegroup.com/ps/i.do?id=GALE%7CA329901514&v=2.1&u=nellco_bpll&it=r&p=LT&ssw=w&asid=85ab808db4e535eb39cd6ae29a90632e.

[54] Krouse, *supra* note 20, at 738.

[55] *Id.*

[56] *Id.* at 741.

[57] *Id.* At 741 ("[A] balance between innovation and regulation needs to be struck because of the extensive investment in the industry by mobile phone companies, third party developers, and medical providers.").

The FDA has classified certain kinds of software apps—such as those running on mobile phones—as devices, and has accordingly set out certain regulatory requirements that apply to those devices.[58] The FDA described the public health risks posed by these apps in its July 2011 guidance regarding Mobile Medical Applications.[59] Most recently, in September 2013, the FDA issued new guidelines, described by some as setting forth a "hands-off, risk-based approach."[60] The guidance indicated that the FDA would only regulate a limited group of apps: medical devices that pose sufficient risks and apps generally that pose "significant risks to patients."[61] If an app is subject to FDA regulation, it must satisfy the "general controls" set forth in the Federal Food, Drug and Cosmetic Act (FD&C Act.)[62] The FDA's guidance states,

> Many mobile apps are not medical devices . . . under section 201(h) of the Federal Food, Drug, and Cosmetic Act . . . and the FDA does not regulate them. 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).[63]

Whether an app constitutes a "medical device" and is hence subject to FDA regulation depends on its intended use and potential risk.[64] The FDA defines a mobile medical app as an app that meets the definition of a device and is "intended to be used as an accessory to a regulated medical device; or to transform a mobile platform into a regulated medical device."[65] An app is considered a medical device under the FD&C Act if it is an "instrument . . . intended for use in the diagnosis of disease or other conditions, or the cure, mitigation, treatment, or prevention of disease, or is intended to affect the structure or any function of the body of man or other animals."[66] Put simply, when the intended use of an app is for diagnosis, treatment or prevention of disease, the app is a device.[67]

Apps that are considered medical devices under the FDA guidance nonetheless may escape regulation if they are not considered high-risk.[68] For example, apps that provide treatment recommendations, offer health information to pregnant women, or share personal medical records may be considered low-risk medical devices; therefore, according to the guidance, these apps may go unregulated.[69] While it is not clear which types of apps the FDA will find high-risk, the guidance makes clear

---

[58] FOOD & DRUG ADMIN., MOBILE MEDICAL APPLICATIONS: GUIDANCE FOR INDUSTRY AND FOOD AND DRUG ADMINISTRATION STAFF 4-5 (2013) [hereinafter GUIDANCE], *available at* http://www.fda.gov/downloads/MedicalDevices/.../UCM263366.pdf.

[59] *Id.* at 6-7 ("As is the case with traditional medical devices, certain mobile medical apps can pose potential risks to public health. Moreover, certain mobile medical apps may pose risks that are unique to the characteristics of the platform on which the mobile medical app is run. For example, the interpretation of radiological images on a mobile device could be adversely affected by the smaller screen size, lower contrast ratio, and uncontrolled ambient light of the mobile platform.").

[60] Brooke Borel, *Health Policy Brief: mHealth and FDA Guidance*, HEALTH AFF. (Dec. 5, 2013), http://www.healthaffairs.org/healthpolicybriefs/brief.php?brief_id=104.

[61] Plank, *supra* note 17.

[62] Yang & Silverman, *supra* note 16, at 223.

[63] GUIDANCE, *supra* note 58, at 4.

[64] *Id.* at 8.

[65] *Id.* at 7.

[66] 21 U.S.C. § 321 (2012).

[67] GUIDANCE, *supra* note 58, at 8.

[68] *Id.*

[69] *Id.* at 16-18.

that the FDA intends to regulate a small subset of mobile medical apps, thereby "ensuring patient safety without stifling innovation."[70]

Apps that display medical device data to allow patient monitoring and apps that use a mobile platform reader are subject to FDA regulation.[71] One example of a commercially available app that uses a mobile platform reader is IBGStar.[72] IBGStar is an FDA-approved medical device app that allows users to check their glucose levels with a glucose strip.[73] The device consists of a glucose monitor that attaches to a mobile phone and relays information to its companion app, which the user can download from the app store.[74] ECG Mobile is another health app that the FDA regulates as a mobile medical device. ECG Mobile is a wireless Electrocardiogram that reports the electrical activity of the heart to the user's smartphone via Bluetooth.[75] The information is then sent to the user's physician, and the physician is sent an alarm if the device's readings are irregular.[76]

According to the September 2013 guidelines, the FDA will also regulate those apps that pose significant risks to users.[77] The FDA has not shed much light on which types of apps fall into this latter category, but the guidance provides some examples of mobile apps that escape FDA regulatory oversight.[78] One group of apps that will not be regulated is those that help patients without providing specific treatment decisions.[79] Additionally, apps that provide easy access to information related to patients' health conditions and those that allow patients to communicate potential medical conditions to providers need not satisfy the requirements set forth under the FD&C Act.[80]

C. HIPAA COMPLIANCE AND MOBILE HEALTH APPS

In addition to being subject to FDA regulatory oversight, some health apps must also comply with the HIPAA.[81] In April 2001, the federal HIPAA privacy rules became effective.[82] These rules authorized the Secretary of Health and Human Services to promulgate regulations safeguarding the privacy of medical records containing personally identifiable information.[83] Part of the motivation behind HIPAA was the desire to protect health information in a world where medical records were becoming increasingly intangible.[84] As more medical records become

---

[70] *See id.*

[71] *Id.* at 14-15.

[72] *See* Brian Dolan, *FDA clears AgaMatrix's iPhone glucose meter*, MOBIHEALTHNEWS (Dec. 7, 2011), http://mobihealthnews.com/15137/fda-clears-agamatrixs-iphone-glucose-meter/.

[73] *Id.*

[74] *Id.*

[75] Jonah Comstock, *FDA clears Android-based continuous ECG monitor,* MOBIHEALTHNEWS (Dec. 5, 2013), http://mobihealthnews.com/27865/fda-clears-android-based-continuous-ecg-monitor/.

[76] *Id.*

[77] Plank, *supra* note 17.

[78] *See* GUIDANCE, *supra* note 58, at 20-22.

[79] *Id.*

[80] *Id.*

[81] Health Insurance Portability and Accountability Act, Pub. L. No. 104-191, 110 STAT. 1936 (Codified as amended in scattered sections of 42 U.S.C.).

[82] Peter A. Winn, *Confidentiality in Cyberspace: The HIPAA Privacy Rules and the Common Law*, 33 RUTGERS L.J. 617, 617 (2002).

[83] George J. Annas, *HIPAA Regulations – A New Era of Medical-Record Privacy?*, 348 NEW ENG. J. MED. 1486, 1486-90 (2003), *available at* http://www.mcmaster.ca/ors/ethics/ncehr/2003/apr2003/1486%20NEJM%20HIPAA%20II.pdf.

[84] Winn, *supra* note 82, at 617.

electronic, Congress began worrying about increased access to and potential misuse of personal health information.[85] The provisions set forth in HIPAA establish a federal floor of protections; states are free to establish more stringent protections of personal health information, but state laws are preempted by the HIPAA privacy rules if they establish lesser protections.[86]

To fall under HIPAA's scope, "protected health information" (PHI) must be communicated between covered entities, including "business associates."[87] 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."[88] "Covered entities" include health plans, healthcare clearinghouses, and healthcare providers who transmit health information in electronic form.[89] 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.[90]

HIPAA's relevant requirements are embodied in the HIPAA Administrative Simplification Regulations, which consist of the Privacy Rule, Security Rule, Enforcement Rule, and Breach Notification Rule.[91] The Privacy Rule describes when PHI may be disclosed generally; in contrast, the Security Rule sets out the requirements for when covered entities disclose PHI in electronic form.[92] Under the Privacy Rule, PHI may be disclosed when authorized or if necessary to protect the public health. However, if the disclosure is in electronic form, it must also satisfy the requirements set forth in the Security Rule.[93]

The HIPAA Privacy Rule is designed to keep personally identifiable health information confidential and to keep patients better informed about what is done with their medical records.[94] Generally, covered entities may not use or disclose PHI without authorization.[95] Patients must be informed that their medical records can be used in certain circumstances, such as for treatment, payment, or healthcare operations.[96] The privacy notice requirement under the HIPAA regulations requires that patients be told who can see and use their medical records.[97] Individuals may authorize the disclosure of their PHI, but in some circumstances, such as to protect

---

[85] *Id.* at 618.

