Northwestern Journal of Technology and Intellectual Property

Volume 18
Issue 1 *Fall*

Article 4

11-2020

PROTECTING UNPROTECTED DATA IN MHEALTH

Jonathan Deitch
Northwestern Pritzker School of Law

Recommended Citation

Jonathan Deitch, *PROTECTING UNPROTECTED DATA IN MHEALTH*, 18 NW. J. TECH. & INTELL. PROP. 107 (2020).
https://scholarlycommons.law.northwestern.edu/njtip/vol18/iss1/4

PROTECTING UNPROTECTED DATA IN MHEALTH

Cover Page Footnote

Northwestern University Pritzker School of Law, J.D., 2021.

NORTHWESTERN
JOURNAL OF TECHNOLOGY
AND
INTELLECTUAL PROPERTY

PROTECTING UNPROTECTED DATA IN MHEALTH

Jonathan Deitch

November 2020 VOL. 18, NO. 1

Copyright 2020 by Jonathan Deitch
Northwestern Journal of Technology and Intellectual Property
Volume 18, Number 1 (2020)

PROTECTING UNPROTECTED DATA IN MHEALTH

*Jonathan Deitch**

ABSTRACT— Health-focused smartphone applications and internet of things (IoT) devices such as wearable fitness trackers (together, "mHealth"), offer a chance to monitor and manage health during the time spent away from a doctor. Unfortunately for consumers, much of personal health data generated by these devices and applications is critically unprotected by existing privacy laws in the United States. Due to the inadequacy of the current regulatory framework, there remain five crucial gaps of oversight and protection which plague many of these health-focused apps and devices: (A) Difference in Individuals' Access Rights; (B) Difference in Re-Use of Data by Third Parties; (C) Difference in Security Standards Applicable to Data Holders and Users; (D) Differences in Understanding of Terminology About Privacy and Security Protections; and (E) Inadequate Collection, Use, and Disclosure Limitations. This Note explores these oversight gaps and analyzes whether proposed and emerging solutions can meet this fundamental regulatory need. These solutions range from sweeping industry-agnostic privacy legislation to proposals targeted to this specific problem in mHealth. Overall, this Note will weigh the costs and benefits of these options as they are currently understood.

[*] Northwestern University Pritzker School of Law, J.D., 2021.

INTRODUCTION

As recently as 2016, Americans visited with their primary care physicians roughly 1.5 times per year on a per capita basis.[1] However, in 2020 the COVID-19 pandemic has at least temporarily altered the provision of healthcare in the United States, rapidly taking a sizeable subset of primary care visits from in-person to online.[2] While regular in-person clinician visits are an essential feature of a sound healthcare regimen, under normal circumstances clinical care accounts for only fifteen percent of overall health outcomes while social and behavioral determinants account for sixty percent.[3] For the health conscious, focusing on these social and behavioral determinants will likely become even more important as the current public health crisis alters the circumstances and manner in which we interact with health professionals. Especially in 2020, health-focused smartphone applications and internet of things devices (IoT), such as wearable fitness trackers (together, "mHealth"), offer a chance to monitor and manage health during the time spent away from a doctor, and show exciting promise for COVID-19 surveillance as well.[4] These applications and devices already collect substantial quantities of consumer health information and will gather exponentially more as their adoption increases and new use-cases are realized.[5] In fact, a recent study notes that the average patient will produce 2,750 times more data related to behavior and lifestyle compared to the data collected from their clinical encounters, with an estimated 1,100 terabytes of

[1] Pinyao Rui & Titilayo Okeyode, *National Ambulatory Medical Care Survey: 2016 Summary Tables* (2016), https://www.cdc.gov/nchs/data/ahcd/namcs_summary/2016_namcs_web_tables.pdf [https://perma.cc/S42Q-X5F2] (indicating that in 2016 Americans visited their primary care physicians 151.6 times per 100 persons per year).

[2] *See, e.g.*, U.S. DEP'T OF HEALTH & HUM. SERVS., MEDICARE BENEFICIARY USE OF TELEHEALTH VISITS: EARLY DATA FROM THE START OF THE COVID-19 PANDEMIC 1 (2020) (stating that 43.5% of Medicare primary care visits in April 2020 were provided via telehealth, compared with 0.1% in February 2020).

[3] Shubham Singhal & Stephanie Carlton, *The Era of Exponential Improvement in Healthcare?*, MCKINSEY & CO. (May 2019), https://www.mckinsey.com/industries/healthcare-systems-and-services/our-insights/the-era-of-exponential-improvement-in-healthcare [https://perma.cc/5F7J-ADRN].

[4] *Id.*; *see* TEJASWINI MISHRA ET AL., EARLY DETECTION OF COVID-19 USING A SMARTWATCH 2 (2020) ("COVID-19 infections are associated with alterations in heart rate, steps and sleep in 80% of COVID-19 infection cases.").

[5] Singhal & Carlton, *supra* note 3.

data produced over the individual's lifetime.[6] The threshold concern this Note will build on is: with greater sums of consumer health data comes greater potential for abuse, especially when this information falls outside of the purview of existing privacy laws.[7]

Perhaps the most famous of these existing privacy laws affecting health data is the Health Insurance Portability and Accountability Act (HIPAA). However, HIPAA's protections are aimed at data sent, received, or maintained by "covered entities" (CEs): health plans, health care clearinghouses, and healthcare providers transmitting health information electronically. HIPAA also applies to "business associates" (BAs): those who receive, maintain, or transmit protected health information ("PHI") on behalf of a covered entity.[8] A considerable subset of health applications, devices, and services available today fit into neither of the listed categories and are therefore outside of HIPAA's protections; these are called non-covered entities (NCEs).[9] NCEs inhabit a regulatory grey area, potentially leaving these new repositories of personal health information critically unprotected.

In addition to evaluating the sufficiency of current regulatory frameworks, this Note will explore the challenges in classifying data's "sensitivity," while concluding with analysis of whether proposed and emerging solutions can meet this fundamental regulatory need. These solutions range from sweeping industry-agnostic privacy legislation to proposals targeted to this specific problem in healthcare. Overall, this Note will weigh the costs and benefits of these options as they are currently understood.

I. SUMMARY OF CURRENT HEALTHCARE PRIVACY REGULATION

A. HIPAA

Seeking to address issues of healthcare fraud, administrative simplification, and the computerization of health information, Congress

[6] *Id.*

[7] *See* discussion *infra* Section II.B and *generally* Section II for examples of abusive data practices. Particularly troubling is the ability to re-identify individuals across anonymous datasets and, subsequently, the ability to make potentially lucrative inferences about an individual's health from even non-health data.

[8] 45 C.F.R. § 160.103(3) (2019).

