Bloomberg BNA

BNA's
Health Law Reporter™

Data Calling: Mobile Apps, the Explosion of Consumer-Generated Health Information and the Future of FTC Oversight



BY JENNIFER S. GEETTER, JULIA JACOBSON AND SCOTT WEINSTEIN

According to at least one recent nationwide poll, 87 percent of adults in the United States report using the Internet and 68 percent connect to the Internet with mobile devices such as smartphones or tablet computers.[1] One of the fastest growing segments of the digital marketplace is health-related apps and online information. From February 2010 to October 2013, the number of consumer health apps for tracking diet, weight and other health-related issues that were available for Apple's iPhone grew from 2,993 to 23,222.[2] The National Institutes of Health website has an estimated 55,000,000 unique monthly visitors.[3]

While consumers using health-related apps and websites may understand that the data they provide—often referred to as consumer-generated health information (CHI)—is digitally stored, they may not necessarily understand the scope of information that they actually are disclosing about themselves, nor the degree to which this information can be used to identify them and track their digital journeys across apps, online environments and commercial purchases. Health and wellness data shared through consumer websites and mobile apps may be tracked and, in many cases, collected and aggregated with data from other sources (*e.g.*, social media, public records and search engine results), as well as with purchases (cross-referenced through credit card and other payment mechanisms), and shared with advertisers and data brokers.[4]

The collection and aggregation of consumer-generated data is commonplace in other sectors of the digital economy. Many of the questions about consumer education, consumer transparency, notice and consent, and evolving privacy frameworks that are explored with respect to CHI are equally relevant in other sectors.

[1] *The Web at 25 In the U.S.*, Pew Research Internet Project, http://www.pewinternet.org/2014/02/27/summary-of-findings-3/ (Feb. 27, 2014).

Jennifer S. Geetter is a partner at McDermott Will & Emery LLP, based in Washington. She advises clients in a number of areas, including life sciences and biomedical innovation, data sharing strategies and data privacy and security. She can be reached at jgeetter@mwe.com.

Julia Jacobson is a partner in the firm's Boston office who focuses her practice on data privacy and security and software, trademark and merchandise licensing. She can be reached at jjacobson@mwe.com.

Scott Weinstein is an associate in the firm's Washington office. He can be reached at sweinstein@mwe.com.

[2] MobiHealthNews Research, Consumer Health Apps By The Numbers (2013).

[3] *See Top 15 Most Popular Health Websites*, eBizMBA, http://www.ebizmba.com/articles/health-websites (accessed Aug. 4, 2014).

[4] Marco D. Huesch, *Privacy Threats When Seeking Online Health Information*, 173 J. Am. Med. Ass'n Internal Med. 1838-9 (2013), *available at* http://archinte.jamanetwork.com/article.aspx?articleid=1710119.

 ISSN 1064-2137

That said, regulators, policy makers and advocacy organizations are increasingly concerned about whether consumers expect, and are entitled to expect, that CHI is treated differently from other types of consumer-generated content.

In her opening remarks to a May 2014 seminar entitled ''Consumer Generated and Controlled Health Data,'' Federal Trade Commission (FTC) Commissioner Julie Brill made clear that she considers CHI sensitive and in need of more careful handling than other types of consumer data.[5] During the FTC seminar, presenters also explored how the current regulatory environment allows for use and disclosure of potentially sensitive CHI in ways that consumers may not anticipate or understand[6] and whether existing privacy frameworks are appropriate for protecting CHI.[7] While the FTC seminar did not produce any specific guidance for businesses seeking to develop digital products involving CHI, the importance of the FTC seminar is clear: the FTC is watching this fast-growing segment of the digital economy.