[86] *Id.*

[87] "Health information" includes information that relates to "past, present, or future physical or mental health or condition of an individual." 45 C.F.R. § 160.103 (2013). "Business associates" include entities that handle PHI on behalf of a covered entity. *Id.* If a covered entity engages with a business associate to help it carry out its healthcare related functions, the covered entity must have a contract or arrangement with the business associate. *Id.* Business associates must also "[r]eport to the covered entity any security incident of which it becomes aware, including breaches of unsecured protected health information." *Id.*; *see also* Greene, *supra* note 18.

[88] 45 C.F.R. § 160.103 (2013).

[89] 45 C.F.R. § 160.103.

[90] *See* Security and Privacy, 45 C.F.R. § 164.104 (2013) (describing HIPAA's applicability to covered entities and business associates).

[91] U.S. DEPT. OF HEALTH & HUMAN SERVS., HIPAA ADMINISTRATIVE SIMPLIFICATION (2013), *available at* http://www.hhs.gov/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf.

[92] Hilary N. Karasz et al., *Text Messaging to Communicate with Public Health Audiences: How the HIPAA Security Rule Affects Practice,* 103 AM. J. PUB. HEALTH 617, 617 (2013).

[93] *Id.* at 618.

[94] *See* Annas, *supra* note 83, at 1487.

[95] 45 C.F.R. § 164.508(a)(1) (2013).

[96] 45 C.F.R. § 164.506(a) (2013).

[97] Patients also have a right of access; they can inspect, copy, and amend their medical records. Annas, *supra* note 83, at 1487.

public health, disclosure may be required even without prior authorization.[98] Importantly, except under limited circumstances, a covered entity or business associate cannot sell PHI.[99]

The HIPAA Security Rule provides protections for electronic personal health information (ePHI).[100] Generally, the Security Rule requires covered entities and business associates to "ensure the confidentiality, integrity, and availability of all electronic protected health information."[101] Covered entities must also "protect against any reasonably anticipated threats or hazards to the security or integrity of such information."[102] To do so, the Security Rule requires covered entities to implement three main protections for ePHI: "Administrative Safeguards," "Physical Safeguards," and "Technical Safeguards."[103] A covered entity must comply with these standards, which in many cases involves following specific measures prescribed by statute.[104]

The "Administrative Safeguards" set forth under the Security Rule require covered entities and business associates to "[c]onduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information."[105] To satisfy the "Physical Safeguards" requirement, a covered entity must "[i]mplement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed."[106] Finally, the Security Rule sets forth "Technical Safeguards" that require the covered entity to "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access."[107] A covered entity must also notify an individual when his or her unsecured PHI is disclosed as a result of a breach.[108]

Recently, the government has begun paying more attention to HIPAA compliance. The Department of Health and Human Services stated that in 2014 it plans to launch a permanent HIPAA Audit Program, authorized under the Health Information Technology for Economic and Clinical Health Act.[109] This program is designed to ensure that covered entities comply with the standards set forth under the Privacy Rule, Security Rule, and Breach Notification.[110] Nevertheless, despite its

---

[98] 45 C.F.R. § 164.512 (2013).

[99] 45 C.F.R. § 164.502 (2013); *see also* U.S. DEPT. OF HEALTH & HUMAN SERVS., *supra* note 91, at 78.

[100] Karasz et al., *supra* note 92, at 618.

[101] 45 C.F.R. § 164.306 (2013).

[102] *Id*.

[103] Karasz et al., *supra* note 92, at 620.

[104] However, while some measures are required, others are "addressable," which means that a covered entity must determine whether that specific measure is "reasonable and appropriate" for implementation. *Id.* at 621. If the measure is not "reasonable and appropriate," then the covered entity must determine whether there is an alternative measure that is necessary for compliance. *Id.*; 45 C.F.R. § 164.306(b) (2013).

[105] 45 C.F.R. § 164.308(a)(1)(II)(A) (2013).

[106] 45 C.F.R. § 164.310 (a)(2)(ii) (2013).

[107] 45 C.F.R. § 164.312(a)(1) (2013).

[108] 45 C.F.R. § 164.404 (2013).

[109] Janet Feldkamp & Daniel O'Brien, *Be Prepared – HIPAA Audits are Coming in 2014,* JD SUPRA (Jan. 29, 2014), http://www.jdsupra.com/legalnews/be-prepared-hipaa-audits-are-coming-in-84533/.

[110] *Id.* ("In recent years . . . the DHHS Office of Civil Rights ("OCR") has demonstrated an increased willingness to levy heavy fines against entities for non-compliance.").

stated goal of protecting patients' privacy and PHI, the HIPAA Privacy and Security Rules are limited in two main ways: First, they do not create a federal private cause of action for those injured by violations;[111] and second, the rules only apply to situations involving PHI, covered entities, and business associates.[112] Therefore, HIPAA rarely extends to apps used only by individuals because consumers using the app outside of a healthcare setting are not "covered entities."[113] Because of the narrow requirements of HIPAA, many health apps are outside of its scope and risky for consumers.[114]

II. ANALYSIS OF THREE COMMERCIALLY AVAILABLE HEALTH APPS

A. TEXT MESSAGING AND HIPAA: HIPAA COMPLIANT APP "TIGERTEXT"

One of the many benefits of mobile phones is that they facilitate communication. Over time, text messaging has become a cornerstone of modern day communication. In 2011, approximately 73% of adults with cell phones reported having sent text messages, with approximately two trillion text messages being sent in the United States.[115] Text messaging has emerged as a simple and highly efficient means of communication, particularly in the healthcare setting.[116] Traditional text messaging involving PHI between physicians or other healthcare entities would fall under HIPAA's scope because it involves PHI communicated among covered entities. However, text messaging is not secure and fails to comply with HIPAA's requirements because once the text message is circulating, "it is under the domain of the wireless telephone carriers with which the health department [has] no contractual agreement."[117] Moreover, "the end user may not password protect his or her mobile phone, which would leave text messages vulnerable to access by an unauthorized individual."[118]

Based on such concerns, in 2011 The Joint Commission (a non-profit healthcare accreditation organization) banned physicians and healthcare professionals from sending text messages containing patient information.[119] However, one way to make text messaging secure, as suggested in HIPAA's Security Rule, is through encryption.[120] TigerText is a smartphone app that uses encryption to provide secure,

---

[111] Winn, *supra* note 82, at 618. *See generally* Miller v. Nichols, 586 F.3d 53, 59 (1st Cir. 2009) ("HIPAA does not create a private right of action."); Acara v. Banks, 470 F.3d 569, 571-72 (5th Cir. 2006) ("Private rights of action to enforce federal law must be created by Congress. . . . HIPAA has no express provision creating a private cause of action, and . . . no private cause of action [exists] under HIPAA.").

[112] *For Covered Entities and Business Associates*, U.S DEPT. HEALTH & HUM. SERVICES, http://www.hhs.gov/ocr/privacy/hipaa/understanding/index.html (last visited Nov. 2, 2014).

