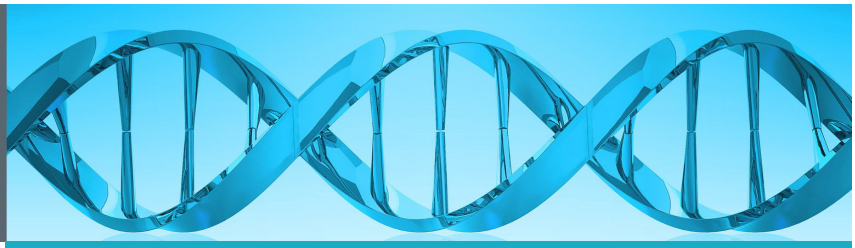
POLSINELLI

in the news

Health Care



August 2016

Agencies Encourage New Privacy Regulations to Close the mHealth Black Hole and Keep Pace with Evolving Technologies

In this Issue:

On July 19, 2016, the ONC[1] submitted a report to Congress which suggests that health privacy regulations soon may be revised to catch up with the universe of mHealth technologies that now use and share personal health data[2]. The report, titled Examining Oversight of the Privacy and Security of Health Data Collected by Entities (the "*Report*"), was drafted by the ONC in collaboration with the Office for Civil Rights ("*OCR*") and US Federal Trade Commission ("*FTC*"). The Report summarizes the regulatory construct currently protecting the privacy of personal health information held by covered entities (and their business associates)[3] and outlines the agencies' concerns regarding the lack of similar regulatory oversight over health data usage by mHealth technology developers and other businesses falling outside the scope of HIPAA[4] (each, referred to as a "*Non-Covered Entity*" or "*NCE*").

Since HIPAA's passage in 1996, health data usage has evolved beyond the simple chart review in the doctor's office or processing of an insurance claim. Scores of new businesses and technologies have emerged that utilize health data in increasingly innovative ways. Now, health data is collected by data aggregators and mined by data analysts for scores of new, innovative purposes—such as, market forecasting and development, advertising, clinical research, predictive analytics for the development of new treatment protocols or clinical decision support algorithms, and structuring patient populations for accountable care organizations. Yet, federal privacy regulations have not evolved to keep pace. The report correctly notes that federal privacy regulations have yet to contemplate the existence of "mHealth technologies" (entities that collect personal health records ("*PHRs*") and cloud-based or mobile software tools that collect health

information directly from individuals and enable health data sharing outside of the traditional healthcare provider context (i.e. wearable fitness trackers)) or "health social media" (websites that encourage health data sharing directly by users). Most actions by these entities, as Non-Covered Entities, are not regulated by HIPAA. While a patchwork of federal and state laws do govern some NCE data practices, rather than enhance privacy protections, the inconsistencies between laws mostly generate confusion among mHealth technology developers and consumers, thereby encouraging risky data management practices by both (e.g. businesses fail to develop security protocols believing they are exempt from HIPAA; consumers input health data into wearable trackers believing HIPAA protects its further disclosure when it does not).

As a first step to a solution, the Report seeks to detail the current gaps in policies governing access, security, and privacy of personal health data. Specifically, the ONC identifies five (5) major areas in which an individual's right to control his or her health data differs markedly based on whether the health data is held by a covered entity (governed by HIPAA) versus an NCE. The five 'gaps in oversight' identified are as follows:

- **Differences in Individual's Right of Access.** First, under current federal laws, an individual's right to access their own health data is not guaranteed when the health data is held by an NCE. When health data is possessed by a covered entity or business associate, HIPAA grants the patient a suite of rights with respect to that data, including a right to access, review, and (in certain instances) request revision of their own health data. But, these rights do not exist when data is held by an NCE (such as a mHealth App or wearable fitness tracker) unless the NCE is acting as a business associate under HIPAA. Typically, NCEs are not subject to HIPAA and, therefore, are not required by law to provide equivalent rights to individuals. Thus, an individual may input their health data into an iphone application or personal health record operated by an NCE and lose the ability to later obtain a copy of the underlying health data, revise the health data to delete inaccuracies, or learn where their health data has been re-disclosed by the NCE vendor, let alone restrict its re-disclosure.

