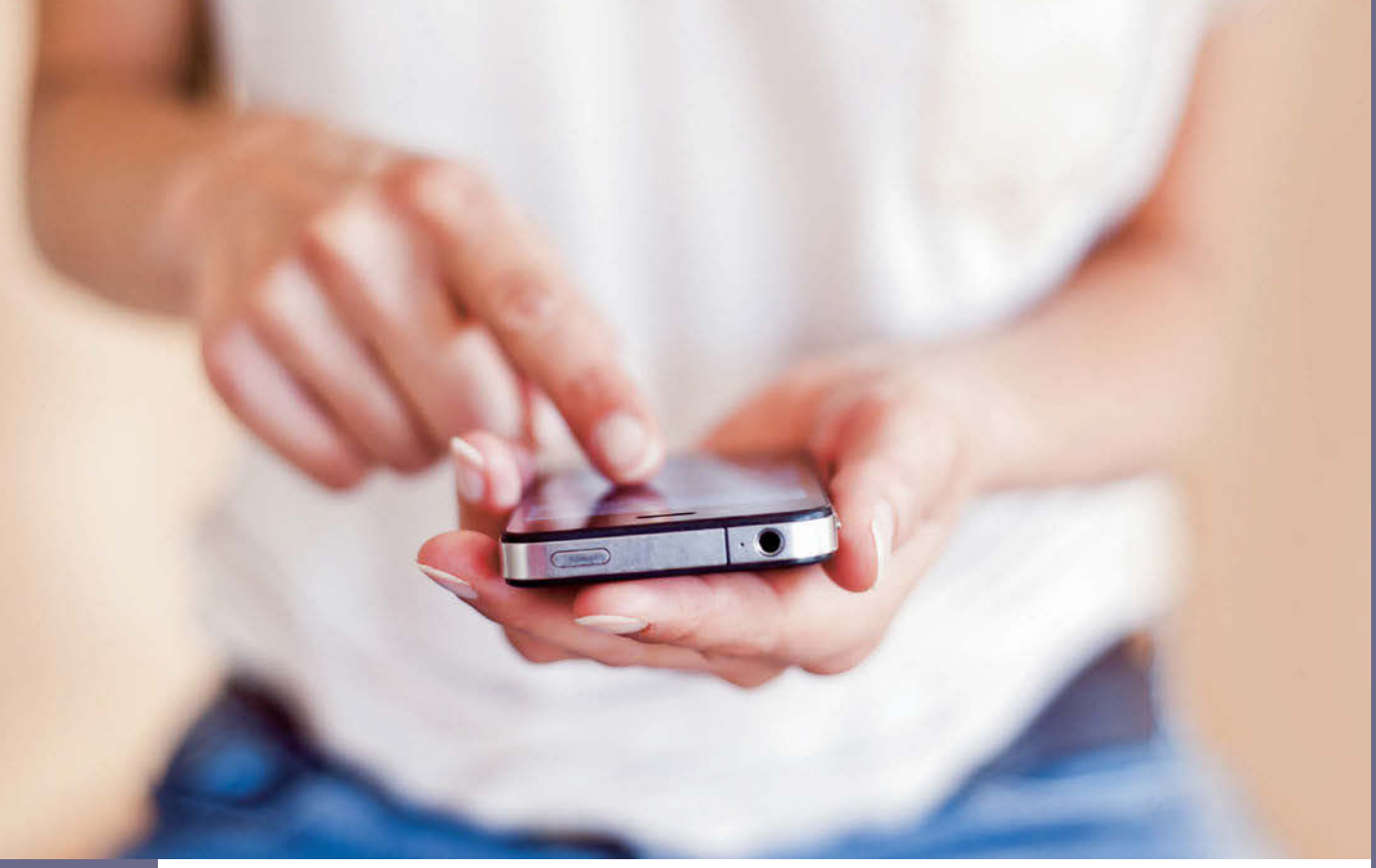
AVAILABLE ONLINE FREE TO MEMBERS | WWW.FDLI.ORG | MAR/APR 2015

UPDATE

Food and Drug Law, Regulation and Education

FDLI
A PUBLICATION OF THE FOOD AND DRUG LAW INSTITUTE

IN THIS ISSUE



HIPAA and MOBILE HEALTH APPS:
What developers need to know about app user privacy