[9] U.S. DEP'T OF HEALTH & HUM. SERVS., EXAMINING OVERSIGHT OF THE PRIVACY & SECURITY OF HEALTH DATA COLLECTED BY ENTITIES NOT REGULATED BY HIPAA 1 (2016) [hereinafter HHS, EXAMINING OVERSIGHT], https://www.healthit.gov/sites/default/files/non-covered_entities_report_june_17_2016.pdf [https://perma.cc/2JZU-DQJF].

enacted HIPAA in 1996.[10] Under Title II of the Act, Congress empowered the Department of Health and Human Services (HHS) Office for Civil Rights (OCR) to promulgate rules to protect the privacy of health information, the sum of which is commonly known as the Privacy Rule.[11] The Privacy Rule "create[d] for the first time, a floor of national protections" for personal health information.[12] Mindful of advances in health information systems, with the Privacy Rule and later the Health Information Technology Economic and Clinical Health (HITECH) Act of 2009, OCR drives compliance principles applicable to electronic transactions of health information executed by CEs or on their behalf by BAs.[13] Data qualifying for protection under HIPAA is PHI, defined as information that "relates to the past, present, or future physical or mental health condition of an individual . . . [and] the provision of health care to an individual."[14] The Privacy Rule mandates collection or eventual use of PHI to the "minimum necessary" extent and features other obligations common in the emerging canon of privacy laws relating to access, notice, and consent while requiring authorization to use or disclose protected information.[15]

Title II of the Act is also home to the Security Rule, which requires CEs and BAs to undertake a 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."[16] The Security Rule also sets forth administrative, physical, and technical safeguards of PHI in the care of CEs and BAs.[17] These safeguards are geared towards the management of: identity and access, security, risk, incident response, and IT best practices.[18] Standards are accompanied by implementation specifications that are either "addressable" or "required," allowing organizations flexibility to choose security measures based on an assessment of the "size, complexity, and capabilities" of the enterprise.[19] For

[10] *See* Deborah F. Buckman, Annotation, *Validity, Construction, and Application of Health Insurance Portability and Accountability Act of 1996 (HIPAA) and Regulations Promulgated Thereunder*, 194 A.L.R. FED. 133 (2004).

[11] *Id.*; 42 §§ U.S.C. 1302(a), 1320d-9; *see* 45 C.F.R. §§ 160, 164.

[12] Standards for Privacy of Individually Identifiable Health Information, 67 Fed. Reg. 53,182 (Aug. 14, 2002) (codified at C.F.R. pts. 160, 164).

[13] Health Information Technology for Economic and Clinical Health (HITECH) Act, 42 U.S.C. § 17921; 42 U.S.C. §§ 17934–40; 45 C.F.R. § 160.103.

[14] 45 C.F.R. § 160.103. HIPAA protects only individually identifiable health information and not de-identified data.

[15] 45 C.F.R. § 164.502(b); 45 C.F.R. § 164.514(d); *see* discussion *infra* Section IV.A.

[16] HHS, EXAMINING OVERSIGHT, *supra* note 9, at 16.

[17] 45 C.F.R. § 164.302.

[18] HHS, EXAMINING OVERSIGHT, *supra* note 9, at 16.

[19] 45 C.F.R. § 164.306.

example, among the technical safeguards in section 164.312, the implementation specification of "encryption" of information at rest and in transit is listed as addressable, permitting a given organization to decide if implementing the safeguard is "reasonable and appropriate . . . in its environment, when analyzed with reference to the likely contribution to protecting health information."[20] Continuing with the same example, if the organization decides encryption is not reasonable and appropriate, the rationale for this must be documented and an equivalent alternative must be implemented—if reasonable and appropriate.[21] Ultimately, "the Security Rule is designed to be flexible and scalable so a covered entity can implement policies, procedures, and technologies that are appropriate for the entity's particular size, organizational structure, and risks to consumers' e-PHI."[22]

HIPAA also features breach notification and enforcement rules.[23] The Breach Notification Rule mandates that CEs and BAs provide notification after a breach of unsecured PHI, defining a breach as an impermissible "acquisition, access, use, or disclosure of protected health information" in a manner not permitted under the Privacy Rule.[24] Such events are "presumed to be a breach" barring a CE or BA's demonstration of low probability that PHI was compromised.[25] Exceptions to the definition of breach include unintentional or inadvertent acquisition, access, or use of PHI by employees or persons acting under authority of CEs and BAs.[26] After a breach, CEs must notify affected individuals, the Secretary of HHS, and prominent media outlets—if the event impacts more than 500 residents of the given state or jurisdiction.[27] HIPAA's Enforcement Rule allows for the imposition of civil and criminal penalties for violations. Civil penalties may reach an annual maximum of $1,500,000 in certain circumstances, and criminal penalties may include both hefty fines and imprisonment.[28]

[20] *Id.*; 45 C.F.R. § 164.312.

[21] 45 C.F.R. § 164.312.

[22] *Summary of the HIPAA Security Rule*, U.S. DEP'T HEALTH & HUM. SERVS., https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html [https://perma.cc/4FNY-9LZJ].

[23] 45 C.F.R. §§ 164.400–414 (Breach Notification Rule); 45 C.F.R. §§ 160.300–312 (Enforcement Rule).

[24] 45 C.F.R. § 164.402; *Breach Notification Rule*, U.S. DEP'T HEALTH & HUM. SERVS., https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html [https://perma.cc/SK32-38UZ].

[25] *Breach Notification Rule*, *supra* note 24.

[26] *Id.*

[27] *Id.*

[28] *See HIPAA Violations & Enforcement*, AM. MED. ASS'N (Dec. 6, 2019), https://www.ama-assn.org/practice-management/hipaa/hipaa-violations-enforcement [https://perma.cc/RC9E-ZS68].

B. FTC

The Federal Trade Commission's jurisdiction stems from section 5 of the Federal Trade Commission Act (FTC Act), which empowers the agency to regulate "unfair or deceptive acts or practices."[29] The FTC Act defines an unfair act or practice as one that "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[30] While no specific definition of a deceptive trade practice exists in the Act, a 1983 policy statement notes that "[t]he Commission will find an act or practice deceptive if there is a misrepresentation, omission, or other practice, that misleads the consumer acting reasonably in the circumstances, to the consumer's detriment."[31] For example, an inaccurate or misleading statement in a privacy policy could be a deceptive practice, while inadequate security protections causing or likely to cause customer injury might be an unfair practice under contemporary interpretations of the Act.[32]

As part of the American Recovery and Reinvestment Act of 2009, Congress directed the FTC to promulgate rules addressing breaches of health data in the care of certain entities not covered by HIPAA.[33] The result was

[29] 15 U.S.C. § 45(a).

[30] *Id.*; *see also* Fed. Trade Comm'n, Commission Statement of Policy on the Scope of the Consumer Unfairness Jurisdiction, *appended to* Int'l Harvester Co., 104 F.T.C. 949, 1070–76 (1984) (providing extra details to three unfairness considerations: (1) whether the practice injures consumers; (2) whether it violates established public policy; and (3) whether it is unethical or unscrupulous).

[31] Fed. Trade Comm'n, Statement of Policy on Deception, *appended to* Cliffdale Assocs., 103 F.T.C. 110, 174–84 (1984).

