COMPLIANCE ELLIANCE JOURNAL

DIGITAL HEALTH REGULATORY GAPS IN THE UNITED STATES

Kirk J. Nahra & Bethany A. Corbin

AUTHORS

Kirk J. Nahra is a partner with Wiley Rein LLP in Washington, D.C., where he specializes in privacy and information security litigation and counseling. He is chair of the firm's Privacy Practice and assists companies in a wide range of industries in analyzing and implementing the requirements of privacy and security laws across the country and internationally. He provides advice on data breaches, enforcement actions, contract negotiations, business strategy, research and de-identification issues, and privacy, data security, and cybersecurity compliance. He also works with insurers and health care industry participants in developing compliance programs and defending against government investigations into their practices. Kirk, a Certified Information Privacy Professional (CIPP/US), is a longtime member of the Board of Directors of the International Association of Privacy Professionals, and serves on the Advisory Board for the Health Law Reporter, the Privacy and Security Law Report, and the Health Care Fraud Report. He has held leadership positions with various groups within the American Health Lawyers Association and the American Bar Association Health Law Section. He is rated by Chambers USA in the nation's top-tier of privacy attorneys. Kirk can be reached at: E-mail: knahra@wileyrein.com; Phone: (202) 719-7335; Twitter: @KirkJNahrawork.

Bethany A. Corbin is a complex litigation and regulatory compliance attorney with Wiley Rein LLP in Washington, D.C. She represents health care, pharmaceutical, telecommunications, and technology clients in judicial and administrative proceedings. She is a Certified Information Privacy Professional (CIPP/US) and provides strategic advice to health care organizations concerning privacy and cybersecurity. In December, Bethany will obtain her Health Care LL.M. from Loyola University of Chicago, where she has focused her studies on the intersection of health care and technology, including the Internet of Medical Things. Bethany currently serves as the Young Lawyer Representative to the Cybersecurity and Data Privacy General Committee of the Tort, Trial, and Insurance Practice Section of the American Bar Association. Bethany can be reached at: E-mail: bcorbin@wileyrein.com; Phone: (202) 719-4418; Twitter: @BethanyACorbin.

ABSTRACT

Digital health in the United States is rapidly and continuously evolving to enhance patient care and revolutionize health care delivery. This technology offers substantial promise to both patients and providers, but lacks a comprehensive regulatory structure to ensure adequate safety and privacy. While the Department of Health and Human Services, the Food and Drug Administration, and the Federal Trade Commission regulate portions of the digital health industry, their oversight is incomplete, with numerous digital health companies falling between the cracks and assuming an unregulated status. This article analyzes the state of digital health legal and regulatory oversight in the United States, discusses how state legislatures and industry organizations have worked to fill existing legal gaps, and presents strategies for encouraging compliance for unregulated entities.

TABLE OF CONTENTS

I. INTRODUCTION

The boundaries and applications of digital health are rapidly evolving. From wearable fitness sensors to ingestible pills to Internet-connected pacemakers and insulin pumps, digital health has the potential to transform the health care sector and revolutionize patient care. The benefits from digital health are undeniable: patients can assume greater responsibility for the management of chronic conditions while accessing medical care at their convenience and in their own homes.[1] Technology-based health care can further reduce the costs of care and help address the physician shortage across America.[2] These benefits are a significant incentive to increase the adoption of mobile and digital technology in the health care industry, and the rate of this adoption is only projected to increase.

While digital health offers substantial promise, it suffers to some extent from a lack of comprehensive regulation. This regulatory gap presents potential concerns both for patients—who may not be provided with appropriate protections—and for the industry, which will see compliance, operational and strategic challenges in designing products that meet with existing standards, potential future regulation, and consumer and regulator expectations. Privacy laws in the United States are sectoral and patchwork in nature, and those related to health care have not been significantly revised to address technological innovation. Privacy and security for digital health applications are therefore in flux, with some subsections of the industry unregulated by federal law. This article analyzes the scope and gaps of health care privacy and security laws in the United States and discusses available privacy and cybersecurity frameworks that exist for unregulated health care actors.