By Cindy J. Alvarado and Rakan F. Ghubej

Cooler weather and a new crop of Apples have become the tell-tale signs of autumn and the hot season for new technology. Apple's 6 Plus delivered *big* (pun intended) last September, but the world of mobile health technology, *m*health, was in the spotlight for all of 2014 and shows no signs of moving. Since the beginning of 2013, more than $750 million in venture capital has been invested in mobile health technology.[1] In September 2013, the Food and Drug Administration (FDA) removed a potential roadblock to growth in the area when the agency identified the types of apps that would be the focus of its regulatory oversight, making both the actual cost and the time cost

Cindy J. Alvarado is an associate of the law firm of Porzio, Bromberg & Newman P.C. in the Life Sciences Compliance, Commercialization and Regulatory Counseling practice, advising pharmaceutical, medical device and biotechnology companies on a variety of compliance-related issues. Cindy also serves as a compliance associate with the firm's subsidiary, Porzio Life Sciences, LLC. She can be reached at cjalvarado@pbnlaw.com.

Rakan F. Ghubej is a Regulatory Analyst for Porzio Life Sciences, LLC, focused on state and federal regulations and legislation affecting the sales and marketing practices of the life sciences industry. Rakan can be reached at ghubej@PorzioLS.com.

involved in app development more predictable.[2] The FDA also identified the types of apps it was less concerned with because of their lower risk to the public.[3] Finally, the agency stated that it would not enforce its regulatory authority over the lower risk apps, at least for now.[4] Game-changing progress in *m*health followed in 2014.

Apple, Google, and Samsung, big names in mobile technology with little to no background in health, made significant contributions to that progress by launching their own developer platforms specifically for the design of health and fitness apps.[5] SAMI (short for Samsung Architecture Multimodal Interactions) was the first developer platform to go public when it launched in late May 2014.[6] Within a month of SAMI's launch, Apple announced the upcoming release of its own health platform, HealthKit, and Google announced its new fitness-focused platform, Google Fit.[7] HealthKit and Google Fit became available to the public last fall.[8]

The health platforms were designed to make app development easier, to increase access to higher-grade data, and to improve app design.[9] All of these factors are expected to contribute to an enhanced and streamlined user experience that the industry hopes will win over, and the sooner the better, reluctant users.[10] Skeptics, however, are not convinced that the technology is catching on with patients.[11] While one study touts skyrocketing usage of health and fitness apps, reporting a 62% increase from December 2013 to June 2014,[12] other reports claim that few of the 100,000+ health apps have had 500 or more downloads and that two-thirds of the users that have downloaded an app no longer use it.[13]

Usage may be low, for now, but the volume is set to skyrocket in the very short term, bringing concerns and increased risks of exposing protected health information to an unintended recipient as data becomes accessible to, and shared between, different applications on a platform.[14] The technology sector has been quick to downplay privacy concerns.[15] Nonetheless, developers should be aware that privacy *is* a developer's responsibility. In fact, developers can be held *directly liable* for a violation of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), even when they are not directly responsible for the violation.[16]

Developers don't have to become privacy law experts, but gaining an understanding of *when* liability could arise is a precaution worth taking. We will provide a brief background on some recent developments in mobile health technology, review the legal implications of sharing personal health data, and present a framework for mobile app developers to better understand when HIPAA might apply and what to do about it.

Tech giants are paving the way for patient-focused mhealth technology.