[32] HHS, EXAMINING OVERSIGHT, *supra* note 9, at 17–18. As an example of a deceptive trade practice in the digital health context, the report cites PaymentsMD, LLC, No. C-4505 (F.T.C. Jan. 27, 2015) (decision and order), https://www.ftc.gov/system/files/documents/cases/150206paymentsmddo.pdf [https://perma.cc/RHU2-KEYV] (alleging company deceived customers who signed up for online billing function by failing to inform them that the company would collect "highly detailed" medical information about them). And, as an example of an unfair trade practice related to inadequate security, the report cites Accretive Health, Inc., No. C-4432 (F.T.C. Feb. 5, 2014) (decision and order), https://www.ftc.gov/system/files/documents/cases/140224accretivehealthdo.pdf [https://perma.cc/ST7P-2WGT] (alleging that medical billing and revenue management services risked consumers' personal and health information, by transporting laptops with sensitive data in a way that made them vulnerable to theft and giving access to personal information to employees who did not need it to do their jobs among other things).

[33] 42 U.S.C. § 17937; 16 C.F.R. § 318.1 (2020). The FTC Rule applies specifically to personal health records ("PHRs") or PHR-related entities. A PHR is defined 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." 16 C.F.R. § 318.2. A variety of mHealth applications, wearables, and other digital health products might fit within the definitions of PHR, PHR-related vendor, and third-party service provider. *See also* Reece Hirsch & Jenny Harrison, *Digital Health Privacy: Old Laws Meet New Technologies*, 27 J. ANTITRUST, UCL & PRIVACY SEC. CALIF. LAWS. ASS'N 21, 28 (2018), https://www.morganlewis.com/-/media/files/publication/outside-publication/article/2018/cal-bar-digital-health-privacy.pdf [https://perma.cc/6BQ6-6W4J] ("A PHR-related entity is an entity that

the FTC Health Breach Notification Rule. Parallel to its HIPAA counterpart, the FTC Rule requires regulated entities to notify affected individuals, the agency, and the media (in certain situations) following a breach of unsecured, individually identifiable health information.[34] Finally, the Commission treats a violation of the FTC Rule as an unfair or deceptive trade practice.[35]

C. FDA

The Food and Drug Administration's (FDA) impact on digital health is through its regulation of medical devices, enabled by the United States Federal Food, Drug, and Cosmetic Act (FDCA).[36] The FDCA defines a device as:

> [A]n instrument, apparatus, implement, machine, contrivance, implant . . . including any component, part, or accessory, which is . . . *intended* for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease . . . or intended to affect the structure or function of the body.[37]

Should a particular mHealth solution qualify as a device in the eyes of the agency,[38] the degree of regulatory oversight for the device varies based on how it is classified.[39] Each classification has a different set of requirements ranging from extensive pre- and post-market checks to a host

interacts with a PHR vendor by either offering products or services through the vendor's website or by accessing information in a PHR or sending information to a PHR.").

[34] 16 C.F.R. § 318.5; HHS, EXAMINING OVERSIGHT, *supra* note 9, at 19. Third-party service providers are obligated to notify their vendor or PHR-related entity. Like HIPAA, cut-off for media notice requirement is a breach affecting 500 or more individuals.

[35] 16 C.F.R. § 318.7.

[36] 21 U.S.C. § 393.

[37] 21 U.S.C. § 321 (emphasis added).

[38] *But see, e.g.*, U.S. FOOD & DRUG ADMIN., GENERAL WELLNESS: POLICY FOR LOW RISK DEVICES: GUIDANCE FOR INDUSTRY AND FOOD AND DRUG ADMINISTRATION STAFF (Sept. 27, 2019) [hereinafter FDA, LOW RISK DEVICES] (indicating that the FDA chooses to not regulate all "devices").

[39] *See Classify Your Medical Device*, U.S. FOOD & DRUG ADMIN., https://www.fda.gov/medical-devices/overview-device-regulation/classify-your-medical-device [https://perma.cc/H47E-G6H9] (noting three classes of device: I, II, and III, each with greater oversight; classification is based on patient risk profile, intended use of device, and indications for use). *But see Device Software Functions Including Mobile Medical Applications*, U.S. FOOD & DRUG ADMIN., https://www.fda.gov/medical-devices/digital-health/device-software-functions-including-mobile-medical-applications, [https://perma.cc/6THA-NCTZ] (indicating that software functions that meet the regulatory definition of a device but pose minimal risk to patients and consumers will not require premarket review applications or registration of software with FDA).

of milder obligations.[40] For example, the FDA *recommends* that, for devices requiring pre-market submissions, manufacturers provide cybersecurity-related supporting documentation including: identification of assets, threats, and vulnerability; assessment of potential impacts on device functionality; assessment of likelihood of vulnerabilities being exploited; determination of mitigation strategies; and more. To further these objectives, the Agency recognizes certain industry standards for dealing with information technology and medical device security.[41] However, regardless of classification and unless excepted, the manufacturers of networked medical devices should have a "Quality System" in place, which includes procedures for identifying potential safety concerns, among them cybersecurity.[42] While the FDA has wielded its regulatory authority over a variety of mHealth contexts, including physical devices and mobile medical applications, recent guidance from the Agency makes clear that it will regulate only software that operates as a medical device whose potential failure risks patient safety.[43] Further, the Agency has indicated that it will not regulate general wellness products, defined as those intended for "general wellness use," that pose low risk to the safety of their users.[44] For these products, the FDA will not attempt to determine whether they fit the definition of a device nor will the Agency assess whether these products require pre-market registration, review, or post-market obligations.[45]

[40] *See* U.S. FOOD & DRUG ADMIN., POLICY FOR DEVICE SOFTWARE FUNCTIONS AND MOBILE MEDICAL APPLICATIONS: GUIDANCE FOR INDUSTRY AND FOOD AND DRUG ADMINISTRATION STAFF (2019) [hereinafter FDA, SOFTWARE FUNCTIONS].

[41] U.S. FOOD & DRUG ADMIN., CONTENT OF PREMARKET SUBMISSIONS FOR MANAGEMENT OF CYBERSECURITY IN MEDICAL DEVICES: GUIDANCE FOR INDUSTRY AND FOOD AND DRUG ADMINISTRATION STAFF (2014) [hereinafter FDA, PREMARKET CYBERSECURITY].

[42] 21 C.F.R. § 820.30(g) (2020) ("Design validation shall include software validation and risk analysis, where appropriate."); FDA, PREMARKET CYBERSECURITY, *supra* note 41 (noting that § 802.30(g) applies to cybersecurity).