II. WHAT IS DIGITAL HEALTH?

The term digital health, at its most basic, refers to the intersection of health care and the Internet. Digital technologies that fall within this category are broad, and may include mobile health (mHealth), health information technology (HIT), wearable devices, telemedicine, the Internet of Things (IoT), and personalized medicine.[3] While these technologies serve different functions—for example, HIT includes electronic health records and e-prescribing whereas IoT concerns sensors that interact between humans and machines to collect relevant health care data for diagnosis and disease management—they share one

---

1 See U.S. DEP'T HEALTH & HUMAN SERVS., EXAMINING OVERSIGHT OF THE PRIVACY & SECURITY OF HEALTH DATA COLLECTED BY ENTITIES NOT REGULATED BY HIPAA 2 (2016), https://www.healthit.gov/sites/default/files/non-covered_entities_report_june_17_2016.pdf (last visited Aug. 20, 2018, 01:30 PM). [hereinafter HHS HIPAA OVERSIGHT REPORT]

2 Jeff Lagasse, *With Physician Shortage Looming, Hospitals Turn to Telehealth Tools*, HEALTHCARE FINANCE (June 1, 2018), https://www.healthcarefinancenews.com/news/physician-shortage-looming-hospitals-turn-telehealth-tools (last visited Aug. 20, 2018, 01:35 PM).

3 Charlotte A. Tschider, *Enhancing Cybersecurity for the Digital Health Marketplace*, 26 (1), ANNALS HEALTH LAW 1, 4 (2017).

fundamental overriding goal: to use technology as a method for improving health care and increase the access and quality of medical services.

The advent and adoption of digital health has the potential to profoundly impact the health care economy over the next several decades. To date, the United States has spent approximately 18% of its Gross Domestic Product on health care every year, and this figure is expected to increase to 20% by 2025.[4] Digital health, however, is simultaneously expected to grow by a compounded annual growth rate of 26% in the upcoming years, and is projected to top $379 billion by 2024.[5] These anticipated technological developments in the health care space may increase pressure to create and implement lower-cost health care solutions and incentivize companies to continue developing digital health products.[6] Significant shifts in the delivery of health care could be witnessed over the next several years.

III. DIGITAL HEALTH RISKS

Although the benefits of digital health are undeniable, concerns exist regarding the privacy and security of data collected through digital technologies. Like all digital platforms, Internet-connected health care devices pose privacy and security risks for their users. First, digital health applications collect and store patient health data, which may contain extremely sensitive information. Without proper security safeguards, this personal data may be unlawfully accessed by unauthorized users, resulting in a breach of personal information. Such a breach not only harms the business and reputation of the digital device manufacturer, but also exposes critically sensitive patient data. There is no shortage of bad actors attempting to access medical data. Indeed, health data is one of the most lucrative objects for sale on the black market, fetching higher prices than social security numbers and financial information.[7] Thus, the traditional data breach risk that is present with any Internet technology is amplified in the health care context due to value-laden sensitive data.

Second, device interoperability and network connectivity bring the possibility for new attack vectors and vulnerabilities.[8] A network hosting interconnected devices exponentially expands its attack surface such that a security flaw or breach in any device operates as a backdoor entry point into the entire system.[9] These digital health devices weaken the

4 Id. at 3.

5 Keith Speights, *What Is Digital Health?*, MOTLEY FOOL (May 9, 2017, 7:04 AM), https://www.fool.com/investing/2017/05/09/what-is-digital-health.aspx (last visited Aug. 20, 2018, 01:37 PM).

6 Tschider, supra note 3, at 4.

7 See generally PRESIDENT'S NAT'L SEC. TELECOMMUNICATIONS ADVISORY COMMITTEE, NSTAC REPORT TO THE PRESIDENT ON THE INTERNET OF THINGS ES-1 (Nov. 19, 2014), https://www.dhs.gov/sites/default/files/publications/NSTAC%20Report%20to%20the%20President%20on%20the%20Internet%20of%20Things%20Nov%202014%20%28updat%20%20%20.pdf (last visited Oct. 23, 2018, 01:35 PM).