[113] Yang & Silverman, *supra* note 16, at 224.

[114] Deven McGraw, *Final HIPAA Rules a Major Step Forward, but There's More Work To Be Done,* IHEALTHBEAT (Feb. 8 2013), http://www.ihealthbeat.org/perspectives/2013/final-hipaa-rules-a-major-step-forward-but-theres-more-work-to-be-done.

[115] Karasz et al., *supra* note 92, at 617.

[116] *See* Fox, *supra* note 28.

[117] Karasz et al., *supra* note 92, at 620.

[118] *Id.*

[119] Andrew A. Brooks, *Healthcare Texting in a HIPAA-Compliant Environment*, AM. ACAD. ORTHOPEDIC SURGEONS NOW (Aug. 2012), http://www.aaos.org/news/aaosnow/aug12/managing5.asp.

[120] *See* 45 C.F.R. § 164.312 (2013) ("A covered entity or business associate must . . . [i]mplement a mechanism to encrypt and decrypt electronic protected health information.").

HIPAA-compliant mobile messaging software to healthcare companies.[121] TigerText Pro, one of their main products, provides HIPAA-compliant doctor-to-doctor, nurse-to-doctor, and hospital-to-doctor communications.[122] When a person sends a text message, the message usually remains on the recipient's phone until he or she decides to delete it.[123] The message also remains on the cell phone company's server indefinitely.[124] In contrast, with TigerText Pro the sender can control when the message is deleted from the recipient's phone and from TigerText Pro's server.[125] TigerText Pro's messages are thus secure because they have a controlled and limited lifespan.[126] As Jeffrey Evans, TigerText's cofounder, describes this security feature, "[a]ll messages and content in the application have a lifespan on the device, so after a set period of time . . . the content is pulled from the device . . . . If a device is lost or stolen, the account passwords are changed and the content can be remotely wiped from the device."[127]

Because the messages sent with TigerText and TigerText Pro are encrypted and have a limited lifespan, they are HIPAA compliant.[128] The software works on Apple, Android, and Blackberry smartphones, and according to the Google Play Store, TigerText Pro has been installed between 500,000 and one million times.[129] As of February 2012, more than twenty healthcare organizations were using TigerText.[130] TigerText therefore exemplifies how health apps can improve access, transparency, and communication among healthcare entities, while still complying with HIPAA and maintaining patients' privacy.

Secure text messaging can benefit both healthcare organizations and patients in a number of ways. Efficient and clear text messaging between doctors and nurses can reduce the number of medical errors, which in turn decreases healthcare costs and improves patient outcomes.[131] As the Chief Medical Officer of TigerText has said, "[i]n most hospitals, the communication process among physicians is arcane, inefficient, and potentially dangerous as it relates to patient care."[132] Studies suggest that many instances of medical malpractice are attributable to miscommunication and/or administrative confusion.[133] For example, the Institute of Medicine reported that of the 98,000 deaths due to human error in 1999, 90% involved failed systems and procedures, including failures in communication.[134] Moreover, according to the

---

[121] *See* Nicole Lewis, *TigerText Investment to Tighten Up Messaging Security*, INFO. WEEK (Feb. 9, 2012, 10:09 AM), http://www.informationweek.com/security/risk-management/tigertext-investment-to-tighten-up-messaging-security-/d/d-id/1102733.

[122] *Id.*

[123] Rick Broida, *App Spotlight: TigerText promises to keep text messages private and secure*, PC WORLD (Feb. 27, 2013, 10:57 AM), http://www.pcworld.com/article/2029496/app-spotlight-tigertext-promises-to-keep-text-messages-private-and-secure.html.

[124] *Id.*

[125] *Id.*

[126] Lewis, *supra* note 121.

[127] *Id.*

[128] *TigerText Secure Messenger App*, GOOGLE PLAY, https://play.google.com/store/apps/details?id=com.tigertext&hl=en (last visited Nov. 2, 2014).

[129] *Id.*

[130] Lewis, *supra* note 121.

[131] *See* Brooks, *supra* note 119.

[132] *Id.*

[133] *See Patient Safety Resources*, AM. MED. ASS'N, http://www.ama-assn.org//ama/pub/about-ama/ama-foundation/our-programs/public-health/health-literacy-program/health-literacy-patient.page (last visited Nov. 2, 2014) ("[M]ore than 80% of medical errors are due to communication breakdowns.").

[134] INST. OF MED., TO ERR IS HUMAN: BUILDING A SAFER HEALTH SYSTEM 26 (Linda T. Kohn et al. eds. 1999), *available at* http://www.fluentmedical.com/docs/To_Err_Is_Human.pdf; Maria Alma

National Council of State Boards of Nursing reports, nurses cite issues communicating with physicians as one of the major factors leading to patient care mistakes.[135] In "To Err is Human: Building a Safer Health System," authors Kohn, Corrigan, and Donaldson recommend focusing on "funding dissemination and communication activities to improve patient safety."[136] Apps like TigerText can help reduce instances of miscommunication between physicians, between physicians and nurses, and most importantly, between physicians and patients.

Several studies investigating what compels patients to file medical malpractice claims suggest that a major theme in these suits is a lack of patient-physician communication; many patient-plaintiffs complain that physicians are misleading and unavailable.[137] As a result, organizations like the American Association of Orthopaedic Surgeons have emphasized the importance of communication in the physician-patient relationship in reaching better patient outcomes and, as a result, in reducing malpractice lawsuits.[138] Because many doctors agree that "the foundation for a good patient-physician relationship is communication," and because studies suggest that many malpractice claims stem from a lack of communication, apps like TigerText that ease and encourage communication in healthcare organizations will likely play a vital role in the future of healthcare.[139]

Secure doctor-to-nurse messaging like TigerText allows doctors to check certain facts about the patient, such as their treatment, medical history, or any other piece of information quickly and efficiently. Messaging apps like TigerText also enable doctors and nurses to quickly and securely send information and discuss test results and patient procedures.[140] Thus, apps like TigerText stand to improve communication in healthcare organizations, reduce administrative errors, and improve the patient's experience. Moreover, because they are secure and HIPAA compliant, apps like TigerText ease some privacy-related concerns about physicians messaging patients' private health information on their smartphones.

HIPAA-compliant, diagnosis-related apps are also increasing access to healthcare. For example, STD Triage, made by iDoc24, claims that it does not collect PHI and allows users to anonymously send their pictures to licensed dermatologists.[141] With STD Triage, users can send pictures of their skin ailments, pay $9.99, and within twenty-four hours receive an email suggesting what the problem may be.[142] The doctors who respond evaluate the user's symptoms and photos and select a few possible diagnoses.[143] The app can also show the user a map

---

Rodriguez et al., *Medical Errors: Physician and Institutional Responsibilities*, 5 J. ONCOLOGY PRAC. 24, 24 (2009), *available at* http://jop.ascopubs.org/content/5/1/24.full.pdf+html.

[135] CATHERINE DINGLEY ET AL., IMPROVING PATIENT SAFETY THROUGH PROVIDER COMMUNICATION STRATEGY ENHANCEMENTS 1-2 (2004), *available at* http://www.ncbi.nlm.nih.gov/books/NBK43663/pdf/advances-dingley_14.pdf.

[136] INST. OF MED., *supra* note 134, at 9.

[137] Beth Huntington & Nettie Kuhn, *Communication gaffes: A Root Cause of Malpractice Claims*, 16 BAYLOR U. MED. CENTER. PROC. 157, 158 (2003), *available at* http://www.ncbi.nlm.nih.gov/pmc/articles/PMC1201002/.

[138] Brooks, *supra* note 119.

[139] Huntington & Kuhn, *supra* note 137, at 157.

[140] *See* Brooks, *supra* note 119.