Illustrative Example

During his annual physical, Adam learns that he is hypertensive and has high cholesterol. Adam's family history and current health status put him at high risk for heart disease. After the appointment, Adam immediately turns to the Internet for help in understanding and managing his hypertension and cholesterol. He finds and downloads two mobile apps. The first app is intended to mimic an in-person support and advocacy group: Adam can enter his medications, diet and wellness strategies into an on-line community to share and compare his experience with other app users. He does not need to share his name or other personally identifiable information to use the app. The second app electronically syncs with a separate blood pressure reader device, allowing him to track his blood pressure and pulse over an extended period of time and to share the readings directly with his doctor. To help put these measurements into greater context for his physician, the second app also incorporates a GPS-based pedometer that can record Adam's physical activity and tools to help Adam track what he eats.

Through patients like Adam, these two mobile apps are able to collect data that may help researchers better understand disease progression and management in patients that fit Adam's profile. But, despite their similarities, they present a number of different issues that underlie the challenges of data stewardship in a consumer-driven and dispersed digital environment.

Consider:

- The first app may give consumers the impression that information is collected anonymously;
- Although the FDA currently considers apps like the second app as posing lower risk to the public and deserving enforcement discretion, the FDA could change its position about whether a blood pressure-related app will be enforced as a ''medical device'';[8]
- Depending on how it is configured, the second app may function as a component of an electronic health record, and may need to meet specific requirements in light of federal-level initiatives to push for the expanded use of electronic health records;[9]
- Depending on the physician's role (if any) in making the app available, the second app may be subject to HIPAA compliance while the first app may not.
- Both apps gather CHI that could have utility outside the disease monitoring context; and
- Though some of the information collected is clearly health-related (such as blood pressure readings), other information (such as meal tracking) may have a health focus when combined with other information but is not generally considered health information.

Current Regulatory Environment for CHI

In the United States, many consumers recognize HIPAA as a law protecting the privacy and security of health information. HIPAA, however, only protects individually identifiable health information created or received by ''covered entities'' (*i.e.*, health plans, most health care providers and health care clearinghouses) and ''business associates'' (*i.e.*, the third parties that support covered entities). HIPAA's jurisdiction follows entities and not data, which means that specific data may be regulated by HIPAA in the hands of some entities but not others.

Both Commissioner Brill and the panel at the FTC seminar noted that consumers may not understand the limited circumstances in which HIPAA regulates entities that collect CHI.[10] They also noted that these consumer misunderstandings may result in inaccurate consumer expectations with respect to the privacy and security of CHI. For example, the same blood pressure reading generated by Adam (the hypothetical patient described above) likely is subject to HIPAA oversight if entered into a website or mobile app provided or arranged by Adam's physician but is not subject to HIPAA if the website or app is not a service provided or arranged by Adam's physician, *even if* Adam's physician recommended the app to him. Adam and consumers like him may not appreciate this distinction.

CHI is, however, generally regulated by the FTC pursuant to its powers under Section 5 of the Federal Trade

[5] *See* Fed. Trade Comm'n, Spring Privacy Series: Consumer Generated and Controlled Heath Data 10 (May 7, 2014), *available at* http://www.ftc.gov/system/files/documents/public_events/195411/2014_05_07_consumer-generated-controlled-health-data-final-transcript.pdf [hereinafter Transcript].

[6] *See id*. at p. 15.

[7] *See id*. at pp. 71-72.

[8] U.S. Food & Drug Admin., Mobile Medical Applications: Guidance for Industry and Food and Drug Administration Staff 8 (2013), *available at* http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM263366.pdf; *See also Mobile Medical Applications*, U.S. Food & Drug Admin., http://www.fda.gov/MedicalDevices/ProductsandMedicalProcedures/ConnectedHealth/MobileMedicalApplications/default.htm (last updated June 4, 2014).

[9] *What is Meaningful Use*?, U.S. Dep't of Health & Human Servs., Office of the Nat'l Coordinator for Health Info. Tech., http://www.healthit.gov/providers-professionals/ehr-incentives-certification (last updated Apr. 4, 2014).

[10] *See, e.g.*, Transcript at p. 8.