8 Id. at 7.

9 See id. at 1.

overall security of a medical IT network by their mere presence on the network, and further create access points that must be monitored and evaluated by the organization's technology team. Unauthorized access into a network further has the potential to compromise data integrity, which can negatively impact patient care and treatment plans.

Finally, digital health offers a unique risk that is not present with all Internet-based platforms: bodily harm. Digital health devices that are implanted into a patient's body, such as a cardiac pacemaker, may use the Internet to receive signals or instructions from a health care provider. Hijacking a pacemaker could allow an unauthorized third party to manipulate the device's functionality and cause significant bodily harm or death. This same scenario is present with digital insulin pumps, where device hijacking could alter the dose of insulin a patient receives.

Thus, digital health presents privacy, security, and resiliency risks that must be addressed and mitigated. These risks are increasingly being discussed in public policy circles, with the widespread recognition that technology advances faster than policy. The result is a crucial gap between legal frameworks and technological reality that heightens the security and privacy risks associated with digital health technology.

IV. DIGITAL HEALTH LEGAL & REGULATORY FRAMEWORKS

Digital health in the United States does not exist in an unregulated environment. Rather, the United States has adopted a sectoral approach to privacy that vests regulatory authority for the health care sector with three federal government agencies (in addition to potential regulation in each of the states): The Department of Health and Human Services (HHS), the Food and Drug Administration (FDA), and the Federal Trade Commission (FTC). In terms of privacy and security, HHS's Office for Civil Rights (OCR) plays a dominant role in its enforcement of the Health Insurance Portability and Accountability Act (HIPAA).[10] HIPAA represents the main legal framework addressing privacy and security requirements for the health care industry, and its applicability to digital health technologies is the focus of this article. In addition to HHS, the FDA regulates the efficacy and safety of medical "devices",[11] and has proposed voluntary cybersecurity guidance for connected medical devices.[12] Finally, the FTC has broad non-industry-specific enforcement powers that stem from Section 5(a) of the Federal Trade Commission Act (FTC Act).[13] Pursuant to the FTC Act, the FTC may regulate unfair and deceptive trade practices in or affecting commerce. While the FTC Act does not specifically mention privacy,

---

10 See HHS HIPAA OVERSIGHT REPORT, supra note 1, at 3.

11 Medical Device Overview, U.S. FOOD AND DRUG ADMINISTRATION (last updated Sept. 14, 2018), https://www.fda.gov/forindustry/importprogram/importbasics/regulatedproducts/ucm510630.htm (last visited Aug. 28, 2018, 01:58 PM).

12 See Postmarket Management of Cybersecurity in Medical Devices - Guidance for Industry and Food and Drug Administration Staff, U.S. FOOD & DRUG ADMINISTRATION (Jan. 22, 2016), https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm482022.pdf (last visited Aug. 28, 2018, 01:53 PM).

13 See HHS HIPAA OVERSIGHT REPORT, supra note 1, at 3.

the FTC has brought numerous cases under Section 5(a) alleging that companies have engaged in deceptive acts by failing to adhere to their stated privacy policies and procedures. This article next considers the scope and gaps of these regulatory frameworks as applied to digital health technology, and discusses efforts by state legislatures to bridge these gaps.

A. The Health Insurance Portability and Accountability Act: Scope & Applicability

In 1996, Congress passed the Health Insurance Portability and Accountability Act to enhance the portability of health insurance coverage and reduce the administrative costs and burdens associated with health care delivery.[14] Neither of these primary goals were directed at privacy and security—instead, the privacy and security rules that resulted from the HIPAA law were not discussed in any substantive way in the HIPAA statute. Instead, when Congress failed to step in and create a privacy and security law, HHS (later supplemented by the Health Information Technology for Economic and Clinical Health Act (HITECH Act)), created federal regulatory protections for the privacy and security of certain health information in certain settings when held by certain entities—with the scope of these rules defined by the "non-privacy" goals of the HIPAA statute.[15] The HIPAA Privacy Rule sets forth required limitations on the use and disclosure of protected health information (PHI),[16] while the HIPAA Security Rule mandates administrative, technical, and physical safeguards for electronic PHI.[17] Essentially, HIPAA seeks to protect health information by prohibiting disclosures of information that are unlawful or unauthorized, and ensuring that applicable health care entities enact reasonable and appropriate security safeguards for the data they collect or store.