[141] Sarah Mitroff, *Got a Burning Question? Calm Your Panic with 'STD Triage' App*, WIRED (Mar. 8, 2013, 9:30 AM), http://www.wired.com/business/2013/03/std-triage/.

[142] STD TRIAGE, http://www.stdtriage.com/ (last visited Nov. 2, 2014).

[143] Mitroff, *supra* note 141; *see also* Robin Wilkey, *STD Triage, App That Helps Identify Sexually Transmitted Diseases, Launches in San Francisco,* HUFFINGTON POST (Mar. 7, 2013, 8:29 pm), http://www.huffingtonpost.com/2013/03/07/std-triage_n_2832828.html.

of local STD clinics.[144] Alexander Borve, Swedish orthopedic surgeon and developer of STD Triage, says that he does not want his app to replace physicians or discourage doctor visits, but rather wants it "to sit in between Google and your doctor, as [a] place to get helpful, correct advice."[145]

As both of these apps show, developers are creating innovative apps that aim to improve communication and access, all while keeping PHI secure.

B. NON-HIPAA-COMPLIANT APP: "MYFITNESS PAL"

While apps like TigerText help healthcare entities communicate, other commercially available apps provide smartphone users with general health information.[146] Called consumer-operated apps, these give users a way to track their exercise, try out new workouts, or maintain their caloric intake.[147] For example, MyFitness Pal is a calorie-counter weight loss app that allows users to set their own diet goals and record their daily food intake and exercise regiments.[148] Users can input the food they have eaten and the app will show how many calories they have consumed and burned throughout the day.[149] If they choose to, users can also share their progress with others.[150]

The FDA does not regulate consumer-operated apps like MyFitness Pal because these types of apps neither constitute medical devices nor pose significant risks as defined in FDA regulations. Moreover, apps like MyFitness Pal need not be HIPAA compliant because they do not involve PHI or covered entities. However, although MyFitness Pal does not transmit PHI, the app still requires users to enter some personal information, and it is not clear how that information is used. For example, in its privacy policy, MyFitness Pal states that with respect to personal information, including name, gender, birthday, zip code, height and weight: "[w]e may . . . draw upon this Personal Information in order to adapt the Website and/or Applications to your needs, to research the effectiveness of our Website and/or Applications, and to develop new tools for our members."[151] The privacy policy goes on to describe how "MyFitness Pal shares anonymized [d]emographic [d]ata with its advertisers and marketing partners so that such third-parties may provide [users] with advertisements tailored to [the users'] interests."[152] As this excerpt illustrates, privacy policies can be unclear. There is no indication of how the "demographic data" is anonymized, and the policy fails to state which third parties might be receiving the allegedly anonymized information. This lack of transparency as to what app developers do with users' personal information is troubling.

Therefore, while consumer-operated health apps need not be HIPAA compliant, they nevertheless collect information including location data, and leave smartphone user health information vulnerable to exploitation by app developers and third party advertisers.

---

[144] Mitroff, *supra* note 141.
[145] *Id.*
[146] *See* Borel, *supra* note 60, at 2.
[147] *Id.*
[148] MYFITNESSPAL, http://www.myfitnesspal.com/mobile/iphone (last visited Nov. 2, 2014).
[149] *Id.*
[150] Haley Tsukayama, *My Fitness Pal app helps you take control of calories*, WASH. POST, Nov. 2, 2013, http://www.washingtonpost.com/business/my-fitness-pal-app-helps-you-take-control-of-calories/2013/11/01/03fc4176-3e93-11e3-b6a9-da62c264f40e_story.html.
[151] *MyFitnessPal Privacy Policy*, MYFITNESSPAL (June 11, 2013), http://www.myfitnesspal.com/welcome/privacy_policy.
[152] *Id.*

C. BORDERLINE CASE: NON-HIPAA-COMPLIANT APP "GLOW"

Thus far, I have presented two different types of apps: first, an app that clearly involves the transmission of patients' PHI between covered entities in a HIPAA-compliant manner; and second, an app that clearly falls outside of the scope of HIPAA, as it involves neither PHI nor covered entities, yet nevertheless poses privacy concerns. The apps that are the most worrisome are those that fall into neither of these cleanly cut categories; I call these the borderline apps.

"Glow" is one example of a borderline app. PayPal co-founder Max Levchin recently developed Glow as an iPhone app designed to help women get pregnant.[153] The app has a fertility tracker and analyzes information on ovulation cycles to help women track the best time to try to conceive.[154] Glow users must enter personal information about their menstrual cycles, body temperatures, and sexual positions.[155] The app then advises the user on her fertility.[156] According to Levchin, Glow also sends cute, personal reminders, including alerting a woman when she is fertile, and occasionally reminding her partner to bring flowers home.[157]

Although the benefits of this app are clear—helping women become pregnant—the privacy concerns are equally clear. As one writer for *Slate* put it, the app is more than a mere ovulation calendar: "it's creepier."[158] The writer continues to express his concern over Glow by writing "[i]t's a data tracker[;] [r]ather than just letting you know when you should try to have a baby, Glow asks users to routinely enter extremely detailed information about their health and sex lives."[159] Levchin has emphasized that privacy will be of the utmost importance, but with respect to HIPAA compliance, the company sought guidance from the FDA and stated it will only be HIPAA compliant if required by regulators to do so.[160] Thus the app does not appear to be HIPAA compliant, and according to the privacy policy, Glow will "share your personal information with employees, affiliates, vendors, partners and third parties as required to offer the [app's products and services]."[161] Glow's privacy policy continues to assert, "we share your personal information as necessary in order . . . to market products and services to you. We also may decide to share your information for joint marketing purposes with other companies."[162]

Borderline apps like Glow powerfully illustrate the tension between the benefits of health apps and the privacy concerns they pose. As with many borderline apps, it is difficult to decipher whether Glow is HIPAA compliant. Although at the time of writing Glow does not currently seem to be HIPAA compliant, it involves the transmission of personal health information. It is unclear whether the transmitted information is individually identifiable. Under HIPAA, health information is

---

[153] Lauren Goode, *Max Levchin's New Plan: To Get You Pregnant (And Improve Healthcare in the Process*), ALL THINGS D (May 29, 2013, 11:14 AM), http://allthingsd.com/20130529/max-levchins-new-plan-to-get-you-pregnant-and-improve-health-care-in-the-process/.

[154] *Id.*

[155] *Id.*

[156] *Id.*

[157] *Id.*

[158] Farhad Manjoo, *Glow vs. Stick*, SLATE (Aug. 8, 2013, 11:00 AM), http://www.slate.com/articles/technology/technology/2013/08/new_fertility_app_glow_it_wants_to_know_absolutely_everything_about_you.html.

[159] *Id.*

[160] Ken Yeung, *PayPal co-founder Max Levchin's Glow launches to improve healthcare, starting with infertility*, TNW (Aug. 8, 2013), http://thenextweb.com/apps/2013/08/08/paypal-co-founder-max-levchins-glow-launches-to-improve-healthcare-starting-with-infertility/#!uZxGR.

[161] *Privacy Policy,* GLOW, https://glowing.com/privacy#mtop (last visited Nov. 2, 2014).

[162] *Id.*

considered individually identifiable, and therefore PHI if "there is a reasonable basis to believe the information can be used to identify the individual."[163] Based on the extent to which users are tracked and linked to their smartphones, as will be discussed below, one could argue that the information a user enters into Glow via her smartphone could be linked to that user's identity and hence qualify as PHI. Furthermore, although it is outside of a healthcare setting, the app could potentially be required to be HIPAA compliant if covered entities like healthcare providers specializing in pregnancy become involved.