   ISSN 1064-2137

Commission Act (the FTC Act).[11] The FTC Act empowers the FTC to enjoin unfair and deceptive business practices. In general, a business practice is unfair if it causes or is likely to cause substantial injury to consumers, cannot be reasonably avoided by consumers and is not outweighed by countervailing benefits to consumer or business competition. A business practice is deceptive if a material representation, omission or practice misleads or is likely to mislead a consumer and the consumer's interpretation of the representation, omission or practice is reasonable under the circumstances.

The FTC has used its regulatory authority to bring numerous actions against businesses operating digital services that have failed to clearly and conspicuously disclose their information collection, use and sharing practices or failed to adhere to the privacy statements displayed on and in their websites or mobile applications.[12] States also have the power to regulate CHI under state consumer protection laws, which, like Section 5 of the FTC Act, prohibit unfair and deceptive trade practices.[13] In July 2013, Illinois Attorney General Lisa Madigan used this power to request from eight health-related websites details about their data processing practices, including ''consumers' health-related information''—in other words, the same CHI that was the subject of the FTC seminar.[14] Specifically, Attorney General Madigan asked for details about how CHI and other information is used and shared and ''the percentage of users'' who clicked through to each website's privacy policy. She noted that ''the disclosures about capturing and sharing [consumers'] information are often buried in privacy policies not found on websites' main pages.''[15]

Defining Health Information

Amid policy and regulatory discussions of how to protect CHI lurks a difficult question: what type of information constitutes consumer-generated *health* information? This question is important because health information is generally more sensitive than other types of consumer-generated information. The question is difficult because, once information is health information, the degree to which it is sensitive varies depending on the individual from whom it is collected and the context in which it is collected and used.

Some types of information are clearly health related, such as traditional medical information or consumer content specifically provided in response to health and wellness questions. Wellness information, such as information about diet and exercise, also is health related. Information disclosed in one context, such as shopping habits, may not look like health information, but when integrated with other information, such as the health-related mobile apps downloaded by a consumer, may become health information or may be considered sensitive by the consumer disclosing it.

During the seminar, Commissioner Brill and the panel discussed scenarios in which data collectors are able to make inferences about a person's health by gathering sufficient information from non-health sources. Commissioner Brill described how using information on the frequency of an individual's online clothing shopping, his or her fast food purchases and whether the individual subscribes to premium cable television, a marketing company was able to more efficiently find and recruit obese participants for clinical trials.[16] Additionally, supermarket rewards card programs have been used to infer significant information about a person's health. For example, the sudden elimination of gluten products from a consumer's purchase history could indicate the start of a diet or a diagnosis of celiac disease.

Some consumers may reveal health information without even realizing it. Information may, for example, take on the attributes of genetic information in certain contexts: a Facebook post announcing that a daughter is ''walking for Mom'' in a breast cancer walk may suggest, inadvertently, a family history of breast cancer (*i.e.*, genetic information). Because of the speed of access in the digital ecosystem, consumers may not always have or take the opportunity to carefully consider the health implications of the information that they elect to share.

Notice and Consent

The FTC seminar also included significant discussions of the role of notice and consumer consent in forward-looking privacy protections. In a recent report on Big Data, the White House suggested that a traditional notice-and-consent model may have limited utility in the realm of Big Data.[17] Presenters at the FTC seminar were not so ready to signal the need for a new framework but did discuss some of the challenges of the notice and consent model.[18]

Panelists suggested that collectors of CHI could use simplified privacy statements or ''just-in-time notifications'' (i.e., notices presented as the data is collected) to more effectively inform consumers about the collection and sharing of their information.[19] Questions remain, however, about whether such notices could capture the

[11] 15 U.S.C. § 45(a) (2012).

[12] *See, e.g.*, Snapchat Inc., File No. 132-3078 (Fed. Trade Comm'n May 14, 2014) (agreement containing consent order), http://www.ftc.gov/system/files/documents/cases/140508snapchatorder.pdf; Google, Inc., Docket No. C-4336, File No. 102-3136 (Fed. Trade Comm'n Oct. 13, 2011) (decision and order), http://www.ftc.gov/sites/default/files/documents/cases/2011/10/111024googlebuzzdo.pdf ; Sears Holding Mgmt. Corp., Docket No. C-4264, File No. 082-3099 (Fed. Trade Comm'n Aug. 31, 2009) (decision and order), http://www.ftc.gov/sites/default/files/documents/cases/2009/09/090604searsdo.pdf.