[43] *See, e.g.*, Letter from Alberto Gutierrez, Director, Office of In Vitro Diagnostics and Radiological Health, FDA, to Ann Wojcicki, CEO, 23andMe, Inc. (Nov. 22, 2013), https://wayback.archive-it.org/7993/20180908082647/https://www.fda.gov/ICECI/EnforcementActions/WarningLetters/2013/ucm376296.htm [https://perma.cc/MF8M-U9PC] (warning that 23andMe's interactive, home DNA testing kit service qualifies as a medical device under FDCA's definition; 23andme is considered a Class III device); FDA, SOFTWARE FUNCTIONS, *supra* note 40, at 9 (noting that regulatory oversight will be aimed at (1) software which is used as an accessory to a regulated medical device or (2) transforms a mobile platform into a regulated medical device).

[44] FDA, LOW RISK DEVICES, *supra* note 38, at 3, 5 (defining general wellness products as those that have an intended use of encouraging a general state of health or a healthy activity, or an intended use that relates the role of a healthy lifestyle with helping to reduce the risk of impact of certain chronic diseases or conditions; defining risk based on whether product is invasive, implanted, or involves intervention/technology that may pose safety risk to users absent regulation).

[45] *Id.*

II. INSUFFICIENCY OF CURRENT REGULATORY FRAMEWORKS

In 2016, HHS released a report to Congress detailing the security and privacy concerns of health data existing outside the protections of HIPAA and other laws impacting health data privacy.[46] In particular, the report focused on mHealth technologies: personal health records, mobile apps, and wearable fitness trackers that collect health information from consumers and facilitate its sharing.[47] Given that these technologies are not typically "offered or provided to the individual" by CEs or BAs, they are outside the scope of HIPAA and are classified as NCEs by HHS.[48] According to the HHS report, NCEs face five major gaps of oversight and protection when compared to entities and associates subject to HIPAA's existing frameworks: "(A) Difference in Individuals' Access Rights; (B) Difference in Re-Use of Data by Third Parties; (C) Difference in Security Standards Applicable to Data Holders and Users; (D) Differences in Understanding of Terminology About Privacy and Security Protections; [and] (E) Inadequate Collection, Use, and Disclosure Limitations."[49]

A. Difference in Individuals' Access Rights

NCEs are under no legal obligation to provide customers access to their own data. While NCEs might voluntarily extend access rights to users, they are not required to do so. The HHS report frames the discrepancies in access rights with NCEs as an issue of transparency because taking advantage of access rights aids a consumer in understanding "policies, procedures, and technologies that directly affect . . . their individually identifiable health information."[50]

B. Difference in Re-Use of Data by Third Parties

In addition to lacking access rights, consumers with data held by NCEs face differences in re-use and sharing standards with third parties. While HIPAA rules restrict both the types of recipients and the purposes for information disclosure, data provided to NCEs lacks similar protections unless the data collector has represented otherwise in the terms of service.[51]

[46] *See generally* HHS, EXAMINING OVERSIGHT, *supra* note 9, at 1.

[47] *Id.*

[48] *Id.* at 4.

[49] *Id.* at 20.

[50] *Id.* at 21 (quoting U.S. DEP'T OF HEALTH & HUM. SERVS., OFFICE OF THE NAT'L COORDINATOR FOR HEALTH INFO. TECH., NATIONWIDE PRIVACY AND SECURITY FRAMEWORK FOR ELECTRONIC EXCHANGE OF INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION 7 (Dec. 15, 2008), https://www.healthit.gov/sites/default/files/nationwide-ps-framework-5.pdf [https://perma.cc/5ZKZ-4ERQ]).

[51] *See supra* Section I.B.

As a result, NCEs may have more latitude to disclose health information for marketing purposes. In fact, a recent study of some of the top-rated Android mHealth applications available in the United Kingdom, the United States, Canada, and Australia describes an expansive and complex network of third and fourth parties with whom health data is shared.[52] Notably, nineteen of twenty-four sampled applications (79%) shared user information to a universe of fifty-five unique entities, which received and processed the data.[53] Of these fifty-five entities, thirty-seven (67%) "provided services related to the collection and analysis of user data, including analytics or advertising, suggesting heightened privacy risks."[54] Further, "[t]hird parties advertised the ability to share user data with 216 'fourth parties,'" the most powerful and common of which are multinational technology companies such as Alphabet (Google), Facebook, and Oracle.[55] Given their stature and reach, these firms collect the largest and most diverse quantities and types of data, respectively—enough to permit re-identification of an individual upon aggregation.[56]

Aggregation of health information at the fourth-party level presents a significant privacy concern according to the study. Accordingly, the authors advise "taking a systems view of the mobile ecosystem," mindful of the "network positions" of several companies who control parts of app development, analytics, and advertising infrastructure.[57] When these companies couple health information with a "semi-persistent" identifier such as an Android ID, they can quickly identify a user and aggregate their activities across the app ecosystem.[58] The study notes that a fourth party, especially one with monopoly position within the mobile ecosystem, could easily compile disparate application data into a rudimentary health profile for an individual. The application data could be any combination of current medications, active problems, past medical history, and more depending on the data sources.[59] Worse yet, another potential scenario involves insurance

[52] Quinn Grundy et al., *Data Sharing Practices of Medicines Related Apps and the Mobile Ecosystem: Traffic, Content, and Network Analysis*, BRIT. MED. J., March 20, 2019, at 1, 1.

[53] *Id.*

[54] *Id.*

[55] *Id.* at 1, 7.

[56] *Id.* at 8. Fourth parties are defined as those entities which are two steps removed from the mHealth company with whom information is shared.

[57] *Id.* at 10.

[58] *Id.*

[59] *Id.*; *cf.* Complaint at 24, Smith v. Facebook, Inc., 262 F. Supp. 3d 943 (N.D. Cal. 2017) (No. 5:16-cv-01282), 2016 WL 1042966 (alleging defendants combined third party tracking data, search requests, and "like" activity to create basic health profiles which it could sell for health-related advertising purposes).

companies obtaining these data aggregates to reveal an individual's medical condition to inform a premium increase or a denial of coverage.[60]

C. Differences in Security Standards Applicable to Data Holders and Users

NCEs might also lack the administrative, technical, and physical safeguards that HIPAA's Security Rule either recommends or requires.[61] Further, the combination of NCEs being outside of HIPAA jurisdiction, the lack of FTC-mandated security standards, and the FDA's choice to not regulate low-risk devices means that NCE platforms might not be protected by any formalized security protocols.[62] Often missing are adequate identity-verification modalities, including password complexity and multi-factor authentication requirements, as well as risk- or audit-assessment capabilities.[63] And, even if NCEs were subject to HIPAA's protections, many of the safeguards that the Security Rule supplies offer little comfort due to their often optional nature and lack of granularity.[64] Returning to a previous example, this means that CEs and BAs implementing the addressable standard of "encryption" are not required to deploy any particular industry standard for encryption.[65] This was no accident; not only was the Security Rule designed to be flexible and scalable, its framers also had an eye toward "technological neutrality" in order to accommodate emerging standards and innovation.[66] Nevertheless, sufficient encryption practices are otherwise prudent for NCEs given the negative incentive of the FTC Breach Notification Rule and its associated enforcement consequences.[67]

[60] Kevin Loria, *Are Health Apps Putting Your Privacy at Risk?*, CONSUMER REP. (Mar. 21, 2019), https://www.consumerreports.org/health-privacy/are-health-apps-putting-your-privacy-at-risk/ [https://perma.cc/ZG56-EWBS].

