JOURNAL OF HEALTH CARE FINANCE

Summer 2020

GAPS AND OVERLAPS IN U.S. DATA HEALTH PRIVACY OVERSIGHT: PREVENTING HEALTH TECH. CONSUMER AND PATIENT HEALTH DATA FROM BECOMING THE PRODUCT

Ana C. Rivera-Rios

I. Introduction

The practice of medicine has taken a shift to a more patient-centered market and data-driven model of healthcare.[1] We have observed increased use of technologies such as health mobile applications, online patient portals, social media, the interoperability of health information exchanges, wearable fitness trackers, and internet connected medical devices.[2] The healthcare market possesses such technologies that essentially allow patients to be more engaged in managing their own health outside of the traditional health care sphere than ever before[3] and improves access to healthcare services.[4] This new model enables physicians to provide faster and perhaps more efficient quality of care.[5] For example, patients now have the option to seek consultations with physicians via telemedicine, search symptoms and treatment plans online using "Google," or "Alexa," access medical records online or through mobile applications, possibly communicate with physicians through electronic mail (e-mail) or an online portal, and use patient driven devices for self-screening. Consumers can also download health related mobile applications to monitor their health through their personal smartphone and wearable fitness devices.[6]

Numerous companies are taking a step further and designing medical diagnostic devices to be used in the comfort of consumers' homes, such as FluxBioscience.[7] Another example, iHealth Align,[8] acts as a portable glucometer connected to a smartphone application and also shares information to a portal for physicians to monitor. Although these new medical technologies benefit public health and practitioners, it is critical and imperative to highlight that advances in health information technology (IT)[9] have outpaced privacy and security protections extended by the federal Health Insurance Portability and Accountability Act of 1996 (HIPAA).[10] Private technology companies launching medical devices connected to the internet and/or health

---

[1] LINDA KOONTZ, *INFORMATION PRIVACY IN THE EVOLVING HEALTHCARE ENVIRONMENT*, 108 (USA:CRC Press, 2nd edition, 2017).

[2] U.S. Dept. of Human and Health Services, *Examining Oversight of the Privacy & Security of Health Data Collected by Entities not Regulated by HIPAA*, 1 (2016), https://www.healthit.gov/sites/default/files/non-covered_entities_report_june_17_2016.pdf [hereinafter HHS, *Examining Oversight*].

[3] *Id.*

[4] Mollie Levy, *Marketing Medicine To Millennials: Preparing Institutions and Regulations for Direct-To-Consumer Healthcare*, 528, 55 CAL. W. L. REV. 521 (Spring 2019).

[5] KOONTZ, *supra* note 1, at 129.

[6] Melanie Fridgant, *Technological Developments in the Health Care Industry: Shaping The Future Of The Patient Physician Relationship*, 237-38, 18 HOUS. J. HEALTH L. & POL'Y 237 (2018).

[7] Shashi Amur, *Biomarker Terminology: Speaking the Same Language*, FDA-NIH-Biomarker Working Group (2016), https://www.fda.gov/files/BIOMAKER-TERMINOLOGY—SPEAKING-THE-SAME-LANGUAGE.pdf. (FluxBioscience is new technological device using saliva, urine, or blood samples to measure biological, pathogenic processes, or responses to a therapeutic intervention in these fluids, known as biomarkers. This product offers a portable magnetic sensing device that "measures biomarkers related to exercise, stress, fertility and diet and will correlate measurements to sleep and activity data collected from wearable technologies." Citing from FluxBioscience webpage https://www.flux.bio.com).

[8] Suvarna Seth, *Diabetes Management: Glucose Monitors that Connect To Your Smartphone* (June 5, 2018), https://dlife.com/diabetes-management-glucose-monitors-that-connect-to-your-smart-phone/ (Discusses other glucose applications, such as Glooko, that track food and medication intake, exercise activity, and allow patients to receive advice based on data being shared).

[9] KOONTZ, *supra* note 1, at 129.

[10] Health Insurance Portability and Accountability Act of 1996, Pub. L. 104-191, 110 (Stat)1936 (codified as amended in sections 18, 26, 29, and 42 U.S.C.); 45 C.F.R. §§160.101-552 (2014); *See* Charles Ornstein *Health Gadgets and Apps Outpace Privacy Protections, Report Finds,* ProPublica (July 19, 2016).

applications[11] may not be regulated by HIPAA.[12] To illustrate this matter, a report from the United States Department of Health and Human Services (HHS) states that "as individuals become more engaged in sharing personal health information online, organizations that are not regulated by HIPAA, the Federal Trade Commission (FTC), or state law may collect, share, or use health information about individuals in ways that may put such data at risk of being shared improperly."[13]

Improper disclosure of sensitive protected health information (PHI)[14] may lead patients to lose trust in their providers and discourage IT growth in the healthcare field.[15] As Linda Koontz explains in her book *Information Privacy in the Evolving Healthcare Environment*, "for EHRs [electronic health records], portals, and other health-related technologies to succeed, patients must not only maintain trust in their providers (and technology companies), but they must also trust the systems that collect, use, and disseminate their personal information. Without trust, patients are likely to withhold sensitive information. As a result, healthcare delivery may be negatively affected and health IT investments may not achieve their anticipated benefits."[16]

Inappropriate disclosure of electronic protected health information (e-PHI) could lead to unfortunate events such as physical injury, or even data identity theft, extortion, threats, discrimination, and humiliation.[17] Furthermore, many advocates believe that such sensitive data could be used to negatively affect career advancement, insurance policies and premiums, and even financial decisions such as whether financial credit will be approved.[18] A number of privacy advocates even suggest that consumers' health information could easily become "the product" for companies' electronic health information to data miners or other third-party intermediaries in exchange for payments.[19] News that Google will acquire Fitbit, Inc., a wearable fitness device, for $2.1 billion,[20] has raised questions and privacy concerns as to who owns consumers' data once "acquired" by the health device.[21] Consumers seeking health application services for free may

---

[11] Fridgant. *supra* note 6, at 242.
[12] KOONTZ, *supra* note 1, at 130.
[13] HHS, *Examining Oversight, supra* note 2, at 3.
[14] *See* 45 C.F.R. §160.103 (2013) (Defines health information as any information, whether oral or recorded, created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse, and relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or past, present, or future payment for provision of health care. Meanwhile, §160.103 defines "individually identifiable health information" as any information, including demographic information collected from individual that is created or received by a health care provider, health plan or health care clearinghouse; and relates to the past, present, or future physical or mental health of individual, the provision of health care, or the past, present, or future payment for provision of health care, and 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).
[15] Fridgant, *supra* note 6, at 239.
[16] KOONTZ, *supra* note 1, at 130.
[17] *Id.*
[18] Bruce Y. Lee, *Google to Buy Fitbit for $2.1 Billion, What About Privacy Concerns?,* FORBES (Nov. 2, 2019, 9:40 AM) https://www.forbes.com/sites/brucelee/2019/11/02/google-to-buy-fitbit-for-21-billion-what-about-privacy-concerns/#30cf83a61489
[19] Mary Meehan, *Data Privacy. Will Be the Most Important Issue in The Next Decade*, FORBES (Nov. 26, 2019, 11:40 AM) http://www.forbes.com/sites/marymeehan/2019/11/26/data-privacy-will-be-the-most-important-issue-in-the-next-decade/#cdfc68218823 (Furthermore, *see* Lee, *supra* note 20, discusses consumer concerns voiced via Twitter comments, alleging and criticizing that because Google is in the advertising and data mining business, there is a concern that consumer's personal, private health data might be used to promote Google's financial interests.)
[20] Lee, *supra* note 18.
[21] Meehan, *supra* note 19; *see* also Janet Rae-Dupree, *Tech Giants Like Apple and Google are Competing to Make it Easier For You to Get Your Health Records, and it Could be a $38 Billion Market.* KAISER HEALTH NEWS (Jan. 21,

unknowingly provide valuable personal data that is generally re-sold to facilitate advertising efforts.[22]

It is easy to visualize how as technology continues to grow exponentially, newer methods of collecting, utilizing and disclosing sensitive personal health information have been outpacing current HIPAA regulation. Health care providers are expected to experience increasing demands in the use of digital technological advances such as capturing PHI in EHR, using health mobile applications, medical devices connected to the internet, direct-to-consumer laboratory testing, accessing medical files through the use of smartphone applications[23] and participating in chats and videoconference in the practice of telemedicine.

HIPAA faces gaps when it comes to third-party intermediaries[24] or secondary uses of health information exchange (HIE) data such as big data, and data analytics for marketing purposes and cloud computing.[25] To better illustrate this issue: mobile health applications help collect and share important PHI among patients and physicians; however, there are circumstances when such PHI shared through a smartphone application might not be protected in its entirety by HIPAA.[26] Many health applications provide free services in exchange for acquiring data to be sold to companies analyzing such data for advertising purposes.[27] One major issue with free to use health applications is that consumers do not fully understand the extent by which their sensitive information could be compromised.[28] The caveats contained in privacy policies are usually difficult for consumers to digest or too lengthy for a consumer to finish reading.[29] Even though these technological developments promise to consumers quicker communications with physicians, they also pose the serious risk of PHI being shared inappropriately.

2020 8:30 AM) https://www.businessinsider.com/apple-google-amazon-microsoft-fhir-tools-for-medical-records-2020-1 (Discussing that a number of privacy data advocates disagree with big tech. companies (such as Google, Apple and Amazon) desires to collaborate with federal government to turn Fast Healthcare Interoperability Resources (FHIR) into a reality. FHIR allows patients to use a single application to upload, store, and share all their health information such as lab tests, symptoms, procedures, diagnoses, and access entire health records); *see* also Lori Basheda, *Startup Seeks To Hold Doctors, Hospitals Accountable on Patient Record Requests,* (Nov. 15, 2019) https://californiahealthline.org/news/startup-seeks-to-hold-doctors-hospitals-accountable-on-patient-record-requests/ (Explaining that many advocates disagree with FHIR due to lack of cohesive U.S. privacy law protecting patient data privacy through a third-party consumer application).

[22] Joanna Kessler, *Data Protection in the Wake of the GPDR: California's Solution for Protecting "The World's Most Valuable Resource"* 1, 93 S. CAL. L. REV. 99 (Nov. 2019).

[23] Natasha Singer, *New Data Rules Could Empower Patients but Undermine Their Practice,* THE NEW YORK TIMES. (March 9, 2020) https://www.nytimes.com/2020/03/09/technology/medical-app-patients-data-privacy.html [hereinafter Singer, *New Data Rules]*

[24] KOONTZ, *supra* note 1, at 130.