[13] Nat'l Consumer Law Ctr. Inc., Consumer Protection in the United States: A 50-State Report on Unfair and Deceptive Acts and Practices Statutes (2009).

[14] *See* Press Release, Lisa Madigan, Ill. Att'y Gen., Popular Health Websites Must Ensure Privacy of Users' Health Information (July 12, 2013), *available at* http://illinoisattorneygeneral.gov/pressroom/2013_07/20130712.html. The eight websites that received these letters are WebMD.com, weightwatchers.com, drugs.com, menshealth.com, mayoclinic.com, about.com, health.com and mercola.com.

[15] *See* Letter from Lisa Madigan, Ill. Att'y Gen., to David Schlanger, Interim C.E.O., WebMD (July 11, 2013), *available at* http://illinoisattorneygeneral.gov/pressroom/2013_07/Information_Request_to_WebMD.pdf.

[16] *See* Transcript at p. 9.

[17] Exec. Office of the President, Big Data: Seizing Opportunities, Preserving Values 54 (May 2014), *available at* http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf [hereinafter White House Big Data Report].

[18] *See, e.g.*, Transcript at p. 71.

[19] *See, e.g.*, Transcript at p. 72.

complexities of the type of collection and sharing of information with so-called downstream entities, i.e., entities that receive data from the original data collector, rather than directly from the data source (consumers). Panelists also discussed the potential role of user fees; consumers could opt to pay a user fee and restrict whether and how their data are shared or consumers could download and use the app for free in exchange for more fluid downstream data use.

The panel discussion highlights a key dilemma: the need to be transparent with consumers about data sharing and use without hampering downstream beneficial research and marketing services that currently require combining different data sources. While this dilemma applies to other types of consumer-generated information, its effect on CHI is particular complex because of the societal benefits arising from the use of data for diagnosis, cure, treatment and prevention of disease.[20]

Data Identifiers

The FTC seminar also explored the meaning of ''anonymized'' and ''de-identified'' in the current digital landscape. The former term is often found in consumer-facing privacy policies to express to users that, when the website or mobile app operator shares data collected from consumers, their identities are not revealed. The latter term describes a standard under HIPAA for stripping data of unique identifiers.

As recently expressed in the White House Big Data Report,[21] the term ''anonymized'' may lose its meaning because data brokers can accumulate data about a person from multiple sources. Presenting an analysis conducted by the FTC's Mobile Technology Unit, Jah-Juin (Jared) Ho, attorney for the Mobile Technology Unit, showed how four of 12 mobile apps analyzed were collecting information tied to device-specific and consumer-specific identifiers and how these 12 apps transmitted information to 76 different third parties. Ho noted that, although a device-specific identifier does not reveal a consumer's identity, data brokers can combine increasing amounts of data about an individual until identification is possible.[22]

In her presentation, the FTC's chief technologist, Latanya Sweeney, Ph.D., described how, with a simple application and payment of a fee, her team obtained hospital discharge data maintained by state departments of health under varying privacy controls.[23] Using one such data set that contained a patient's age, ZIP code and month of discharge, Sweeney showed that this information could be re-identified by comparing it to publicly available databases.

A common theme between Sweeney and Ho's presentations is data they observed were not de-identified to the HIPAA standard because the data were held by a non-HIPAA-regulated entity. The HIPAA de-identification standard would typically require the stripping of more identifiers, including ZIP code, device-specific identifier and month of discharge, before the information is freely shared. Thus, whether concerns regarding re-identification of CHI persist if HIPAA standards apply is unclear.