- **Differences in Individual's Right to Control Third Party Use of Data.** Second, an individual's ability to control third party use of their health data is markedly less when the health data is held by an NCE versus a covered entity (or business associate). The HIPAA rules restrict a covered entity's (or business associate's) ability to re-disclose an individual's health data. Yet, once the health data is shared by an individual/consumer with an NCE, HIPAA does not apply to constrain further use or sharing of the data with third parties. Consequently, once a person provides health data to an NCE, he or she loses many of the re-disclosure protections offered by HIPAA (such as HIPAA's protections against unwanted marketing). Then the relationship between the individual and NCE defaults to the Terms of Use, which controls the permitted uses of data. Only if the NCE discloses consumer health data contrary to its Terms of Use, could the FTC pursue the NCE for a violation of Section 5 of the FTC Act; but, the FTC Act, unlike HIPAA, offers no ability to prohibit a downstream recipient's further use of the health data once it is in the downstream recipient's hands.

- **Differences in Security Standards.** Third, NCEs are not required to adhere to the same security standards and safeguards as those imposed by HIPAA and the HITECH Act. Consequently, NCEs are unlikely to protect health

data to the same degree. In particular, an ONC study found that NCE vendors engage in varying levels of encryption—which is considered a best practice for protecting health data. Some Private Health Record ("PHR") vendors (which are NCEs) do not encrypt data at all; while, others fail to describe their security practices in their Terms of Use to indicate if encryption is used or not. Other security safeguards employed also may be inadequate. Furthermore, unlike covered entities, NCEs (like PHR and mHealth technology vendors) may not embed security software, engage in risk assessments and audits, or employ adequate security policies. An ONC study found that many PHR vendors do not understand the security standards prescribed by HIPAA, suggesting they do not deploy equivalent practices.

- **Differences in Understanding of Privacy and Security Protections Terminology.** Fourth, the Report discusses the agencies' concern that mhealth technology developers and consumers typically understand little about the universe of privacy laws beyond HIPAA that may regulate their products and services. HIPAA regulates data based on both the possessor's identity (as a covered entity or business associate) and the substantive characteristics of the data (whether it constitutes PHI or not). Per the Report, this mixed approach to regulating data access and usage, when combined with the mixed legal terminology employed by the various federal privacy regulations[5], complicates layman's efforts to decipher whether their data activities are regulated by HIPAA or other privacy laws.[6] Consequently, businesses and mHealth technology developers may not understand HIPAA's scope and presume it is inapplicable; while, consumers may rely falsely on HIPAA's protections when electing to share their health data with NCEs. Further, HIPAA requires covered entities to issue privacy policies and notices that are understandable to patients. NCEs are not required by federal regulations to issue privacy policies or privacy notices that would inform consumers about the NCE's privacy practices. Consequently, notices regarding NCE privacy practices are often missing, hidden, or deficient. The Report cited a study concluding that only 30.5% of mHealth apps had privacy policies and most were incomprehensible to the average consumer.[7] The Report noted that NCE privacy policies are also often purposefully difficult to locate. As a result, the agencies believe that most consumers are ill-informed about the health data usage practices of the mHealth technologies with which they share their information.

- **Inadequate Data Collection, Usage, and Disclosure Limitations.** The Report noted that NCEs, which operate outside of HIPAA, often engage in online advertising, marketing, behavioral tracking practices, and re-selling of data with deficient notices or opt-out provisions for consumers. While individuals may control what they initially share with an NCE, they likely cannot control the NCE's further use of the information once it is shared with the NCE. Further, since NCEs are not subject to HIPAA, the Report noted that it is unlikely that NCEs limit their re-disclosures of health data to others based on minimum necessary standards—the standard commonly employed across the healthcare industry. Once health data is held by an NCE, the Report noted that the health data is likely to proliferate across the public domain at a far greater rate than any health data shared with a HIPAA covered entity or business associate, compounding the risks of identity theft for users.

The Report does not go as far as to recommend solutions for the noted gaps in oversight. Yet, ONC's publication of this Report, detailing for Congress the identified gaps in privacy protections, could signal that new regulations directly or indirectly governing NCE data practices may be forthcoming. mHealth technology developers (including, vendors of personal health records, mobile health applications, wearable health data trackers, or others), websites actively collecting health data, social media health platforms (e.g. patient-peer networking websites or websites tracking biometric data), and others handling health data as non-covered entities should monitor congressional activities for any new regulatory developments that would impact their data collection, management, and sharing practices.

1 Office of the National Coordinator for Health Information Technology ("ONC") of the U.S. Department of Health and Human Services.