While the scope of HIPAA appears broad, its privacy and security requirements apply only to health care organizations that qualify as "covered entities."[18] A covered entity is any health plan, health care provider, or health care clearinghouse, as those terms are statutorily defined (again, driven by concerns about portability and administrative simplification and not privacy or security).[19] In 2009, the HITECH Act extended HIPAA's provisions to "business associates," which include persons or organizations that perform certain functions on behalf of a covered entity involving the use or disclosure of PHI—essentially, service providers to these covered entities where the services involve individual information.[20] PHI, in turn, is defined as individually identifiable health information

---

14 Kirk J. Nahra, *HIPAA Privacy and Security for Beginners*, WILEY REIN (July 2014), https://www.wileyrein.com/newsroom-newsletters-item-5029.html (last visited Aug. 28, 2018, 01:55 PM).

15 See id.

16 See 45 C.F.R. § 164.502; DEP'T HEALTH & HUMAN SERVS. OFFICE FOR CIVIL RIGHTS, SUMMARY OF THE HIPAA PRIVACY RULE 1 (last revised May 2003), https://www.hhs.gov/sites/default/files/privacysummary.pdf?language=en (last visited Aug. 28, 2018, 02:05 PM).

17 See 45 C.F.R. §§ 164.308-312.

18 See, e.g., 45 C.F.R. § 164.502.

19 Id. § 160.103; Nahra, supra note 14.

20 See 45 C.F.R. § 160.103.

that a covered entity or its business associate holds or transmits in any form or media.[21] The foundational principle of HIPAA is that a covered entity or business associate may not use or disclose PHI except as either expressly permitted in the Privacy Rule, or as authorized by the patient in writing. A covered entity is only required to disclose PHI in two circumstances: (1) to the patient herself when requested; and (2) to HHS as part of a compliance investigation or enforcement action.[22] A covered entity is permitted—but not required—to disclose PHI without first obtaining the patient's authorization (with presumed consent under the HIPAA Privacy Rule) for the "core" purposes of the health care system—treatment, payment, and performance of health care operations (TPO) (essentially the administrative operations of a health care business).[23] There also are various "public policy" rationales for the use and disclosure of PHI. All other uses and disclosure of PHI not expressly permitted by the Privacy Rule require an individual's written authorization.

B. HIPAA and Digital Health Technology: Assessing the Gaps

Although HIPAA may appear at first blush to be a comprehensive privacy framework for the health care industry, it has significant gaps and limitations when applied to digital health technology.[24] First, HIPAA's protections only extend to digital health actors that qualify as covered entities. When HIPAA was originally drafted, HHS only had authority to create a privacy rule applicable to covered entities such as health care providers and health insurers.[25] This means organizations that do not qualify as covered entities or business associates typically have no obligation to comply with HIPAA's requirements. For example, a company manufacturing a fitness tracker that collects basic health information such as height, weight, and biometric data, would not be subject to HIPAA's regulations because the company provides this product directly to an individual consumer without the involvement of a doctor or health insurer. The company does not provide or pay the cost of an individual's medical care, does not provide medical services, and does not process non-standard data received from another entity into a standardized format (e.g., billing companies, community health management information systems, etc.). In other words, the company is not a covered entity (i.e., it is not a health plan, a health care provider, or a health care clearinghouse). Thus, this company would fall outside the bounds of HIPAA's privacy and security regulations despite the fact that it collects sensitive health data.

---

21 Id.

22 Id. § 164.502; Nahra, supra note 14.

23 45 C.F.R. § 164.502; Nahra, supra note 14.

24 See HHS HIPAA OVERSIGHT REPORT, supra note 1, at 20; Kirk J. Nahra, *What Closing the HIPAA Gaps Means for the Future of Healthcare Privacy*, HITECH ANSWERS (Nov. 9, 2015), https://www.hitechanswers.net/what-closing-the-hipaa-gaps-means-for-the-future-of-healthcare-privacy-2/ (last visited Aug. 28, 2018, 03:14 PM).

