Examining Oversight of the Privacy & Security of Health Data Collected by Entities Not Regulated by HIPAA

U.S. Department of Health and Human Services

200 Independence Avenue, S.W.

Washington, DC 20201

TABLE OF CONTENTS

I. INTRODUCTION

The health information marketplace of 2016 is filled with technology that enables individuals to be more engaged in managing their own health outside of the traditional health care sphere than ever before. The wearable fitness trackers, social media sites where individuals share health information through specific social networks, and other technologies that are common today did not exist when Congress enacted the Health Insurance Portability and Accountability Act of 1996 (HIPAA) (Pub. L. 104-191).[1] While HIPAA serves traditional health care well and continues to support national priorities for interoperable health information with its media-neutral Privacy Rule, its scope is limited. It applies only to organizations known as "covered entities,"[2] health plans, health care clearinghouses, and health care providers conducting certain electronic transactions, and their "business associates," 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.[3] Today, in addition to these traditional health care organizations, scores of new businesses that collect, handle, analyze, and disclose health information about individuals have emerged. This Report: 1) analyzes the scope of privacy and security protections of an individual's health information for these new and emerging technology products that are not regulated by HIPAA; 2) identifies key gaps that exist between HIPAA regulated entities and those not regulated by HIPAA; and 3) recommends addressing those gaps in a way that protects consumers while leveling the playing field for innovators inside and outside of HIPAA.[4]

This Report focuses on "mHealth technologies" and "health social media." The former includes entities that collect or deal in personal health records (PHRs)[5] and cloud-based or mobile software tools that intend to collect health information[6] directly from individuals and enable sharing of such information, such as wearable fitness trackers. The latter includes internet-based social media sites on which individuals create or take advantage of specific opportunities to share their health conditions and experiences. Taken together, these mHealth technologies and health social media that are outside the scope of HIPAA are referred to as "non-covered entities" or NCEs. This Report does not cover products, services, and data sources where health information is derived from other data (such as GPS reporting, where one can infer an individual's physical activity, [7] or air quality reporting data from which respiratory health might be inferred), or

[1] Health Insurance Portability and Accountability Act, Pub. L. 104-191, 110 Stat. 1936 (1996).
[2] 45 C.F.R. 160.103.
[3] Individuals who are members of a covered entity's workforce are not considered business associates.
[4] This report was initially required by Congress in Section 13424 of the Health Information Technology for Economic and Clinical Health Act (HITECH Act) of 2009, and is herewith submitted, Pub. L. 111-5, Div. A, Title XIII, § 13424, Feb. 17, 2009, 123 Stat. 276. The HITECH Act was enacted as part of the American Recovery and Reinvestment Act (ARRA) of 2009.
[5] PHRs are on-line tools that consumers use to manage their health information. When not offered to a consumer by a HIPAA covered entity, the PHR is not regulated by HIPAA.
[6] This report uses the term "health information" in a generic sense to mean information about the health or health care of an individual regardless of who creates or maintains the data and not as that term is defined in the HIPAA Rules. See Analysis section, infra, pp. 21 – 22.
[7] Ralph Maddison and Cliona Mhurchu, *Global Positioning System: A New Opportunity in Physical Activity Measurement*, Int J Behav Nutr Phys Act. 2009; 6: 73 (Nov. 2009), *available at:* http://www.ncbi.nlm.nih.gov/pmc/articles/PMC2777117/.

information casually disclosed by individuals, such as a personal Facebook post that one has the flu. Products that may meet the definition of a device under section 201(h) of the Federal Food, Drug, and Cosmetic Act (FD&C Act), such as apps that can control the inflation and deflation of a blood pressure cuff or the delivery of insulin on an insulin pump, also are not discussed here, though these tools also may not be regulated by HIPAA.[8]

This Report is a snapshot as of July 2016 and is organized as follows: Section II contains an executive summary of key concepts and describes the Report's methodology. Section III outlines how health information about individuals is collected today, including a discussion of mHealth technologies. Section IV describes the federal legal landscape of health information privacy and security and summarizes the scope of HIPAA, Section 5 of the Federal Trade Commission (FTC) Act, and breach notification rules for health information about individuals that the Department of Health and Human Services' (HHS) Office for Civil Rights (OCR) and FTC have promulgated. Section V analyzes how the laws or gaps impact the privacy or security of individuals' health information in various scenarios. Finally, Section VI provides key findings and conclusions to consider as potential next steps.

II. EXECUTIVE SUMMARY

Nearly every aspect of the modern citizen's life has a virtual or electronic component. In this environment, people choose every day to share information online at the click of a button, and health care information is no exception. Sharing information electronically can offer real benefits, such as saving time, improving services, and increasing engagement.[9] However, it also exposes the shared information to additional risks. The widespread nature of this data sharing and collection in all sectors, not just the health care sector, is well documented in a recent FTC report on the Internet of Things (IOT Report).[10] This Report focuses specifically on the gaps in oversight between HIPAA-covered entities that collect health data from individuals and those that are not regulated by HIPAA.

[8] The Food and Drug Administration (FDA) published guidance that informs manufacturers, distributors, and other entities about how FDA intends to apply its regulatory authorities to select software applications intended for use on mobile platforms. FDA, *Mobile Medical Applications: Guidance for Industry and Food and Drug Administration Staff* (FDA MMA Guidance) (Feb. 9, 2015), p. 14, a*vailable at: http://www.fda.gov/downloads/MedicalDevices/.../UCM263366.pdf*.

[9] *See, e.g.*, *Are Mobile Medical Apps Good For Our Health* (March 17, 2015), *available at:* http://www.marketwired.com/press-release/are-mobile-medical-apps-good-our-health-a-new-study-research-now-reveals-that-doctors-2001197.htm.

[10] FTC Staff Report, *Internet of Things: Privacy & Security in a Connected World* (IOT Report) (January 2015), *available at*: http://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

Health information technology (health IT) allows individuals to more conveniently access and manage their health information.[11] Health IT encompasses a variety of products and services, including electronic health records (EHRs)—record-keeping systems typically found within traditional health care and thus subject to HIPAA—as well as more consumer oriented mHealth technologies.[12]

In the traditional health care industry, where care is provided by a provider or hospital and paid for through health insurance, an individual's health information is protected in three main ways: First, HIPAA, a federal law that establishes a nationwide floor of privacy and security standards, imposes protections through its implementing Privacy, Security, and Breach Notification Rules. Those rules are enforced by OCR, while criminal penalties for certain disclosures are enforced by the Department of Justice.[13] Second, the FTC enforces the FTC Act's consumer protection prohibition against acts or practices that are unfair or deceptive. These could include, for example, failing to comply with an entity's own privacy policy, deceptively failing to disclose material information about the use of personally identifiable information, or failing to reasonably secure this information. Third, approximately half the states have enacted health privacy rules that apply in addition to, and are more protective of patient privacy than, HIPAA but which concern specific clinical conditions or circumstances (HIV/AIDS status, mental or reproductive health conditions, or the health information of teenagers, for example).[14] Yet, as the electronic sharing and storage of health information increases, and as individuals become more engaged in sharing personal health information online, organizations that are not regulated by HIPAA, the FTC, or state law may collect, share, or use health information about individuals in ways that may put such data at risk of being shared improperly.[15]

---

[11] Numerous forces are driving the health care industry toward the use of health IT, such as the potential for reducing medical errors and health care costs, and increasing individuals' involvement in their own health and health care. To facilitate this advancement and reap its benefits while reducing the risks, it is important to consider individual privacy interests together with the potential benefits to population health. U.S. Department of Health and Human Services, Office of the National Coordinator for Health Information Technology (ONC), *Nationwide Privacy and Security Framework For Electronic Exchange of Individually Identifiable Health Information* (ONC P & S Framework) p. 1 (Dec. 2008), *available at:* https://www.healthit.gov/policy-researchers-implementers/nationwide-privacy-and-security-framework-electronic-exchange.

[12] Multifunctional products, such as EHRs, may have functionalities that meet the definition of a device under section 201(h) of the Food Drug &Cosmetic Act of 1938, 21 U.S.C § 301 et seq., and such device functionalities are subject to FDA oversight.

[13] *See, infra* HIPAA Jurisdiction section (section II-A) of this Report.

[14] HIPAA sets a legal floor. States are permitted to, and do, enact additional health privacy laws that provide privacy and security in excess of what is protected by or required under HIPAA. *See* 45 CFR Part 160 Subpart B; *See* NGA Center for Best Practices, *State and Federal Consent Laws Affecting Interstate Health Information Exchange* (March 2011), *available at:* http://www.nga.org/files/live/sites/NGA/files/pdf/1103HIECONSENTLAWSREPORT.PDF. *See also* ONC's *Health Information Privacy & Security Collaborative Final Report on Intra and Interstate Consent Policy Options*, *available at*: http://www.healthit.gov/policy-researchers-implementers/intrastate-and-interstate. A complete discussion of the impact of state privacy laws is beyond the scope of this Report.

[15] ONC P& S Framework, p. 5 *supra*, note 11 (noting that "if individuals and other participants in a network lack trust in electronic exchange of information due to perceived or actual risks to individually identifiable health information or the accuracy and completeness of such information, it may affect their willingness to disclose necessary health information and could have life-threatening consequences").

Challenges of Safeguarding Electronic Health Information

While technological innovation has advanced at an extraordinary pace in recent years, privacy and security protections of health information have not kept up:

New types of entities that collect, share, and use health information are not regulated by HIPAA: Health information is increasingly collected, shared, or used by new types of organizations beyond the traditional health care organizations currently covered by HIPAA,[16] such as peer health communities, online health management tools, and websites used to generate information for research, any of which might be accessed on computers or smart phones and other mobile devices. If they are not determined to be health plans, health care clearinghouses, or health care providers conducting certain electronic transactions, and they are not acting on behalf of, or providing a service to, a HIPAA covered entity, they are not subject to the HIPAA standards for covered entities and business associates. We call entities not subject to HIPAA non-covered entities or NCEs in this Report.

Individuals may have a limited or incorrect understanding of when data about their health is protected by law, and when it is not: Individuals who share their health information with NCEs might not fully understand where the protections afforded by HIPAA begin and end. They may incorrectly think HIPAA provides standards for privacy and security in all contexts where their health information is collected, shared, or used. Consequently, individuals may inadvertently consent to unanticipated types of information sharing and use by NCEs collecting their health information.[17] Although the conduct may be regulated by the FTC's consumer protection oversight, which does not depend on whether the conduct is subject to HIPAA, this oversight does not provide the same type or level of protection as HIPAA. In short, consumers may not be equipped to evaluate the privacy and security implications that attach to the NCEs with which they interact every day.

Health information collected in more places without consistent security standards may pose a cybersecurity threat (of which individuals may be unaware): As more and more data is stored electronically, and as information is stored in multiple locations, the new locations for storage and new collection points make the data increasingly vulnerable to cybersecurity attacks. Because this concern was discussed in depth in the FTC's IOT report, this Report will not examine it extensively here.[18] But it is important to note for our purposes that while HIPAA imposes security standards for individually identifiable health information held by covered entities and business associates, such legal standards do not necessarily apply to NCEs, although to the extent NCEs fail to reasonably secure consumers' personal information, they might run afoul of the FTC Act's prohibition on unfair or deceptive acts or practices described below.

---

[16] Many of these entities are covered by the FTC Act, irrespective of the fact that they are not covered by HIPAA, but the protections are not identical under the two statutory schemes.

[17] NCVHS, Letter to the Secretary Kathleen Sebelius, *Protection of the Privacy and Security of Individual Health Information in Personal Health Record*s, p. 2 (Sept. 2009), *available at*: http://www.ncvhs.hhs.gov/wp-content/uploads/2014/05/090928lt.pdf.

[18] IOT Report, pp. 10-14, *supra* note 10.