Apple, Google and Samsung created their developer platforms to enable the aggregation and exchange of information between *m*health apps.[17] Interestingly, each platform is unique as far as the apps and devices it works with and who will be the ultimate "owner" of the data that is accessible to the platform.[18] SAMI is the most "open" platform as it functions like cloud storage for your health information, capable of accepting data from any app, wearable or device, and performing analytics on the data that users elect to make available to the open cloud platform.[19] SAMI facilitates communication between devices, enables the portability of user data from all platforms, and has the ability to collect data from multiple devices and sources to create a better picture of one's health and fitness levels.[20] To promote greater integration, among as many devices and applications as possible, Samsung has made its SimBand technology available to all manufacturers hoping others will build mobile devices using the same framework.[21]

Similar to SAMI, Google Fit is also capable of accessing data from its own apps, wearables and devices, as well as those of third parties, and will be able to perform analytics on all collected data.[22] HealthKit, on the other hand, is a developer tool specific to the Apple iOS 8 operating system, so it is designed to only work with apps built by, or approved by, Apple.[23] Users of all three platforms will ultimately decide what information they share with the platform as well as which applications will be authorized to share data and leverage data from the platform.[24] Nonetheless, once the user shares their information, Apple and Google will gain ultimate authority over the data shared with their respective platforms.[25] Samsung, however, truly sets itself apart from the competition by allowing SAMI users to remain the "owners" of their own health data, even after it is shared with the platform, an attractive selling point for SAMI.[26] The key for users and developers is to be aware of these distinctions because data captured by each platform will be used in accordance with that platform's view on acceptable use of customer data.[27]

Based on the U.S. market shares of Google and Apple alone, the volume of health and fitness data that could be made available via their developer platforms is unparalleled. In May 2014, 52.1 percent of smartphones in the U.S. ran on Google's Android operating system, while another 41.9 percent ran on Apple's iOS.[28] Together, that means 160 million

smartphones, or 94 percent of the smartphones sold to U.S. subscribers, run on an Android or iOS operating system.[29] That only accounts for shares of the domestic market. Mid-2014 projections estimated Google's Android would reach 80 percent of the global smartphone market by the end of 2014, and Apple would hold another 14.8% globally.[30]

There is a downside to (health) data sharing (but don't worry, there's an app for that).

Handling health data is a complicated task at any level, but the volume of data that may be accessible by these platforms makes health information privacy a huge undertaking for these tech giants, particularly when you consider HealthKit is Apple's first foray into the health care space and Google Fit is only Google's second (Google abandoned the aptly named, but otherwise unsuccessful, "Google Health" in January 2012).[31] Apple seems to have recognized the impending hurdles and has partnered with Epic Systems and IBM, no strangers to health data.[32] Notwithstanding any strategic partnerships, none of the developer platforms have offered app developers any solutions for protecting patient privacy and meeting standards imposed by HIPAA.[33] That said, not all developers will need a solution.

HIPAA imposes technical, administrative and physical safeguard requirements for storing and transmitting Protected Health Information (PHI) and limits the use and disclosure of such data.[34] Mobile health apps capture a wide range of user data, from calories consumed, miles run, and steps climbed, to more sensitive information, such as medical diagnoses and prescription medications taken.[35] Not all of the data captured will fall under HIPAA, so it is important for developers to gain an understanding of what PHI is and whether their applications could maintain or transmit it.[36]

PHI is individually identifiable health information (IIHI) that is transmitted or maintained in any form or medium, including electronic media, by a "covered entity" or a "business associate."[37] IIHI refers specifically to data that (i) identifies an individual, or reasonably could identify an individual; and (ii) relates to the individual's demographics, physical or mental health, or the provision of, or payment for, health care.[38] Since there is no PHI without individually identifiable information, it is also important to be familiar with "de-identification." De-identification refers to the removal of certain identifiers from a data set, such as names, cities, dates or social security numbers, so that an individual who could have been identified by the data set before de-identification could no longer be identified after de-identification.[39] Therefore, if circumstances allow for removal of certain data elements from a set of data, de-identification may be an option for avoiding HIPAA altogether.[40]

For example, where a health care provider transmits a patient's PHI to another health care provider, the transmission will be governed by HIPAA and would have to meet certain privacy and security requirements. However, if the health care provider sending the data first removed a number of identifiers from the data so the recipient could no longer identify who the patient was, then transmission of the data would not be governed by HIPAA and the health care provider would not be required to comply with any HIPAA requirements in transmitting or storing the data.