[25] KOONTZ, *supra* note 1, at 125 (*See* KOONTZ, at 186-90 and 226-33 Suggesting to companies involved in "Big Data" to pay close attention use of appropriate de-identification to benefit from data's secondary use, such as for research purposes or for medication recommendations, without creating undue privacy risks. De-identification of data could be done by removing 18 identifiers noted in HIPAA's Privacy Rule. However, the author warns that there is no 0% risk of re-identification with other public available information, entailing potential disclosure of PHI without the data owner's knowledge).

[26] Alexis Guadarrama, *Content: Mind the Gap: Addressing Gaps in HIPAA Coverage In the Mobile Health Apps Industry,* 1003, 55 HOUS. L. REV. 999.

[27] Kessler, *supra* note 22, at 1.

[28] Matthew Humerick, *The Tortoise and the Hare of International Data Privacy Law: Can the United States Catch Up to Rising Global Standards?,* 89, 27 CATH. U. J. L. 7 TECH. 77 (Fall, 2018).

[29] Kessler, *supra* note 22, at 1.

For instance, mental health applications such as Ginger.io[30] are designed to data mine smartphone GPS tags, call logs, messaging histories, and identify patterns of stress, anxiety and depression, alerting both physicians and patients to seek care or specific drug prescriptions.[31] What seems to be a great milestone in the healthcare industry could also be a huge drawback as consumers' sensitive health data (e.g., prescription drug history) could lead to job discrimination or higher insurance rates.[32] As perfectly stated by the Chair of the American Medical Association's Board, Dr. Jesse M. Ehrenfeld *"*Patients simply may not realize that their genetic, reproductive health, substance abuse disorder, mental health information can be used in ways that could ultimately limit their access to health insurance, life insurance or even be disclosed to their employers."[33] Other types of privacy data breaches, such as access to consumers' location tracking history collected by a wearable fitness device, could pose a great threat to an individual's physical safety.[34] The aforementioned situations are just a few examples demonstrating that HIPAA's specific regulatory language and gaps are no longer responsive to emerging technologies in health care and the privacy protections expected today.

Over the last years, mobile health application downloads have exploded,[35] and the market for these applications is estimated to reach $102.35 billion by 2023.[36] Surprisingly, there have been reports showing that 26% of free applications and 40% of paid health mobile applications do not have privacy policies in place.[37] It was reported that by 2020, companies will have manufactured nearly "'100 million wearable remote patient monitoring (RPM) devices, including blood pressure and glucose monitors."[38] Furthermore, the U.S. government is currently pushing rules that allow consumers to access medical records, including clinical notes, via third-party mobile application, such as Apple's Health Records.[39] This trend adds to the urgency of adopting a comprehensive federal legislation addressing HIPAA's lack of privacy oversight over current emergent direct-to-consumer health products, such as the use of mobile health applications. Strengthening privacy protection of patient's electronic private health information (e-PHI), regardless of who collects and stores the data, will encourage patients to trust and facilitate incorporating these technological developments more often in the delivery of care.[40] Consumer trust and adequate protection of private health information can be achieved through the development and enforcement of a reformed and enhanced, comprehensive HIPAA that will simultaneously protect health

---

[30] *See* Ginger's mobile application Privacy Policy and About Us, https://www.ginger.io/privacy-policy and https://www.ginger.io/about-us (last visited April 21, 2020).
[31] Adam Bluestein, *What Dr. Smartphone Can Do For You,* FAST COMPANY https://infographics.fastcompany.com/magazine/162/smartphone-health.html (last visited Feb. 15, 2020).
[32] Natasha Singer, *When Apps Get Your Medical Data, Your Privacy May Go With It,* THE NEW YORK TIMES(Sept. 3, 2019) [hereinafter Singer, *When Apps Get Your Medical Data*].
[33] *Id.*
[34] FTC Staff Report, *Internet of Things: Privacy and Security in a Connected World,* 13 (Jan. 2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf [hereinafter FTC Staff Report, *IOTs*]
[35] KOONTZ, *supra* note 1, at 134.
[36] Knowledge Sourcing Intelligence LLP, *Mobile Health (mHealth) App Market-Industry Trends, Opportunities and Forecasts to 2023, (Nov. 2017)* https://www.researchandmarkets.com/research/pv554v/28_32_billion?w=5
[37] Stacey-Ann Elvy, *Commod*ifying Consumer Data in the Era of the Internet of Things, 439, 59 B.C. L. REV. 423 (2018)
[38] *Id.* at 437.
[39] Singer, *New Data Rules supra* note 23.
[40] KOONTZ, *supra* note 1, at 134.

information and encourage the growth and use of emerging technologies in the delivery of healthcare.

Part I of this paper describes the existing regulatory environment regarding digital health and illustrates how the current regulatory HIPAA framework failed to contemplate and keep pace with emerging technologies transforming the health marketplace. Because certain states have implemented stricter data privacy legislations, Part II will discuss today's far-reaching privacy statutes across the U.S., such as the California's Confidentiality of Medical Information Act and Consumer Privacy Act. Part III compares the U.S.'s current regulatory framework with the European Union's General Data Protection Regulation. Part IV proposes a robust federal level reformed HIPAA to be implemented nationally to protect patient and consumer's e-PHI as healthcare technology evolves to "direct-to-consumer medicine." [41] Furthermore, part IV will provide recommendations to entities handling PHI to keep in compliance with the proposed federal privacy legislation.

Specifically this paper argues that U.S.'s current patchwork of sector-specific laws, competing state laws, and overlapping governmental agency oversight fails to adequately protect e-PHI in various circumstances. Including circumstances when entities or devices produce, receive and store e-PHI but are not subject to comply with HIPAA because they do not fall within HIPAA's scope of applicability. For these reasons, the U.S. will strongly benefit from a reformed and enhanced, comprehensive HIPAA law, harmonizing state privacy laws and mandating stronger privacy protection for health information based on the type of data and not based on its source.

A reasonable starting point would be for a new reformed HIPAA to adequately address the scope of, and broaden HIPAA's existing definition for, health care providers. Stricter privacy protections, such as those in California's Confidentiality of Medical Information Act (CMIA), define "provider of health care" to include any business that offers software or hardware, designed to store medical health information, including mobile health applications or related devices.[42] Contrary to CMIA, when defining "provider of health care", HIPAA does not mention or include mobile health application businesses or other medical devices connected to the internet processing e-PHI. These types of Non-Covered Entities (NCEs), such as mobile health applications, fall into a loophole within HIPAA, potentially subjecting patients to vulnerable situations as new health oriented technologies continue to be used.

Second, to encourage companies to strongly comply with the reformed HIPAA, the proposal should mirror California's stricter privacy laws, providing a right of civil action for patients to recover damages, if any, for improper e-PHI disclosure.[43] Currently, HIPAA does not provide individuals with a private right of action,[44] even though their data may become "the product" for some companies selling sensitive information.[45] When there is a PHI breach,

---

[41] *Id.*at 2.

[42] Confidentiality of Medical Information Act, Cal. Civ. Code §56.06 (as amended by Assembly Bill No. 2402 (effective Jan. 1, 2019)

[43] California Consumer Privacy Act of 2018, Title 1.81.5 Cal. Civ. Code §1798.150(a)(2018) (as amended by Assembly Bill 1355 (effective Oct. 10, 2019)

[44] *See* 45 C.F.R. §160.306 (2013); *see* Valerie J. Lopez, *Health Data Privacy: How States Can Fill the Gaps in HIPAA,* 313, 50 U.S.F. L. REV. 313, (2016) (citing *Acara v. Banks,* 470 F. 3d 569 (5th Cir. 2006) holding that HIPAA does not create a private right of action for violations of confidentiality under the Act); *see* Roger Hsieh, *Improving HIPAA Enforcement and Protecting Patient Privacy in Digital Healthcare Environment,* 215, 46 LOY. U. CHI. L.J. 175 (Fall 2014).

[45] Valerie J. Lopez, *Health Data Privacy: How States Can Fill the Gaps in HIPAA,* 324, 50 U.S.F. L. REV. 313, (2016).

consumers generally have the right to report the violation to the Department of Health and Human Services (HHS), which then decides whether to pursue the investigation or not.[46] While some companies may profit from selling consumer's sensitive data, it is unclear how HIPAA's current monetary penalties for data breaches directly benefit the owners of PHI disclosed inappropriately.[47]

Third, HIPAA has a serious shortcoming in that it does not provide patients with a right to delete consumer data (also known as right to erasure or "right to be forgotten").[48] This right to erasure is extended both in California's Consumer Privacy Act of 2018 (CCPA) and the European Union's General Data Protection Regulation (GDPR).[49] Fourth, HIPAA does not protect specific identifiers that are considered protected sensitive data by some state laws, such as race, religion, username, password, sexual orientation, marital status, browsing history, search history, information regarding consumer's interaction with an internet website, application or advertising, and web tracking.[50] Because an individual's web entries through a web search engines could include health information, a proposal for extending HIPAA protection to an individual's browsing and search history (e.g. researching symptoms and treatments through Google) is highly recommended. This proposal should aid with proper de-identification of sensitive data that may identify an individual,[51] thus limiting improper disclosures of PHI. [52]

Lastly, other stringent privacy laws, such as the GDPR, provide consumers with wider rights and transparency compared to HIPAA. Wider transparency will enable health technology consumers to make fair choices over their data, control how PHI may be used (including future uses), and provide a genuine and informed data authorization. All of these shortcomings need to be addressed in a more comprehensive, "second generation" reformed HIPAA.

---

[46] Patrick Ouellette, *Will Walgreens Breach Ruling Affect Future HIPAA Violations?*, HEALTH IT SECURITY, (August 13, 2013) https://healthitsecurity.com/news/will-walgreens-breach-ruling-affect-future-hipaa-violations/

[47] *Id.*

[48] Cal. Civ. Code §1798.105.

[49] Cal. Civ. Code, §1798.105; *see* Commission Regulation 2016/679, of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data on the Free Movement of Such Data, Art. 17, 2016 O.J. (L 119) (EU) (May 4, 2016).

[50] *Id.*at §1798.140 (o)(1)(F)

[51] *See* 45 C.F.R. §164.514 (a) and (b) (§164.514(a) Defines de-identified protected health information as health information that does not identify an individual and there is no reasonable basis to believe that the information can be used to identify an individual. Clarifies that properly de-identified data is not individually identifiable information. At the same time; and (b)(2) lists 18 identifiers that must be removed to consider protected health information properly de-identified, and none of them specifically mention browsing internet history, search history and web tracking).