Individuals generally have greater rights regarding access to data held by HIPAA covered entities than data held by Non-Covered Entities: The HIPAA Rules give individuals specific rights to access individually identifiable health information about them held by covered entities. Those rights include the provision of the information in a timely manner, in the form and format requested by the individual if it is readily producible, and in electronic form if the information is maintained electronically. The individual also has the right to direct the covered entity to transmit a copy of the information directly to another person designated by the individual. In addition, the HHS Office of the National Coordinator for Health Information Technology (ONC) published the 2015 Edition Health Information Technology Certification Criteria Final Rule (2015 Edition Final Rule), which provides a technical standard by which individuals can take advantage of their HIPAA access rights[19] and supports the patient engagement requirements of the Medicare and Medicaid Programs Electronic Health Record Incentive Program Stage 3,[20] commonly known as the Meaningful Use program. ONC's 2015 Edition Final Rule supports the use of "Application Programming Interfaces" (APIs) to facilitate patient access to electronic health information pursuant to patients' HIPAA access rights.[21] Where HIPAA does not apply, however, it is unclear whether individuals have any rights to access data about themselves held by others. NCEs may grant individuals such access through the terms of use for their products or services, but such access may not be required by law.[22]

Lack of understanding of what rules apply may hinder economic growth and development of beneficial products that could help generate better health, smarter spending, and healthier people: Health privacy and security law experts have a reasonably clear idea of where HIPAA protections end, but the layperson likely does not. Moreover, even entrepreneurs, particularly those outside the health care industry, seeking to take advantage of health information technology and develop mHealth technologies and health social media, may not have a clear understanding of where HIPAA oversight begins and ends. This lack of clarity may impede innovation that could improve health or otherwise benefit individuals or the nation.[23] For example, for HIPAA covered entities, it is often unclear to developers which information is considered to be or defined as "individually identifiable health information" that is subject to

[19] ONC 2015 Edition Health Information Technology Certification Criteria Final Rule (ONC 2015 Edition Certification Final Rule) 80 Federal Register No. 200, 62602 (October 16, 2015), a*vailable at:* http://www.gpo.gov/fdsys/pkg/FR-2015-10-16/pdf/2015-25597.pdf.

[20] 80 F.R. 62762 (October 16, 2015)

[21] 45 C.F.R. §§ 164.524, 164.528, 164.526, 164,522, 164.530, and 160.306.

[22] *See e.g.*, University of Chicago's Contracting Over Privacy Forum (October 15, 2015), a*vailable at:* http://www.law.uchicago.edu/events/2015-10-16-contracting-over-privacy, noting that best practices regarding notice do not change consumer behavior. In the consumer reporting context, the Fair Credit Reporting Act (FCRA), 15 U.S.C. § 1681-1681x, provides consumers with certain rights regarding access and correction of credit data: *A Summary of Your Rights Under the Fair Credit Reporting Act*, www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf.

[23] Secretary's Letter to ACT (HHS Response Letter) (Nov. 21, 2014), *available at*: http://actonline.org/wp-content/uploads/2015/01/HHS-Response-Letter-to-Defazio.pdf. *See also* White House: *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy.* (February 2012), *available at:* https://www.whitehouse.gov/sites/default/files/email-files/privacy_white_paper.pdf.

protection by the HIPAA Rules, and which is not.[24] (This is discussed in detail below in section V, including examples of confusing terminology.) Additionally, if the way in which technology is used evolves over time, federal requirements for health information privacy may apply to the new uses but not the old ones, or vice versa, resulting in shifting regulatory requirements and expectations for developers and entrepreneurs.

This Report finds that large gaps in policies around access, security, and privacy continue, and finds that confusion persists among both consumers and innovators.

Methods

Beginning in 2010, ONC conducted a study reviewing and analyzing the application of privacy and security requirements to non-HIPAA covered entities and business associates.[25] The study consisted of multiple components, including a white paper exploring the privacy and security practices of entities dealing with PHRs and other NCEs.[26] ONC also leveraged existing work products and resources from the FTC, OCR, and National Committee on Vital and Health Statistics (NCVHS). Additional activities informing the study included the following:

- ONC hosted a free, day-long public roundtable, entitled "Personal Health Records – Understanding the Evolving Landscape" (PHR Roundtable).[27] The PHR Roundtable improved ONC's understanding of the latest generation of PHRs and other emerging health information technologies and assisted with the identification of privacy and security issues. The PHR Roundtable included four panels of prominent researchers, legal scholars, representatives of consumers, and industry organizations.

- In conjunction with the PHR Roundtable, ONC solicited public comment on the following issues relating to PHRs: 1) privacy and security and emerging technologies; 2) consumer expectations about collection and use of health information; 3) privacy and security requirements for NCEs; and 4) any other comments on PHRs and NCEs. In

[24] ONC *Roundtable: Personal Health Records, Understanding the Evolving Landscape* (December 3, 2010). PHR Roundtable Transcript, p. 374 (noting that "The borders are very blurred as between what health information is and what other information is, that the mode of holding information is very blurred between what an electronic health record might be, a PHR might be and any other mode, and that it's very difficult to put boundaries around these different things and to know how to manage them."), a*vailable at:* https://www.healthit.gov/sites/default/files/120310_onc_editedc.pdf.

[25] Maximus Federal Services, *Non-HIPAA Covered Entities: Privacy and Security Policies and Practices of PHR Vendors and Related Entities Report* (Maximus Report) (December 13, 2012), *available at:* https://www.healthit.gov/sites/default/files/maximus_report_012816.pdf.

[26] The Maximus Report, as well as this Report, is not intended to be a comprehensive explanation of all of HIPAA or of all laws that regulate information about individuals. Rather, the reports explain the provisions of HIPAA relevant to the Report's scope.

[27] For more information about the *Personal Health Records – Understanding the Evolving Landscape*, s*ee* ONC's PHR Roundtable Blog (Dec. 29, 2010), *available at:* http://www.healthit.gov/buzz-blog/from-the-onc-desk/personal-health-records-roundtable/. A representative from the OCR and the FTC's Bureau of Consumer Protection, Division of Privacy and Identity Protection, participated in the panel discussion regarding the federal enforcement authority of their respective agencies. Additional information about the Roundtable is *available at*: https://www.healthit.gov/policy-researchers-implementers/mobile-devices-roundtable-safeguarding-health-information

response to this inquiry, ONC received 337 public comments from a wide range of stakeholders. ONC collated and analyzed these comments and drew upon them to inform this final Report.

- OCR, in consultation with ONC, analyzed PHRs in the context of the HIPAA Privacy Rules and delineated the types of PHRs offered by HIPAA covered entities/business associates.[28] ONC drew upon the principles of the *Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information* (Privacy and Security Framework) to help inform the final recommendations included in this Report. This framework was developed by ONC to address specifically how the Fair Information Practice Principles (FIPPs) should apply in electronic health information exchange.[29]

- In March 2012, ONC hosted a Mobile Devices Roundtable, entitled "Safeguarding Health Information: Real World Usages and Real World Privacy & Security Practices." At this roundtable, consumers, developers, and privacy and security experts provided information and input about rapidly evolving mobile health technologies.[30]

- In preparing this Report, ONC engaged in extensive discussions with representatives from the FTC's Division of Privacy and Identity Protection within the Bureau of Consumer Protection and with OCR on key issues associated with the privacy and security of non-HIPAA covered entities/business associates.

III. HOW HEALTH INFORMATION ABOUT INDIVIDUALS IS COLLECTED TODAY

This section describes some of the ways in which health information is being collected by entities not subject to the HIPAA Privacy and Security Rules. In section IV, below, we discuss what rules apply to health information collected within and outside the HIPAA context.

[28] OCR issued HIPAA privacy components of the *Health IT Privacy and Security Toolkit*. U.S. Department of Health and Human Services, Office for Civil Rights, *Health IT Privacy and Security Toolkit*, a*vailable at:* http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/healthit/index.html. *Personal Health Records and the HIPAA Privacy Rule* guidance document, *available at:* http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/special/healthit/phrs.pdf. This second guidance document describes some examples of PHRs that would not be covered by HIPAA. To analyze how a covered entity might interact with a non-covered PHR, this document also discusses how HIPAA- covered entities might transfer information to a non-covered PHR.

[29] ONC P&S Framework, *supra* note 11.

[30] Materials and a transcript of the mobile health roundtable are *available at*: https://www.healthit.gov/policy-researchers-implementers/mobile-devices-roundtable-safeguarding-health-information.

One way health information is collected is through mHealth technologies, including tablets, smartphones, software applications, and wearable sensors.[31] mHealth technology allows individuals to monitor daily activities and record vital signs or other biometric data outside of equipment in their doctor's office.[32] These applications enable individuals to become more engaged in their health and serve as a means of collecting and sharing health information. Some have the ability to link to a physician's EHR system or to link to a PHR selected by the individual.[33] Some store data locally on a patient's mobile device as well as with the vendor.[34] However, these technologies may present privacy issues.[35] Absent the protections of the HIPAA Rules, device vendors may also share the data with multiple other parties, although this sharing would be subject to FTC enforcement if it were to violate the FTC's prohibition on unfair or deceptive conduct.[36]

---

[31] The House Energy and Commerce Committee sent letters to 34 application developers for Apple Inc.'s mobile devices asking about their information collection and use practices. *See* Committee on Energy and Commerce, *Ranking Members Waxman and Butterfield Launch Inquiry Into Information Collection and Use Practices of Social Apps for Apple Devices* (Mar. 22, 2012), *available at:* http://democrats.energycommerce.house.gov/index.php?q=news/ranking-members-waxman-and-butterfield-launch-inquiry-into-information-collection-and-use-pract. *See also* Conne Guglielmo, "*Congress Queries Apple, iPhone App Developers About Privacy*, Forbes (Mar. 22, 2012), *available at:* http://www.forbes.com/sites/connieguglielmo/2012/03/22/congress-queries-apple-iphone-app-developers-about-privacy/, (noting that "the members are seeking to better understand what, if any, information these particular apps gather, what they do with it, and what notice they provide to app users").

[32] Eric Wicklund, *mHealth Apps Help with Medication Adherence, Healthcare IT News* (Jan. 25, 2012), *available at:* http://www.healthcareitnews.com/news/mhealth-apps-help-medication-adherence, (noting that one mobile health technology solution that "aggregates a patient's prescription drugs and provides clear images of those drugs stored in their containers," and offers real-time connectivity as part of the medication adherence service).

[33] *See, e.g.,* Kaiser's web-based myHealth Manager PHR, *available at:* https://healthy.kaiserpermanente.org/health/care/consumer/my-health-manager.

[34] *See, e.g.,* Capzule PHR, http://www.capzule.com/phr/.

[35] *See* Chris Gullo, *Leveraging Location in Consumer Health Apps*, mobihealthnews.com (Oct. 14, 2011), *available at:* http://mobihealthnews.com/13755/leveraging-location-in-consumer-health-apps/ (referring to Tomorrow Networks, a new mobile advertising network for health care providers); The Federal Communications Commission (FCC) *Helping Consumers Harness the Potential of Location-Based Services Forum* (June 28, 2011), *available at:* http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-308022A1.pdf (participants acknowledged the trend toward collecting increasingly granular location information, emphasizing both the value of precise services and the need for user control to address the attendant privacy and security issues); Aarathi Prasad, *Exposing Privacy Concerns in mHealth Data Sharing*, Dartmouth Computer Science Technical Report TR2012-711, 3 (January 2012), *available at:* http://www.cs.dartmouth.edu/site-content/reports/TR2012-711/ (noting that individuals may share their personal information without considering the different sharing options of a mHealth solution); Groupe Spécial Mobile Association (GSMA), *Privacy Design Guidelines for Mobile Application Development* (Feb. 22, 2012), *available at:* http://www.gsma.com/publicpolicy/mobile-and-privacy/design-guidelines, (noting that even mobile "applications that legitimately access and use personal information may fail to meet the privacy expectations of users . . ."). The GSMA recently released a set of universal mobile principles that describe the way in which mobile consumers' privacy could be respected and protected.