If Glow were required to be HIPAA compliant, the app would have to follow the "Technical Safeguards" such as implementing certain "Access Controls" that limit access to the software and data.[164] Under HIPAA Glow would also have to assign users a unique name-tracking identity[165] and "respond to suspected or known security incidents [and] mitigate, to the extent practicable, harmful effects of security incidents."[166] More importantly, if Glow fell under HIPAA's umbrella, the app's developers likely could not sell users' PHI.[167]

The lack of transparency in privacy policies ultimately presents the question: when a non-HIPAA-compliant app like Glow prompts a user to input information about her menstrual cycle or her sex life, where does this information go?

III. SMARTPHONE APPLICATIONS AND PRIVACY CONCERNS

A. PRIVATE INFORMATION – WHERE DOES IT GO?

Every smartphone has a unique number that serves as an identifier ("Unique ID"), which allows companies to gather information and create profiles of cell phone users for advertisers.[168] The number is most commonly set by the phone's operating system or phone carrier, and remains on the phone forever (or, in the case of Android devices, until the user resets the phone and deletes the settings.)[169] Unique IDs pose serious privacy risks, as they are extremely difficult or impossible to delete and can be tied to other information including the users' locations.[170]

Jessica Rich, the Deputy Director of the Bureau of Consumer Protection at the Federal Trade Commission, suggests, "consumers have no idea about the layers of sharing [data] that goes on behind the scenes."[171] In 2010, the *Wall Street Journal* conducted a study investigating what exactly occurs behind the scenes of smartphone apps.[172] Researchers discovered that out of 101 popular apps, fifty-six transmitted users' smartphone Unique IDs.[173] The study revealed that, among others, the prominent music app Pandora sent information including age, gender, location,

---

[163] 45 C.F.R. § 160.103 (2013).

[164] *See* 45 C.F.R. § 164.312(a)(1) (2013).

[165] *See* 45 C.F.R. §164.312(a)(2)(i).

[166] 45 C.F.R. § 164.308(a)(6)(ii) (2013).

[167] *See* 45 C.F.R. § 164.502(a)(5)(ii)(A) (2013) ("Except pursuant to and in compliance with § 164.508(a)(4), a covered entity or business associate may not sell protected health information.").

[168] *See* Jennifer Valentino-DeVries, *Unique Phone ID Numbers Explained*, WALL ST. J., Dec. 19, 2010, http://blogs.wsj.com/digits/2010/12/19/unique-phone-id-numbers-explained/.

[169] *Id.*

[170] *Id.*

[171] Julianne Pepitone, *Apple and Google get grilled on Privacy,* CNN (May 10, 2011, 5:14 PM), http://money.cnn.com/2011/05/10/technology/apps_privacy_hearing/.

[172] Scott Thurm & Yukari Iwatani Kane, *Your Apps Are Watching You,* WALL ST. J., Dec. 18, 2010, http://online.wsj.com/news/articles/SB10001424052748704694004576020083703574602.

[173] *Id.*

and Unique IDs to networks of advertisers.[174] Recently, there have been a few cases challenging the use and collection of Unique IDs by telecommunication companies, including Microsoft and Apple.[175] For example, in the 2012 case *Cousineau v. Microsoft Corp.,* a Washington court addressed the issue, stating that "[o]f particular concern is Microsoft's alleged collection of unique phone identifiers because of their potential to enable Microsoft or another company to link users' personal information with their current physical location."[176]

B. PRIVATE INFORMATION – HOW IS IT USED?

Many apps have access to users' smartphone GPS receivers, cameras, and microphones.[177] Thus, as one researcher put it, "users must blindly trust that applications will properly handle their private data."[178] When app developers access private information, not much is known about how that private information is *actually* used.[179] To discover what happens to personal information entered into an app, researchers developed an Android mobile-phone platform called "TaintDroid" to track the flow of private data through third-party applications.[180] Those researchers discovered that apps used sensitive data suspiciously in two-thirds of applications.[181] In one instance, fifteen out of thirty applications reported users' locations to advertising companies.[182]

Many app developers have unbridled access to location data, which can be tied to sensitive and personal information such as visits to the hospital.[183] As one article noted:

> [T]his location data reveals extremely detailed information about consumer activity, considerably more so than traditional computer operating systems. Although these companies assert that data they receive from consumers is anonymized and used merely to build out their databases of access points, these limitations are self-imposed, not required by law.[184]

Both Apple and Google have repeatedly and publicly acknowledged the importance of customers' privacy, and they champion the fact that users consent before revealing information.[185] However, as the *Wall Street Journal* reported, "these rules can be skirted . . . [s]martphone users are all but powerless to limit the

---

[174] *Id.*

[175] *See, e.g.*, *In re* iPhone Application Litig., No. 11-MD-02250-LHK, 2013 WL 6212591, at *2 (N.D. Cal. Nov. 25, 2013) (granting summary judgment to Apple despite Plaintiffs' claim that Apple's "representations regarding a user's ability to disable Location Services were false and misleading because Apple . . . continued to collect wifi hotspot and cell tower information from the iPhones, even after users . . . turned off the Location Services on their devices").

[176] Cousineau v. Microsoft Corp., 992 F. Supp. 2d 1116, 1123 (W.D. Wash. 2012).

[177] William Enck et al., *TaintDroid: An Information-Flow Tracking System for Realtime Privacy Monitoring on Smartphones*, 32 TRANSACTIONS ON COMPUTER SYS. 5:1, 5:2 (2014).

[178] *Id.*

[179] *Id.*

[180] *Id.*

[181] *Id.* at 5:3.

[182] *Id.*

[183] *See id.* at 5:2.

[184] Leslie Harris, *Mobile Phone Tracking Highlights Need For Baseline Privacy Law*, HUFFINGTON POST (May 10, 2011), http://www.huffingtonpost.com/leslie-harris/mobile-phone-tracking-hig_b_859908.html?.

[185] Thurm & Kane, *supra* note 172.

tracking."[186] According to the investigation, some apps send location information to advertisers without first obtaining user approval.[187] Moreover, although app developers insist that the information they pass on to advertisers is not linked to an individual's name, an individual's Unique ID links that person to their phone, and phone manufacturers can link a smartphone to a person's name and email.[188] Apple considers an iPhone's Unique ID to be "personally identifiable information" because it can be connected to personal details such as a name and email address.[189] Even more troubling, many apps do not have a privacy policy.[190] Out of the 101 apps investigated by the *Wall Street Journal*, forty-five did not have privacy policies on their websites, and neither Apple nor Google requires apps to have such policies.[191]

Collecting smartphone users' information is becoming a growing industry, as evidenced by Mobclix, a company that profits from smartphone users' data.[192] Mobclix compiles data about a phone's location, uses that information to guess where that user lives, and then assigns that person a spending and demographic category.[193] After gathering this information, Mobclix sends it to advertisers.[194] Google's advertiser network, AdMob, also helps advertisers target certain smartphone users by location and demographic data.[195] Apple has also signaled that it will gather information about users' friends via social networking sites and compile that information to help advertisers target individual people.[196] The data gathered from a user's smartphone "helps mobile advertising companies . . . create detailed profiles of people based on how they use their mobile device, where they travel."[197] Smartphone apps have unfettered access to copious amounts of users' data and therefore, particularly in the context of health-related apps, raise a number of privacy and security concerns.

C. BEYOND HIPAA & FDA: THE ROLE OF OTHER AGENCIES

There are a number of agencies that have been, and likely will continue to be, involved in the regulation of health apps: the FDA, the Federal Communications Commission (FCC), the Federal Trade Commission (FTC), the Office for Civil Rights of the Department of Health and Human Services (HHS), and the National Institute of Standards and Technology.[198] However, as Glow demonstrates, many apps that pose serious privacy concerns fall outside these current regulations.