[52] *See* Stacey A. Tovino, *Going Rogue: Mobile Research Applications and the Right to Privacy,* 194-95, 95 NOTRE DAME L. REV. 155, (November, 2019) citing note 236, *e.g.*, Cameron F. Kerry, *Why Protecting Privacy Is a Losing Game Today-and How to Change the Game, Brookings Institution,* (July 12, 2018), https://www.brookings.edu/research/why-protecting-privacy-is-a-losing-game-today-and-how-to-change-the-game/ ("To most people, 'personal information' means information like social security numbers, account numbers, and other information that is unique to them. U.S. privacy laws reflect this conception by aiming at 'personally identifiable information,' but data scientists have repeatedly demonstrated that this focus can be too narrow. The aggregation and correlation of data from various sources [even de-identified data] make[s]it increasingly possible to link supposedly anonymous information to specific individuals and to infer characteristics and information about them. The result is that today, a widening range of data has the potential to be personal information, i.e. to identify us uniquely. Few laws or regulations address this new reality.").

II. Current U.S. Regulatory Framework on Health Data Protection

In a traditional healthcare setting, where a patient seeks health care services from a health care provider (physician or hospital), the patient's PHI is protected by HIPAA, state laws or various agencies. In regards to governmental agencies, PHI meeting HIPAA's definition parameters,[53] is enforced and overseen by the Department of Health and Human Services' Office for Civil Rights (HHS).[54] In the case of health data shared with mobile health applications, there are two main regulators, the Federal Trade Commission (FTC) and the Food and Drug Administration (FDA).[55] The FDA's oversight focus is on mobile health application's efficacy and safety.[56] The FTC protects consumers from certain privacy violations.[57] The FTC is an independent administrative agency responsible for protecting consumer's data by prohibiting unfair and deceptive privacy and security practice.[58] For instance, relying on Section 5 of the Federal Trade Commission Act, the FTC has used its authority to penalize an entity it had reason to believe made false or misleading claims about its privacy or health data security procedures and as a result caused substantial injury to a consumer[59] by publishing their doctor's notes on the Internet, easily accessible through an Internet search.[60] In addition, the FTC has used its authority to protect patients from insecure devices transmitting data between places via the internet, widely known as Internet of Things (IoT).[61]

In addition to HIPAA, there are also specific federal laws that apply to specific types of health information, such as the Family Educational Rights and Privacy Act (FERPA), which limits access to health data preserved in school records;[62] and the Genetic Information Nondiscrimination Act of 2008 (GINA), prohibiting group health plans and employers from discriminating based on genetic test results or family history.[63] The HIPAA Privacy Rule allows unauthorized disclosure of PHI when required by state and other federal laws for disaster relief,[64] disclosures about victims

---

[53] Jianyan Fang, *Health Data at Your Fingertips: Federal Regulatory Proposals for Consumer-Generated Mobile Health Data*, 143, 4 GEO. L. TECH. REV. 125 (2019).
[54] HHS, *Examining Oversight, supra* note 2, at 1; *See* Fang, *supra* note 53, at 128.
[55] Fang, *supra* note 53, at 129.
[56] *Id.* at 143.
[57] HHS, *Examining Oversight, supra* note 2, at 3.
[58] 15 U.S.C. § 45 (a) (2006)
[59] HHS, *Examining Oversight, supra* note 2, at 18.

[60] *See GMR Transcription Services, Inc*., No. C-4482 FTC (Aug. 14, 2014)http:s//www.ftc.gov/enforcement/cases-proceedings/122-3095/gmr-transcription-services-inc-matter (Discussing court decisions and orders).

[61] FTC Staff Report, *IOTs, supra* note 34, at 4.
[62] 20 U.S.C. 1232g; 30 C.F.R. Part 99 Part D (1974) §99.30-99.39
[63] *See* Table including a summary of existing sector specific privacy laws in the U.S., *Summary of Selected Federal Laws and Regulations Addressing Confidentiality, Privacy and Security,* 3, HEALTHIT.GOV https://www.healthit.gov/sites/default/files/privacy-security/federal-privacy-laws-table2-26-10-final.pdf (Feb. 18, 2010; (*see* for further examples of sector-specific federal laws overlapping: FERPA, COPPA (15 U.S.C. §6501.6506 (1998)) and FTC's interpretation; *see* FTC, *Complying with COPPA: Frequently Asked Question, M. COPPA and SCHOOLS* https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions#Schools (March 20, 2015)).

[64] 45 C.F.R. §164.510 (b)

of abuse, neglect or domestic violence,[65] or for law enforcement purposes.[66] This piecemeal approach to privacy protection, however, can lead to confusion.

The intricacies surrounding the U.S.'s current privacy health data legislation are further exacerbated as a number of states have enacted health privacy rules, complementary to HIPAA, but more protective in terms of patient privacy. As a general rule, states typically defer to HIPAA because it is a federal law that establishes a nationwide floor of privacy and security standards.[67] However, states are permitted to adopt more stringent privacy laws,[68] as long that particular state law is not preempted by federal requirements.[69] These state level health privacy rules concern specific clinical conditions such as HIV/AIDS status, mental or reproductive health, among other health circumstances.[70]

Two examples of more stringent privacy state laws that will be discussed in this paper are California's Confidentiality of Medical Information Act (CMIA), and effective as of January 1, 2020, the California's Consumer Privacy Act (CCPA). CCPA provides the state of California with the strongest data privacy rights in the U.S. and intends to return power and control to consumers over their sensitive personal data.[71] Allowing a patchwork of state laws laying out different definitions, scope, and applications may create inconsistencies for entities doing business across state lines.

A. General Background Information on HIPAA's Statutory Framework

On August 21, 1996,[72] Congress enacted HIPAA, Public Law 104-191, to address the privacy concerns of patients over the security of their health information in a clinical setting.[73] HIPAA's main intention at the time was to ensure individuals maintained health insurance between job changes, to extend health insurance coverage to individual and group markets, and to combat waste, fraud, and abuse in health care insurance and delivery, among other objectives.[74] Congress later acknowledged the need to protect the privacy of health information as technology kept advancing.[75]

---

[65] 45 C.F.R. §164.412 (c)
[66] 45 C.F.R. §164.152 (f)
[67] *See* List of HIPAA's Privacy Rule questions and answers, *Health Privacy: HIPAA Basics,* PRIVACY RIGHTS CLEARINGHOUSE, (Feb. 1, 2015) https://privacyrights.org/consumer-guides/health-privacy-hipaa-basics [hereinafter Health Privacy Q's and A's]
[68] 45 C.F.R. §160.202(1)
[69] 45 C.F.R. §160.203
[70] Health Privacy, Q's and A's, *supra* note 67.
[71] *See* Alastair Mactaggart, *A Letter from Alastair Mactaggart, Founder & Chair of Californians for Consumer Privacy*, https://www.caprivacy.org (last visited April 21, 2020); *see* CA's Attorney General Alastair Mactaggart, *Re: Submission of Amendments to the California Privacy Rights and Enforcement Act of 2020, Version 2, No. 19-0021,* (Nov. 4, 2019) https://oag.ca.gov/system/files/initiatives/pdfs/19-0021A1%20%28Consumer%20Privacy%20-%20Version%203%29_1.pdf
[72] *See* 45 C.F.R. §160; *see* Institute of Medicine (US) Committee on Health Research and the Privacy of Health Information: *HIPAA, the Privacy Rule, and Its Application to Health Research*; Nass SJ, BEYOND THE HIPAA PRIVACY RULE: ENHANCING PRIVACY, IMPROVING HEALTH THROUGH RESEARCH. (2009) available from: https://www.ncbi.nlm.nih.gov/books/NBK9573/ (last visited April 21, 2020) [hereinafter HIPAA's Privacy Rule and Its Application to Health Research]
[73] Levy, *supra note* 4, at 13.
[74] Public Law 104-191 (1996), (HIPAA's synopsis).
[75] HIPPA's Privacy Rule and Its Application to Health Research, *supra* note 72, at 2.

Consequently, the Department of Health and Human Services (HHS), the federal agency in charge of creating Rules to properly implement HIPAA, adopted the *Standards for Privacy of Individually Identifiable Health Information* (Privacy Rule) in 2002.[76] HIPAA's Privacy Rule adoption established for the first time national standards to protect health information,[77] with an effective compliance date for 2003.[78] In 2003, HHS also published a final Security Rule establishing national standards for protecting the integrity and confidentiality of stored and transferred electronic protected health information.[79] HIPAA's Security Rule does not apply to PHI transmitted orally or in writing, because it only requires the security of health information in electronic form.[80] That same year, the Enforcement Rule was adopted to address compliance, investigations and list penalties for HIPAA Privacy and Security Rule violations.[81] HIPAA's Breach Notification Rule requires notifications to be issued after a breach of unsecured PHI has taken place.

A breach takes place when PHI has been acquired, accessed, used, or disclosed in a manner not permitted by the HIPAA Privacy Rule, compromising the security or privacy of PHI.[82] Breach notification is not required when the disclosure was either acquired unintentionally or inadvertently and was not further used or disclosed inappropriately.[83] If an individual's PHI has been, or is reasonably believed to have been accessed, acquired, used, or disclosed as result of such breach, he or she should be notified no later than 60 days after discovery of the breach.[84] If the breach impacts more than 500 individuals, a media notice should be released within 60 days after discovery of the breach.[85]

Overall, through the implementation of the three HIPAA rules (Privacy, Security, and Breach Notification Rule), HIPAA requires health care providers, as well as those entities working for the providers, to ensure the confidentiality and security of PHI when transferred, received, handled, or shared.[86] Within the HHS, the Office of Civil Rights (OCR) has the responsibility to enforce HIPAA's Privacy and Security Rule, and to impose civil monetary penalties when applicable.[87]

---

[76] Stacey A. Tovino, *Teaching Health Law: Teaching the HIPAA Privacy Rule*, 471, 61 ST. LOUIS L. J. 469 (Spring 2017). [hereinafter Tovino, *Teaching Health Law]*

[77] Privacy of Individually Identifiable Health Information, 45 C.F.R. §164.500-164.534, Subpart E (2016); *See* U.S. Dept. of Human and Health Services, OCR Privacy Breach, *Summary of the HIPAA Privacy Rule*, 2 (Last revised 05/03) https://www.hhs.gov/sites/default/files/privacysummary.pdf

[78] *HIPAA History*, HIPAA JOURNAL https://www.hipaajournal.com/hipaa-history/ (last visited April 21, 2020) [hereinafter *HIPAA history]*.

[79]45 C.F.R. §160, Subparts A and C of part 164; *see* Office of Civil Rights (OCR), U.S. Dept. of Health and Human Services, *HIPAA for Professionals*, HHS.GOV https://www.hhs.gov/hipaa/for-professionals/index.html (last reviewed on June 16, 2017) [hereinafter OCR, *HIPAA for Professionals*]; *see* U.S. Dept. of Health and Human Services-OCR, 45 C.F.R. Parts 160 and 164, Federal Register, Vol. 78, No. 17, Part II, Rules and Regulations (Jan. 25, 2013) https://www.govinfo.gov/content/pkg/FR-2013-01-25/pdf/2013-01073.pdf

[80] OCR, *HIPAA for Professionals*, *supra* note 79.