[36] David Pogue, *Fitness Trackers Are Everywhere, but Do They Work?,* Scientific American (December 16, 2014), *available at:* http://www.scientificamerican.com/article/fitness-trackers-are-everywhere-but-do-they-work/. *See also* Nancy Shute, *Apps Can Help You Take A Pill, But Privacy's A Big Question*, SHOTS - NPR Blog (Dec. 2, 2011), *available at:* http://www.npr.org/blogs/health/2011/12/02/143005028/apps-can-help-you-take-a-pill-but-privacys-a-big-question; Eric Engleman and Adam Satariano, *Lawmakers Press Apple, Google on Privacy*, Bloomberg BusinessWeek (May 10, 2011), *available at:* http://www.bloomberg.com/news/2011-05-10/google-defends-use-of-location-data-in-congressional-testimony.html (noting that smartphone application developers often share location data with downstream advertising and analytics companies).

mHealth technology extends to applications, or "apps," that consumers download onto their smartphones or tablets.[37] When an app is not offered by a HIPAA covered entity or a business associate, it is outside the scope of HIPAA's protections. A common example is wearable fitness trackers sold to a consumer directly.[38] Where mHealth technology is used by a covered entity, such as a health care provider,[39] and that technology collects, stores, or uses individually identifiable health information, the health information on the device is protected by the HIPAA Rules. Thus, mHealth technology used by individuals to manage their own health, but not offered or provided to the individual by a covered entity or business associate, is outside of HIPAA's scope.[40] mHealth technology may, however, be subject to other federal laws, in

[37] HIPAA applies to PHI stored within these devices. HHS HIPAA Security Guidance (December 2006), *available at*: http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/remoteuse.pdf. *See* Brian Dolan and Neil Versel. *Epocrates launches EHR; iPhone App Soon* (July 27, 2011), *available at:* http://mobihealthnews.com/12150/epocrates-launches-ehr-with-iphone-app/; Brian Dolan, *Aetna Connecting Mobile Apps to Its PHR* (Aug. 7 2009), *available at:* http://mobihealthnews.com/3737/aetna-connecting-mobile-apps-to-its-phr/. Although the FDA has some security requirements related to design and manufacture of devices, specific privacy and security regulations have not been promulgated by the FDA, causing medical device privacy and security practices to vary widely. *Improving the Security and Privacy of Implantable Medical Devices*, N. Engl. J. Med. 362; 2 (Apr. 1, 2010), *available at:* http://www.cs.washington.edu/homes/yoshi/papers/IMD/NEJM-Maisel-Kohno.pdf. A National Academies report recently called for coordination between the Office of the National Coordinator and the FDA to provide better guidance to developers of information technologies to better address the needs of home health consumers. *Health Care Comes Home: The Human Factors*, National Academies Report Brief, p. 4 (July 2011), *available at:* http://www.nap.edu/catalog/13149/health-care-comes-home-the-human-factors.

[38] FDA MMA Guidance, *supra* note 8. The guidance outlined FDA's narrowly-tailored, functionality-based approach to mobile apps that focuses its oversight on a subset of functionalities that the agency already regulates and that present a greater safety risk to patients if they do not work as intended. FDA refers to this subset of mobile apps as mobile medical apps (MMA). The MMA guidance does not discuss privacy and security requirements for these apps. Specifically, the MMA guidance explains that FDA intends to exercise patient safety enforcement discretion for certain mobile apps, including, among others, apps that enable patients or providers to interact with PHRs or EHR systems. The FDA offered other examples of mobile apps for which it does not intend to enforce FDA requirements, including health and wellness apps, apps that supplement clinical care by coaching or prompting to help patients manage their health, and apps that help users organize and track their health information. As is pointed out elsewhere, however, the subset of mobile apps on which FDA intends to focus its regulatory oversight is a small subset of the overall health app market.
Additionally, in 2014, IMS Institute for Healthcare Informatics analyzed 43,689 healthcare and fitness apps available for download from the U.S.; few of these would be the type regulated by the FDA. *See e.g.* IMS Institute for Healthcare Informatics, *Patient Apps for Improved Healthcare: From Novelty to Mainstream*. New Jersey: IMS Institute for Healthcare Informatics, p. 4 (2013). It is estimated that in 2014, almost one-third of U.S. smartphone owners, which is about 46 million unique people, used apps from the fitness and health category. *See* http://www.nielsen.com/us/en/insights/news/2014/hacking-health-how-consumers-use-smartphones-and-wearable-tech-to-track-their-health.html; *see also* http://mobihealthnews.com/32183/nielsen-46-million-people-used-fitness-apps-in-january/.

[39] Even if the medical devices are not covered entities/business associates, HIPAA's rules apply to patient information stored within these devices because the devices are being used by a doctor or hospital staff.

[40] This assumes the mobile application or device used by the patient is not offered by or on behalf of a covered entity. Even if the mobile application allowed the individual to send information to his/her provider, the mobile application would not be subject to HIPAA, although the information would become subject to HIPAA once the provider, a HIPAA-covered entity, received it. For further discussion of this issue, *see* Adam Greene, *When HIPAA Applies to Mobile Applications* (June 16, 2011), *available at:* http://mobihealthnews.com/11261/when-hipaa-applies-to-mobile-applications/ (noting that if a health plan provides enrollees with an application that allows them to track their weight on their smartphones, the application is not subject to HIPAA because it is used by an NCE). This Report's analysis shows that if the application stores data on the health plan's server, however, the information on the health plan's server would be subject to HIPAA.

particular the FTC Act.[41] Given this environment, it would not be surprising if individuals are confused, and do not understand, that HIPAA may not protect the privacy and security of their health information collected by equipment or an app if that collection of information is not offered by the individual's provider or on its behalf. As illustrated in their communications with HHS, some mHealth developers themselves may not be aware of the regulatory requirements that attach to their work and have requested additional guidance.[42]

A second way in which health information is collected is through health social media. Social networking and patient peer-networking websites related to health are increasingly prevalent. Social media are interconnected, multi-directional means of communication. Social media allows sharing of information, preferences, and views among individuals and groups, and allows self-disclosure of health information. These websites are frequently used by patients to discuss treatment options and to provide support networks. Some websites are specific to individuals with chronic conditions[43] or shared health concerns (e.g., genetic information).[44] To help manage their conditions and sort through medical information, individuals are increasingly turning to online health communities as a potential source of health information.

Similar to the way mobile mHealth technologies collect health data, some websites and social media sites allow individuals to enter their health information to monitor blood sugar, eating habits, or sleeping patterns. Other health data websites may provide information or send out e-mails with information about medications or specific conditions such as allergies, asthma, arthritis, or diabetes. Twenty-seven percent of internet users and 20 percent of adults have tracked their weight, diet, exercise routine, symptoms, or another health indicator online.[45]

---

[41] For example, if a mobile application shares individual information in violation of the application developer's stated privacy policy or fails to have reasonable data security practices, this might constitute a deceptive or unfair trade practice subject to the FTC's consumer protection enforcement authority. In addition, the FTC has brought enforcement actions against companies that make false or deceptive claims regarding what their health apps can do. For example, the FTC recently settled with two marketers for deceptively claiming their mobile apps could detect symptoms of melanoma. *FTC v. New Consumer Solutions LLC*, *et al,* No.15-cv-01614 (N.D. Ill. April 30, 2015) (stipulated final judgment and order), *available at:* https://www.ftc.gov/enforcement/cases-proceedings/132-3210/new-consumer-solutions-llc-mole-detective. *See also Health Discovery Corporation*, No. C-4516 (F.T.C. March 30, 2015) (decision and order*), available at:* https://www.ftc.gov/enforcement/cases-proceedings/132-3211/health-discovery-corporation-melapp-matter; *Dermapps*, No. C-4337 (F.T.C. Oct. 13, 2011) (decision and order), *available at:* https://www.ftc.gov/enforcement/cases-proceedings/102-3205/brown-koby-individually-dba-dermapps-et-al-matter; and *Andrew N. Finkel*, No. C-4338 (F.T.C. Oct. 13, 2011) (decision and order), *available at:* https://www.ftc.gov/enforcement/cases-proceedings/102-3206/finkel-andrew-n-individually (pair of cases alleging that app developers violated Sections 5 and 12 of the FTC Act by claiming, without substantiation, that their apps provided an effective treatment for acne). Press release: http://ftc.gov/opa/2011/09/acnecure.shtm.

[42] HHS Response Letter, *supra* note 23.

[43] *See, e.g.*, PatientsLikeMe, *available at:* http://www.patientslikeme.com/.

[44] Susannah Fox, *The Social Life of Health Information, 2011*, Pew Research Center's Internet & American Life Project, p. 6 (May 12, 2011), *available at:* http://www.pewinternet.org/~/media/Files/Reports/2011/PIP_Social_Life_of_Health_Info.pdf.

[45] *Id.* at p. 3. (stating that the online conversation about health is being driven by 1) the availability of social tools and 2) the motivation, especially among people living with chronic conditions, to connect with each other. These factors may indicate that online health care conversations are likely to continue or grow).

While benefits could be realized through the use of these various forms of social media, individuals are often unaware about possible future uses of the health information they share and the potential consequences of sharing the information. One recent study examining social networking sites that target people living with diabetes found that less than half of the sites offered safeguards for protecting the individuals' personal health information. The study also identified conflicts of interest, such as ties to the pharmaceutical industry, which were not disclosed to individuals using these sites.[46] On the other hand, analysis of information shared on social media may be beneficial for public health. For instance, Twitter content has been successfully analyzed to evaluate public health trends.[47]

Although some websites that allow individuals to enter health information are hosted or sponsored by HIPAA covered entities, such as health plans or provider networks,[48] many of the websites operate independently, or through a direct relationship to the individual, not through any covered entities or business associates.[49]

IV. FEDERAL LEGAL LANDSCAPE OF HEALTH INFORMATION PRIVACY AND SECURITY

In Section III, we discussed how data was collected. In this section, we discuss how health information is regulated once it is collected by a HIPAA covered entity or an NCE.

The United States has a number of sector-specific laws regulating individual or consumer information security and privacy.[50] For example, in the health sector, the current federal laws

---

[46] Molly Merrill, *Social Networking Sites for Diabetes Patients Lacking in Quality*, Healthcare IT News, Privacy (Feb. 8, 2011), *available at:* http://www.healthcareitnews.com/news/social-networking-sites-diabetes-patients-lacking-quality-privacy.

[47] Michael J. Paul and Mark Dredze, "*You Are What You Tweet* (July 5, 2011), *available at:* http://www.cs.jhu.edu/~mpaul/files/2011.icwsm.twitter_health.pdf.

[48] iHealthBeat.org , *Mayo Clinic Launches Social Networking Site on Health Care Issues* (July 15, 2011), *available at:* http://www.ihealthbeat.org/articles/2011/7/15/mayo-clinic-launches-social-networking-site-on-health-care-issues.aspx(Mayo clinic reports that it was unaware of other online communities like the Mayo only community created by medical provider groups or hospital systems).

[49] *See, e.g.,* Nicole Lewis, *Healthcare Social Media Sites Neglect Privacy Protections*, InformationWeek Healthcare (February 14, 2011), *available at:* http://www.informationweek.com/news/healthcare/patient/229218547 (noting that results from a study of 10 diabetes-focused social networking sites showed that the technological safety was poor, with almost no use of procedures for secure data storage and transmission).

[50] HITECH § 13424, which commissions this report, requests a report "on privacy and security requirements for entities that are not covered entities or business associates . . ."13424(b)(1). There are numerous additional federal laws that might be interpreted to regulate individually identifiable information about health in certain circumstances. Among the more well-known are: the Gramm-Leach-Bliley Financial Services Modernization Act (GLBA), Title V of the Financial Services Modernization Act of 1999, Pub. L. No. 106-102, 113 Stat. 1338 (Nov. 12, 1999) (*codified at* 15 U.S.C. §§ 6801, 6809, 6821, and 6827); 16 C.F.R. Part 313 (implementing privacy rules pursuant to GLBA and regulates information about individuals that may derive from financial transactions related to health, such as a health savings account); Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g, 34 C.F.R. Part 99 (may apply to student health centers); the Children's Online Privacy Protection Act of 1998 ("COPPA"), 515 U.S.C. §§ 6501 -6506 and 16 C.F.R. Part 312, (COPPA Rule); or the Privacy Act, 5 U.S.C. § 552a (applies to data held by the United States). However, given this Report's focus on health information as defined, we focus solely on HIPAA, section 5 of the FTC Act, and the FTC's Health Breach Notification Rule.

protect an individual's health information based upon the type of entity holding the information rather than solely upon characteristics of the information itself. Existing sector-specific federal privacy and security protections for health information are established primarily in HIPAA as amended by HITECH[51] and the HIPAA Privacy, Security, and Breach Notification Rules. Collectively, these rules apply to health plans, most health care providers, health care clearinghouses, and other entities that work with protected health information (PHI)[52] on behalf of covered entities (i.e., business associates).[53] The FTC Health Breach Notification Rule also protects some health information collected, shared, and used in the health sector.[54] While the HIPAA Breach Notification Rule applies to HIPAA covered entities and business associates,[55] the HITECH Act also directed the FTC to implement a temporary rule – the Health Breach Notification Rule – that certain non-HIPAA businesses must follow if there is a security breach.[56] The Rule applies to PHRs (vendors of personal health records), entities that interact with PHRs ("PHR-related entities"), and their service providers.[57] Per HITECH, this rule sunsets if Congress enacts new legislation to require breach notification by entities that are not covered entities or business associates, and that has not occurred.