25 Nahra, supra note 24.

Second, HIPAA only protects and regulates PHI. PHI refers to individually identifiable health information (including demographic data) that relates to a person's physical or mental health, the provision of health care services to that individual, or payment for health care services, and that identifies the individual or would provide a reasonable basis for identification.[26] Health care data that does not satisfy this definition may be collected, used, and disclosed by a company without running afoul of HIPAA. For example, where health information has been de-identified or aggregated without disclosing individual identifiers, it does not constitute PHI and may be disclosed without an individual's consent or authorization.[27] In State ex rel. Cincinnati Enquirer v. Daniels, for instance, the Ohio Supreme Court held that the Cincinnati Enquirer could obtain copies of lead-contamination notices issued by the Cincinnati Health Department.[28] The court found that the notices did not reveal PHI even though they referenced an unnamed child whose blood test showed an elevated lead level.[29] Similarly, guidance on HHS's website notes that merely reporting the average age of health plan members is not PHI because the aggregated data does not identify any individual plan member.[30]

These limitations in HIPAA's scope present large regulatory gaps when applied to the digital health sector (except in those situations where a digital health product is provided directly by a HIPAA covered entity or in a business partnership with a provider or insurer). Today, with minor exceptions, most digital health companies do not qualify as covered entities or business associates, and remain unregulated by HIPAA. Similarly, some of these organizations may collect sensitive health data that does not qualify as PHI. When either of these scenarios occurs, the digital health company is not subject to HIPAA's privacy and security regulations, and may operate with significantly less federal oversight. The regulatory scheme created by HIPAA focuses largely on which entity holds the data, and not on the nature or sensitivity of the information being collected. This, in turn, allows a significant portion of the digital health sector to avoid compliance with these crucial HIPAA privacy and security standards.

C. FDA, FTC, and Medical Device Regulation

In addition to HHS's oversight of HIPAA, the Food and Drug Administration assumes a key role in the regulation of medical devices, including Internet-connected medical technology. The FDA's role, however, is limited primarily to ensuring the safety and efficacy of certain classifications of devices, and not all mobile or digital technologies will trigger

---

26 Id. § 160.103.

27 Id. § 164.502(d).

28 844 N.E.2d 1181 (Ohio 2006).

29 Id. at 523; Cuyahoga Cty. Bd. of Health v. Lipson O'Shea Legal Group, 50 N.E.3d 499, 501 (Ohio 2016)

30 Guidance Regarding Methods for De-Identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule, DEP'T HEALTH & HUMAN SERVS., https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/De-identification/hhs_deid_guidance.pdf (last updated Nov. 6, 2015).

FDA scrutiny.[31] Moreover, FDA regulations are not typically geared towards protecting patient privacy or security. While the FDA has released voluntary guidance "for managing postmarket cybersecurity vulnerabilities for marketed and distributed medical devices," this guidance is not mandatory.[32] The FDA does not require cybersecurity testing for any device, and relies on the device manufacturer to perform any voluntary security testing.[33] Further, the FDA does not regulate device privacy, leaving such devices to be covered (if at all) by HIPAA.

Similarly, the Federal Trade Commission has played a crucial part in privacy policy, enforcement, and best practices since the 1970s.[34] The FTC is an independent federal agency responsible for protecting consumers and promoting competition. While the FTC is not specific to health care, its regulatory authority extends to unfair and deceptive acts or practices, which may occur in the health care industry.[35] In particular, the FTC can bring enforcement actions to halt violations of privacy and security laws. The FTC has brought more than 500 enforcement actions to protect consumer privacy, and these actions address a wide range of issues, including spyware, mobile devices, file sharing, and spam.[36] Cases may also involve non-adherence to a privacy policy. Similarly, the FTC has initiated over 60 cases since 2002 against companies that failed to adequately protect consumers' personal data.[37] In this manner, FTC's authority is broad, but is not directed at preventing or regulating privacy and security standards in the health care industry. Instead, FTC acts as a watchdog to enforce existing privacy and security standards, but does not create those standards. Thus, while FTC may enforce existing privacy and security laws in the digital health context, it does not address legislative gaps that may leave digital health technology unregulated.