2 The term 'health data' is used throughout this Article as a proxy for the following legal terms: "health information", "individually identifiable health information", "protected health information", and "personally identifiable information". Since NCE's deal with health information that is not necessarily restricted to the protected health information governed by HIPAA, this broader term is used to reference the health-related information individuals share with mHealth technologies, social media, personal health records, and other NCE's.

3 See 42 C.F.R. §160.103 (HIPAA only applies to organizations known as "covered entities", defined as health plans, health care clearing houses, and health care providers conducting certain electronic transactions, and their "business associates", defined as persons or entities that perform certain functions or activities involving the use or disclosure of individually identifiable health information on behalf of or in providing services to covered entities.).

4 Health Insurance Portability and Accountability Act of 1996, Pub. L. 104-191, 110 Stat. 1936 (1996), as amended by the Health Information Technology for Economic and Clinical Health Act of 2009 ("HITECH Act") and implementing regulations (collectively, "HIPAA")

5 For example, PHI, health information, personally identifiable health information, and subsets of specifically protected information (AIDS and HIV related information, information related to sexually transmitted diseases, genetic information, mental health diagnosis and treatment, etc.

6 The following legal terms are used to refer to an individual's health information in laws and regulations; yet, carry different legal rights and obligations which may confuse consumers and product developers: "health information", "individually identifiable health information", "protected health information", and "personally identifiable information".

7 Report at 25 citing Ali Sunjaev, et. al, Availability and Quality of Mobile Health App Privacy Policies, J. of Am Informatics Assn. available at http://www.ncbi.nlm.nih.gov/pubmed/25147247.

POLSINELLI

real challenges. real answers. SM

For More Information

For questions regarding this information, please contact one of the authors below, a member of Polsinelli's Health Care practice, or your Polsinelli attorney.

Erin Fleming Dunlap
314.622.6661
edunlap@polsinelli.com

Laura Little
404.253.6055
llittle@polsinelli.com

Zuzana S. Ikels
415.248.2114
zikels@polsinelli.com

Sidney Welch
404.253.6047
swelch@polsinelli.com

To contact a member of our Health Care team, click here or visit our website at www.polsinelli.com > Services > Health Care Services > Related Professionals.

To learn more about our Health Care practice, click here or visit our website at www.polsinelli.com > Services > Health Care Services.

POLSINELLI
real challenges. real answers. SM

About Polsinelli's Health Care Practice

The Polsinelli Health Care practice represents one of the largest concentrations of health care attorneys and professionals in the nation. From the strength of its national platform, the firm advises clients on the full range of hospital-physician lifecycle and business issues confronting health care providers across the United States. Recognized as a leader in health care law, Polsinelli is ranked as "Law Firm of the Year" in Health Care by *U.S. News & World Report* (November 2014), no. 1 by *Modern Healthcare* (June 2015) and nationally ranked by *Chambers USA* (May 2015). Polsinelli's attorneys work as a fully integrated practice to seamlessly partner with clients on the full gamut of issues. The firm's diverse mix of attorneys enables our team to provide counsel that aligns legal strategies with our clients' unique business objectives.
One of the fastest-growing health care practices in the nation, Polsinelli has established a team that includes former in-house counsel of national health care institutions, the Office of Inspector General (OIG), and former Assistant U.S. Attorneys with direct experience in health care fraud investigations. Our group also includes current and former leaders in organizations such as the American Hospital Association. Our strong Washington, D.C., presence allows us to keep the pulse of health care policy and regulatory matters. The team's vast experience in the business and delivery of health care allows our firm to provide clients a broad spectrum of health care law services.

About Polsinelli

real challenges. real answers.[SM]

Polsinelli is an Am Law 100 firm with more than 800 attorneys in 19 offices, serving corporations, institutions, and entrepreneurs nationally. Ranked in the top five percent of law firms for client service*, the firm has risen more than 50 spots in the past five years in the Am Law 100 annual law firm ranking. Polsinelli attorneys provide practical legal counsel infused with business insight, and focus on health care, financial services, real estate, intellectual property, mid-market corporate, and business litigation. Polsinelli attorneys have depth of experience in 100 service areas and 70 industries. The firm can be found online at www.polsinelli.com. Polsinelli PC. In California, Polsinelli LLP.

**2016 BTI Client Service A-Team Report*

About this Publication

Polsinelli provides this material for informational purposes only. The material provided herein is general and is not intended to be legal advice. The choice of a lawyer is an important decision and should not be based solely upon advertisements.
Polsinelli PC. In California, Polsinelli LLP.

POLSINELLI
real challenges. real answers. SM