In addition to these sector-specific laws protecting health information, the FTC has broad authority[58] to enforce the FTC Act against for-profit entities engaging in unfair and deceptive acts or practices in or affecting commerce. This is a standard that the FTC has applied to a wide variety of entities, including those collecting, storing, and disposing of PHI on behalf of an entity covered by HIPAA.

To provide a sufficient summary of the gaps in oversight, these various regulatory schemes will be discussed in greater detail below, including: (1) the types of entities to which HIPAA applies and does not apply; (2) the basic structure of the HIPAA Privacy, Security, and Breach Notification Rules; (3) Section 5 of the FTC Act and how the Act's protection against unfair and deceptive practices applies to both HIPAA and non-HIPAA covered entities, in contrast to HIPAA's privacy and security protections;[59] and (4) the interim breach notification rules the FTC has promulgated relating to breaches suffered by entities within the FTC's purview.

---

[51] HITECH Act supra § 13041, codified at 42 U.S.C. § 17934.
[52] *See* 45 C.F.R. 164.514(b)(2)(i), which identifies the 18 data points that have to be removed to render data *not* PHI under the HIPAA de-identification safe harbor method. For example, both direct identifiers (name, birthdate, SSN) and indirect identifiers, such as zip code, must be removed to render data "de-identified" under the HIPAA standard and thus not PHI subject to HIPAA's Privacy Rule.
[53] *See* 45 C.F.R. Part 160 and Subparts A, C, E of Part 164.
[54] HITECH Act, § 13407(g)(1).
[55] 45 C.F.R. §§ 164.404 – 164.410.
[56] HITECH Act, § 13407(g)(1). The rule is temporary by virtue of a sunset provision that is included in the law at (g)(2).
[57] 16 C.F.R. Part 318.
[58] 15 U.S.C. § 45.
[59] *See ONC Guide to Privacy and Security of Electronic Health Information* (ONC Privacy and Security Guide), p. 11 (April 2015), *available at:* http://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf. *See also* HHS Guidance Specifying the Technologies and Methodologies that Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals, 74 Federal Register No. 79 19006 (April 27, 2009), *available at*: http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/federalregisterbreachrfi.pdf.

HIPAA's Scope

Under HIPAA and HITECH, OCR enforces: the HIPAA Privacy Rule, which protects the privacy of protected health information (PHI) in the hands of HIPAA covered entities and their business associates, discussed in more detail below; the HIPAA Security Rule, which sets national standards for the security of electronic protected health information (ePHI); and the HIPAA Breach Notification Rule, which requires covered entities to provide notification following a breach of unsecured protected health information (all together, "the HIPAA Rules"). Congress also granted State Attorneys General the authority to enforce the HIPAA Rules and called on the U.S. Department of Justice to enforce violations of the criminal provisions of HIPAA.[60] The Rules serve as the foundation for federal protection of the privacy and security of PHI and apply in conjunction with state laws that impose more stringent privacy and security protections.[61] The HIPAA Rules currently apply to a broad range of organizations, but they do not cover all organizations that handle an individual's health information. In fact, as discussed below, a growing number of organizations that maintain, transmit, or receive health information about individuals fall outside the scope of HIPAA.

Where health information is protected: covered entities and their business associates

The HIPAA Rules apply only to organizations known as covered entities[62] and their business associates. HIPAA does not apply to individuals or to other types of organizations that do not qualify as covered entities or business associates, even those that may handle or store an individual's health information. There are three types of covered entities:

- Health plans include health, dental, vision, health maintenance organizations (HMOs), Medicare, Medicaid, and long-term care insurers (excluding nursing home fixed-

[60] The HHS Secretary initially delegated the authority to administer and enforce the Security Rule to the Centers for Medicare and Medicaid Services (CMS), and from 2003 to July 27, 2009, CMS administered the Security Rule. However, in recognition of the future increase in electronic PHI as a result of the adoption of electronic health records, and in recognition of the HITECH Act's provisions regarding privacy and security enforcement, the Secretary re-delegated the authority to administer and enforce the Security Rule to OCR on July 27, 2009. Federal Register Notice, Vol. 74, No. 148, 38630 (Aug. 4, 2009), a*vailable at:* https://www.gpo.gov/fdsys/pkg/FR-2009-08-04/pdf/E9-18544.pdf. *See also* HITECH Act § 13410(e) (allowing state attorneys general to bring HIPAA enforcement actions on behalf of the people of their state). OCR coordinates HIPAA enforcement with the U.S. Department of Justice, which shares enforcement jurisdiction over HIPAA violations. If a complaint implicates the criminal provision of HIPAA, OCR will refer the complaint to the Department of Justice. HIPAA gives the U.S. Department of Justice criminal enforcement authority for HIPAA violations. 42 U.S.C. § 1320d-6. U.S. Department of Health and Human Services, Office for Civil Rights, Leon Rodriguez's Testimony before the Senate Subcommittee on Privacy, Technology and the Law (Nov. 2011), *available at:* http://www.judiciary.senate.gov/meetings/your-health-and-your-privacy-protecting-health-information-in-a-digital-world. Loretta E. Lynch, then U.S. Attorney for the Eastern District of New York testified before the Senate Subcommittee on Privacy, Technology and the Law to discuss the examination of the enforcement of federal health information privacy laws (November 9, 2011), *available at:* http://www.judiciary.senate.gov/meetings/your-health-and-your-privacy-protecting-health-information-in-a-digital-world.

[61] Many state laws provide individuals with greater control that HIPAA provides, especially but not only with respect to sensitive health information such as AIDs/HIV status, genetic information, and mental health status. Similarly, 42 CFR Part 2 provides for a higher degree of patient control for drug and alcohol treatment records from federally funded programs. *See supra* note 14.

[62] 45 C.F.R. § 160.103 (providing definitions of key terms).

indemnity policies). Health plans also include employer-sponsored group health plans, government and church-sponsored health plans, and multi-employer health plans;

- Health care clearinghouses are entities that process nonstandard information they receive from another entity (usually a health plan or health care provider) into standard data elements or a standard transaction, or vice versa; [63] and

- Health care providers who electronically conduct certain transactions, such as claims submissions and prior authorizations.

In general, a business associate is a person or organization that uses PHI to perform covered functions or activities on behalf of a covered entity. These include certain claims processing, data analysis, utilization review, and billing functions and services.[64] Such services can be legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial functions or activities. If a covered entity hires an organization to offer a PHR in the covered entity's name and to host the health information collected in that PHR for the covered entity, that PHR vendor is acting as the covered entity's business associate.[65] Under HITECH, business associates must comply with the Security Rule as well as certain other provisions of the HIPAA Rules.[66]

HIPAA Privacy Rule Basics

The HIPAA Privacy Rule provides federal protections for individually identifiable health information held by covered entities and their business associates and gives patients an array of rights with respect to that information. The Privacy Rule protects individually identifiable health information held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral. This information is PHI.[67] Individuals have the right to obtain a copy of their PHI held by a covered entity or business associate; to know the identity of those who received the records; to request corrections to the information; to direct that an electronic copy of the record be sent to a designated third party, including a PHR vendor;[68] to request limits on who may see the information; and to submit complaints to the covered entity and OCR.

---

[63] 45 C.F.R. § 160.103 (For purposes of HIPAA Administrative Simplification regulations, "transaction" means the transmission of information between two parties to carry out financial or administrative activities related to health care. It includes the following types of information transmissions: (1) health care claims or equivalent encounter information, (2) health care payment and remittance advice, (3) coordination of benefits, (4) health care claim status, (5) enrollment and disenrollment in a health plan, (6) eligibility for a health plan, (7) health plan premium payments, (8) referral certification or authorization, (9) first report of injury, (10) health claims attachments, (11) other transactions that the Secretary may prescribe by regulation). *See also supra* note 6.
[64] *Id*.
[65] HITECH Act, § 13404. *See also* 45 C.F.R. § 160.103.
[66] *Id.*
[67] 45 C.F.R. § 160.103.
[68] 45 C.F.R. §§ 164.524, 164.528, 164.526, 164,522, 164.530, and 160.306.

Generally, subject to the applicable requirements, a covered entity is permitted to use and disclose PHI without needing to obtain the individual's formal authorization for a number of purposes or situations, including the following (which is not an exhaustive list):

(1) for treatment, payment, and health care operations of the disclosing or receiving entity;

(2) directly to family, friends and others involved in the individual's care unless the individual objects;

(3) for certain specified activities beneficial to the public, such as public health activities;

(4) where expressly required by law; and

(5) as a Limited Data Set for the purposes of research, public health, or health care operations.[69]

Covered entities may rely on professional ethics and best judgments in deciding whether to use or disclose PHI as permitted by HIPAA. A covered entity must obtain written authorizations from individuals to use or disclose their information for purposes not expressly permitted by HIPAA.[70] Where the recipient of the disclosed information is another covered entity or business associate, the HIPAA Rules' protections continue to apply. This is true whether the PHI is clinical data from a physician's EHR or PHI from claims data.[71]

The HIPAA Privacy Rule does not extend to NCEs

The HIPAA Privacy Rule does not protect all health information wherever it is found. Because the rules apply only to covered entities and their business associates, the protections do not extend to data about the health of individuals held by NCEs. HIPAA also does not apply to health information about an individual that has been de-identified; however, entities covered by HIPAA must de-identify data in accordance with the HIPAA Privacy Rule.[72] NCEs are not subject to any de-identification standards. Thus, there is currently little understanding of how NCEs' sharing of so-called de-identified or anonymous information impacts individuals' privacy, and whether the data an NCE anonymizes may be less de-identified than would be the case under HIPAA.[73]

Since 2003, when OCR's enforcement of the HIPAA Privacy Rule began, OCR's enforcement activities have generated significant results that have improved the privacy practices of covered entities and the protection of health information for all individuals they serve. OCR has investigated and resolved over 23,873 cases by requiring changes in privacy practices and corrective actions by, or providing technical assistance to, HIPAA covered entities and their business associates. Regional investigators open compliance reviews of the entities involved in

[69] 45 C.F.R. § 164.514(e).

[70] For more information on this topic, *see* http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/research/index.html. *See also* ONC Privacy and Security Guide, p. 14-21, *supra* note 59.

[71] HIPAA regulates ePHI without distinguishing between clinical information such as that held in a provider's EHR, and claims information, such as that which flows between a provider and a payer. Therefore, where HIPAA applies, clinical and claims data are treated the same. Similarly, where there are legal gaps, those gaps may exist for both clinical or claims data.

[72] 45 C.F.R. §§ 164.502(d); 164.514(b).

[73] Health IT Policy Committee Privacy and Security Workgroup, *Health Big Data Recommendations* (August 2015), *available at:* https://www.healthit.gov/sites/faca/files/HITPC_Health_Big_Data_Report_FINAL.pdf.

all reported breaches affecting 500 or more individuals. OCR publishes the results of breach investigations, including the negotiation of settlement agreements and imposition of civil money penalties, in part to educate and incent other covered entities and business associates to do better.[74]

The HHS Breach Notification Rule, following the occurrence of a breach of unsecured PHI, requires covered entities to promptly notify affected individuals of the breach and to notify the HHS Secretary within specific timeframes. When a breach affects more than 500 individuals, the media must also be notified. In the case of a breach of unsecured protected health information at or by a business associate of a covered entity, the business associate must notify the covered entity of the breach.