---

31 See Kirk J. Nahra, *New York Attorney General Addresses Key Health Care Privacy Gaps*, WILEY REIN (Apr. 2017), https://www.wileyrein.com/newsroom-newsletters-item-April_2017_PIF-NY_AG_Addresses_Key_Health_Care_Privacy_Gaps.html (last visited Aug. 28, 2018, 03:15 PM).

32 Postmarket Management of Cybersecurity in Medical Devices - Guidance for Industry and Food and Drug Administration Staff, U.S. FOOD & DRUG ADMINISTRATION 4 (Dec. 28, 2016), https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm482022.pdf (last visited Aug. 28, 2018, 01:43 PM).

33 Adam Brand, *Closing the Gap in Medical Device Cybersecurity*, PROTIVITI (Jan. 3, 2018), https://blog.protiviti.com/2018/01/03/closing-gap-medical-device-cybersecurity/ (last visited Aug. 28, 2018, 01:43 PM).

34 Protecting Consumer Privacy and Security, FEDERAL TRADE COMMISSION, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy-security (last visited Sept. 29, 2018, 04:33 PM).

35 See Privacy & Data Security Update:2017, FEDERAL TRADE COMMISSION, at 1 (Jan. 2017 – Dec. 2017), https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2017-overview-commissions-enforcement-policy-initiatives-consumer/privacy_and_data_security_update_2017.pdf (last visited Sept. 29, 2018, 04:19 PM).

36 Id. at 1-2.

37 Id. at 4.

D. State Regulatory Frameworks

As the gaps associated with federal legislation become more apparent, states have begun stepping in to ensure comprehensive privacy and security standards apply to digital health. In March 2017, for example, New York Attorney General Eric Schneiderman announced that his office settled three cases with various mobile health applications for insufficient or inappropriate privacy practices, and misleading privacy and security claims.[38] In bringing these cases, New York acted to fill a regulatory gap in FDA oversight—these digital health devices had not triggered FDA review—and the HIPAA Privacy Rule.[39] Specifically, although digital health devices were being used in these cases, the companies did not qualify as covered entities and, therefore, no federal privacy structure governed these organizations. The New York Attorney General stepped in to ensure privacy protections would be applicable to these digital health applications despite the absence of a comprehensive federal regulatory structure.[40] Such action signifies a potential shift toward "regulation through enforcement,"[41] which states may begin to use more frequently if federal privacy and security standards are not properly updated.

In addition to New York's enforcement action, states have also begun implementing legislation to patch the holes in federal regulations. The most recent and innovative action by a state is S.B. 327, a cybersecurity bill governing Internet of Things devices in California.[42] California Governor Jerry Brown recently signed this bill into law, making it the first state in the nation to adopt IoT legislation. This new law, which becomes effective on January 1, 2020, will mandate that any manufacturer or developer of a "smart" device—including connected health devices—ensure that the product is equipped with reasonable security features to protect the device and the information it houses.[43] Advocates of the bill hope that the new law will focus nationwide attention on the issue of IoT security, which extends beyond state boundaries.

Legislation, such as S.B. 327, is intended to bridge gaps in federal regulatory frameworks. Whereas a digital health company may escape HIPAA's grasp because it does not qualify as a covered entity, the company would still be subject to minimum privacy and security standards if it conducts business in California. The goal of such legislation is to minimize opportunities for organizations to collect sensitive data without being subject to some form of regulatory structure simply because the pace of technological innovation outpaces policy discussions.

As the nation reacts to S.B. 327, it will be interesting to observe whether other states implement comparable legislation, and whether upcoming bills will spur the federal legislature to create a comprehensive regulatory framework. Addressing privacy and security for

---

38 Nahra, supra note 31.

39 Id.

40 Id.

41 Id.

42 Senate Bill No. 327 (Cal. Sept. 28, 2018), available at https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201720180SB327 (last visited Sept. 29, 2018, 03:19 PM).