[81] 45 C.F.R. §160, Subparts C, D, and E; *see* Office of Civil Rights (OCR), U.S. Dept. of Health and Human Services, *HITECH ACT Enforcement Interim Final Rule, HHS.GOV*, https://www.hhs.gov/hipaa/for-professionals/special-topics/hitech-act-enforcement-interim-final-rule/index.html (last reviewed on June 16, 2017)

[82] 45 C.F.R. §164.400-414

[83] 45 C.F.R. §164.402

[84] 45 C.F.R. §164.404

[85] 45 C.F.R. §164.406 (*see* §164.408 In addition, HHS must be notified if a data breach has been discovered for incidents involving 500 or more individuals, and within 60 days of the end of the calendar year, if the breach involved less than 500 individuals).

[86] HHS, *Examining Oversight*, *supra* note 2, at 3.

[87] OCR, *Summary of the HIPAA Privacy Rule*, HHS.GOV (July 26, 2013) https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html [hereinafter OCR, *Summary of HIPAA Privacy*]

Meanwhile, the Department of Justice has the duty to oversee and impose criminal penalties for unauthorized PHI disclosures.[88] Additionally, HHS (OCR) is authorized to impose Civil Monetary Penalties (CMP) and the Attorney General's Office (AG) is authorized to review and address HIPAA violations complaints.[89]

B. HIPAA's Privacy Rule

Up until 2002, privacy data protections relied mostly on state laws and some sector-specific federal laws.[90] In 2002, HHS adopted the first national data protection privacy law—the HIPAA Privacy Rule.[91] State laws enacted previous to 2002, and providing stronger privacy data protections than HIPAA's Privacy Rule, continue to be implemented complementary to HIPAA.[92] HIPAA's Privacy Rule gives individuals specific rights with respect to their protected health information (PHI), such as the right to request restrictions on uses and disclosures of PHI,[93] right of access to PHI,[94] right to amend PHI,[95] and the right to an accounting of disclosures of PHI[96] HIPAA's Privacy Rule is sometimes referred to as the "Disclosure Rule" because it defines when, how, and under what circumstances an individual's PHI can be disclosed.[97]

Essentially, HIPAA's Privacy Rule defines PHI and its limited uses and disclosures. PHI is any individually identifiable health information (IIHI) held by the entities subject to HIPAA, regarding the health status, provision of health care services, or payment of health services transmitted or maintained in electronic or in any other form or medium.[98] As a general rule, HIPAA's Privacy Rule extends protection to identifiable health information, created or received by a Covered Entity (CE),[99] and guarantees certain rights in regards to that information.[100] Properly de-identified data, however, is not subject to HIPAA legislation because it is not considered individually identifiable health information.[101]

HIPAA defines individually identifiable health information (IIHI) as health information collected from an individual, including demographic information, and created or received by a health care provider, health plan, employer, or health care clearinghouse that either identifies or

---

[88] HHS, *Examining Oversight*, *supra* note 2, at 3.
[89] OCR, *Summary of HIPAA Privacy*, *supra* note 87.
[90] OCR, For Professional FAQ, *Why is the Privacy Rule needed?* HHS.GOV (July 23, 2013) https://www.hhs.gov/hipaa/for-professionals/faq/188/why-is-the-privacy-rule-needed/index.html [hereinafter FAQ Privacy Rule]
[91] *HIPAA History*, *supra* note 78.
[92] FAQ Privacy Rule, *supra* note 90.
[93] 45 C.F.R. §164.522
[94] 45 C.F.R. §164.524
[95] 45 C.F.R. §164.526
[96] 45 C.F.R. §164.528
[97] *See*. Tovino, *Teaching Health Law*, *supra* note 76, at 476.
[98] 45 C.F.R. §160.103 (The Privacy Rule defines individually identifiable health information (IIHI) as information that is a subset of health information, including demographic information collected from an individual, and: (1) is created or received by a health care provider, plan, employer, or health care clearinghouse; and (2) relates to the past, present, or future of physical or mental health status; the provision of health care; or the past, present, or future payment for provision of health care services; and (i) identified the individual, or (ii) with respect to which there is a reasonable basis to believe the information can be used to identify the individual.)
[99] 45 C.F.R. §160.103 (Covered entities are health care providers, plans, and clearinghouse who transmit electronic protected information in electronic form as part of its services. Covered Entities are subject to HIPAA compliance.)
[100] Guadarrama, *supra* note 26, at 1006.
[101] 45 C.F.R. §164.514 (a)

could be used to identify an individual.[102] In addition, the information relates or could relate to the past, present, or future of physical or mental health condition of an individual, to any service provided or payment made for the provision of health care service.[103] Examples of individually identifiable health information identifiers include: names; zip codes, health care service date, contact information, medical record numbers, health plan beneficiary numbers; or Web Universal Resource Locators (URLs) and Internet Protocol (IP) numbers.[104]

To expand further on HIPAA's Privacy Rule application, HIPAA applies to CEs to ensure the privacy of PHI.[105] There are three types of CEs: health care providers, health plans, and health care clearinghouses which transmit health information in electronic form.[106] Health care providers include: physicians, hospitals, psychologists, chiropractors, dentists, pharmacies, urgent care clinics, among other health care providers.[107] Health plans are defined as those paying for the cost of medical services or care.[108] Health plans include health insurance companies, health maintenance organizations (HMO's), company health plans, group health plans sponsored by an employer, Medicare and Medicaid, and the military and veterans' health care programs.[109] Finally, the third type of covered entities are health care clearinghouses, which could include billing services and other services that facilitate the process of PHI so that it transmitted in a standard format between entities.[110] For example, a clearinghouse may take notes from a physician and convert it into a standard coded format to be transferred for billing and insurance purposes.

In 2009, the Health Information Technology for Economic and Clinical Health (HITECH) Act was enacted, as part of the American Recovery and Reinvestment Act of 2009, to promote the adoption of meaningful use of health information technology[111] as a result of newer technology changes in the medical landscape. HITECH also included authority to issue health data breach notice.[112] HITECH was primary enacted to encourage entities to adopt computerized patients' medical records, also known as Electronic Health Records (EHRs).[113] In 2013, HITECH expanded direct applicability of HIPAA to another type of entity, known as Business Associates (BA),[114]

---

[102] 45 C.F.R. §160.103

[103] 45 C.F.R. §160.103

[104] 45 C.F.R. §160.514 (b)(2) (Further examples of include: geographic subdivisions smaller than a State (address or full zip codes); elements of dates (except year) for dates directly related to individual (birth date, admission date, service date, discharge date, date of death); fax numbers; social security numbers; certificate/license numbers; vehicle identifiers (includes license plate numbers); device identifiers and serial numbers; account numbers, Web Universal Resource Locators (URL's); Internet Protocol (IP) address numbers; biometric identifiers (including finger and voice prints); and full face photographic images).

[105] 45 C.F.R. §160.103

[106] 45 C.F.R. §164.103

[107] OCR, For Professional FAQ, *Covered Entities and Business Associates*, HHS.GOV (June 16, 2017) https://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html [hereinafter OCR FAQ, Covered Entities]

[108] 45 C.F.R. §160.103

[109] 45 C.F.R. §160.103; *see* OCR FAQ, Covered Entities *supra* note 107..

[110] 45 C.F.R. §160.103

[111] OCFR, *HITECH Act Enforcement Interim Final Rule*, HHS.GOV (June 16, 2017) https://www.hhs.gov/hipaa/for-professionals/special-topics/hitech-act-enforcement-interim-final-rule/index.html; *see Health Information Technology for Economic and Clinical Health Act*, §13410, Pub. L. No. 111-5, 123 Stat. 226 (2009), codified at various sections of 42 U.S.C.

[112] *Id.*

[113] Glyn Cashwell, *Cyber-Vulnerabilities and Public Health Emergency Response*,39, 21 J. HEALTH CARE L. & POL'Y 29, (2018).

[114] *see* Modifications to HIPAA Privacy, Security, Enforcement and Breach Notification Rules, 78 Fed. Reg. 5565 (Jan. 25, 2013) (codified at 45 CFR Parts 160 and 164) (adopting 45 C.F.R. §160.103 and providing a new definition of business associate). (Business Associate is defined as a person or organization who: (1) on behalf of a

such as outside billers and health care consultants.[115] BAs create, receive, maintain or transfer PHI on behalf of CEs or another BA who is authorized to work on behalf of the BA as a subcontractor.[116] Examples of BA services working on behalf of a CE could range from administrative work to legal, accounting, data aggregation, data analysis, consulting, document shredding, billing services, among others.[117] Most of the examples listed under HIPAA's Privacy Rule definition of BAs, often refer to types of services that don't require patient interaction with the BA.[118] HITECH also requires BAs subcontractors to equally protect PHI that it creates or receives on behalf of the BA.[119]

As a general rule, under HITECH, BAs of a CE are required to be in compliance with HIPAA's Privacy and Security Rules.[120] Similarly, a subcontractor that creates, maintains or transmits PHI on behalf of a BA is also legally responsible to be HIPAA compliant.[121] HIPAA defines "subcontractor" as a person or entity to whom a business associate delegates a function, activity, or service, other than in the capacity of a member of the workforce of such business associate.[122] HITECH also strengthened HIPAA's Privacy Rule limitations on the use and disclosure of PHI for marketing and fundraising purposes, and prohibited sale of PHI without an individual's authorization by those entities required to comply with HIPAA.[123]

The HIPAA Rules provide a number of protections and rights for data subjects over PHI held by CEs or BAs.[124] As a general rule, data subjects' written authorizations must be obtained before use or disclosure of subject's PHI.[125] As an exception to the general rule, PHI may be used or disclosed without an individual's authorization subject to HIPAA's specific permitted uses: for the CE to carry out their own treatment,[126] payment,[127] and health care operations,[128] as well as allowed

---

covered entity, but other than in the capacity of a member of the workforce of a covered entity, create, receive, maintain, or transmit PHI for a function or activity regulated by the HIPAA Privacy Rule; and (2) provide, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for the covered entity.) [hereinafter Fed. Reg. Modifications to HIPAA]

[115] 42 U.S.C. 201 Subtitle D-Privacy also see: https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html

[116] 45 C.F.R. §160.103

[117] 45 C.F.R. §160.103

[118] See 45 C.F.R. §160.103 (List of examples included in "business associate" definition).

[119] 45 C.F.R. 160.103 (Business Associate definition extends scope to subcontractors that create receive, maintain, or transmit PHI on behalf of BA.)

[120] *See* Fed. Reg. Modifications to HIPAA, *supra* note 114.