In addition to understanding *what* type of information HIPAA applies to, developers must also understand *who* needs to comply with HIPAA's standards.[41] Originally, HIPAA only applied to "covered entities," *i.e.*, health plans, health care clearinghouses, and health care providers.[42] Recently, however, HIPAA's reach was expanded by the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH Act).[43] The HITECH Act called for "business associates" of covered entities to comply with HIPAA as well.[44] A covered entity's business associate is any person or entity that "creates, receives, maintains, or transmits" PHI on behalf of a covered entity, without being an employee of that covered entity. HITECH also expanded the definition of business associate to include persons or entities that perform services for, or on behalf of, business associates, such as vendors or subcontractors, if they create, receive, maintain, or transmit PHI.[45] Basically, HIPAA could apply to just about everyone now.

Here are a few extra points for developers to consider in determining whether their apps need to comply with HIPAA. First, at least with respect to HealthKit and SAMI, these platforms were designed to enable users to not only collect their health data and transmit that data to their health care providers via the apps on the platform, but also support transmission of patient health data *by a health care provider.*[46] In fact, in late 2014, the European Commission released a green paper in which it estimated a total of 97,000 health apps were available, 70 percent targeting the consumer wellness and fitness market and 30 percent targeting health care professionals.[47] These 30 percent of *m*health apps include providing easier access to patient data, electronic patient consultation and monitoring, digitizing diagnostic imaging, or providing

information regarding pharmaceuticals and enabling e-prescribing.[48]

Another important point for developers to understand is that an entity can be a business associate if it maintains PHI on behalf of a covered entity, or another business associate, *even if that entity never views the PHI.*[49] For instance, cloud computing storage providers will be considered business associates if they have covered entity or business associate customers and those customers store PHI with the storage provider, even if the storage provider, *as a rule,* does not access customer data.[50] Finally, developers should be aware that intent plays no part in determining whether a HIPAA violation has occurred, though it does factor in to the penalties for a violation.[51] *This is why it is important to consider* whether it is possible *for an app to create, receive, maintain or transmit PHI for, or on behalf of, a covered entity or a business associate.* If it is possible*, then the safe bet is to make that app HIPAA compliant.*

If a developer determines that it functions as a business associate, it should be aware that its vendors or subcontractors that create, receive, maintain or transmit PHI on the developer's behalf, are also business associates and must also comply with HIPAA's requirements.[52] *Developers have a personal stake in their vendors' compliance because they can be held liable for HIPAA violations committed by their vendors.*[53]

While Google, Apple, and Samsung have not addressed HIPAA issues facing users of their platforms outright, brand new compliance solutions are already emerging.[54] One solution that was introduced July 2014 is Medable, a startup from Palo Alto offering a platform service that is expected to assist developers in making existing mobile digital health applications HIPAA-compliant and assist in creating HIPAA-compliant apps from scratch.[55] Medable's plans include offering full support applications to allow patient to provider and community communication as well as data sharing via wearables, implantables, and other devices.[56] Another solution, TrueVault, is said to offer a secure HIPAA-compliant application programming interface (API) for storing health data.[57] Developers can use these and other solutions to address privacy and security issues without the need to become data security experts.[58]

Considering the following two questions will help developers determine which apps in development they should worry about, which they shouldn't, and when it might be time to call the experts:

(i) Could the app create, receive, maintain or transmit Protected Health Information?

(ii) If so, would the app do so on behalf of a covered entity or business associate?

Health care's relationship with health tech.