---

[186] *Id.*
[187] *Id.*
[188] *See id.*
[189] *Id.*
[190] *Id.*; *see also Healthcare On-The-Go: Pros and Cons of Mobile Health Apps*, SUPPLEMENTAL HEALTHCARE (Aug. 17, 2013), http://www.supplementalhealthcare.com/blog/2013/healthcare-go-pros-and-cons-mobile-health-apps ("Up to 50% of mHealth apps have vague or non-existent privacy policies.").
[191] Thurm & Kane, *supra* note 172.
[192] *Id.*
[193] *Id.*
[194] *Id.*
[195] *Id.*
[196] *See id.;* Julia Angwin & Jennifer Valentino-Devries, *Apple, Google Collect User Data*, WALL ST. J., Apr. 22, 2011, http://online.wsj.com/news/articles/SB10001424052748703983704576277101723453610.
[197] James Glanz et al., *Spy Agencies Tap Data Streaming From Phone Apps*, N.Y. TIMES, Jan. 27, 2014, http://www.nytimes.com/2014/01/28/world/spy-agencies-scour-phone-apps-for-personal-data.html?_r=0.
[198] Yang & Silverman, *supra* note 16, at 223.

Beyond HIPAA and FDA regulation, the Computer Fraud and Abuse Act (CFAA)[199] and the Electronic Communications Privacy Act (ECPA) also regulate the privacy of personal electronic data.[200] The CFAA does not offer much additional protection to health app consumers, however, because many users voluntarily grant apps access to personal data by downloading the apps, and the CFAA only protects against unauthorized access.[201] The ECPA likewise cannot bolster smartphone users' privacy protections because it contains an exception for user consent, and many users consent to third party requests to access their information (often without realizing what their consent allows).[202]

Customer Proprietary Network Information (CPNI) regulations also provide various protections for smartphone user information.[203] CPNI is defined as "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 telecommunications carrier."[204] Under CPNI regulations, "[e]very telecommunications carrier has a duty to protect the confidentiality of proprietary information of, and relating to, other telecommunication carriers, equipment manufacturers, and customers."[205]

The Telecommunications Act of 1996 gave the FCC the authority to enforce consumer information privacy provisions and set forth regulations as to how CPNI can be used.[206] Recently, on June 27, 2013, the FCC issued a declaratory ruling clarifying their CPNI regulations.[207] The ruling stated:

> [W]hen information that meets the statutory definition of CPNI is stored on the customer's mobile device, and the carrier has both caused such information to be stored on the device and has access to or control over that information, the carrier is responsible for safeguarding such information. Thus, for example, customer-specific data stored on a mobile device, such as information regarding phone numbers called, the location from which the calls were made, and the time, duration of calls, must be protected.[208]

Importantly, however, Commissioner Rosenworcel of the FCC explained that the declaratory ruling is limited; it does not apply to mobile phone manufacturers or third-party app developers.[209] This is particularly troublesome because third-party app developers are the ones gaining access to information and relaying that

---

[199] 18 U.S.C § 1030 (2012).
[200] 18 U.S.C. §§ 2510–2522 (2012).
[201] *See* Yang & Silverman, *supra* note 16, at 224.
[202] *See id.* at 225.
[203] *See* Harris, *supra* note 184.
[204] 47 U.S.C. § 222 (2012).
[205] *Id.*
[206] *See* 47 U.S.C. § 201 (2012) ("The Commission may prescribe such rules and regulations as may be necessary in the public interest to carry out the provisions of this chapter."); *see also* AT&T Corp. v. Iowa Utils. Bd., 525 U.S. 366, 378 (1999) (noting that the FCC has rulemaking authority under the Telecommunications Act of 1996).
[207] James M. Smith et al., *FCC Issues Declaratory Ruling Clarifying That CPNI Rules Apply to Personal Information Stored on Wireless Devices*, DAVIS WRIGHT TREMAINE LLP (June 28, 2013), http://www.dwt.com/FCC-Issues-Declaratory-Ruling-Clarifying-That-CPNI-Rules-Apply-to-Personal-Information-Stored-on-Wireless-Devices-06-28-2013/.
[208] *Id.*
[209] Nickolas Milonas et al., *FCC Privacy Rules Updated for Smartphone Era*, TMT LAW WATCH (July 1, 2013), http://www.tmtlawwatch.com/2013/07/articles/fcc-privacy-rules-updated-for-smartphone-era/.

information to advertising companies. While these laws aim to protect location information and to prevent telecommunications companies from marketing user information, "there are no clear rules for the disclosure of this data and often no way for consumers to control the data they reveal" when it comes to using an app that is separate from the telecommunications carrier.[210]

The FTC is also involved with regulating health apps. For example, in 2011, the FTC fined app developers who claimed their app treated acne.[211] Moreover, the FTC has made various privacy-related suggestions for app developers. The FTC's 2013 Staff Report on Mobile Privacy Disclosure stated, "app developers should provide just-in-time disclosures and obtain affirmative express consent when collecting sensitive information . . . such as . . . health, or children's data . . . or sharing sensitive data with third parties."[212] In the Mobile Privacy Report, the FTC also described the unique privacy challenges presented by mobile apps:

> First, more than other types of technology, mobile devices are typically personal to an individual, almost always on, and with the user. This can facilitate unprecedented amounts of data collection. The data collected can reveal sensitive information, such as communications with contacts, search queries about health conditions, political interests, and other affiliations, as well as other highly personal information. This data also may be shared with third parties, for example, to send consumers behaviorally targeted advertisements.[213]

The creation of the U.S. Senate Subcommittee on Privacy, Technology and the Law constituted another attempt to address the privacy-related issues posed by smartphones and other technologies.[214] In 2011, the Subcommittee questioned both Apple and Google about how each company tracks and stores users' location information.[215] Both Apple and Google claimed that obtaining users' location information is necessary for many apps to function and maintained that the databases do not contain any customer names.[216] Both companies also reiterated that the smartphones collect information data only with the users' consent, and urged the Subcommittee to look instead at the role of the third-party developers.[217]

---

[210] Harris, *supra* note 184.

[211] Yang & Silverman, *supra* note 16, at 223.

[212] FED. TRADE COMMISSION, MOBILE PRIVACY DISCLOSURES: BUILDING TRUST THROUGH TRANSPARENCY 23 (2013), *available at* http://www.ftc.gov/sites/default/files/documents/reports/mobile-privacy-disclosures-building-trust-through-transparency-federal-trade-commission-staff-report/130201mobileprivacyreport.pdf.

[213] *Id.* at 2.

[214] The Subcommittee's website describes its jurisdiction as: "(1) Oversight of laws and policies governing the collection, protection, use and dissemination of commercial information by the private sector, including online behavioral advertising, privacy within social networking websites and other online privacy issues; (2) Enforcement and implementation of commercial information privacy laws and policies; (3) Use of technology by the private sector to protect privacy, enhance transparency and encourage innovation; (4) Privacy standards for the collection, retention, use and dissemination of personally identifiable commercial information; and (5) Privacy implications of new or emerging technologies." *Subcommittee on Privacy, Technology and the Law,* U.S. SENATE COMMITTEE ON JUDICIARY, http://www.judiciary.senate.gov/about/subcommittees#privacy (last visited Nov. 2, 1014)

[215] Pepitone, *supra* note 171.

[216] *Id.*

[217] *Id.*

Senator Al Franken, the chair of the Subcommittee sums up the issue well: "I love that I can use Google maps -- for free, no less. I love that I can look up the [local] weather on my iPad. But we need a balance."[218]

D. PRIVACY COSTS VS. HEALTHCARE BENEFITS—STRIKING A BALANCE

As demonstrated by apps like Glow, and the companies that profit from gathering smartphone users' personal health information, smartphones and health apps present serious risks to personal privacy. One possible way of addressing these privacy concerns would be expanding regulation by, for example, requiring more apps to be HIPAA compliant. Increased regulation comes at a high cost, however, as unclear regulations and regulatory expenses may make app developers wary of developing new beneficial apps.[219] Given the boundless advantages of health apps, the benefits generally outweigh the privacy costs. However, as discussed in the next section, setting forth explicit requirements for health apps and third party app developers would help clarify the muddled assortment of various agencies and regulations currently involved in regulating these apps.