[121] 45 C.F.R. §160.103 (*See* American Academy of Pediatrics, professional resources *Business Associates,* https://www.aap.org/en-us/professional-resources/practice-transformation/managing-practice/Pages/Business-Associates.aspx (last visited March 18, 2020) Includes examples of Business Associate's subcontractors: when BA hires outside company to complete services provided to a CE, such as shredding documents containing PHI, data conversion of PHI, de-identification of PHI, or provide cloud services for data storage.)

[122] 45 C.F.R. §160.103

[123] *See* Fed. Reg. Modifications to HIPAA, supra note 114.

[124] *See* HHS, *Examining Oversight, supra* note 2.

[125] HHS, *Examining Oversight, supra* note 2, at 14.

[126] 45 C.F.R. §165.501 (Treatment is define by the provision, coordination, or management of health care and related services by one or more health providers, including coordination or management of health care by a provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care to another).

[127] *Id.*

[128] *Id.*

for public benefit activities.[129] Moreover, HIPAA provides data subjects with individual rights, such as the right to be notified of and complain about PHI breaches, access and obtain copies of their EHRs,[130] amend their PHI,[131] and restrict their PHI uses and disclosures, such as restricting disclosures to health plan concerning treatment for which patient paid out of pocket in full.[132] In return, CEs have a 30 day deadline to respond to PHI access,[133] and 60 days to act upon an individual's request to amend PHI.[134]

C. HIPAA Rules' Weaknesses

i. HIPAA's loophole for non-covered entities:

As mentioned above, HIPAA only applies to Cover Entities (CEs) and Business Associates (BAs) or its subcontractors. When HIPAA Privacy Rules define business associates, there is no mention of "direct-to-consumer" smartphone health applications nor other businesses offering software for health devices connected to the internet. HIPAA's statutory language technically excuses certain health technology companies from being HIPAA noncompliant even though health information is regularly received, stored, or processed as part of their business. Non-Covered Entities or non-covered Business Associates (hereinafter NCEs) are widely used today by technology driven consumers, inadvertently falling within a HIPAA loophole.[135] Examples of companies that frequently receive, store and transfer health information and not subject to HIPAA are: gyms and fitness clubs; life insurance companies; search engines or websites that provide health or medical information and are not operated by a CE; direct to consumer genetic testing entities; and many health and fitness mobile applications.[136]

Because HIPAA applies to traditional health care services and settings, its design is flawed and outdated when it comes to patient's PHI in alternate non-traditional digital or direct-to-consumer contexts.[137] An example of today's direct-to-consumer devices being integrated into the healthcare delivery system are mobile health applications, data storage companies to support them,[138] wearables, or other wireless medical devices that by themselves or connected to smartphone applications process health information wirelessly, such as the Internet of Things (IoT).[139] IoT's

---

[129] 45 C.F.R. §164.512(a), (c), (f), (i), (l) (CE may use and disclose PHI for different public activities without prior written authorization of data subject. *See* §164.512 (a)-(l). These public interest activities include, but not limited to, when disclosure is required by law, for public health activities, for law enforcement purposes, for research, and for workers' compensation activities.)

[130] 45 C.F.R. §164.524

[131] 45 C.F.R. §164.526 (a)

[132] *See* Fed. Reg. Modifications to HIPAA, *supra* note 114.

[133] 45 C.F.R. §154.524 (b) (2)

[134] 45 C.F.R. §164.526 (b)(2)(i)

[135] *See* Jessica Davis, *HHS Clarifies HIPAA Liability Around Third-Party Health Apps*, XTELLIGENT HEALTHCARE MEDIA, (April 12, 2019), https://healthitsecurity.com/news/hhs-clarifies-hipaa-liability-around-third-party-health-apps [hereinafter Davis, HHS Clarifies HIPAA]

[136] Health Privacy Q's and A's *supra* note 67.

[137] Levy, *supra* note 4, at 21.

[138] Stacey A. Tovino, *Going Rogue: Mobile Research Applications and the Right to Privacy*, 158, 95 NOTRE DAME L. REV. 155, (Nov. 2019) [hereinafter Tovino, *Going Rogue*]

[139] Fang, *supra* note 53, at 132. (Discusses various types of mobile health applications as studied by scholars. One scholar, Nathan Cortez, divided mobile health applications into categories based on their respective functions: (1) connectors which connect mobile devices to FDA-regulated devices and thus amplify such regulated devices' functionalities; (2) replicators which turn mobile devices into FDA-regulated devices; (3) automators and customizers which use different methodologies including questionnaires, and medical calculators to aid clinical

are devices connected to the internet for the purpose of monitoring a patient's health.[140] Sensitive information being shared through the internet, such as the use of health applications or smartphone video consults could cause patients' private health information to be left vulnerably exposed to hackers who wish to access unsafe networks containing a large amount of protected health information.[141] Additionally, this situation could also pose a risk to a patient's physical safety. For instance, hackers may remotely join into internet connected insulin pumps, and change their settings to the extent that a patient could be harmed by missing an insulin dose.[142]

When the federal health privacy legislation was enacted, serious privacy and security risk considerations were not possible because advanced patient-based technologies were not designed or integrated into the healthcare system. In other words, HIPAA's specific language regarding its applicability translates to a major handicap in today's technology-oriented healthcare system. This occurs because HIPAA only applies to healthcare entities that fall within the CE or BA definition.[143] HIPAA's strict statutory language, specifically when it comes to its applicability, strips away protection of identifiable health information[144] collected by entities not listed in the statutory definition.[145] If an organization is considered a NCE, then the NCE collecting electronic health information is not subject to HIPAA regulation. Consequently, any additional sharing of the electronic health information by the NCE is not considered a breach of data,[146] clearly denying patients' rights to own and control how and to whom their PHI is shared with.

For example, the Food and Drug Administration (FDA), a federal agency that regulates medical technology, states that digital health includes "mobile health (mHealth), health information technology (IT), wearable devices, telehealth and telemedicine, and personalized medicine."[147] But, these new "digital health" devices[148] collecting PHI, were not initially contemplated by HIPAA, and HIPAA has not been amended to include them. Despite advocates' push to amend the U.S. privacy data regulation to include a neutral language in its applicability, some emerging patient-based health technologies are still not subject to privacy data regulations.[149] This creates a privacy risk for patients' PHI or may cause consumers to access consumer oriented health technology that may be misleading, overpromising, and unregulated.[150]

The failure to safeguard private health information shared with NCEs is such that an individual loses control and ownership over their sensitive health information. Unfortunately, gaps and overlaps in U.S. privacy laws have opened an avenue for NCEs to profit from selling aggregate

---

decisions; (4) informers and educators which primarily inform and educate users; (5) administrators which automate office functions such as identifying insurance billing codes or scheduling patient appointments; and (6) loggers and trackers which allow users to log, record, and make decisions about general health and wellness.)

[140] Cashwell, *supra* note 113, at 4.

[141] *Id.*

[142] FTC Staff Report, *IOTs, supra* note 34, at 13.

[143] 45 C.F.R. §160.102.

[144] HHS, *Examining Oversight, supra* note 2, at 1.

[145] *See* Latena Hazard, *Is Your Health Data Really Private: The Need to Update HIPAA Regulations to Incorporate Third-Party and Non-Covered Entities*, 25 CATH. U. J. L. & TECH. 447 (March 2017) (discussing HIPAA rules and their effect on health applications, and arguing that HIPAA needs to be adjusted to incorporate non-covered entities).

[146] Charlotte A. Tschider, *Enhancing Cybersecurity for the Digital Health Marketplace,* 10, 26 ANN. HEALTH L. 1 (Winter 2017)

[147] FDA, *Digital Health*,FDA.GOV https://www.fda.gov/medical-devices/digital-health (last visited Nov. 25, 2019).

[148] Tschider, *supra* note 146, at 5.

[149] Levy, *supra* note 4, at 21.

[150] *Id.*

personal data to third parties (e.g. advertising and analytics companies).[151]Sometimes, sensitive data could be acquire from a consumers' internet searches on symptoms, exercise, diet routines or other topics.[152] In fact, "mundane data that is not inherently health-related could reveal health-related correlations or conclusions if aggregated and analyzed with other datasets."[153]

ii. HIPAA's lack of focus and scope on data sensitivity:

Recapitulating, HIPPA clarifies that CEs include different categories such as health care plans, health care clearinghouse, and healthcare providers that transmit protected health information electronically.[154] Meanwhile, BAs are statutorily defined as entities that assist CEs' operations by receiving, maintaining or transmitting PHI.[155] Based on this statutory definition, an inference could be made that classifying an organization as a BA is contingent on the primary organization's being considered a CE under HIPAA regulation.[156] "In sum, the amount of protection health data receives depends on who holds the data, not the type of information being held. This gap in regulation leaves a large part of the mobile health apps industry essentially unregulated and many health application consumers mistakenly thinking that the information they share is afforded more protection that it really is."[157]

The issue with HIPAA's limited statutory definition extending regulation to only two types of entities is that the general public has a limited or incorrect understanding as to who is required to protect health information. The lay person may incorrectly think HIPAA provides standards for privacy and security in all contexts where their health information is collected, shared, or used. However, HIPAA's privacy protection is based on "who holds the data, not the type of information being held."[158] "HIPAA focuses on how health data should be channeled, instead of how the private interests attached to health data should be safeguarded."[159] Unfortunately, individuals may inadvertently consent to unanticipated types of information sharing and disclosure by NCEs.

Although data privacy authorization may be regulated by the Federal Trade Commission (FTC's) consumer protection oversight, this oversight does not provide the same type or level of protection as HIPAA. Generally, the FTC enforces the FTC Act's consumer protection prohibition against acts or practices that are unfair or deceptive.[160] "These could include, for example, failing to comply with an entity's own privacy policy, deceptively failing to disclose material information about the use of personally identifiable information, or failing to reasonably secure this information."[161]

---

[151] *See* FTC, Transcript on Spring Privacy Series: Consumer Generated and Controlled Health Data, (May 7, 2014) https://www.ftc.gov/system/files/documents/videos/spring-privacy-series-consumer-generated-controlled-health-data/ftc_spring_privacy_series_-_consumer_generated_and_controlled_health_data_-_transcript.pdf [hereinafter FTC, Transcript on Spring Privacy Series].
[152] *Id.*
[153] Fang, *supra* 53, at 135; (*see* Fang, *supra* 53, at 142, suggesting that re-identification of mobile health application data could identify an individual when analyzed in conjunction with other available datasets, due to Big Data analytics.).
[154] 45 C.F.R. §160.103
[155] 45 C.F.R. §160.103
[156] Tschider, *supra* note 146, at 10.
[157] Guadarrama, *supra* note 26, at 1004.
[158] Guadarrama, *supra* note 26, at 2.
[159] Fang, *supra* note 53, at 146.
[160] 15 U.S.C. § 45 and §52.
[161] HHS, *Examining Oversight*, *supra* note 2, at 3.