HIPAA Security Rule Basics

The HIPAA Security Rule requires that covered entities and their business associates perform a security risk assessment to identify and mitigate risks to the confidentiality, integrity, and availability of the electronic protected health information (ePHI) they create, receive, maintain, or transmit. Additionally, the Security Rule specifies a series of administrative, physical, and technical safeguards that covered entities and their business associates must implement to prevent unauthorized or inappropriate access, use, or disclosure of ePHI. Administrative safeguards include risk analysis and management, access management, workforce training, and evaluation of security measures. Physical safeguards are physical measures, policies, and procedures to safeguard the covered entity or business associate's electronic information systems. They include facility access controls, workstation use, workstation security, and device and media controls. Technical safeguards include access controls, audit controls, integrity, person or entity authentication, and transmission security. A key concept in applying the Security Rule is that it is scalable and flexible to allow implementation of the standards as appropriate for the entity's size, complexity, and capabilities, including its technical, hardware, and software infrastructure. For example, the Rule requires covered entities to implement procedures to verify the identity of a person or entity seeking access to electronic PHI. Thus, the Security Rule mandates an outcome: reasonably verified identity. But, it does not specify how to verify the identity of an electronic user, such as by using a card and a personal identification number or a biometric identifier. The Security Rule requires that appropriate safeguards be implemented, but – in light of evolving standards and developments in the security space – does not mandate particular technical solutions or specify the adoption of any particular standard on identity, such as the one established by the Department of Commerce's National Institute of Standards and Technology (NIST).[75]

[74] U.S. Department of Health and Human Services, Office for Civil Rights, *HIPAA for Professionals, Enforcement, Case Examples*, *available* http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/examples/all-cases/index.html

[75] National Institute of Standards and Technology, *Electronic Authentication Guideline* (August 2013), *available at:* http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf.

The FTC Act's Scope

The FTC enforces several statutes and rules that impose obligations upon businesses to protect consumer data.[76] Of particular import for this Report, the Commission enforces the proscription against unfair or deceptive acts or practices in Section 5 of the Federal Trade Commission Act.[77] A company acts deceptively if it makes misleading material statements or omissions about a matter and such statements or omissions are likely to mislead reasonable consumers.[78] A company engages in unfair acts or practices if its practices cause or are likely to cause substantial injury to consumers that is neither reasonably avoidable by consumers nor outweighed by countervailing benefits to consumers or to competition.[79] The Commission has used its authority under Section 5 in cases where, for example, it has reason to believe that a business made false or misleading claims about its privacy or data security procedures or failed to employ reasonable security measures and, as a result, causes or is likely to cause substantial consumer injury.

Section 5 authority extends to both HIPAA and non-HIPAA covered entities

The FTC's Section 5 authority extends to both HIPAA and non-HIPAA covered entities,[80] though generally this authority does not reach nonprofit entities or companies engaged in the business of insurance to the extent that such business is regulated by state law.[81] Moreover, the FTC Act is currently the primary federal statute applicable to the privacy and security practices of businesses that collect health information where those entities are not covered by HIPAA.

The FTC has brought numerous cases against businesses alleging privacy and security-related violations, including a number of cases to protect consumers from companies' deceptive and unfair practices with regard to their health data. One recent example of a privacy-related violation involving health information is the Commission's settlement with medical billing

---

[76] 15 U.S.C. § 45(a) (Section 5 of the FTC Act); 15 U.S.C. §§ 6801-6809 (GLBA); 15 U.S.C. § 1681 (FCRA); 15 U.S.C. §§ 6501-6506 (COPPA) and 16 C.F.R. Part 312 (COPPA Rule).

[77] 15 U.S.C. § 45(a).

[78] Federal Trade Commission Policy Statement on Deception, appended to *Cliffdale Assocs., Inc.*, 103 F.T.C. 110, 174 (1984).

[79] 15 U.S.C. § 45(n); Federal Trade Commission Policy Statement on Unfairness, appended to *Int'l Harvester Co*., 104 F.T.C. 949, 1070 (1984).

[80] HHS and the FTC have worked closely in areas of concurrent jurisdiction, as they have common interests in ensuring the privacy and security of health information for individuals, whether that health information is within or outside the scope of HIPAA. For example, FTC staff collaborated with OCR to bring a set of cases involving faulty data security practices that implicated both HIPAA and the FTC Act. *See Rite Aid Corporation*, No. C-4308 (F.T.C. Nov. 12, 2010) (decision and order), *available at:* https://www.ftc.gov/enforcement/cases-proceedings/072-3121/rite-aid-corporation-matter; *see also CVS Caremark Corporation*, No. C-4259 (F.T.C. June 18, 2009) (decision and order), *available at:* https://www.ftc.gov/enforcement/cases-proceedings/072-3119/cvs-caremark-corporation-matter. *See also* comments of Loretta Garrison and Adam Greene, PHR Roundtable Transcript, pp. 318 – 21, *supra* note 24.

[81] 15 U.S.C. §§ 44 & 45(a). The FTC's Section 5 jurisdiction also does not extend to banks, savings and loan institutions, Federal credit unions, or common carriers. Although the FTC Act does grant the FTC rule making authority to address unfair or deceptive acts or practices, the FTC must follow statutory procedures that go beyond standard "notice-and-comment" rulemaking under the Administrative Procedure Act. 15 U.S.C. § 57a(b) (2011). The FTC does have the authority to make certain rules protecting security and privacy, as directed by Congress, under several other statutes, such as the FCRA and GLBA.

company PaymentsMD and its former CEO, Michael C. Hughes.[82] The complaint alleged that the company deceived thousands of consumers who signed up for an online billing portal by failing to adequately inform them that the company would seek highly detailed medical information about them from pharmacies, medical labs, and insurance companies. Specifically, the company allegedly used the sign-up process for the "Patient Portal" – where consumers could view their billing history – as a pathway to deceptively seek consumers' consent to collect detailed medical information from other entities.[83]

The FTC has also used its Section 5 authority to bring enforcement actions against companies that fail to have reasonable and appropriate data security practices regarding consumer data, including health data.[84] For example, the Commission recently settled an enforcement action with GMR Transcription Services in which the Commission alleged that the medical and legal transcription company outsourced transcription services to a third party without adequately checking to make sure they could implement reasonable security measures. According to the Commission's complaint, among other things, the service provider stored transcribed notes in clear text on an unsecured server. As a result, consumers found their doctors' notes of their physical examinations freely available through Internet searches.[85]

Scope of FTC Breach Notification Rule

The FTC Health Breach Notification Rule[86] applies to certain types of entities that fall outside of the scope of HIPAA and therefore are not subject to the HIPAA Breach Notification Rule. In particular, the FTC Rule applies to vendors of PHRs (entities that offer or maintain personal health records), PHR-related entities (entities that interact with vendors), and third party service

[82] *PaymentsMD, LLC*, No. C-4505 (F.T.C. Jan. 27, 2015) (decision and order), a*vailable at:* https://www.ftc.gov/enforcement/cases-proceedings/132-3088/paymentsmd-llc-matter.
[83] *Id.*
[84] The FTC conducts its data security investigations to determine whether a company's data security measures are reasonable and appropriate in light of the sensitivity and volume of consumer information it holds, the size and complexity of its data operations, and the cost of available tools to improve security and reduce vulnerabilities.
[85] *GMR Transcription Services, Inc*., No. C-4482 (F.T.C. Aug. 14, 2014) (decision and order), *available at:* https://www.ftc.gov/enforcement/cases-proceedings/122-3095/gmr-transcription-services-inc-matter. *See also Accretive Health, Inc.*, No. C-4432 (F.T.C. Feb. 5, 2014) (decision and order), *available at:* https://www.ftc.gov/enforcement/cases-proceedings/122-3077/accretive-health-inc-matter (alleging that medical billing and revenue management services company put consumers' personal information, including health information, at risk by, among other things, transporting laptops with sensitive data in a way that made them vulnerable to theft and giving access to personal information to employees who didn't need it to do their jobs). *See also Genelink, Inc.*, No. 4456 (F.T.C. May 8, 2014) (decision and order), *available at:* https://www.ftc.gov/enforcement/cases-proceedings/112-3095/genelink-inc-matter; *foru™ International Corporation formerly known as Genewize Life Sciences, Inc*., No. 4457 (F.T.C. May 8, 2014) (decision and order), a*vailable at:* https://www.ftc.gov/enforcement/cases-proceedings/112-3095/forutm-international-corporation-matter (pair of cases against makers of genetically customized nutritional supplements who deceptively and unfairly claimed they had reasonable security measures to safeguard and maintain personal information, including genetic information); *CBR Systems, Inc*., No. 4400 (F.T.C. Apr. 29, 2013) (decision and order), *available at* https://www.ftc.gov/enforcement/cases-proceedings/112-3120/cbr-systems-inc-matter (settlement with cord blood bank over its inadequate security practices).
[86] Congress directed the FTC to implement this temporary rule that specific non-HIPAA covered entities must follow if there is a security breach. *See* HITECH Act §13407 (2010). FTC enforcement began on February 22, 2010. *See also* 16 C.F.R. Part 318.

providers to these PHR vendors or PHR-related entities.[87] The FTC Rule requires PHR vendors and PHR-related entities to notify individuals, the FTC, and in some cases the media when there is a breach of unsecured, electronic health information. Similar to the breach notification requirements of the HIPAA Breach Notification Rule, the FTC Rule requires service providers to notify their vendor or PHR-related entity client in case of a breach.[88] Also similar to the requirements of the HIPAA Rule, the FTC Rule applies only to health information in PHRs that is not secured through technologies specified by OCR.[89]

Fair Information Practice Principles (FIPPS)

In January, 2008, ONC published the *Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information* (referred to elsewhere in this report as the ONC P&S Framework) to establish a single, consistent approach to addressing the privacy and security challenges related to electronic health information exchange through a network for all persons, regardless of the legal framework that may apply to a particular organization.[90] This framework document was informed by a number of key privacy and security principles including the Department of Health, Education and Welfare's (HEW) (now the Department of Health and Human Services) Code of Fair Information Practices, also known as fair information practice principles (FIPPS). In 2008, ONC added additional concepts from expert sources to reflect the changing nature of data since 1973 from paper-based to digital. The FIPPS identify the following eight key principles (also referred to in ONC's Interoperability Roadmap) for guiding information practices while advancing technology:

1. Individual access
2. Correction
3. Openness and transparency
4. Individual choice
5. Collection, use and disclosure limitation
6. Data quality and integrity

---

[87] 16 C.F.R. § 318.1. Section 318(2)(d) defines a personal health record as an electronic record of "identifiable health information on an individual that can be drawn from multiple sources and that is managed, shared, and controlled by or primarily for the individual." Section 318(2)(f) defines a PHR-related entity as an entity (not covered by HIPAA and not a business associate) that "(1) offers products or services through the website of a vendor of personal health records; (2) offers products or services through the websites of HIPAA-covered entities that offer individuals personal health records; or (3) accesses information in a personal health record or sends information to a personal health record." Section 318(2)(h) defines a "[t]hird party service provider" as an entity that "provides services to a vendor of personal health records in connection with the offering or maintenance of a personal health record or to a PHR related entity in connection with a product or service offered by that entity; and (2) accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses unsecured PHR identifiable health information as a result of such services."

[88] 16 C.F.R. §318.3(b).

[89] U.S. Department of Health and Human Services, Office for Civil Rights, *Guidance Specifying the Technologies and Methodologies That Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals*, *available at:* http://www.hhs.gov/hipaa/for-professionals/breach-notification/guidance/index.html, 45 C.F.R. §§160 and 164; *see also* FTC *Breach Notices Received by the FTC* (2014), *available at:* https://www.ftc.gov/system/files/documents/rules/health-breach-notification-rule/draft_breach_notices_received_by_ftc_2014.pdf.

[90] ONC P&S Framework, *supra* note 11.