[61] *See supra* note 16 and accompanying text.

[62] *See supra* text accompanying notes 16–22; *see also* discussion *supra* Sections I.B–C.

[63] HHS, EXAMINING OVERSIGHT, *supra* note 9, at 23–24.

[64] Tim Wafa, *How the Lack of Prescriptive Technical Granularity in HIPAA Has Compromised Patient Privacy*, 30 N. ILL. U.L. REV. 531, 542 (2010).

[65] *Id.*

[66] *Id.* at 543 (citing 68 Fed. Reg. 8334–36 (Feb. 20, 2003) (codified at 45 C.F.R. pts. 160, 162, 164)).

[67] *See supra* text accompanying notes 33–35; *see also* U.S. FED. TRADE COMM'N, CAREFUL CONNECTIONS: BUILDING SECURITY IN THE INTERNET OF THINGS (2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0199-carefulconnections-buildingsecurityinternetofthings.pdf [https://perma.cc/P33S-ATRP] (suggesting best-practices to secure internet of things devices).

D. Differences in Understanding of Terminology About Privacy and Security Protections

According to the HHS report, NCEs are fraught with inconsistencies in terms of privacy policy content, if not lacking privacy policies altogether.[68] At present there are no federal requirements for NCEs to have privacy policies or notices informing consumers about data-use practices that may impact their health information.[69] In addition, definitions of key terms like "health information," "individually identifiable health information," and "protected health information" are often inconsistent across NCE platforms despite having fixed meanings within various privacy laws.[70] For example, "protected health information" under HIPAA is defined based on both its content and its association with CEs and BAs, whereas "health information" also has a lay meaning to consumers that is likely different than HIPAA's.[71] Even if a privacy policy does exist for an NCE, it may be modified without notice to the consumer.[72] In addition, the actual content of privacy policies may be difficult for lay consumers to understand.[73] In one sampling of mHealth apps, the average grade-level readability was 13.78 for privacy policies and 15.24 for terms of service.[74] This risks "overwhelm[ing] the reader with detail . . . and exceptions within exceptions," making it hard for lay consumers to determine important data-use practices, including whether any sharing of their health information with third parties takes place.[75]

Ultimately, the relative dearth of privacy policies and inconsistencies with their content betray a lack of transparency within the ecosystem of NCEs.[76]

E. Inadequate Collection, Use, and Disclosure Limitations

The final thematic issue identified in the HHS report is that NCEs are not forthrightly limiting their collection, use, or disclosure of consumer health data.[77] HIPAA's Privacy Rule mandates collection or eventual use of

[68] Julie M. Robillard et al., *Availability, Readability, and Content of Privacy Policies and Terms of Agreements of Mental Health Apps*, 17 INTERNET INTERVENTIONS 1, 2 (2019) (noting that of 369 unique mental health apps only 18% of iOS and 4% of Android apps had privacy policies, and 15% and 3% had terms of agreement, respectively).

[69] HHS, EXAMINING OVERSIGHT, *supra* note 9, at 25.

[70] *Id.* at 28.

[71] *Id.*

[72] *Id.*

[73] Robillard et al., *supra* note 68, at 5.

[74] *Id.* at 2.

[75] HHS, EXAMINING OVERSIGHT, *supra* note 9, at 26–27.

[76] *Id.*; Robillard et al., *supra* note 68, at 1.

[77] Robillard et al., *supra* note 68, at 1.

PHI to the "minimum necessary" extent with additional limitations on its disclosure to other parties.[78] NCEs are not bound by such limitations, potentially leaving consumers in the dark about how their health data is being used. NCEs and their associated third and fourth parties engage in marketing, advertising, and behavioral tracking indicating "information use that is likely broader than what individuals would anticipate," leading individuals to unwittingly supply sensitive data to these other parties.[79]

III. DIFFICULTIES IN CLASSIFYING AND DEFINING SENSITIVE INFORMATION

Privacy laws in the United States are a patchwork of overlapping sector-specific and sector-agnostic frameworks, which typically "rely on determinations about the *nature, type,* or *category* of information to assess its sensitivity and riskiness."[80] Regulating data in this manner also reflects the public's perceptions of sensitivity across various industries and ultimately, categories of information.[81] In the case of HIPAA and its various subparts, Congress signaled that PHI in the care of CEs and BAs deserved special protections.[82] However, with the rapid emergence of NCEs and their control of vast amounts of health data, new solutions are needed. Assigning the same sensitivity level to all health data risks "potentially dangerous oversimplification."[83] Thus, expanding the reach of a legacy privacy law like HIPAA risks conferring inadequate protections as HIPAA is much less likely to provide protections commensurate with advances in data science such as technologists' ability to "take information that appears on its face to be non-identifiable and turn it into identifiable data."[84] This is due in part to pitfalls of the "nature, type, or category" approach rather than one that is geared

[78] 45 C.F.R. § 164.502(b); 45 C.F.R. § 164.514(d).

[79] HHS, EXAMINING OVERSIGHT, *supra* note 9, at 29–30.

[80] Müge Fazlioglu, *Beyond the "Nature" of Data: Obstacles to Protecting Sensitive Information in the European Union and the United States*, 46 FORDHAM URB. L.J. 271, 286 (2019) (emphasis in original).

[81] *Id.* at 300 (citing David L. Mothersbaugh et al., *Disclosure Antecedents in an Online Service Context: The Role of Sensitivity of Information*, 15 J. SERV. RES. 76, 90–91 (2012)).

[82] *See* discussion *supra* Section I.A.

[83] Fazlioglu, *supra* note 80, at 300 ("For instance, the term *health data* may refer to a diagnosis of a common illness, such as a cold or the flu, as well as to a serious disease associated with stigmatization."); *see supra* note 6 and accompanying text.

[84] Fazlioglu, *supra* note 80, at 297; Paul M. Schwartz & Daniel J. Solove, *The PII Problem: Privacy and A New Concept of Personally Identifiable Information*, 86 N.Y.U. L. REV. 1814, 1816 (2011); *see also supra*, note 59 and accompanying text.

towards the *context* of data use—mindful of distinctions between harmful and beneficial use-cases.[85] Such an approach:

> considers how the context in which information is used affects its level of sensitivity. This perspective shifts the focus away from the *category* of data, avoiding the question of what categories are or are not sensitive, to the *manner of data use* and its eventual consequences.[86]

In 2010, Professors Paul Schwartz and Daniel Solove of UC Berkeley and George Washington School of Law, respectively, proposed a context-based model premised on a reimagining of the paradigm of "personally identifiable information" (PII)—common in most data privacy laws.[87] Mindful of how the risks and benefits of data practices may differ situationally, the authors suggest a "PII 2.0" that

> places information on a continuum that begins with no risk of identification at one end, and ends with identified individuals at the other . . . [divided into] three categories, each with its own regulatory regime . . . information can be about an (1) identified, (2) identifiable, or (3) non-identifiable person.[88]

Under PII 2.0, where a given data practice falls on the spectrum is a context-sensitive determination.[89] On a sliding scale of sorts, the scholars

[85] *See* Fazlioglu, *supra* note 80, at 286, 288, 291–92 (citing Michal Kosinki et al., *Private Traits and Attributes Are Predictable from Digital Records of Human Behavior*, 110 PROC. NAT'L ACAD. SCI. 5802, 5802 (2013)). Fazlioglu notes that through

> "a mechanism used by Facebook users to express their positive association with . . . online content," researchers developed a predictive model that managed to discover sensitive information about users, including their sexual orientation, ethnicity, and religious and political beliefs . . . mak[ing] "guesses" about a person's sensitive data with a high degree of accuracy, between 85% and 95%.