Regardless of the proper disclosure of material information to consumers, due to the complex nature distinctive to legislation surrounding health data privacy rights, many patients are not equipped to scrutinize the privacy and security implications accompanying their everyday interactions with NCEs.[162] In fact, even though a patient might think health information obtained at a CE is protected by HIPAA "the applicable data protection rules may vary as data changes hands. For example, a patient's blood pressure stored in a hospital's Electronic Health Record (EHR) is initially regulated by HIPAA, but it may escape from HIPAA's regulation once the patient downloads and input the same information into a consumer-facing mHealth [mobile health] app."[163] Lastly, note that NCEs are not required by any legislation to provide information as to what data was shared or re-disclosed, curtailing individuals' rights to access their own health data.[164] When an entity is not regulated by HIPAA, it becomes unclear to individuals if they have the right to access and review their own health data held by these NCE's unregulated by HIPAA.[165]

iii. De-Identified data:

De-identified data is health information that has had 18 specific identifiers removed and makes the individual, otherwise the subject of the PHI, unidentifiable.[166] This method of de-identification is known as the "Safe Harbor Method."[167] The goal of de-identification is to remove these identifiers to protect PHI's privacy while still permitting data to be used for other purposes, such as public health and research.[168] Proper de-identified data is not considered individually identifiable health information[169] and therefore not subject to HIPAA.

What happens when the de-identified data is combined with other data and re-identifies an individual? Recently, one main issue with de-identified data is that de-identified data could be easily re-identified.[170] The two methods used to de-identify data[171] do not protect against future uses of data that could re-identify individual or used to infer the individual's identity.[172] Once the de-identified data is re-identified, that re-identified data generally is no longer protected by HIPAA.[173] If the re-identified data is shared with a NCE, the PHI could be shared freely and still not be considered a HIPAA violation.[174] This is mainly because NCEs are not subject to the same standards as CEs or BAs. [175] However, it would be protected if the re-identified data comes into the hands of a CE or BA.

---

[162] HHS, *Examining Oversight*, *supra* note 2, at 4.
[163] Fang, *supra* note 53, at 134.
[164] HHS, *Examining Oversight*, *supra* note 2, at 21.
[165] HHS, *Examining Oversight*, *supra* note 2, at 5.
[166] 45 C.F.R. §164.514 (b)(2)
[167] William W. Stead, letter regarding recommendations on de-identification of PHI under HIPAA, HHS.GOV, 5,7 (Feb. 23, 2017) https://ncvhs.hhs.gov/wp-content/uploads/2018/03/2017-Ltr-Privacy-DeIdentification-Feb-23-Final-w-sig.pdf (Letter explaining two known methods to de-identify protected health information: Safe Harbor method and Expert Determination method.) [hereinafter Stead, letter on de-identification recommendations]
[168] KOONTZ, *supra* note 1, at 226.
[169] 45 C.F.R. §164.514
[170] *See* Stead, letter on de-identification recommendations, *supra* note 167, at 5.
[171] 45 C.F.R. §165.514 (b) (2); 45 C.F.R. §165.514 (b)(1); (*see* Letter on de-identification recommendations, *id.* listing two methods for de-identifying data: Safe Harbor and Expert Determination Method).
[172] Stead, letter on de-identification recommendations, *supra* note 167, at 3.
[173] *Id.* at 5.
[174] *Id.*
[175] HHS, *Examining Oversight*, *supra* note 2, at 15.

As it becomes more increasingly common for consumers' medical data to be combined with non-health related data,[176] the risk of sharing health information without data subjects' consent becomes more problematic. In fact, Big Data analytics is capturing data and changing the context of data use and data's sensitivity and significance.[177] It can even capture non-health related data that in combination with other datasets could reveal health-related correlations or conclusions.[178] Recommending a proposal to add more individual identifiers to be considered PHI, such as an individual's browsing search and history of medical symptoms and treatments, would help to prevent sensitive health information from being shared without the data subject's knowledge and authorization. Greater transparency for how de-identified data is being used would help getting individuals more control over their PHI and de-identified health data,[179] which is equally as valuable in the era of Big Data analytics.

iv. No private right of action provided:

HIPAA does not provide individuals with a private right of action for data breaches. In *Logan v. VA*, 357 F. Supp. 2d 149 (D.D.C. 2004), the plaintiff filed a claim against the Department of Veterans Affairs for disseminating information in violation of HIPAA. The Court dismissed the action for lack of subject in matter jurisdiction because HIPAA does not create a private cause of action. Similarly, in *Runkle v. Gonzales*, 391 F. Supp. 2d 2010 (D.D.C. 2005), the Court dismissed a HIPAA violation claim. The Court further clarified that although HIPAA provides for civil and criminal penalties against those who improperly disclose individual's health information, the Federal Court has never concluded that Congress intended for HIPAA to create a private right of action. As will be subsequently discussed, strong compliance may be more achievable if a private right of action could be extended by HIPAA, similar to California's privacy state laws and the GDPR..

v. No unified data privacy protection agency:

An additional concern stems from the fact that there is still no single, unified data protection agency overseeing all the privacy data being exchanged in today's technology-based era.[180] Because the European Union (EU) has had a uniform law since 1995,[181] and a European Data Protection Board, data privacy enforcement and interpretation has been more constant across the EU compared to U.S.[182] Moreover, as technology advanced and the internet developed new forms of communications, the EU recognized the urgency to extend modern protections to its residents.[183]

---

[176] Stead, letter on de-identification recommendations, *supra* note 167, at 7.

[177] Fang, *supra* note 53, at 135. (Big data analytics is defined as analysis "large volumes of high-velocity, complex, and variable data that require advanced techniques and technologies to enable the capture, storage, distribution, management, and analysis of the information," and "ubiquitous collection of consumer data from a variety of sources, the plummeting cost of data storage, and powerful new capabilities to analyze data to draw connections and make inferences and predictions.")

[178] *Id.*

[179] Stead, letter on de-identification recommendations, *supra* note 167, at 11.

[180] Nicolas P. Terry, *Regulatory Disruption and Arbitrage in Health Care Data Protection*, 153, 17 YALE J. HEALTH POL'Y L. & ETHICS 143 (Winter 2017).

[181] Terry, *supra* note 180, at 151.

[182] *Id.*

[183] Ben Wolford, *What is GDPR, the EU's New Data protection law?*, GDPR.EU, https://gdpr.eu/what-is-gdpr/ (last visited Feb. 12, 2020). [hereinafter Wolford, What is GDPR?]

Consequently, the GDPR was enacted in 2016 and became effective as of May 25, 2018.[184] The GDPR created more uniformity among the EU members and any entities outside of the EU handling personal information of EU's residents.

In this paper we will explore and analyze California's privacy state laws and GDPR's privacy language regarding electronic sensitive data, and briefly compare them to HIPAA's current regulations. This analysis will confirm HIPAA's existing weaknesses, which have been more evident as newer methods of capturing, storing and disclosing sensitive health information has been outpacing current HIPAA regulation. The analysis will also help to develop ideas to propose a robust, comprehensive federal level reformed HIPAA, to better protect patients' electronic health information.

III. California's Stringent Privacy State Laws: CMIA & CCPA

HIPAA usually supersedes any contrary state law provision, unless the state law imposes more stringent requirements than those imposed by HIPAA.[185] A state law is deemed more stringent than HIPAA when the state law provides the patient more rights and control over their PHI than HIPAA.[186] In California, the following state laws regarding medical health information and privacy data protection are considered more stringent than HIPAA: the Confidentiality of Medical Information Act (CMIA) and California's Consumer Data Protection Act (CCPA).

A. California's Confidentiality of Medical Information Act (CMIA)

California's Confidentiality of Medical Information Act (CMIA) provides broad and strong privacy protection for personal health information. CMIA is complementary to HIPAA and enhances privacy protection over confidentiality of individually identifiable medical information obtained by a health care provider.[187] In fact, unlike HIPAA's lack of oversight over NCE's, CMIA extends protection to health information collected by businesses offering software or hardware to store and share medical information, such as mobile health applications and IoTs.[188] Specifically CMIA states "any business that offers software or hardware to consumers, including a mobile application or other related device that is designed to maintain medical information, […] in order to make the information available to an individual or a provider of health care at the request of the individual or a provider of health care, for purposes of allowing the individual to manage his or her information, or for the diagnosis, treatment, or management of a medical condition of the individual, shall be deemed to be a provider of health care subject to the requirements of this part."[189] Additionally, pursuant to CMIA, any business that offers software or hardware to consumers to share and store medical information, must maintain the same standards of confidentiality required of a provider of health care with respect to medical information disclosed to the business.[190]

---

[184] *Id.*
[185] Miles J. Zaremski and Douglas M. Belofsky. *HIPAA's Privacy Rule and State Privacy Laws: Roadblocks to Medical Organization's Self-Policing Expert Medical Testimony,* 173, 28 ANN. HEALTH L. 149 (Winter 2019).
[186] *Id.*
[187] Davis, HHS Clarifies HIPAA, *supra* note 135.
[188] Cal. Civ. Code §56.06 (b)
[189] Cal. Civ. Code §56.06(b)
[190] Cal. Civ. Code §56.06 (d)

CMIA defines medical information as individually identifiable information, in electronic or physical form, in the hands of health care providers, a service plan, pharmaceutical company or contractor.[191] In turn, individually identifiable information means medical information that contains any element of personal identifying information sufficient to allow identifying an individual, including other types of "information that, alone or in combination with other publicly available information, reveals the individual's identity."[192] Examples of individual identifiers would be patient's name, address, electronic mail address, telephone number, or social security number, or other information which when combined with publicly available information, reveals the individual's identity.[193]

All businesses subject to CMIA are also subject to the penalties for improper use and disclosure of medical information.[194] Additional to other remedies available by law, CMIA extends data subjects the right to bring private action against any entity or person who has negligently released confidential information, for either or both nominal damages of $1,000 and the amount of actual damages.[195] Prior lawsuits under CMIA, alleging damages caused by negligent disclosure of PHI, have clarified that for a cause of action to be considered sufficient for court consideration, the plaintiff needs to establish a breach of confidentiality by alleging that an unauthorized person viewed medical information.[196] Additionally, CMIA allows either the State Attorney General, assigned County Counsel, District Attorney, City Attorney of a city or county, Prosecutor or State Public Officer to file a civil action on behalf of State of California to recover monetary penalties for PHI violations committed by a health care providers or business in California.[197]

B. California's Consumer Privacy Act of 2018 (CCPA)

California's Consumer Privacy Act (CCPA) attempts to mirror the EU's General Data Protection Regulation (GDPR) to make privacy law more consistent with entities that have to comply with the GDPR.[198] Sometimes, it has been referred to as the mini-GDPR.[199] CCPA also elevates the bar for all U.S. companies protecting data privacy.[200] CCPA applies to businesses that have annual gross revenue in excess of $25,000,000, or receive or sell personal information of