Health apps not only threaten users' personal privacy, but they also potentially expose physicians to HIPAA and medical malpractice liability. Because HIPAA tends to err towards safeguarding patients' privacy, some have suggested that doctors who recommend certain privacy-exposing apps to their patients could be liable for violating HIPAA.[220] Additionally, as Deborah Runkle, the Associate Staff Officer of the National Conference of Lawyers and Scientists, suggested, it is "likely that malpractice lawyers will take advantage of emerging [health app] technologies as a new opportunity for litigation."[221] Once a physician-patient relationship is formed, a doctor could be liable for any adverse consequences of recommending or using a health app.[222] However, as of right now, "medical liability in the mobile arena is uncharted territory," and it is not clear to what extent physicians or developers could be liable to patients in the future.[223]

Security and privacy-related issues aside, health apps are becoming an increasingly valuable tool in the healthcare system. Health apps make healthcare access merely a touch away for those that have smartphones. Moreover, health apps increase communication—both between healthcare entities and between physicians and patients—thereby improving care and potentially reducing medical errors and medical malpractice suits. With better communication, patients are better informed of worrisome side effects and can be reminded to take prescriptions, thereby reducing hospital readmissions, which in turn decreases healthcare costs generally.

A balance therefore needs to be struck between protecting users' personal health information and capitalizing on the numerous benefits that health apps offer. Many would argue for less regulation and suggest that health apps like Glow need not be

---

[218] *Id.*

[219] Scott D. Danzis & Christopher Pruitt, *Rethinking the FDA's Regulation of Mobile Medical Apps,* SCITECH LAWYER (Winter/Spring 2013), *available at* http://www.cov.com.

[220] Sue Ter Maat, *Health, fitness apps pose HIPAA risks for doctors,* AM. MED. NEWS (Aug. 5, 2013), http://www.amednews.com/article/20130805/business/130809993/7/?utm_source=feedly

("By recommending apps that compromise patients' privacy, doctors could be seen as complicit if there is any breach, although there is no apparent legal precedent for that.").

[221] Runkle, *supra* note 53.

[222] *Id.*; *see also* Ter Maat, *supra* note 220 ("Just recommending apps may put doctors at risk for violations of the Health Insurance Portability and Accountability Act.").

[223] Runkle, *supra* note 53.

HIPAA compliant because users consent and voluntarily share their information.[224] 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.[225] 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."[226] Thus there are reduced privacy protections when people input information into apps because they are essentially putting that information out into the public.[227]

While it is true that smartphone users voluntarily share this private health information, many likely think and hope that this information stays protected with the app. Research shows, however, that such information is in fact commonly shared with third parties.[228] From the point of view of developers or engineers, it may be unreasonable to expect that information will be kept private. However, the average user likely does not know whether, to whom, and to what extent personal information is shared, especially given that many apps fail to have clear privacy policies.[229] Moreover, as smartphones become more commonplace, users will likely feel more comfortable sharing private information on various apps and will potentially fall prey to third party advertising companies, who gather and compile personal user data. Even if users know they are sharing their information, they likely do not understand to what extent they are leaving their private health information continuously at risk while the information is stored indefinitely at the mercy of those who have collected it. This privacy violation is not limited to the first instance of sharing information because, as Michael Froomkin wrote in his *Stanford Law Review* article, "once created or collected, data is easily shared and hard to eradicate; the data genie does not go willingly, if ever, back into the bottle."[230]

IV. SUGGESTIONS & SOLUTIONS

Overall, given the myriad of benefits that accompany health apps and the importance of innovation, the best option may not be expanding current regulations, but rather clarifying and simplifying them. HIPAA, as it is, seems to properly balance innovation with regulation. For example, HIPAA's definition of covered entities could be broadened to include more of the aforementioned worrisome borderline apps. However, broadening HIPAA compliance comes at a high cost, namely, stifling innovation.[231]

---

[224] *See* Pepitone, *supra* note 171 (quoting Apple Vice President Guy L. Tribble's remarks concerning availability of user data being pendent on user consent).

[225] Following *Katz v. United States*, the protections of the Fourth Amendment are implicated when a search or seizure has occurred where a person reasonably expects privacy, and society must consider that expectation to be reasonable. Katz v. United States, 389 U.S. 347, 353 (1967).

[226] *Id.* at 357.

[227] David Kravets, *Feds Say Mobile-Phone Location Data Not 'Constitutionally Protected'*, WIRED (Sept. 5, 2012), http://www.wired.com/threatlevel/2012/09/feds-say-mobile-phone-location-data-not-constitutionally-protected/ ("The Obama administration told a federal court Tuesday that the public has no 'reasonable expectation of privacy' in cellphone location data . . . .").

[228] *See* Harris, *supra* note 184.

[229] *See id.* ("Consumers who download apps often don't know what information they are revealing about themselves, to whom and for what purpose.").

[230] Michael A. Froomkin, *The Death of Privacy?*, 52 STAN. L. REV. 1461, 1469 (2000).

[231] Peter Kilbridge, *The Cost of HIPAA Compliance*, 348 NEW ENG. J. MED. 1423, 1423 (2003), *available at* http://www.mcmaster.ca/ors/ethics/ncehr/2003/apr2003/1423%20NEJM%20HIPAA.pdf; *see also* Borel, *supra* note 60.

Another possible solution is for the FDA to more broadly interpret apps that "pose significant risks" to include those like Glow that collect personal information and share it with third parties. As previously discussed, the FDA has suggested that apps that merely help patients without providing treatment decisions escape FDA oversight. Even these apps can pose significant privacy risks because of the extent of personal information the developer of the app can collect. Nevertheless, in weighing regulation and innovation, FDA's hands-off, risk-based approach also seems to be the most effective way to regulate threatening apps while allowing app developers to explore the potentially boundless types of health apps.

Despite the balancing justifications behind HIPAA and the FDA's approach, mobile phones and advertising companies still raise serious privacy concerns. These privacy concerns are magnified when a person utilizes health apps on his or her mobile phone. In order to address the serious privacy concerns posed by smartphones, the best option is to clarify the current mixed bag of agencies and regulations involved and establish an over-arching consumer privacy-based regulation. As phrased by one commentator, "it is imperative that Congress establish baseline legislation that protects users' privacy and trust, not only for location and other highly sensitive information but also for all collection of consumer data."[232]

Because of the limitations of the FDA and HIPAA, the government should adopt some sort of "broad-based consumer privacy regulations."[233] As one article noted, the United States does not have general, broad privacy regulations despite the fact that Canada and many European states do.[234] As Jason Weinstein, the Deputy Assistant Attorney General at the Department of Justice has said, "there is no comprehensive federal regulation that enforces data breach disclosure."[235] Additionally, the array of different actors involved in addressing mobile phone privacy concerns (including the FTC, FCC, and FDA) only serves to further confuse the situation. Because of the number of different administrative bodies and regulations involved, developers, users, and technology companies are left without much guidance: "[t]he main reason technology companies and developers are having problems with the current process is because very little clarity exists."[236] Therefore, there ought to be clear, privacy-based regulations for telecommunications companies, third party app developers, and advertising companies, particularly in the health app context. As one writer suggested, "[t]he end goal for the FDA, companies, and developers should be to create a more predictable regulatory process."[237] Third-party app developers and advertising companies need clear guidelines around user privacy.

Regulations could offer some clarity on the issues posed when apps prompt users to input personal information, fail to have clear and complete privacy policies,

---

[232] Harris, *supra* note 184.