7. Safeguards
8. Accountability

The HIPAA Privacy Rule builds on these principles through its individual rights and information protections. Some of the key HIPAA protections include:[91]

1. Requirement that individuals have a right to access and to some degree control the data (Principles 1, 2, and 4);[92]
2. Requirement for covered entities to be transparent about the ways the data may be used and disclosed—for what purposes and to whom (Principle 3);[93]
3. Requirement, in general, that information be used and disclosed only for purposes related to the purpose for which it was obtained, with exceptions for disclosures in the public good and disclosures specifically authorized by the individual (Principle 5);[94]
4. Requirements on entities to be thoughtful stewards of the data by implementing policies, procedures, and other steps to safeguard the information from inappropriate use/disclosures (Principles 6, 7, and 8).[95]

V. ANALYSIS

Our analysis illustrates five major areas in which HIPAA's privacy and security oversight and protections are different than those of NCEs:

A. Difference in Individuals' Access Rights
B. Differences in Re-Use of Data by Third Parties
C. Differences in Security Standards Applicable to Data Holders and Users
D. Differences in Understanding of Terminology About Privacy and Security Protections[96]
E. Inadequate Collection, Use, and Disclosure Limitations

Difference in Individuals' Access Rights

Perhaps the most important difference between HIPAA-covered entities and NCEs is that individuals enjoy a suite of rights with regard to the protected health information held by a covered entity or business associate. In most cases, the rights delineated under the FIPPS, including access to information, ability to demand an accounting of certain disclosures, and some control over how the information is used and shared, do not exist for information held by NCEs. The current practices of NCEs often lack transparency, despite the fact that the FIPPS require

[91] See FIPPS referred to in ONC's Final Nationwide Interoperability Roadmap, p. 17 (October 6, 2015), *available at*: https://www.healthit.gov/sites/default/files/hie-interoperability/nationwide-interoperability-roadmap-final-version-1.0.pdf; *see also* Supplemental Materials, p. 15 (October 6, 2015), *available at:* https://www.healthit.gov/sites/default/files/hie-interoperability/Interoperibility-Road-Map-Supplemental.pdf.
[92] 45 C.F.R. § 164.524.
[93] 45 C.F.R. §§ 164.520, 164.528, and 164.404.
[94] 45 C.F.R. §§ 164.502(b); 164.514(d).
[95] 45 C.F.R. § 164.530.
[96] For example, this Report documents confusion by individuals who may think their health data is similarly protected in all environments and by developers who do not understand what they must do for HIPAA compliant products versus those that are for non-covered entities.

it.[97] NCEs are not obligated by a statute or regulation to provide individuals with access to data about themselves. Although an NCE may make representations to consumers about access, these are not required by law. Thus, an individual may share data about his or her health through mHealth technologies or health social media but may not have the ability to later obtain a copy of the underlying information or learn where the data was re-disclosed. Findings from ONC's background study highlighted areas where organizations may be lacking "openness and transparency about policies, procedures, and technologies that directly affect individuals and/or their individually identifiable health information."[98] For key initiatives that leverage electronic health information, such as the President's Precision Medicine Initiative, it is increasingly important that individuals be able to direct that health information about them be sent where they wish.[99] OCR recently clarified how strong this right is for individuals under HIPAA,[100] but, outside of HIPAA, there is no legal right to access one's health data.

Specific circumstances where health information about individuals may be outside the scope of HIPAA's access rights provisions may include:

- PHRs offered or sold to an individual directly rather than through a covered entity or business associate;
- mHealth technologies, sold directly to individuals, that collect, share, and use information about the individual, when this equipment is not sold through or sponsored by a covered entity or business associate;
- Health information registries that are not sponsored by covered entities or public health agencies (for example, some health information registries are sponsored by professional societies);
- Individual-directed and self-disclosed health information for research or analysis, like direct-to-consumer genome sequencing, collected by organizations not regulated by HIPAA;[101]
- Health social media where individuals self-disclose health information; and
- Information collected, shared, or used by providers of health care and related services not subject to HIPAA, such as boutique clinics that require patients to self-pay and do not conduct electronic transactions under HIPAA.[102]

---

[97] Maximus Report, *supra* note 25.
[98] ONC P&S Framework, *supra* note 11.
[99] White House *Precision Medicine Initiative: Privacy and Trust Principles* (Nov. 9, 2015), *available at:* https://www.whitehouse.gov/sites/default/files/microsites/finalpmiprivacyandtrustprinciples.pdf (highlighting the importance of an individual's access to health information about him or her).
[100] HHS Office for Civil Rights, Guidance on Individuals' Right Under HIPAA to Access Their Health Information Under 45 CFR § 164.524, *available at:* http://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html.
[101] The Common Rule applies to any research conducted or supported by a federal agency that has codified the regulation, except if the research falls into one of the excepted categories; s*ee supra* pp. 8 – 11.
[102] National Committee on Vital and Health Statistics, Letter to Secretary Leavitt, *Update to Privacy Laws and Regulations Required to Accommodate NHIN Data Sharing Practices*, p. 3 (Jun. 21, 2007), *available at:* http://www.ncvhs.hhs.gov/wp-content/uploads/2014/05/070621lt2.pdf.

Therefore, because these entities fall outside the scope of HIPAA, health information maintained or stored by them is not required to be protected the way that PHI is protected and does not implicate the same access rights.[103]

Differences in Re-Use of Data by Third Parties

The HIPAA Rules circumscribe to whom and for what purpose a covered entity may disclose protected health information. However, once the information is released, the protections of the Rules may not apply. Specifically, if the recipient of health information is not a covered entity or a business associate, HIPAA does not apply to its activities. Consequently, HIPAA's constrained/defined list of permissible disclosures helps limit the amount of sensitive health information in the hands of third parties who are not subject to any rules governing how the information is subsequently used and disclosed. One way this difference plays out is in the use of health information for marketing. The HIPAA Rules limit the use or disclosure of PHI for marketing.[104] This protection, strengthened by HITECH, provides individuals with greater control over how their health information is used for marketing purposes. However, individuals who have provided data to NCEs likely will not enjoy the same protection against unwanted marketing unless the data collector has promised in its terms of use not to use data for marketing and does not change its terms of use.

A similar result could also occur if the individual exercises her right of access under HIPAA, but then provides the data to an NCE. As noted previously, the HIPAA protections will not necessarily follow the data, as they apply only to HIPAA covered entities and business associates. The recipient could be a retail PHR, a research organization, a neighborhood social services organization that is not a HIPAA covered entity, or a health social media site.

As discussed above, these recipients might be covered by the FTC and subject to its Section 5 enforcement authority. To the extent these entities engage in unfair or deceptive acts or practices, which include the failure to live up to privacy promises they make to consumers and the failure to implement reasonable data security protections, they would run afoul of this authority. In the context of the Commission's FTC Act enforcement authority, the Commission could not, however, prohibit the downstream use of information by marketers or mandate consumer access to their information in the absence of a specific showing of deception or unfairness.[105]

---

[103] Consistent with the scope of the Report overall, this section does not analyze the impact of *other* federal laws on the privacy or security of health data about individuals; that is, there is no analysis regarding the GLBA, FERPA, FCRA or COPPA, *supra* note 50.

[104] 45 C.F.R. §§ 164.501; 164.508.

[105] In addition to enforcement, the Commission is also committed to promoting better privacy and data security practices through policy initiatives and consumer education and business guidance and has addressed the importance of transparency and access through these materials. *See* FTC Report: *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* (March 2012), *available at:* https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf; FTC Staff Report: *Mobile Privacy Disclosures: Building Trust Through Transparency (*February 2013), *available at:* https://www.ftc.gov/reports/mobile-privacy-disclosures-building-trust-through-transparency-federal-trade-commission; FTC *Disputing Errors on Credit Reports* (March 2014), *available at:* http://www.consumer.ftc.gov/articles/0151-disputing-errors-credit-reports.

Differences in Security Standards Applicable to Data Holders and Users

ONC's analysis and findings indicate that NCEs may not be ensuring health information is "protected with reasonable administrative, technical, and physical safeguards to ensure its confidentiality, integrity, and availability and to prevent unauthorized or inappropriate access, use, or disclosure, as is required of covered entities and business associates by the HIPAA Rules."[106] To the extent these NCEs fail to reasonably secure consumer personal information, they might run afoul of the FTC Act's prohibition on unfair or deceptive acts or practices.[107]

In particular, the study found the following:

Lack of encryption[108]

Encryption has long been regarded as a best practice for maintaining the confidentiality of health information transmitted across networks. Encryption provides for information security by using an algorithm so that unauthorized persons are unable to understand the data without a de-encryption key or other confidential process.[109] Encryption is commonly used to protect both data in motion and data at rest.[110] Effective encryption practices may reduce the likelihood that an entity will experience a breach under the FTC breach notification rule.

Encryption practices by NCE vendors may not be uniform, and data about those practices may not be available. For example, according to one study, some PHRs may not encrypt all data. Some PHRs do not indicate in their policies whether data would be encrypted or truthfully describe their security practices.[111] Moreover, a recent study found that only six percent of free health apps and 15 percent of paid health apps always used encrypted SSL connections when sending data to third parties.[112]

Other security safeguards may not adequately safeguard health information

Identity verification or proofing and authentication establish and validate a person's identity prior to allowing access to health information, including verification that a person or entity seeking access to electronic health information is the one claimed. For patients, this identity proofing is often performed with a combination of username and password (single factor

---

[106] ONC P&S Framework, p. 9, *supra* note 11.
[107] *See supra* at p. 17 – 18, discussing the FTC Act's scope.
[108] HIPAA requires encryption at rest and in transit unless the covered entity or business associate can document why encryption is not reasonable and appropriate and implement an equivalent measure instead to meet the access control and transmission security standards. 45 C.F.R. § 164.312.
[109] 45 C.F.R. § 164.304.
[110] For example, the FTC recently settled an action against Henry Schein Practice Solutions, Inc., a provider of office management software for dental practices, for misrepresenting that its software provided industry-standard encryption of sensitive patient information. *Henry Schein Practice Solutions, Inc.*, No. 1423161 (F.T.C. Jan. 5, 2016) (complaint and proposed consent order), *available at* https://www.ftc.gov/enforcement/cases-proceedings/142-3161/henry-schein-practice-solutions-inc-matter.
[111] Maximus Report, *supra* note 25.
[112] Privacy Rights Clearinghouse, *Mobile Health and Fitness Apps: What are the Privacy Risks Study (*July 15, 2013), *available at*: https://www.privacyrights.org/mobile-medical-apps-privacy-alert.

authentication). Additional basic security features include password complexity requirements.[113] Enhanced authentication processes require additional factors to confirm that the person seeking access to the health information in the app is the individual and not an unauthorized party.

A recent ONC data brief reported that 49 percent of non-federal acute care hospitals, which are HIPAA regulated, had the capability to support two-factor authentication to their HIPAA-regulated electronic health records.[114] NCEs such as PHRs or mHealth technologies have no regulatory minimum to meet, so their practices may not align with the safeguards in HIPAA, and they may not meet the FTC's Section 5 requirements for reasonable data security.[115]

Security risk assessment and audit capabilities may be misunderstood

NCEs operated by vendors who are not HIPAA covered entities may lack consistent and appropriately defined risk assessment and audit capacities. If NCE vendors are not engaging in the risk assessments or audits specified by the Security Rule, those systems will not be appropriately safeguarded. For example, only a few PHR websites referenced whether the PHR implemented activities to perform risk assessments or review security policies.[116] Only five PHR vendors surveyed referenced audits, access logs, or other methods to detect unauthorized access to health information in PHRs.[117] Even if those PHR vendors who did not describe risk assessment and audit capabilities actively employed a relevant policy, the individual's inability to understand these processes may still mean that individuals do not have complete information about the data use practices of the vendor.