---

[191] Cal. Civ. Code §56.05 (j)
[192] Cal. Civ. Code §56.05 (j).
[193]Cal. Civ. Code §56.05 (j)
[194] Cal. Civ. Code §56.06 (e)
[195] Cal. Civ. Code §56.36 (b)
[196] *See* Sutter Health v. Superior Court, 227 Cal. App. 4th 1546, 174 Cal. Rptr. 3d 653 (2014). (In this case the plaintiff alleged theft of provider's computer containing medical records, but failed to allege that the medical information was actually viewed by an unauthorized person and thus that there was a breach of confidentiality under CMIA. Court of Appeal clarified that "the mere possession of medical information or records by an unauthorized person is insufficient to establish breach of confidentiality if the unauthorized person has not viewed the information or records.")
[197] Cal. Civ. Code §56.36 (f)
[198] *See* Jessica Davis, *How the Federal Data Privacy Debate, Regulations May Impact*, HIPAA and Compliance News, Healthcare, XTELLIGENT HEALTHCARE MEDIA (March 4, 2019) https://healthitsecurity.com/news/how-the-federal-data-privacy-debate-regulations-may-impact-healthcare
[199]W. Gregory Voss and Kimberly A. Houser, *Personal Data and the GDPR: Providing a Competitive Advantage of U.S. Companies*, 307, 56 AM. BUS. L.J. 287 (Summer 2019) [hereinafter Voss and Houser, *Personal Data*]
[200] John Stephens, *California Consumer Privacy Act,* ABA (Feb. 14, 2019) https://www.americanbar.org/groups/business_law/publications/committee_newsletters/bcl/2019/201902/fa_9/

50,000 or more consumers, or devices, or derive 50% or more of its annual revenues from selling consumers' personal information.[201]

The CCPA extends wider rights to California consumers regarding their personal information than HIPAA. Pursuant to the CCPA, California consumers have the right to request information about the type of personal information covered entities have collected, sold or disclosed and for what purpose the personal information is used.[202] This provision is similar to EU's GDPR. Additionally, California's consumers have the right to know the categories of third parties with whom the business shares personal information, and the business purpose for collecting or selling personal information.[203]

CCPA also extends the right to request businesses to delete any personal information about the consumer that the entity has collected, unless the business demonstrates that the information is necessary to provide services.[204] This provision is also similar to the EU's GDPR and not included in HIPAA's statutory language. Lastly, and more protective than HIPAA protections, under CCPA a third party may not sell personal information about a consumer that has been sold to the third party by a business, unless the consumer has received explicit notice and is provided at any time with the opportunity to opt-out.[205]

Compared to HIPAA, CCPA defines personal information more broadly to include as individual identifiers such items as internet or other electronic network activity information. This category includes and is not limited to, "browsing history, search history, and information regarding a consumer's interaction with an internet website, application, or advertisement."[206] This right could be useful when data subjects prefer to delete information when they have withdrawn their consent for processing or where the processing of their personal data otherwise does not comply with law.[207] It also includes inferences that could be drawn from any personal information as defined by CCPA, to "create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes."

As delineated and explained above, CCPA's Privacy protections are clearly more extensive than HIPAA's requirements to simply obtain patient's authorization to sell PHI for marketing purposes. CCPA makes a clear distinction when consumers are at least 13 years old and less than 16 years of age. These consumers are required to opt-in when they would like to sell their personal information.[208] If the individual is less than 13 years age, then the consumer's parent or guardian would have to opt-in.[209] In addition, CCPA clearly states that California's consumers' rights to direct a business to not sell PHI has to be included in a clear link on the company's Internet

[201] Title 1.81.5 Cal. Civ. Code §1798.140 (c) (1) (§1798.140(c) list that a business that sells consumers' personal information, or discloses consumers' personal information for a business purpose, shall disclose the categories of consumers' personal information it has sold or for business purpose, or if the business had not sold (or for business purpose) consumers' personal information, it shall disclose that fact.)
[202] Cal. Civ. Code §1798.100 (a) and (b) and §1798.115 (a) and (c).
[203] Cal. Civ. Code §1798.110 and §1798.115.
[204] Cal. Civ. Code §1798.105 (The right to delete data is also known as "right to erasure" or "right to be forgotten." This right is also included in European Union's GDPR).
[205] Cal. Civ. Code §1798.115 (d) and §1798.120(a).
[206] Cal. Civ. Code 140 (o)(1)(F);
[207] Michael L. Rustad, *How the EU's General Data Protection Regulation Will Protect Consumers Using Smart Devices,* 257, 52 SUFFOLK U. L. REV. 227 (2019) (Discusses right of erasure pertaining to GDPR. Same analysis could be applied to CCPA's right of erasure privacy right.
[208] Cal. Civ. Code §1798.120 (b)
[209] Cal. Civ. Code §1798.120 (b)

homepage, titled "Do Not Sell My Personal Information, or direct to an Internet web page enabling the consumer or authorized person to opt out of sale of the consumer's personal information.[210] No such requirements are provided by HIPAA.

Most importantly, unlike HIPAA, CCPA provides California's consumers the right to initiate a private right of action for unauthorized access of personal information, and theft or disclosure as a result of the entity's failure to maintain reasonable security procedures in place to protect personal information.[211] Individuals are able to recover damages in the amount not less than $100 and not greater than $750 per consumer per incident or the amount of actual damage incurred, whichever is greater.[212] Individuals also have right to seek an injunctive or declaratory relief, or any other relief a court deems appropriate.[213]

The first lawsuit filed alleging violation of the new California's Consumer Privacy Act, among other laws, is Cullen v. Zoom video Communications, Inc., No. 20-cv-02155. The class action suit was filed on March 30, 2020 at the Northern District of California.[214] Zoom is an application that allows users to join video or audio meetings for free. Plaintiffs allege CCPA violation due to improper safeguarding of information, and inadequate notice or authorization of sharing disclosure of personal information, such as device's protected unique advertising identifier to third parties (including Facebook, Inc.), consequently invading the privacy of its users.[215] As the case progresses, individuals will gain better understanding as to how the new CCPA will be enforced.

IV. EU's GDPR: General Data Protection Regulation

The European Union's (EU) General Data Protection Regulation (GDPR) became enforceable May 25, 2018.[216] GDPR has a direct impact in all 28 Member States of the EU[217] and any global entity processing personal data of EU residents as part of their business and services.[218] GDPR became effective in response to a rapidly emerging new technological environment and an increased use of internet and cloud-based services and storage for health services. [219] GDPR's goal

---

[210] Cal. Civ. Code §1798.135(a)(1)
[211] Cal. Civ. Code §1798.150 (a)
[212] Cal. Civ. Code §1798.150 (A)
[213] Cal. Civ. Code §1798.150 (B) and (C); (*see* Cal. Civ. Code §1798.150(b) dictating a 30-day prior notice requirement for allegations of claims, for businesses to have an opportunity to cure alleged noncompliance and harm before moving forward with civil cation. If seeking guidance from Attorney General and business fails to cure alleged violations within 30 days after being notified of alleged noncompliance, any business or person in violation could be subject to an injunction and liable for a civil penalty. Of no more than $2,500 for each violation or $7,500 for each intentional violation in an action by the AG.)
[214] *See* Robert Cullen v. Zoom Video Communications, Inc. No. 20-cv-02155, U.S. District Court of Northern District of California (San Jose).
https://www.courtlistener.com/recap/gov.uscourts.cand.357336/gov.uscourts.cand.357336.1.0.pdf (last visited April 26, 2020). (Zoom is an application that allows users to join video or audio meetings for free).
[215] *Id.*
[216] Commission Regulation 2016/679, of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data on the Free Movement of Such Data [hereinafter GDPR], 2016 O.J. (L 119) (EU) (May 4, 2016).
[217] Victoria Hordern, *The Final GDPR Text and What It Will Mean for Health Data,* HOGAN LOVELLS, (Jan 20, 2016) https://www.hldataprotection.com/2016/01/articles/health-privacy-hipaa/the-final-gdpr-text-and-what-it-will-mean-for-health-data/
[218] Wolford, What is GDPR?, *supra* note 183.
[219] *Id.*

is to harmonize the regulatory environment for businesses handling private data,[220] and to create more consistent and uniform privacy protection of personal data,[221] while embracing emerging technologies.

GDPR has become one of the toughest privacy and security laws in the world.[222] With regards to whom the protection is extended, GDPR's focus is on EU residents' location and their personal identifiable information (PII)[223] Any entity handling a EU residents' PII or monitoring their behaviors, as long as behavior takes place in the EU, could be subject to GDPR regulations.[224] As a general rule, GDPR's territorial scope includes organizations operating within the EU, or when entity is outside of the EU but the data being process belongs to an EU resident or involves behavior monitoring as far as the behavior takes place in EU.[225] It also includes entities located outside of the EU, but cater goods and services to EU residents.[226] GDPR also applies when the national law of an individual Member State applies due to public international law interest.[227] In contrast, HIPAA only applies to either covered entities and/or business associates handling patient protected health information (PHI) within the United States only.[228]

One main difference between the EU's GDPR and HIPAA is that the GDPR's definition of protected data is "broad and open-ended."[229] The GDPR's broad definition of personal data permits better inclusion of data usage by newer technology platforms and devices.[230] The GDPR defines "personal data" as "any information related to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online behavioral data, an online identifier or to one or more factors specific to the physical, psychological, genetic, mental, economic, cultural or social identity of that natural person."[231] GDPR's definition of personal data specifically states and includes genetic identity and location data (GPS) into smartphone applications.[232]

Because GDPR is much broader and has a wider applicability than HIPAA,[233] the statute further defines "data concerning health" as personal data related to physical or mental health,

---

[220] *See Questions and Answers-Data Protection Reform Package,* EUROPEAN COMMISSION, https://ec.europa.eu/commission/presscorner/detail/en/MEMO_17_1441 (last visited April 23, 2020; (*see* Kimberly A. Houser and W. Gregory Voss, *GDPR: The End of Google and Facebook or a New Paradigm in Data Privacy?*, 1, 25 RICH. J.L. & TECH. 1 (2018) Suggesting GDPR is also intended to hold all companies in the tech field to the same standards).

[221] Terry, supra note 180, at 151.

[222] Wolford, What is GDPR?, *supra* note 183.

[223] *See* GDPR, *supra* note 216.

[224] GDPR, *supra* note 216, at Art. 3.

[225] *Id*. (In regards to mobile applications, GDPR applies when personal data is collected from a data subject who is located in the European Union at the time data is collected. GDPR does not apply when EU citizens have their data collected outside of the European Union).

[226] *Id*.

[227] *Id*.