Id. *See also supra* note 59 and accompanying text; Curt Woodward & Hiawatha Bray, *A Company Sent Anti-Abortion Ads by Phone. Massachusetts Wasn't Having It*, BOSTON GLOBE (Apr. 4, 2017), https://www.bostonglobe.com/business/2017/04/04/healey-halts-digital-ads-targeted-women-reproductive-clinics/AoyPUG8u9hq9bJUAKC5gZN/story.html [https://perma.cc/PAJ8-J7MD] (describing a circumstance where an advertising company used "geofencing" to reach the smartphones of women near reproductive health clinics with anti-abortion messaging).

[86] Fazlioglu, *supra* note 80, at 304 (quoting Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 WASH. L. REV. 119, 119 (2004)).

[87] Schwartz & Solove, *supra* note 84, at 1816, 1831–32 (citing Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501–6506 (2006)) (defining PII initially as "'individually identifiable information about an individual collected online,' including first and last name, physical address, social security number, telephone number, and e-mail address"); *see also supra* note 14 and accompanying text (stating that HIPAA protects only individually identifiable health information). Current U.S. privacy laws often rely on definitions of PII to trigger jurisdiction while betraying the "basic assumption—that in the absence of PII, there is no privacy harm." Schwartz & Solove, *supra* note 84, at 1816.

[88] Schwartz & Solove, *supra* note 84, at 1877.

[89] *Id.* at 1878.

propose applying a full suite of privacy principles to the data of identified persons, such as:

> (1) limits on information use; (2) limits on data collection, also termed data minimization; (3) limits on disclosure of personal information; (4) collection and use only of information that is accurate, relevant, and up-to-date (data quality principle); (5) notice, access, and correction rights for the individual; (6) the creation of processing systems that the concerned individual can know about and understand (transparent processing systems); and (7) security for personal data.[90]

For information less likely to be identified, the authors recommend scaling down these principles.[91] For example, with merely *identifiable* data, it is likely unnecessary to extend full notice, access, and rectification rights.[92] However, principles of security, transparency, and data quality might remain important in these situations, and security protocols should be subsequently tailored to the nature of the information and the risk of disclosure.[93] Other contextual factors should influence this determination such as "the lifetime for which information is to be stored, the likelihood of future development of relevant technology, and parties' incentives to link identifiable data to a specific person."[94]

IV. THE ROAD AHEAD: EVALUATING PROPOSED AND UPCOMING SOLUTIONS

Presently, there are a number of suggested or impending solutions that could meet the regulatory needs outlined in the HHS Report.[95] This section will evaluate three such solutions. First, this section will discuss the industry-agnostic California Consumer Privacy Act of 2018 (CCPA).[96] Second, this section will discuss the industry-specific bill that U.S. Senators Amy Klobuchar and Lisa Murkowski introduced in 2019, the Protecting Personal

[90] *Id.* at 1880 (citing Paul M. Schwartz, *Preemption and Privacy*, 118 YALE L.J. 908 (2009)).

[91] *Id.*

[92] *Id.* ("For one thing, if the law created such interests, these obligations would decrease rather than increase privacy by requiring that all such data be associated with a specific person.").

[93] *Id.* at 1881.

[94] *Id.* at 1878; *see also* Khaled El Emam, *Heuristics for De-Identifying Health Data*, IEEE SECURITY & PRIVACY, July–Aug. 2008, at 58; Khaled El Emam, *Risk-Based De-Identification of Health Data*, IEEE SECURITY & PRIVACY, May–June 2010, at 64, 66–67 (noting that computer scientists have also devised metrics that quantify the risk of re-identification, with one scientist's work focusing on "mitigating controls" available to entities in possession of data and the likely "motives and capacity" of other parties who might want to associate that information to an individual).

[95] *See supra* Section II.

[96] California Consumer Privacy Act of 2018, CAL. CIV. CODE § 1798.100 *et seq.* (West 2018) (effective Jan. 1, 2020) (extending privacy rights and obligations to California residents and those doing business in California, respectively).

Health Data Act.[97] Finally, this section will conclude with analysis of a proposal offered by Professor Charlotte Tschider to expand FDA oversight to include all mHealth platforms regardless of their risk to patients because "the framework for pre-market disclosures, quality management programs, and post-market obligations matches most product development lifecycles."[98]

A. CCPA

The CCPA is the strictest data protection and consumer privacy law in the United States and is already impacting the mHealth sector. [99] Businesses subject to the CCPA are required to extend to consumers rights of access, deletion, disclosure, and the ability to opt-out of information sales.[100] While the CCPA is a state law jurisdictionally limited to California residents ("consumers") and entities doing business in the state ("businesses"), it offers a viable template for analyzing how an industry-agnostic privacy law could regulate NCEs if applied on a national scale.[101]

1. Impact on NCEs

Many of the rights and obligations imposed by the CCPA would fill the regulatory gaps noted in the HHS Report. First, the CCPA would impose a host of disclosure requirements on NCEs by requiring notice at or before the point of information collection.[102] A compliant notice informs consumers of categories of personal information collected and the purposes for which the categories will be used.[103] Under the CCPA's notice requirements, NCEs must inform consumers whether information has been sold or disclosed to third parties while providing an opt-out right if information *may* be sold.[104] Finally, if the NCE subsequently collects additional categories of personal information or has new purposes for collection of the existing information,

[97] Protecting Personal Health Data Act, S. 1842, 116th Cong. (2019) (acting specifically on NCEs and the findings of the HHS Report).

[98] Charlotte A. Tschider, *Enhancing Cybersecurity for the Digital Health Marketplace*, 26 ANNALS HEALTH L. 1, 32 n.185 (2017).

[99] EHEALTH INITIATIVE FOUND., RISKY BUSINESS? SHARING DATA WITH ENTITIES NOT COVERED BY HIPAA 5 (2019), https://www.ehidc.org/sites/default/files/resources/files/Sharing%20Data%20with%20Non-HIPAA%20Entities%20March%202019.pdf [https://perma.cc/AH4S-K4DL] (noting that the CCPA also has a carve out exempting CEs and BAs covered by HIPAA).