43 Id.

digital health and other Internet-connected devices on a state-by-state basis risks inconsistent standards and approaches, which could make it more difficult for digital health companies to determine their obligations, duties, and responsibilities. Comprehensive federal legislation could add consistency and predictability to privacy and security standards in digital health. However, until the federal legislature takes action, such standards will have to be developed and enforced by states and industry organizations.

V. THE DANGERS OF NON-REGULATION

Inconsistent or non-regulation of health care entities presents numerous risks that are unacceptable to both organizations and patients. Importantly, the lack of a mandatory regulatory regime may lead some digital health companies to avoid basic privacy and security practices altogether and endanger patient data. In many instances, economic incentives can cause digital health companies to push their devices to market with little consideration for security measures.[44] These devices, in turn, may be particularly susceptible to hacking, which can lead to the unauthorized acquisition of patient health data. Moreover, these devices may operate on larger health care networks and create backdoor entry points to accessing data from an entire health system that is otherwise secure. Such devices not only jeopardize the confidentiality and integrity of their own users' data, but also have the potential to create widespread breaches of health data at larger institutions.

Moreover, consumers are often not equipped to understand the difference between covered entities and non-covered entities and how this distinction drives digital health compliance. Instead, consumers may assume that their sensitive health data is protected and that adequate security measures will protect them from harm despite a contrary reality. The current regulatory framework assigns consumers the hardship of understanding the applicability of complex legal regulations to protect their own privacy and security.

Consumers, however, are not the only group harmed by gaps in digital health regulation. Digital health innovators and entrepreneurs are also adversely affected. In particular, having separate rules that apply to covered and non-covered entities can create confusion among tech innovators as to whether their products would be regulated under federal frameworks. This uncertainty may result in hesitant investors, which can delay or stifle technological innovation in the health care industry.[45] Further, a breach from lax security practices may cause immense reputational damage to the digital health company.

VI. ENCOURAGING COMPLIANCE

While federal regulatory compliance may not be mandatory for a large portion of the digital health industry, digital health companies should nonetheless ensure they are adhering to adequate privacy and security standards. The reason for this is, at a minimum, three-

44 See Paul Merrion, DHS Warns Insecure Internet of Things Could Spur Product Liability Lawsuits, CQ ROLL CALL WASH. DATA PRIVACY BRIEFING (Nov. 16, 2016), available at 2016 WL 6774799.

45 Alexis Guadarrama, *Mind the Gap: Addressing Gaps in HIPAA Coverage in the Mobile Health Apps Industry*, 55 (4) HOUSTON LAW REVIEW 999, 1017 (2018).

fold. First, consumers expect minimum privacy and security standards to be associated with their products, and can negatively impact a company's market share if that company fails to satisfy consumer expectations. Second, it is inevitable that unregulated digital health companies will eventually be subject to a privacy and security regulatory scheme. While the form of this comprehensive regulatory framework is currently unknown, the risks associated with unregulated digital health products are too great to leave this industry unattended. This has become evident with California's implementation of S.B. 327—if the federal legislature does not act, states will. Companies that delay implementing basic privacy and security standards now will be adversely impacted if a new regulatory structure takes effect. Moreover, it is likely that regulations for digital health companies will mirror privacy and security best practices in effect today. Digital health companies have the opportunity now to build strong compliance programs and privacy policies, which will result in a smooth transition under future regulations.

Finally, by participating in the privacy and security dialogue today, digital health companies can help establish the standards and requirements for future regulations that will govern their industry. Public-private stakeholder participation is actively encouraged as policymakers think through how to regulate new technologies without stifling innovation.[46] By engaging with privacy and security concerns today, digital health companies can advocate for regulations that will promote their business interests while protecting consumer data.