During the panel discussion, Joseph Hall, the chief technologist at the Center for Democracy & Technology, highlighted the FTC's de-identification guidance from a 2012 FTC report.[24] This report did not call for a defined de-identification standard like HIPAA, but challenged companies to take reasonable measures to ensure the data are de-identified, publicly commit not to re-identify the data and, perhaps most importantly, contractually prohibit downstream recipients from trying to re-identify data.[25] The FTC framework offers flexibility for different industries to adopt a de-identification standard based on the sensitivity of the data being shared and the risk of re-identification. Privacy advocates, however, question whether contractual obligations are sufficient to prevent purposeful or accidental re-identification as increasing amounts of consumer data are gathered and aggregated.

Together, these presenters and the panel discussion highlight the limitations of the concepts of anonymous and de-identified data and the caution with which those terms should be used in describing data-sharing practices to consumers.

Conclusion

The proliferation of CHI clearly has caught the attention of government regulators. In many cases, the attention is positive, such as the Department of Health and Human Services's enthusiasm toward mobile health applications and its messaging that consumer access to health information empowers patients to proactively participate in their own treatment.[26] At the same time, the FTC appears to be concerned about potential harms arising from the storage and sharing of health-related information outside of a HIPAA-regulated environment and how to strike a regulatory balance between promoting the development and use of digital services that generate CHI and protecting the privacy of the consumers from whom the information is generated.

Whether the FTC will undertake regulatory and/or enforcement action about CHI is unclear. Some of the comments submitted in response to the FTC seminar support new legislation, while others support extending existing laws and regulations to the CHI context.[27] As the FTC considers its next steps, the following proactive

---

[20] *See, e.g.*, Comments by Med. Device Privacy Consortium, NetChoice, U.S. Chamber of Commerce, and Computer & Communications Indus. Ass'n, #547: Request for Comments and Announcement of FTC Workshop on Spring Privacy Series: Consumer Generated and Controlled Health Data, http://www.ftc.gov/policy/public-comments/initiative-547 (last accessed Aug. 12, 2014).

[21] *See* White House Big Data Report at 8-9, 54.

[22] *See* Transcript at p. 28.

[23] *See* Transcript at pp. 15-18.

[24] Fed. Trade Comm'n, Protecting Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers 21 (2012), *available at* http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

[25] *Id.*

[26] U.S. Dep't of Health and Human Servs., Office of the Nat'l Coordinator for Health Info. Tech., Fact Sheet: Using Technology to Manage Your Health Care, *available at* http://www.healthit.gov/sites/default/files/2013_0809_consumer_fact_sheet_final.pdf (accessed Aug. 7, 2014); *HHS Text4Health Projects*, U.S. Dep't of Health and Human Servs., http://www.hhs.gov/open/initiatives/mhealth/projects.html (accessed Aug. 7, 2014).

[27] See Fed. Trade Comm'n, #547: Request for Comments and Announcement of FTC Workshop on Spring Privacy Series: Consumer Generated and Controlled Health Data, http://

   ISSN 1064-2137

steps may help a mobile app, website or other digital service operator handling CHI avoid regulatory scrutiny:

- Evaluate representations in privacy policies about CHI and take steps to improve company transparency with respect to data-sharing practices.
- Assess and modify as needed representations in privacy statements about sharing only ''anonymous'' or ''de-identified'' data, as well as current de-identification or anonymization methods in light of increasing skepticism about the efficacy of de-identification in a digital environment.
- Consider implementation of the best-practice ''minimum necessary'' approach to consumer data capture in general and/or sharing CHI in particular.
- Re-evaluate contractual requirements about how downstream entities use and disclose CHI and determine whether representations made to consumers at the time of collection match long-term strategic priorities and vendor contracts.
- Examine and coordinate the terms of use, privacy statement and notice of privacy practices presented for each digital service to clarify which set of privacy protections control each encounter with the digital service.

With these proactive steps, companies collecting, using and sharing CHI might reduce the risk of a privacy incident or data use misunderstanding that can damage a company's reputation with consumers and investors.

---

www.ftc.gov/policy/public-comments/initiative-547 (last accessed Aug. 12, 2014).