[100] CAL. CIV. CODE §§ 1798.100(a)–(d), 1798.105(a), (c), (d), 1798.120, 1798.135(a)(1).

[101] *Id.* § 1798.140; *see generally Examining Legislative Proposals to Protect Consumer Data Privacy: Hearing Before the S. Comm. on Com., Sci., & Transp.*, 116th Cong. (2019) (holding a hearing regarding a potential national privacy law incorporating elements of the GDPR and the CCPA).

[102] CAL. CIV. CODE § 1798.100(b).

[103] *Id.*

[104] *Id.* §§ 1798.115(c)–(d); 1798.120(b).

additional notice must be given.[105] Consistent with the HHS Report, the CCPA's robust disclosure requirements would address the relative dearth of privacy policies among NCEs, improve existing policies' content, and require additional notice if any changes are made.[106]

On the issue of access, the CCPA obligates NCEs to heed a consumer request to access their data up to twice in a twelve-month period and must ensure its portability in either electronic format or by mail.[107] The CCPA also addresses information sales to third parties by letting consumers learn details about these parties, along with other categorical distinctions about the information sold.[108] Thus, the CCPA's access rights and obligations would inform consumers about "policies, procedures, and technologies that directly affect . . . their individually identifiable health information."[109]

In addition to mandating transparency through disclosure and access, the CCPA gives consumers rights to opt-out of information sales and to request deletion of their personal information subject to certain exceptions.[110] When heeding a consumer deletion request, the CCPA would obligate an NCE to direct any service providers to delete the information as well.[111] Also under the CCPA, *third parties* must provide explicit notice and opt-out rights if re-selling data to fourth parties.[112] Taken together, the CCPA gives consumers the ability to check potentially harmful information practices at the third- and fourth-party levels as discussed previously in this Note.[113]

Finally, the CCPA does not mandate any specific formalized security protocols.[114] Instead, the law extends a private right of action to consumers whose nonencrypted information was obtained through "unauthorized access

[105] *Id.*

[106] *See* discussion *supra* Sections II.C, II.D.

[107] CAL. CIV. CODE §§ 1798.100(a), (d), 1798.110(a)(1)–(4) (Consumers have the right to access categories of personal information collected, categories of its sources, purposes for collecting, and certain details about information sold/disclosed to third parties.).

[108] *Id.* §§ 1798.110(a)(4), 1798.115(a)(2)–(3).

[109] HHS, EXAMINING OVERSIGHT, *supra* note 9, at 21 (quoting U.S. DEP'T OF HEALTH & HUMAN SERVS., OFFICE OF THE NAT'L COORDINATOR FOR HEALTH INFO. TECH., NATIONWIDE PRIVACY AND SECURITY FRAMEWORK FOR ELECTRONIC EXCHANGE OF INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION 7 (2008), https://www.healthit.gov/sites/default/files/nationwide-ps-framework-5.pdf [https://perma.cc/KT6M-3CGE]).

[110] CAL. CIV. CODE § 1798.105(a), (c)–(d).

[111] *Id.* § 1798.105(c).

[112] *Id.* § 1798.115(d).

[113] *See* discussion *supra* Section II.B.

[114] *See* Bret Cohen et al., *California Consumer Privacy Act: The Challenge Ahead – The CCPA's "Reasonable" Security Requirement*, HOGAN LOVELLS: CHRONICLE OF DATA PROTECTION (Feb. 7, 2019), https://www.hldataprotection.com/2019/02/articles/consumer-privacy/california-consumer-privacy-act-the-challenge-ahead-the-ccpas-reasonable-security-requirement/ [https://perma.cc/LSW2-L4A6].

and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information[.]"[115] Although the CCPA does not define what constitutes "reasonable" under the circumstances, the state Attorney General's office has endorsed the Center for Internet Security's safeguards to act as a baseline.[116]

2. *Is the Definition of PII Context-Based?*

The CCPA defines personal information as that which "identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household."[117] In addition to listing common identifiers, the law gives examples of other novel sources of protected personal information including: network activity, search history, biometric data, geolocation data, and any "inferences drawn . . . to create a profile about a consumer."[118] This is an expansive definition of personal information seemingly cognizant of the fact that "every scrap of data could assist reidentification."[119] While broad definitions of personal information might proscribe many of the harmful data practices of NCEs discussed earlier in this note, they also risk chilling those that benefit consumers and society at large, thus betraying insensitivity to context.[120] Notably, the law's carve-out for medical research is one such confusing circumstance.[121]

In sum, while the CCPA targets some of the most invasive big data behaviors, imprecision in certain areas hinders the law's attempts at achieving optimal context sensitivity.[122]

[115] CAL. CIV. CODE § 1798.150(a)(1).

[116] *Download the CIS Controls® V7.1 Today*, CENTER FOR INTERNET SECURITY, https://learn.cisecurity.org/cis-controls-download [https://perma.cc/WC5S-BS4M].

[117] CAL. CIV. CODE § 1798.140(o)(1).

[118] *Id. But see id.* § 1798.140(o)(2) (excepting publicly available information, i.e., that which is made available from federal, state, or local government records).

[119] Eric Goldman, *A Privacy Bomb Is About to Be Dropped on the California Economy and the Global Internet*, TECH. & MKTG. L. BLOG (June 27, 2018), https://blog.ericgoldman.org/archives/2018/06/a-privacy-bomb-is-about-to-be-dropped-on-the-california-economy-and-the-global-internet.htm [https://perma.cc/7HPJ-3WL7].

[120] *See supra* Section III; *e.g.*, CAL. CIV. CODE §§ 1798.140(s), 1798.125(a)(2) (indicating potentially beneficial use case where businesses could provide better prices and service because of consumer data).

[121] *See* Mike Hintze, *Science and Privacy: Data Protection Laws and Their Impact on Research*, 14 WASH. J.L. TECH. & ARTS 103, 129–31 (2019) (indicating that the CCPA's implications for data-driven medical research are uncertain). Negative impacts might be felt if a consumer exercises their opt-out and deletion rights when data is being used for genuine research purposes. *Id.* Plus, the law has vexing definitions of the terms "sale" and "research," which the author believes could discourage these beneficial use cases. *Id.*

[122] *Id.*; *see also* Fazlioglu, *supra* note 80, at 301.