Despite the buzz surrounding *m*health, the "traditional" Life Sciences industry has a reputation for playing the tortoise to health tech's hare, a cautious approach more than justified in light of the strict regulations imposed on the industry by the FDA, HHS, OIG, FTC, and other agencies. Interestingly, unverified reports released in late 2014 suggested the FTC already sought assurances directly from Apple that it would prevent sensitive health data collected by its upcoming smartwatch and other devices from being used without owners' consent.[59] That said, the future of health care calls for the types of advantages that mobile health apps now offer, especially the ability for health care providers to monitor patients, particularly those that suffer from chronic conditions, without requiring in-office visits as well as a low cost and convenient method for assisting patients with prevention and early detection of major health events, among countless other benefits.

The recent buzz around the new developer platforms, and other developments making the technology more accessible on an individual level, such as advancements in wearables, have informed even the less tech savvy about the potential benefits of *m*health. A recent study demonstrated the potential for significant health benefits and cost savings, not only for patients but for health care systems, through programs which use wearables and *m*health apps to monitor and communicate with patients outside of regular office visits to improve patient management of chronic conditions.[60] Over only six months, the study resulted in improvements in patient health translating into savings of $1,000 or more per patient from doctor visits and treatments that could be avoided as a result of a program with a cost of only $300 per patient.[61] For an industry shifting from a pay per procedure system to a pay for value system, when value is measured in terms of actual benefit to a patient's health, these study results offer the kind of numbers that should get the whole industry thinking mobile.

1. Nanette Byrnes, *Mobile Health's Growing Pains*, 117 MIT Tech. Rev., no. 5, Sept./Oct. 2014 at 7, 8, *available at* http://www.technologyreview.com/news/529031/mobile-healths-growing-pains/.
2. *See* Food and Drug Administration (FDA), *Mobile Medical Applications - Guidance for Industry and Food and Drug Administration Staff ("Mobile Medical App Guidance")*, (Sept. 25, 2013), *available at* http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM263366.pdf; Sabrina Tavernise, *F.D.A. Will Apply Its Rules To Only Some Health Apps*, N.Y. Times,

Sept. 24, 2013, at A12, *available at* http://www.nytimes.com/2013/09/24/health/fda-to-regulate-only-some-health-apps.html?_r=2&.