Differences in Understanding of Terminology About Privacy and Security Protections

Specific data that would be protected as PHI by a covered entity or business associate may also be protected by regulations in other sectors. For example, HIPAA protects an individual's Social Security number when it appears in a medical or billing record maintained by a covered entity or business associate. Capture of that number on a financial statement issued by a financial services company might be regulated by other state or federal laws. The differential status of particular data may lead to confusion regarding what information is protected and by what means.[118] HHS stakeholder outreach suggests that developers and entrepreneurs may not know which laws they

[113] White House: *Executive Order Improving the Security of Consumer Financial Transactions* (Oct. 17, 2014), *available at:* http://www.whitehouse.gov/the-press-office/2014/10/17/executive-order-improving-security-consumer-financial-transactions. However, there are no mandatory minimum standards for password complexity, with even NIST stating that the complexity of a password should be organizationally defined.
[114] ONC *State and National Trends of Two-Factor Authentication for Non-Federal Acute Care Hospitals*, ONC Data Brief No. 32 (November, 2015), *available at:* https://www.healthit.gov/sites/default/files/briefs/oncdatabrief32_two-factor_authent_trends.pdf.
[115] For example, in its settlement with Twitter, the FTC alleged that the company failed to provide reasonable security by, among other things, failing to establish or enforce policies sufficient to make administrative passwords hard to guess, including policies that prohibit the use of common dictionary words as administrative passwords and require that such passwords be unique. *Twitter, Inc*., No. C-4316 (F.T.C. March 2, 2011) (decision and order), *available at*: https://www.ftc.gov/enforcement/cases-proceedings/092-3093/twitter-inc-corporation.
[116] Maximus Report, *supra* note 25.
[117] *Id.*
[118] GLBA; 16 C.F.R. Part 313 (implementing privacy rules pursuant to GLBA).

must look to as they build mHealth technologies or health social media sites.[119] Determining where the HIPAA Rules apply and where they do not can be complicated by the use of many terms that may have both a general lay meaning and a specific legal meaning. Individuals and businesses alike may not understand these distinctions and their legal ramifications.

Lack of appropriate and understandable privacy policies and notices

The rapidly increasing mobile technology environment enables the sharing of information with many different parties in a variety of ways. However, for NCEs, there are no federal requirements for policies, or related notices, to inform individuals about practices that may impact the privacy and security of their health information. In the absence of a nationwide standard, some states have enacted state-specific legislation,[120] but others have not, leading to a patchwork approach.

Similarly, when a consumer purchases mHealth technology and reads its privacy notice,[121] the consumer may or may not understand whether federal health information privacy and security protections attach to the technology that is collecting data about the consumer's health. If not, the consumer may make choices that put the data at risk for misuse and re-disclosure.

A 2014 study published in the Journal of the American Informatics Association found that of the 600 most commonly used mHealth apps studied, only 183 (30.5 percent) had privacy policies, and that the average reading level necessary to understand the privacy policy was that of a college senior. Worse, two-thirds (66.1 percent) of privacy policies did not specifically address the app itself.[122] The policies of mHealth developers using the Apple or Google smartphone platforms may be inconsistent, not articulated to individuals, or simply ignored by web developers skirting the rules that operating system developers attempt to impose upon them. As a result, individuals are ill-informed about health information usage practices in this evolving and highly innovative medium, even as these new technologies continue to be adopted by consumers and providers.[123]

---

[119] *See* HHS Response letter *supra,* note 23.

[120] *See* Cal. Bus. & Prof. Code §§ 22575-22579; Conn. Gen. Stat. § 42-471; Del. Code Tit. 6 § 205C; M.S.A. § 325M.02; Texas Health and Safety Code §181.001(b)(2)(B).

[121] There also is confusion between a HIPAA required "notice of privacy practices" and the privacy notice included in websites. The former specifically discusses health information that is regulated by HIPAA, whereas the latter discusses how the website host will collect and use information about the individual's web browsing habits. *See, e.g.*, *California Online Privacy Protection Act of 2003*, *available at:* http://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=BPC&division=8.&title=&part=&chapter=22.&article.

[122] Ali Sunyaev, et. al, *Availability and Quality of Mobile Health App Privacy Policies* J. of Am Informatics Assn. pii: amiajnl-2013-002605. doi: 10.1136/amiajnl-2013-002605 (Aug 21, 2014), abstract *available at*: http://www.ncbi.nlm.nih.gov/pubmed/25147247.

[123] Recent survey results indicate that users are concerned about privacy and want more transparency and control over the collection and use of their personal information as well as choices about advertising and geolocation tracking. *See* TRUSTe and Harris Interactive, *Mobile Privacy: A User's Perspective* (Apr. 2011)*, available at:* https://www.truste.com/resources/harris-mobile-survey/. *See also* Mark Hachman, *Most Mobile Apps Lack Privacy Policies*: *Study*, PC Magazine (Apr. 27, 2011), *available at:* http://www.pcmag.com/article2/0,2817,2384363,00.asp.

Privacy policies may be difficult to locate and read

Some NCEs may limit the openness and transparency of their privacy policies by placing these policies in obscure locations or otherwise preventing them from being readily visible. For example, some websites examined required individuals to click through multiple links to find privacy policies or go out of their way when completing a transaction to locate the privacy policy.[124] Other sites scattered privacy information among multiple documents that were not labeled as privacy policies, for example placing this information in Terms and Conditions pages or in Frequently Asked Questions (FAQs) pages. Some privacy policies could be found only after scrolling through advertisements.[125] These practices limit an individual's ability to locate an entity's privacy policy and may suggest a lack of openness and transparency. In turn, consumers may not properly understand what individually identifiable information is collected, how it may be used by the vendor, and to what extent the users are able to control the use of that data.

Additionally, mHealth technologies' privacy policies, terms of service and other notices are frequently difficult to read.[126] In particular, presenting a comprehensive privacy policy and other critical information over a device with relatively small screens is challenging. In 2013, FTC staff issued a report examining these challenges and recommending ways that key players in the mobile marketplace can better inform consumers about their data practices.[127]

The content of privacy notices and policies may be misunderstood or lacking

Privacy Notices

Where NCEs do have privacy policies, the study found that individuals may not fully understand the content provided in the policies, the full scope of data use and sharing described by the policy, or specific jargon used within privacy policies. For example, some policies employ language that is incomprehensible to the average reader, overwhelm the reader with detail, and

---

[124] *See* FTC Report, *Protecting Consumer Privacy in an Era of Rapid Change*, *supra* note 105. In addition, some websites link to privacy policies that were in small type or located at the bottom of the vendor's websites where an individual may have difficulty locating the policy.

[125] Maximus Report, *supra* note 25.

[126] Center for Democracy & Technology (CDT) and Future of Privacy Forum, *Best Practices for Mobile Application Developers,* Beta Version (Dec. 21, 2011), *available at:* https://www.cdt.org/files/pdfs/Apps%20Best%20Practices%20v%20beta.pdf (releasing a primer for mobile application developers who are interested in preserving consumer privacy); Mobile Marketing Association (MMA) Privacy & Advocacy Committee, *Mobile Application Privacy Policy* (Dec. 2011), *available at:* http://www.mmaglobal.com/whitepaper-request?filename=MMA_Mobile_Application_Privacy_Policy_15Dec2011PC_Update_FINAL.pdf (releasing a mobile application privacy policy framework guideline document for the mobile application development community); Groupe Spécial Mobile Association (GSMA), Mobile and Privacy, *Privacy Design Guidelines for Mobile Application Development* (March 2012), http://www.gsma.com/documents/privacy-design-guidelines-for-mobile-application-development/20008.

[127] FTC Staff Report: *Mobile Privacy Disclosures, supra* note 105. The report describes themes from the FTC's related workshop, including lack of consumer awareness and understanding about mobile collection and use practices, the importance of design to address limitations of notice on small screens, and the key role of platforms. It also suggests some best practices for the various players in the ecosystem.

include exceptions within exceptions.[128] Some are not even available in the user's preferred language and literacy level. Privacy policies may also note that information is shared with affiliates. Individuals may not realize that an organization could have hundreds of affiliates or that third parties combine consumer data with other consumer data obtained from other sources.[129] Individuals may believe that if a website offers a privacy policy then that means that the individuals' data is protected by the website.[130] Individuals may not appreciate that privacy policies actually define what data use policies the vendor engages in and provide the consumer the opportunity to acknowledge and agree to those data use practices.

In short, vendors' privacy policies may not qualify as open and transparent when individuals may not be able to properly interpret and assess privacy and security practices of non-HIPAA covered PHRs and other online vendors by reading them.

Consistent Definitions of Key Terms

The terms "health information," "individually identifiable health information," "protected health information," and "personally identifiable information" have specific regulatory meanings. Personal health information and sensitive health information are not so defined but are often used in discussion of health information privacy and their inferential meanings often overlap. Yet, an individual or a product developer may not know these specific meanings or think only of either content or who holds the data, but not both, when thinking about data protections.

Further, privacy policies may also use specific terminology without properly defining those terms within the context of information use practices.[131] One particular practice – a PHR's assurance that its privacy policy is "HIPAA-compliant" – suggests some official designation from regulators, which is not the case, and may also create confusion among consumers. Some PHRs state that their privacy policies are "HIPAA-compliant" or their policies "adhere to" or "follow" HIPAA standards, or "use HIPAA as a guideline." These general statements may fail

[128] *See* Sunyaev, *supra* note 122.
[129] *See* FTC Report, *Protecting Consumer Privacy in an Era of Rapid Change*, *supra* note 105.
[130] *See* FTC "Exploring Privacy" Roundtables, *1st Roundtable, Remarks of Joseph Turow, University of Pennsylvania* (citing surveys showing that most respondents believe incorrectly that the existence of a privacy policy means that a company protects privacy by not sharing consumer information), *available at* http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.164.508&rep=rep1&type=pdf. *See also Written Comment of Lorrie Faith Cranor, Timing is Everything? The Efforts of Timing and Placement of Online Privacy Indicators,* cmt. #544506-00039, p. 2, ("[m]any Internet users erroneously believe that websites with seals have adopted consumer-friendly privacy practices."); *see also* Chris Hoofnagle, Jennifer King, Su Li, and Joseph Turow, *How Different are Young Adults from Older Adults when it Comes to Information Privacy Attitudes & Policies (*April 14, 2010), *available at:* http://ssrn.com/abstract=1589864 (noting that individuals may believe that the existence of a privacy policy on a website means that their privacy is protected and that they have legal rights to sue if it is not).
[131] For example, policies may use phrases indicating the vendor will "aggregate" or "anonymize" data, without specifically explaining what that means. For example "aggregating" data may not fully explain to a consumer the specific actions the vendor may take with her health information, while a commitment to "anonymize" data may not fully explain the likelihood of re-identification of her data.

to explain to consumers that the PHR is not legally required to follow HIPAA and also may not indicate to what degree the PHR's privacy policy actually follows the mandates of HIPAA.[132]

Furthermore, HIPAA defines "health information" in reference to both *who* creates or receives it and *what* the information collected consists of. For example, under HIPAA, health information is "any information, whether oral or recorded in any form or medium, that: (1) is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse, *and* relates to (a) the past, present, or future physical or mental health or condition of an individual; (b) the provision of health care to an individual; or (c) the past, present, or future payment for the provision of health care to an individual."[133] In contrast, the term "health information" also has a common, or layperson's, meaning, which is how we are most commonly using it in this Report.[134]

Privacy policies for websites and mHealth technologies change without notice and may be focused on internet web tracking, not use of data supplied by individuals

A final issue regarding privacy policies identified in the study is that where entities do have privacy policies, they may modify those policies without notice. The study found that NCEs may adopt practices when updating their privacy policies that individuals may not understand and that may change the individual's legal rights and obligations. Many of the non-HIPAA covered entities examined as part of the study simply informed individuals that the vendor will post material changes to the entity's privacy policy on its website and that the consumers' continued use of the website indicates the individuals' acceptance of the changes to the policy's terms.[135] Several PHRs simply informed individuals that changes to the PHR's privacy policy would be effective immediately, even if not yet posted to the PHR website.[136]

---

[132] These types of activities may violate the FTC's prohibition on unfair or deceptive acts or practices. For example, in the FTC's recent settlement with Henry Shein Practice Solutions, Inc., *see supra* note110, the FTC's complaint alleged, among other things, that the software provider misrepresented that its software provided industry-standard encryption as required by HIPAA. *Henry Schein Practice Solutions, Inc.*, No. 1423161 (F.T.C. Jan. 5, 2016) (complaint and proposed consent order), *available at:* https://www.ftc.gov/enforcement/cases-proceedings/142-3161/henry-schein-practice-solutions-inc-matter. Further, other PHR privacy policies surveyed do not discuss HIPAA at all. In the absence of an assurance that HIPAA does not cover the vendor's PHR, a consumer may conclude that the PHR provides the same privacy and security protections to health information that HIPAA-covered PHRs are required to provide. Maximus Report, *supra* note 25.