B. Protecting Personal Health Data Act, Senate Bill 1842

In direct response to the findings of the HHS Report, U.S. Senators Klobuchar and Murkowski have introduced the Protecting Personal Health Data Act, Senate Bill 1842, to address the myriad of privacy issues observed among NCEs.[123] This legislation would reach direct-to-consumer devices, services, applications, and software whose substantial purpose or use is to use or collect health data.[124] Excluded from the law are "products on which personal health data is derived solely from other information that is not personal health data, such as Global Positioning System data," as well as those products designed or marketed for CEs and BAs.[125] Bill 1842 defines personal health data as:

> any information, including genetic information, whether oral or recorded in any form or medium, that relates to the past, present, or future physical or mental health or condition of an individual and that identifies the individual or with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.[126]

Further, Bill 1842 directs the HHS Secretary with the help of other "relevant stakeholders" to promulgate regulations, notably those that "account for differences in the nature and sensitivity of the data collected or stored on the consumer device, service, application, or software."[127] In addition, Bill 1842 requests that the Secretary consider uniform standards for access, deletion, correction, and consent or its withdrawal for information-sharing practices.[128] Finally, Bill 1842 calls for the creation of a task force to evaluate and provide input on the effectiveness of de-identification methodologies as well as security, encryption, and transfer protocols.[129] If passed, Bill 1842 would presumably meet the needs highlighted in the HHS Report because it was drafted explicitly to address them.[130] Bill 1842 broadens the applicability of the PHI framework to NCEs, and it invites the creation of uniform standards around disclosure, access, third parties, and

[123] Protecting Personal Health Data Act, S. 1842, 116th Cong. (2019).

[124] *Id.* § 3.

[125] *Id.* § 3(1)(C).

[126] *Id.* § 3(5).

[127] *Id.* §§ 3(6), 4(b) (including consultation with the "Chairman of the Federal Trade Commission, the National Coordinator . . . and heads of such other Federal agencies as the Secretary considers appropriate . . . ").

[128] *Id.* § 4(b)(2)(A).

[129] *Id.* § 5.

[130] *Id.* §§ 2, 4.

security specifically tailored to NCEs.[131] However, there are reasons for skepticism.

First, Bill 1842 invites federal agencies to "account for differences in the nature and sensitivity of the data."[132] While Bill 1842 extends HIPAA's PHI definition to NCEs, it also asks for rules that might overlay the concept of PHI as it is currently understood. Seemingly, Bill 1842 compels federal agencies to commit to a "nature, type, or category" approach to understanding data sensitivity rather than to one that focuses on the *manner of use* and any context-sensitive risks to consumers.[133]

Second, Bill 1842 exempts "products on which personal health data is derived solely from other information that is not personal health data, such as Global Positioning System data."[134] This stands in contrast with the CCPA, which reaches geolocation data and "[i]nferences" used to create a profile of an individual.[135] In one troubling example from 2017, an advertising company placed "geofencing" around reproductive health centers to target women eighteen to twenty-four years-old with anti-abortion messages.[136]

Mindful of the ability to assemble health data through other information, any rulemaking that flows from Bill 1842 ought to consider the sliding scale posited in Schwartz and Solove's PII 2.0 proposal, where processors of identified, identifiable, and non-identifiable data face different obligations depending on context.[137]

C. *Expanding FDA Oversight*

In a 2017 article, Professor Charlotte Tschider proposed greater involvement of the FDA to meet cybersecurity needs in the mHealth arena.[138] Professor Tschider states that the Agency "has the regulatory structure, function, and focus to effectively regulate the digital health marketplace with some involvement from OCR, FTC, and ONC partners."[139] To achieve more complete oversight, the FDA would need to include mHealth platforms in its definition of a medical device, which might coax the industry into compliance with Quality System measures and extend natural benefits to the

[131] *Id.* §§ 3–4.

[132] *Id.* § 4.

[133] Fazlioglu, *supra* note 80, at 286, 288, 304 (emphasis omitted).

[134] S. 1842 § 3.

[135] CAL. CIV. CODE § 1798.140(o)(1); *cf.* Woodward & Bray, *supra* note 85.

[136] Woodward & Bray, *supra* note 85.

[137] Schwartz & Solove, *supra* note 84, at 1877.

[138] Tschider, *supra* note 98, at 31–32. *But see* 21 U.S.C. § 321(h) (indicating that the FDA chooses to not regulate all "devices").

[139] Tschider, *supra* note 98, at 32.

consumer.[140] In addition, the FDA would need to overhaul pre-market requirements by making all manufacturers of Class I and II digital health devices (under the new definition) submit a 501(k).[141] This would provide greater confidence in products due to the extensive disclosure obligations attached to 501(k) submissions.[142] Within these existing requirements could be an additional mandate to disclose cybersecurity risk management processes because "Class I devices, like mobile apps, also likely involve processing, transfer, and storage of highly sensitive health information, making them more likely to be a conduit for healthcare fraud."[143] Finally, the FDA can rely on previous experience enforcing Quality System measures to ensure steady compliance with cybersecurity standards.[144]

Overall, increased FDA involvement is an attractive solution to regulating mHealth and NCEs because of the Agency's existing infrastructure, which is conveniently geared towards ensuring consumer safety in a variety of contexts.

CONCLUSION

As consumers gain the ability to track personal behavior and lifestyle in new and meaningful ways, the need to protect this data increases as well. Ideally, a national general data privacy law resembling the CCPA would provide consumers with a clear set of rights and recourse to check harmful or risky data practices.[145] However, in the current public health crisis due to COVID-19, health data privacy has taken a back seat as even HIPAA enforcement has been relaxed to facilitate expansion of telehealth and remote patient encounters.[146] Global health crisis notwithstanding—more marginal

[140] *Id.* ("Many benefits to the consumer will naturally extend from FDCA regulatory controls, including required inclusion of a quality management system, policy development and standard operating procedures, accountability, and employee training. These general controls map well to a standardized cybersecurity program.").

[141] *Id.*

[142] *Id.* at 32–33 ("The FDA could easily incorporate a requirement for organizations to disclose details of their cybersecurity risk management programs.").

[143] *Id.* at 33, 35.

[144] *Id.* at 35 (citing U.S. Food & Drug Admin., *Federal Judge Approves Consent Decree with Maquet Holding B.V. & Co*, EIN PRESSWIRE (Feb. 4, 2015), https://www.einpresswire.com/article/248127168/federal-judge-approves-consent-decree-with-maquet-holding-b-v-co [https://perma.cc/Y5D5-8MWW]).

[145] *See, e.g.*, Data Broker Accountability and Transparency Act of 2020, H.R. 6675, 116th Cong. (2020) (proposing new national data privacy law with optimal context sensitivity, based on relative privacy harms of certain data practices).

[146] *See Notification of Enforcement Discretion for Telehealth Remote Communications During the COVID-19 Nationwide Public Health Emergency*, U.S. DEP'T OF HEALTH & HUMAN SERVS. (March 20, 2020), https://www.hhs.gov/hipaa/for-professionals/special-topics/emergency-preparedness/notification-enforcement-discretion-telehealth/index.html [https://perma.cc/VDZ6-QFGM].

and less disruptive enhancements like Bill 1842 or use of the FDA's existing infrastructure might still provide quicker protection for consumers because those solutions likely have a greater chance of becoming law.[147]

[147] Protecting Personal Health Data Act, S. 1842, 116th Cong. (2019) (functioning as an enhancement/expansion of HIPAA protections, and FDA oversight expansion would simply involve new rulemaking and/or guidance).