The question then becomes which frameworks should digital health companies adhere to when implementing privacy and security standards? The obvious choice is HIPAA, particularly for data security, even though its requirements are not yet mandatory for a significant portion of the digital health industry. As an established framework governing health care privacy and security compliance, HIPAA contains sufficient flexibility to adapt to varied circumstances and organizations, including digital health. By voluntarily complying with HIPAA (or trying to meet its standards where they make sense for the business), digital health companies can ensure they are implementing best practice standards in effect for the health care industry. Such compliance will also create consistency across the health care sector and avoid inconsistent application of privacy and security rules. Consumers will be better able to gauge their privacy and security rights and remedies with uniform implementation of HIPAA's rules. Indeed, numerous experts have counseled in favor of expanding HIPAA's reach to the digital health industry.[47] The downside to voluntary compliance with HIPAA, however, is not only the costs associated with implementing adequate standards, but also the concern that the traditional TPO model of disclosure under HIPAA may not fit well with consumer facing products.

An alternative is for digital health companies to implement industry-created cybersecurity

---

46 See Bethany Corbin & Megan Brown, *Partnerships Can Enhance Security in Connected Health and Beyond*, CIRCLEID (Dec. 14, 2017, 8:30 AM), http://www.circleid.com/posts/20171213_partnerships_can_enhance_security_in_connected_health_and_beyond/ (last visited Sept. 30, 2018, 05:19 PM).

47 See Mary Butler, *Is HIPAA Outdated? While Coverage Gaps and Growing Breaches Raise Industry Concern, Others Argue HIPAA is Still Effective*, 88 J. AHIMA 14 (2017), http://bok.ahima.org/doc?oid=302073#.W6TW0a2ZP-Y (last visited Sept. 29, 2018, 03:19 PM).

frameworks. Many HIPAA-regulated entities also follow one or more security frameworks developed by industry professionals to enhance the security and availability of patient data. Numerous frameworks exist, enabling digital health companies to adopt the framework that best meets their organizational structure and needs. The 2018 HIMSS Report surveyed health care organizations and identified the five primary security frameworks in use throughout the health care industry today:[48] (1) National Institute of Standards and Technology (NIST);[49] (2) Health Information Trust Alliance (HITRUST);[50] (3) Center for Internet Security (CIS) Critical Security Controls;[51] (4) International Organization for Standardization (ISO);[52] and (5) Control Objectives for Information and Related Technologies (COBIT).[53] Adoption of one of these voluntary cybersecurity frameworks will assist digital health companies with remaining up-to-date on cybersecurity hygiene and can offer insight into guarding against common security threats affecting the industry

VII. CONCLUSION

Digital health represents an advantageous development to enhancing patient wellness and health care delivery in the United States. With the potential to lower medical costs and serve broader patient populations, digital health is only projected to grow in the coming years. As this technological frontier develops, it is crucial that federal regulations evolve to safeguard patient privacy and security. The current regulatory framework for the health care industry contains significant gaps that exclude a majority of digital health companies from necessary federal oversight in their data collection practices. As Congress considers the most effective method to remedy these gaps, digital health companies should be proactive in their approach to privacy and security, including voluntary compliance with HIPAA and industry-created cybersecurity frameworks. Such proactive behavior not only promotes consumer confidence in the digital health company, but also enables the company to contribute to the dialogue on best practice standards for the digital health industry.

---

48 HIMSS, *2018 Himss Cybersecurity Survey,* 18 (2018), https://www.himss.org/sites/himssorg/files/u132196/2018_HIMSS_Cybersecurity_Survey_Final_Report.pdf (last visited Sept. 28, 2018, 02:49 PM).

49 National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity Version 1.1* (Apr. 16, 2018), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf (last visited Sept. 28, 2018, 03:19 AM).

50 CSF Version 9.1, HITRUST, https://hitrustalliance.net/hitrust-csf/ (last visited Sept. 21, 2018, 10:35 AM).

51 Download the CIS Controls V7 Today, CENTER FOR INTERNET SEC., https://learn.cisecurity.org/20-controls-download (last visited Sept. 21, 2018, 11:03 AM).

52 ISO 27001 - Information security management systems, INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, https://www.iso.org/isoiec-27001-information-security.html (last visited Sept. 21, 2018, 10:42 AM).

53 COBIT 4.1: Framework for IT Governance and Control, ISACA, https://www.isaca.org/knowledge-center/cobit/Pages/Overview.aspx (last visited Sept. 21, 2018, 10:44 AM).