[133] 42 U.S.C. § 1320(d)(4) (2011); 45 C.F.R. § 160.103 (2011).

[134] *Supra* note 6.

[135] Maximus Report, *supra* note 25.

[136] Testimony of Matthew Wynia, NCHVS Subcommittee on Privacy, Confidentiality, and Security, Hearing on Personal Health Records (May 8, 2009), *available at:* http://www.ncvhs.hhs.gov/wp-content/uploads/2014/05/090521p6.pdf. The FTC has previously alleged that a company's retroactive application of a materially changed privacy policy to information it had previously collected from consumers was an unfair practice under Section 5. *Gateway Learning Corp.*, No. C-4120 (F.T.C. Sept. 10, 2004) (decision and order), a*vailable at:* https://www.ftc.gov/enforcement/cases-proceedings/042-3047/gateway-learning-corp-matter (settling allegations against marketer of learning products that revised its privacy policy to permit third party sharing of consumers' personal information and then, without further alerting consumers, applied this policy to personal information it had previously collected from consumers when its privacy policy stated it would not share this information). *See also* Maximus Report, *supra* note 25. If an individual is notified of a changed PHR privacy policy, but finds the new terms unacceptable and has no ability to opt out of the changed policy, then the consumer may be frustrated at her lack of control over the site's data usage policies after having selected and managed her PHR at that site.

Inadequate Collection, Use, and Disclosure Limitations

One key element of FIPPS is the principle of collecting only the information that is needed (limitation), then collecting it and subsequently using or sharing it for a specific context (use). [137] While FIPPS, as principles, are available to inform any data collection processes and businesses, study findings suggest that NCEs may not adopt the FIPP of collecting only the information necessary. In other words, NCES may not ensure health information is "collected, used and/or disclosed only to the extent necessary to accomplish a specified purpose, and never to discriminate inappropriately."[138] Individuals may be able to control what they initially share with the NCE, for example by choosing to give health information to the NCE, or not. Individuals may not realize, however, that once they do give data to the NCE there is a possibility that they could lose control over the information or that once information is divulged, the information may leave the hands of the NCE or the NCE may further share the information, perhaps for a fee. Among the studies, the following areas of concern were identified:

Advertising practices and third-party personal data collection may lack limitations on information sharing or use of information for marketing

According to the background study, NCEs have been found to engage in a variety of practices such as online advertising and marketing,[139] commercial uses or sale of individual information, and behavioral tracking practices, all of which indicate information use that is likely broader than what individuals would anticipate. NCEs have addressed this in different ways. For example, some PHR vendors inform individuals that advertising may be present on the PHR site and that use of the site indicates consent to the advertising. Others may offer a free version of their product with advertising and a paid version without advertising, while some sites allow the consumer to opt out of advertisements on the PHR.

Although many NCEs explain their policies on tracking devices such as cookies and web beacons, or inform individuals that the website will not allow advertisers or entities providing services through their websites to collect individual information, some NCEs do not explain what preventing the collection of identifying information means and how that is accomplished.[140] In addition, individuals may have difficulty distinguishing off-site linkages from NCE websites because a website may not clearly signal to an individual when the individual has left the NCE's website and entered the website of an advertiser offering services or products that may seek to collect individual data.[141] The variety of advertising, data collection, and behavioral tracking

[137] Contextual collection is described in detail in the IOT report, p. 39-46, *supra* note 10.
[138] ONC P&S Framework, *supra* note 11.
[139] Online behavioral advertising is the practice of collecting information about individuals' online interests in order to deliver targeted advertising to them. *See* FTC Staff Report , *Self-Regulatory Principles for Online Behavioral Advertising*, at 2 (Feb. 2009), *available at*: https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-staff-report-self-regulatory-principles-online-behavioral-advertising/p085400behavadreport.pdf (stating that such advertising and marketing "involves the tracking of consumers' online activities in order to deliver tailored advertising").
[140] Some tracking companies use unique phone identification numbers to create profiles of cellphone users for marketing purposes. Wall Street Journal Staff, WSJ Blog, *Unique Phone ID Numbers Explained* (December 19, 2010), *available at:* http://blogs.wsj.com/digits/2010/12/19/unique-phone-id-numbers-explained/.
[141] Links may also be to third-party service providers that may be interested in collecting health information.

practices that PHR vendors and other NCEs engage in may lead individuals to unknowingly supply data to other entities.[142] In the U. S. economy, health care spending is approximately 17 percent of GDP.[143] Globally, mHealth has been projected to be a $60 billion worldwide financial opportunity.[144] Thus the significant gap between restrictions on the use of health information for marketing by entities that are and are not covered by HIPAA has significant ramifications.

VI. SUMMARY & CONCLUSIONS

To ensure privacy, security, and access by consumers to health data, and to create a predictable business environment for health data collectors, developers, and entrepreneurs to foster innovation, the gaps in oversight identified in this Report should be filled. Some policymakers have noticed the gaps in oversight of NCEs and have worked in collaboration with industry to fill these gaps and identify best practices while keeping pace with the rapid development of technology. For example, the efforts-to-date of the FTC include:

(1) Enforcement against entities engaging in privacy and security-related violations under the FTC Act.
(2) Policy and informational initiatives, such as the FTC's IOT Report, the FTC's report on Mobile Privacy Disclosures, and the FTC's 2014 seminar on Consumer Generated and Controlled Health Data.[145]
(3) Consumer education and business outreach.[146]

Similarly, the Department of Health and Human Services has worked to improve patient access to PHI, to educate users on risks to the confidentiality, integrity, and availability of ePHI, to empower patients to move their data when and where they need it, and to develop substantial educational materials[147] and provide robust technical assistance to help entities covered by

[142] Maximus Report, *supra* note 25.
[143] *See* Centers for Medicare & Medicaid Services Report: *National Health Expenditures 2014 Highlight* (May 5, 2014), *available at:* www.cms.gov/.../NationalHealthExpendData/Downloads/highlights.pdf.
[144] Teresa Wang and Gandhi Malay, *Digital Health Consumer Adoption* (2015), *available at:* http://rockhealth.com/reports/digital-health-consumer-adoption-2015/.
[145] IOT Report, *supra* note 11; FTC Staff Report: *Mobile Privacy Disclosure, supra* note 139. *See also* Consumer Generated and Controlled Health Data seminar (May 7, 2014), *available at:* https://www.ftc.gov/system/files/documents/public_events/195411/consumer-health-data-webcast-slides.pdf.
[146] *See, e.g.*, *Careful Connections: Building Security in the Internet of Things* (Jan. 2015), *available at:* https://www.ftc.gov/system/files/documents/plain-language/pdf0199-carefulconnections-buildingsecurityinternetofthings.pdf; *Mobile App Developers: Start with Security* (Feb. 2013), a*vailable at:* https://www.ftc.gov/tips-advice/business-center/guidance/mobile-app-developers-start-security.
[147] *See* http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/special/healthit/phrs.pdf; http://www.hhs.gov/hipaa/for-individuals/guidance-materials-for-consumers/index.html; and http://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html (OCR guidance on the right of individuals under HIPAA to access their health information). In addition, to support transparent information practices to consumers by NCEs, ONC has published in the Federal Register a Request for Information to update its "model privacy notice," an open-source tool ONC published in 2011 for developers and consumers, *available at*: https://www.federalregister.gov/articles/2016/03/01/2016-04239/request-for-information-on-updates-to-the-onc-voluntary-personal-health-record-model-privacy-notice.

HIPAA comply with the rules.[148] HHS has also committed to providing more guidance for developers of technologies offered by NCEs, as well as for entities that are unsure whether they are covered by HIPAA.[149] These efforts are consistent with overall efforts of the Obama Administration to improve data security, privacy, and consumer protection through legislative proposals,[150] regulations,[151] Executive Orders,[152] and the Precision Medicine Initiative.[153] The private sector has attempted to fill the gaps as well, through published codes of conduct that private sector organizations can adopt if they choose. For example, in October 2015, the Consumer Electronics Association (CEA) issued "Guiding Principles on the Privacy and Security of Personal Wellness Data."[154] These guidelines *can* be adopted by companies, but are not required of CEA members. As of July 2016, we have been unable to identify any companies that have adopted the guidelines.[155] In short, despite the best efforts of the Administration, the FTC, and industry, no widely adopted, comprehensive voluntary code of conduct has emerged.

A critical piece of improving health care for patients in today's system involves the patient being at the center of his or her care. This includes having access to data about their health, while maintaining the confidentiality and integrity of that data. FTC and HHS each have broad experience in protecting consumers against privacy and security risks to health data to the extent of their existing statutory authorities (as described in more detail in this Report). FTC has a well-developed body of law enforcing privacy and security practices that are unfair and deceptive, including taking action against an organization that adopts a code of conduct, but does

---

[148] *See* https://www.healthit.gov/providers-professionals/your-mobile-device-and-health-information-privacy-and-security; OCR App Developer Portal, *available at:* http://hipaaqsportal.hhs.gov/; and ONC 2015 Edition Final Rule, *supra* note 8.

[149] HHS Response Letter, *supra* note 23; *see also*, White House: *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy* (February 2012), *available at*: https://www.whitehouse.gov/sites/default/files/email-files/privacy_white_paper.pdf; HHS Office for Civil Rights, *Health App Use Scenarios and HIPAA* (Feb. 11, 2016), *available at:* http://www.hhs.gov/blog/2016/02/11/ocr-adds-new-health-app-use-scenarios-to-developer-portal.html.

[150] President's proposal on Cybersecurity Legislation (Jan. 13, 2015), *available at:* https://www.whitehouse.gov/the-press-office/2015/01/13/securing-cyberspace-president-obama-announces-new-cybersecurity-legislat. The Consumer Privacy Bill of Rights Act (Feb. 27, 2015), *available at:* http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf.

[151] ONC 2015 Edition Certification Final Rule, *supra* note 20, and OCR Omnibus HIPAA Rule, http://www.hhs.gov/about/news/2013/01/17/new-rule-protects-patient-privacy-secures-health-information.html#.

[152] White House *Executive Order 13636 on Improving Critical Infrastructure Cybersecurity* (Feb. 12, 2013), *available at:* https://www.whitehouse.gov/issues/foreign-policy/cybersecurity/eo-13636; White House *Executive Order 13931 on Promoting Private Sector Cyberthreat Information Sharing* (Feb. 13, 2015), *available at:* https://www.whitehouse.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari.

[153] White House *PMI Privacy and Trust Principles*, *supra* note 99, and White House, PMI Data Security Policy Principles and Framework, *available at:* https://www.whitehouse.gov/sites/whitehouse.gov/files/documents/PMI_Security_Principles_and_Framework_FINAL_022516.pdf.

[154] Consumer Electronics Association, *Guiding Principles on the Privacy and Security of Personal Wellness Data(*Oct. 20, 2015), *available at:* https://www.cta.tech/News/Press-Releases/2015/October/Association-Unveils-First-of-Its-Kind,-Industry-Su.aspx.

[155] If an entity were to adopt the CEA guidelines, the FTC would have the authority to enforce failures to abide by them, as described in the body of the Report.

not adhere to that code. HHS' experience includes well-established regulations about health data privacy and security, as well as in-depth knowledge of the ways that very sensitive data moves (and will move in the future) among FDA-regulated devices, EHRs, mHealth apps connecting into medical environments, and the emerging connectivity among them in health care delivery settings.

As this Report shows, however, large gaps in policies around access, security, and privacy continue, and confusion persists among both consumers and innovators. Wearable fitness trackers, health social media, and mobile health apps are premised on the idea of consumer engagement. However, our laws and regulations have not kept pace with these new technologies. This Report identifies the lack of clear guidance around consumer access to, and privacy and security of, health information collected, shared, and used by NCEs.