3. *Id*.
4. *Id*. Notably, in December 2014, U.S. Senators Michael Bennet (D-CO) and Orrin Hatch (R-UT) introduced the Medical Electronic Data Technology Enhancement for Consumers' Health ("MEDTECH") bill, which "would exempt low-risk medical software and mobile apps from FDA regulation and provide greater certainty regarding what software will be regulated by the agency to protect consumers." *See*, *Bennet, Hatch Introduce Bill to Cut Red Tape, Boost Innovation in Health IT*, Jan 2, 2015, *available at* http://www.bennet.senate.gov/?p=release&id=3192. According to Senator Bennet's website, MEDTECH will clarify the FDA's role in conjunction with the regulation of "wellness and lifestyle products" and "software that aids health care providers in developing treatment recommendations for their patients." More specifically, MEDTECH will, among other things, clarify that "products for use in activities unrelated to the clinical treatment of a disease or disorder and that are for the purpose of maintaining health and conditioning" will not be considered covered devices under the Federal Food, Drug and Cosmetic Act. *The Medical Electronic Data Technology Enhancement for Consumers' Health (MEDTECH) Act*, S. 2977, 113th Cong. (2014), *available at* http://thomas.loc.gov/cgi-bin/bdquery/z?d113:s2977.
5. *See, e.g.,* Aditi Pai, *Google unveils Google Fit, a fitness platform for developers*, MOBIHEALTHNEWS, (June 25, 2014), *available at* http://mobihealthnews.com/34430/google-unveils-google-fit-a-fitness-platform-for-developers/; Nathanael Arnold, *Google Fit to Challenge Apple and Samsung in Health-Tracking Arena*, WALL ST. TECH CHEATSHEET, (June 13, 2014), *available at* http://wallstcheatsheet.com/technology/google-fit-to-challenge-apple-and-samsung-in-health-tracking-arena.html/?a=viewall; Parmy Olson, *Exclusive: Google Wants To Collect Your Health Data With 'Google Fit,'* FORBES, (June 12, 2014, 6:00 PM), *available at* http://www.forbes.com/sites/parmyolson/2014/06/12/exclusive-google-to-launch-health-service-google-fit-at-developers-conference/.
6. *See* Brian Dolan, *Samsung unveils prototype health device a week before Apple's expected Healthbook launch*, MOBIHEALTHNEWS, (May 29, 2014), *available at* http://mobihealthnews.com/33595/samsung-unveils-prototype-health-device-a-week-before-apples-expected-healthbook-launch/; Michelle Maisto, *Apple, Samsung Taking Different Roads to Consumer Health Empowerment*, EWEEK.COM, (Sep 6, 2014), *available at* http://www.eweek.com/mobile/apple-samsung-taking-different-roads-to-consumer-health-empowerment.html.
7. *See* Arnold, *supra* note 5.
8. *See* Dan Diamond, *Apple's HealthKit Is Finally Here -- After Bugs, Botches, And Boatloads Of Apple Hype*, FORBES, (Sept. 26, 2014, 6:12 AM), *available at* http://www.forbes.com/sites/dandiamond/2014/09/26/apples-healthkit-finally-arrives-after-bugs-botches-and-boatloads-of-apple-hype/; Alyssa Bereznak, *Apple HealthKit vs. Google Fit: Survival of the Fittest*, YAHOO.COM, October 30, 2014, *available at* https://www.yahoo.com/tech/apple-health-vs-google-fit-survival-of-the-fittest-101279995574.html.
9. *See* Jeff Danley, *What Google Fit and HealthKit Mean for the Future of Pharma Companies*, (July 28, 2014), *available at* https://www.linkedin.com/today/post/article/20140728170449-521552-what-google-fit-and-healthkit-mean-for-the-future-of-pharma-companies.
10. *See id.*
11. *See, e.g.*, Mark Sullivan, *Sorry, but doctors aren't interested in your FitBit data*, MEDCITY NEWS, (August 15, 2014, 1:41 PM), *available at* http://medcitynews.com/2014/08/guess-doctors-dont-care-fitbit-data/.
12. Simon Khalaf, *Health and Fitness Apps Finally Take Off, Fueled by Fitness Fanatics*, FLURRY (June 19, 2014), *available at* http://www.flurry.com/blog/flurry-insights/health-and-fitness-apps-finally-take-fueled-fitness-fanatics#.U_TVg_RDt8F.
13. *See* Byrnes, *supra* note 1, at 7.
14. *See generally,* John Cox, *Will federal privacy rules afflict Apple's new iOS HealthKit?*, NETWORK WORLD, (June 5, 2014, 8:53 AM), *available at* http://www.networkworld.com/article/2360163/wireless/will-federal-privacy-rules-afflict-apple-s-new-ios-healthkit-.html#social.
15. *See* Byrnes, *supra* note 1, at 8.
16. *See* 45 C.F.R. § 160.402(c)(2).
17. *See* Arnold, *supra* note 5.
18. Matt Weinberger, *The Samsung Simband is cool, but the health platform is* cooler, CITEWORLD.COM (May 28, 2014), *available at* http://www.citeworld.com/article/2198148/internet-of-things/samsung-sami-health-data-platform.html.
19. *Id*.
20. *Id.*
21. *Id.*
22. *See* Arnold, *supra* note 5.
23. *Id*.
24. *See* Danley, *supra* note 9 (discussing HealthKit and Google Fit); Weinberger, *supra* note 18 (discussing SAMI).
25. *See* Ewan Spence, *Google Fit vs Apple HealthKit: Developers Get Preview Access To The Next Smartphone Battleground*, FORBES, (Aug. 7, 2014, 8:15 PM), *available at* http://www.forbes.com/sites/ewanspence/2014/08/07/google-fit-vs-apple-healthkit-developers-get-preview-access-to-the-next-smartphone-battleground/.
26. *See* Weinberger, *supra* note 18.
27. *See* Spence, *supra* note 25.
28. Jess Bolluyt, *Apple Holds Its Lead Over Samsung in U.S. OEM Market Share*, WALL ST. TECH CHEATSHEET, (July 5, 2014), *available at* http://wallstcheatsheet.com/technology/apple-holds-its-lead-over-samsung-in-u-s-oem-market-share.html/?a=viewall.
29. *See id.*
30. *See* Olson, *supra* note 5.
31. *Data-Driven Health Care: Companies to Watch*, 117 MIT TECH. REV., no. 5, Sept./Oct. 2014 at 15, 16, *available at* http://www.technologyreview.com/businessreport/data-driven-health-care/free/.
32. *See* Shaun Sutner, *Apple-Epic-IBM intent on dominating mHealth market*, TECHTARGET, (Aug. 4, 2014), *available at* http://searchhealthit.techtarget.com/news/2240226156/Apple-Epic-IBM-intent-on-dominating-mHealth-market.
33. *See* Jess Bolluyt, *Health Data Startup Addresses HIPAA Issues Apple Hasn't*, WALL ST. TECH CHEATSHEET, (July 16, 2014), *available at* http://wallstcheatsheet.com/technology/health-data-startup-addresses-hipaa-issues-apple-hasnt.html/?a=viewall.
34. *See* U.S. Dept. of Health & Human Services, *Summary of the HIPAA Privacy Rule*, Health Information Privacy, http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html;