[233] Nancy J. King, *Direct Marketing, Mobile Phones, and Consumer Privacy: Ensuring Adequate Disclosure and Consent Mechanisms for Emerging Mobile Advertising Practices*, 60 FED. COMM. L.J. 229, 238 (2008); *see also* Gail Lasprogata et al., *Regulation of Electronic Employee Monitoring: Identifying Fundamental Principles of Employee Privacy Through a Comparative Study of Data Privacy Legislation in the European Union, United States and Canada,* 2004 STAN. TECH. L. REV. 4, 9-15, *available at* http://weblifebalance.com/wp-content/uploads/2013/09/Lasprogata-RegulationElectronic.pdf.

[234] King, *supra* note 233, at 238. Others have looked to the European system, and have suggested that the United States adopt a similar decentralized approach, "allowing incentivized developers [to] analyze and approve the products." Krouse, *supra* note 20, at 763.

[235] Pepitone, *supra* note 171.

[236] Krouse, *supra* note 20, at 763.

[237] *Id.* at 757.

and then opaquely share this data with unknown third parties. One proposed solution was the 2013 bill brought to Congress by U.S. Representative Hank Johnson: the Application Privacy, Protection, and Security Act of 2013 (APPS Act).[238] The APPS Act would require app developers to "(1) provide users with a method to withdraw such consent and to request that the developer delete personal data or refrain from further data collection or sharing, and (2) take measures to prevent unauthorized access to personal and de-identified data."[239] This bill would give users more control over their data: "[m]ost controversially, the act proposes that consumers should be able to delete their data at any time."[240] The act also directs the FTC to promulgate regulations and enforce the provisions under the act.[241] In sum, this bill could be a key step towards addressing app-related privacy concerns and requiring app developers to notify users about the collection, use, and sharing of personal information. Importantly, the bill also identifies FTC as the agency heading the enforcement of these laws, thereby clarifying the previously discussed confusion caused by various administrative bodies involved in the regulation of smartphone apps.

At a minimum, phone companies like Google and Apple, and third-party app developers, ought to be required to always obtain users' informed consent prior to prompting users to input personal, health-related information. One of the main arguments on which app developers and phone manufacturers rely is that users consent before revealing personal information on phone apps. However, the aforementioned study conducted by the *Wall Street Journal* suggests that many apps skirt around obtaining users' consent. In the context of health apps and health-related intimate information, apps should do more than ask users to consent to share information; rather, they ought to inform users whether, and how, apps will retain and share their personal health information. App developers should be held to the standard of "reasonable disclosure of the choices . . . and the dangers inherently and potentially involved," the same informed consent standard used with physicians in medical malpractice claims.[242] As suggested in Representative Johnson's APPS Act, users also ought to be able to later withdraw consent.

Second, all apps ought to be required to have clear and complete privacy policies that spell out with whom and to what extent users' personal information is shared. Despite their lack of privacy protection, many apps do not have privacy policies.[243] Although many argue that users never look at privacy policies,[244] there is evidence that people's attitudes towards electronic privacy are changing. A 2013 study conducted by the University of Colorado suggests that as people are becoming

---

[238] *See* Dara Kerr, *Congressman touts draft bill aimed at mobile app privacy*, CNET (Jan. 17, 2013 8:57 PM), http://www.cnet.com/news/congressman-touts-draft-bill-aimed-at-mobile-app-privacy/.

[239] APPS Act of 2013, H.R. 1913, 113th Cong. (2013), *available at* http://beta.congress.gov/bill/113th-congress/house-bill/1913.

[240] Jim Edwards, *Congress's New 'Apps Act' Could Change How You Use Your Mobile Phone Forever*, BUS. INSIDER (Jan. 18, 2013 9:50 AM), http://www.businessinsider.com/the-apps-act-2013-1.

[241] H.R.1913.

[242] Canterbury v. Spence, 464 F.2d 772, 782 (D.C. Cir. 1972).

[243] Thurm & Kane, *supra* note 172.

[244] *See* Susan E. Gindin, *Nobody Reads Your Privacy Policy or Online Contract? Lessons Learned and Questions Raised by the FTC's Action Against Sears,* 8 NORTHWESTERN J. TECH. & INTELL. PROP. 1 (2009), *available at* http://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1094&context=njtip (discussing studies that suggest online users are "click-happy" and, while they are "aware of privacy risks, they tend to ignore them").

more aware of the ways in which apps threaten personal privacy, they are increasingly willing to pay more for an app that keeps information private and advertisements out.[245] The study showed that people were willing on average to pay $1.19 for an app that did not track location and $3.58 to keep an app from accessing text messages.[246] This suggests that users are becoming more aware of the privacy concerns posed by apps, and that users may be more willing to read and respond to privacy policies.

Some have suggested prohibiting apps from collecting location information altogether.[247] However, phone manufacturers, mainly Apple and Google, maintain that they need this information and that users benefit from apps that record location data.[248] A simpler way to address the issue is education—informing users how their information is used. Commissioner Rosenworcel of the FCC has suggested that the Commission "take a more proactive role in educating consumers and simplifying privacy policies in conjunction with the Federal Trade Commission."[249] Additionally, with respect to employers who have adopted the aforementioned BYOD programs, one solution is to require employers to take various protective measures, such as installing remote wiping software.[250] Employers should also educate and train their employees on the risks associated with personal smartphone use at work.[251]

V. CONCLUSION

The influx of health apps is revolutionizing healthcare and the doctor-patient relationship. Health apps present a myriad of health and social benefits. Health apps not only will help to lower sky-high healthcare costs, but will also improve doctor-patient communications and increase access to healthcare. Despite their innumerable advantages, however, health apps also expose users to illegitimate information and privacy risks. Users should therefore be wary of releasing health information on health apps, as many apps share information with third parties, and it is unclear what these apps do with allegedly "anonymous" and protected information.[252]

With the advent of apps, especially health apps, it is nearly impossible to keep personal preferences and medical history private, as technology has created an alarmingly transparent world. Moreover, given their intimate and personal nature, there are additional privacy concerns with health apps. As one writer stated, "[p]rivacy . . . encompasses much more than just control over a data trail, or even a set of data. It encompasses ideas of bodily and social autonomy, of self-determination, and of the ability to create zones of intimacy and inclusion that define and shape our relationships with each other."[253] It is therefore the way health apps blur zones of intimacy and trespass on social autonomy that make them a privacy-harming force with which to be reckoned.

---

[245] Rebecca J. Rosen, *Study: Consumers Will Pay $5 for an App That Respects Their Privacy,* ATLANTIC (Dec. 26, 2013 2:57 PM), http://www.theatlantic.com/technology/archive/2013/12/study-consumers-will-pay-5-for-an-app-that-respects-their-privacy/282663/.

[246] *Id.*

[247] *See id.*

[248] *See id.*

[249] Smith et al., *supra* note 207.

[250] Fox, *supra* note 28.

[251] *Id.*

[252] *See id.*

[253] Froomkin, *supra* note 230, at 1466.

The scope of FDA regulation and HIPAA compliance of health apps is limited, despite the fact that many health apps prompt users to input private health information and then distribute that information to various advertising companies. As evidenced from the current unclear status of regulation, "legal protections cannot keep pace with a changing technological landscape."[254] Thus the main challenge when it comes to regulating mobile health apps is that the technology behind smartphones and apps typically moves extremely quickly.[255] For example, reports suggest that by 2015, 500 million people will have downloaded health apps onto their smartphones.[256]

By limiting regulation, society can take more advantage of these beneficial apps; however, the increasing number of smartphone users ought to be aware of what is done with their personal information. Therefore, there ought to be clear consumer privacy regulations for telecommunication companies and app developers, at a minimum requiring complete consent and privacy policies. This would be an important step towards striking a balance between capitalizing on the benefits of health apps while protecting individuals' privacy rights.

[254] Yang & Silverman, *supra* note 16, at 224.
[255] *See* Krouse, *supra* note 20, at 762.
[256] *Id.*