see generally, 45 C.F.R. 164 *et seq.*

35. Arthur Allen, *Health apps boom while regs lag*, Politico, (June 3, 2014, 7:30 PM), *available at* http://www.politico.com/story/2014/06/health-apps-boom-while-regs-lag-107345.html; *see also* Cox, *supra* note 14.
36. *See* Cox, *supra* note 14; *see also*, Bolluyt, *supra* note 33.
37. 45 C.F.R. § 160.103.
38. *Id*.
39. *Id*.
40. *See generally*, 45 C.F.R. § 164.514(a)(b).
41. *See* Cox, *supra* note 14; *see also*, Bolluyt, *supra* note 33.
42. *See* 45 C.F.R. § 160.102(a); U.S. Dept. of Health & Human Services, *supra* note 34.
43. *See generally,* 45 C.F.R. §§ 160, 164(A),(E); 45 CFR § 164.306(a).
44. *See* U.S. Dept. of Health & Human Servs., *Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules; Final Rule ("Final Rule")*, 78 Fed. Reg. 5565, 5598 (Jan. 25, 2013), *available at* http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/FR-2013-01-25.pdf.
45. *Id*.
46. *See* Bolluyt, *supra* note 33.
47. European Commission, *Green Paper*, Oct. 10, 2014, p. 6-7, *available at* http://ec.europa.eu/digital-agenda/en/news/green-paper-mobile-health-mhealth.
48. *Id*.
49. *See Final Rule*, 78 Fed. Reg. at 5572.
50. *See* Stephen Wu, *Deadline Ahead: Last-Minute HIPAA Business Associate Compliance*, Journal of AHIMA, (Sept. 11, 2013, 8:00 AM), *available at* http://journal.ahima.org/2013/09/11/deadline-ahead-last-minute-hipaa-business-associate-compliance/; *see also Final Rule*, 78 Fed. Reg. at 5572.
51. See 78 Fed. Reg. at 5580.
52. *See id*. at 5598.
53. *See id*. at 5580.
54. *See* Bolluyt, *supra* note 33.
55. *Id*.
56. *Id*.
57. *Id*.
58. *See id*.
59. *See* Christina Farr and Diane Bartz, *U.S. FTC asking Apple about health data protection*, www.reuters.com, (Nov. 13, 2014, 4:29 PM), *available at* http://www.reuters.com/article/2014/11/13/us-apple-ftc-exclusive-idUSKCN0IX2I520141113.
60. *See* Byrnes, *supra* note 1, at 8.
61. *Id.*