[228] Fair Warning Articles, *GDPR and HIPAA Compliance: What are the Differences and How Can I Work Towards Compliance?* FAIRWARNING.COM (February 4, 2020) https://www.fairwarning.com/insights/blog/gdpr-and-hipaa-compliance-what-are-the-differences-and-how-can-i-work-towards-compliance

[229] Voss and Houser, *Personal Data, supra* note 199, at 323.

[230] *Id*. at 324.

[231] GDPR, *supra* note 216, at Art. 4 (1).

[232] Voss and Houser, *Personal Data, supra* note 199, at 315.

[233] *Id*. at 291.

including provision of health care services revealing an individual's health status.[234] For example, health data could include all data revealing a "disease, disability, disease risk, medical history, clinical treatment or the physiological or biomedical state of the data subject independent of its source."[235] Moreover, GDPR includes a category of sensitive information known as "special categories of information." In regards to health information, "special categories of information" includes processing of genetic data, biometric data for purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sexual orientation."[236] HIPAA does not list these specific definitions in its statutory language.

GDPR's long list of detailed definitions demonstrates that GDPR is based on how "personal data" is defined and processed.[237] Contrary to GDPR, HIPAA's main focus relies on who is holding and transferring PHI. GDPR stands out as the strongest data privacy law mainly because it is oriented to guarantee transparent notification and communication to data subjects. For instance, GDPR requires companies to clearly inform data subjects of their privacy rights, as granted by the GDPR. This notification of individual's privacy act must be concise, transparent, intelligible, easily accessible, and using clear and plain language.[238]

GDPR requires wider transparency than HIPAA. For instance, GDPR requires companies to notify data subjects when their data is transfer, the categories of data being transfer, for how long data will be kept, and for what purposes.[239] In addition, it guarantees data subjects to be provided with the legal basis for processing their data, and be explained the legitimate interest of a third party wishing to access their sensitive information.[240] Similar to CCPA, GDPR provides its data subjects with a right of erasure, also known as the right to be forgotten.[241] Data subjects could ask for the deletion of data no longer necessary in relation to the purpose for which it was collected, when data subject withdraws consent, or when personal data have been unlawfully processed.[242] The right of erasure is important especially when the consent was given but data subject later realizes that the consent notice was inappropriate and decides to withdraw data provided.

In terms of properly authorizing personal data disclosure, GDPR lists the conditions that are required to be met and the controller shall be able to corroborate compliance.[243] When written consent is given under the GDPR legislation, the language must be clear, plain, intelligible, and the consent form must be easily accessible.[244] Similarly, if individuals' wish to withdraw consent, then the process should be as easy to achieve as to when the consent was given.[245] In case of a personal data breach, GDPR affords data subjects to be notified, without undue delay, no later than

---

[234] GDPR, *supra* note 216, at Art. 4 (15).
[235] Tovino, *Going Rogue*, *supra* 138, at 183.
[236] GDPR, *supra* note 216, at Art. 9. (As listed in European Union's GDPR, special categories of information also include personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership).
[237] Voss and Houser, *supra* note 199, at 323.
[238] GDPR, *supra* note 216, Art. 12.
[239] *Id*. at Art. 13.
[240] *Id*.
[241] *Id*. at Art. 17.
[242] *Id*. (There are exceptions to the right of erasure, especially when retention is required for public health or scientific archiving reasons).
[243] GDPR, *supra* note 216, Art. 8(1) and Art. 4. (GDPR defines data controller as any " natural or legal person, public attorney, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.")
[244] GDPR, *supra* note 216, at Art. 8 (2).
[245] *Id*. at Art. 8 (3).

72 hours after becoming aware of a data breach.[246] Similar to CMIA and CCPA, GDPR provides data subjects the right to claim for material or non-material damages as a result of a breach of GDPR.[247]

V. Proposal

As illustrated in this paper, HIPAA sets the baseline for regulatory compliance regarding patient health information.[248] In fact, states can exceed HIPAA regulations and impose stronger privacy protections regarding health data, as long as the provisions do not conflict with HIPAA protections.[249] An example of stricter U.S. data privacy laws is California's Confidentiality of Medical Information Act (CMIA). This legislation specifically governs the privacy of health information in the state of California, and extends greater standards of protection than HIPAA itself. Because newer "direct-to-consumer" technologies are being integrated into healthcare today, HIPAA should be reformed to mirror CMIA's extended definition of health care provider(s) and scope of application. Specifically, HIPAA should extend its privacy protection to health information collected by businesses offering software or hardware to store or share sensitive health information.[250] In fact, similar to CMIA's, the new reformed HIPAA should include as health care providers mobile applications and other businesses offering software to collect and store health information, therefore assuring stronger compliance to protect health data.[251] The reason why these health technological business are considered provider of health care by CMIA, is because its capacity to store and process health information or any data that could be used for diagnosis, treatment, or management of a medical condition.[252]

On the other hand, CCPA's scope of applicability incorporates as consumer-specific identifiers "the internet or other electronic network activity information,"[253] extending privacy protection to any sensitive data processed through the internet. Pursuant to CCPA's statutory language, internet activity includes "browsing history, search history, and information regarding a consumer's interaction with an internet website, application or advertisement."[254] The new reformed HIPAA should include more identifiers considered as protected health information, such as the ones contemplated in CCPA. Similar to CCPA, the reformed HIPAA should extend privacy protection to internet searches and browsing history. In the end, anything searched through these platforms, could turn into data when aggregated with other available datasets, increasing the potential of re-identifying or identifying the data subject.[255] This protection could be significant to individuals searching their symptoms, diagnostic and treatment plans via "Google" or "Alexa" and wish to keep their information anonymous from friends, family and malicious actors such as hackers.

---

[246] *Id*. at Art. 33.
[247] *Id*., at Art. 82.
[248] Health Privacy Q's and A's, *supra* note 67.
[249] *Supra* note 69.
[250] *See* Cal. Civ. Code §56.06.
[251] *Id*.
[252] Cal. Civ. Code §56.06(b).
[253] Cal. Civ. Code §140(o)(1)(F)
[254] *Id*.
[255] *See* Stead, letter on de-identification recommendations, *supra* note 167, at 5. ("Even data properly de-identified under the Privacy Rule may carry with it some private information, and, therefore, poses some risk of re-identification, a risk that grows into the future as new datasets are released and as datasets are combined.")

The right of erasure afforded both in CCPA and EU's GDPR, is not observed in HIPAA's statutory language. The reformed HIPAA should similarly grant the right to delete health data if such information is no longer necessary, relevant, or was obtained unlawfully.[256] Similar to both CMIA and CCPA, HIPAA should provide data subjects with a private right of action for damages caused, if any, for inappropriate and unauthorized disclosure of PHI.[257] It is important to acknowledge that "health data has become one the most lucrative data type being sold in the black market, netting $10 per record."[258] Health data obtained during a cybersecurity breach, sometimes is used by hackers to file tax returns, receive benefits such as having access to free medical prescriptions, or used to file false medical claims against insurance.[259] It is unclear how current HIPAA monetary penalties for data breaches directly benefits the owners of PHI disclosed inappropriately,[260] when many companies may be profiting from individuals' sensitive information and utilizing as their "selling product."[261]

As a closing argument for this proposal, I strongly encourage the reformed legislation to protect health care based on its context and provide data subjects with wider transparency. EU's GDPR protects individuals' personal information from misuse, regardless of who holds the data, specific sector or situation involved.[262] The proposed comprehensive, reformed HIPAA should apply to all institutions, not just to specific sectors such as CEs and BAs. Protecting personal data should be prioritized as the digital age continues to be highly integrated into the medical industry. Any health information should be deemed sensitive whether it falls in the hands of CEs or BAs, or other entities, such as health applications, IoTs,[263] wearable fitness devices, or other miscellaneous mobile applications used for telemedicine, EHR storage, or other medical purposes.

---

[256] *See* GDPR, *supra* 216, at Art.17; (*see* Fang, *supra* note 53, at 125 proposing same idea regarding the right of erasure).

[257] *See* Roger Hsieh, *Improving HIPAA Enforcement and Protecting Patient Privacy in a Digital Healthcare Environment*, 217-18, 46 LOY. U. CHI. L.J. 175 (Fall 2014) (Author also proposing to allow private right of action under HIPAA, but also encouraging Congress to "consider forcing plaintiffs to seek administrative adjudication prior to filing suit in order to filter weaker claims out of the judicial system. […] Because OCR already conducts an intake and review of HIPAA complaints, OCT could potentially serve as the administrative body that filters HIPAA complaints that fail to state a claim from the judicial system. Like state agency-AG partnerships, private rights of action would likely address both willful and negligent breaches. The threat of HIPAA investigations and litigation by private parties may motivate covered entities to better implement and enforce security procedures.")

[258] Tschider, *supra* note 146, at 8.

[259] *Id.*

[260] *Id.*

[261] *See* FTC, Transcript on Spring Privacy Series, *supra* note 151.

[262] Andrea C. Mciejewski. *Medical Records and Privacy Rights: The Unintended Consequences of Aggregated Data in Electronic Health Records*, 1145, 90 U. Colo. L. Rev. 1111 (Fall, 2019).

[263] Elvy, *supra* note 37, at 497-98 (Stating that "many IoT companies do not qualify as "covered entities" because they are unlikely to provide "medical or health services," health insurance plans, or process health care information in connection with the sale of IoT devices and the provision of related services and software to consumers. The use of health-related data shared by consumers who use IoT devices is likely to be governed mainly by the entities' privacy policy." Also stating that "IoT companies also may not qualify as business associates under HIPAA regulation because they are unlikely to be hired to perform activities or services, such as "claim processing, administration [and] data analysis," in connection with "protected health information" on behalf of HIPAA covered entities. If IoT companies begin to integrate their services and devices with the offerings of HIPAA covered entities and handle "protected health information" on behalf of such entities, there would be a stronger argument for HIPAA compliance."); (*see id.* 426-27, Explaining that IoT devices can collect biometric and health-related data, such as fingerprint scans, facial scans, heart rates, fitness level, temperature, blood sugar levels, among other things).

Mirroring one of the strongest data protections existing today, the GDPR, the new reformed HIPAA should regulate data based on its context and on its purpose.[264] Health data could be limited based on its purpose, mainly by requiring entities collecting sensitive health data to collect "for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes."[265] Offering wider transparency will enable health technology consumers to trust these new medical advancements improving public health, and will enable data subjects to make fair and educated choices over their own data.

VI. Compliance Advice

If this new reformed HIPAA is adopted and enforced, health care providers and entities who are subject to comply with the new reformed HIPAA should study and understand the new requirements, and perform a risk assessment.[266] As part of the risk assessment, the entities subject to the reformed HIPAA should review and identify if they collect, process, or store personal/sensitive health data that could be considered individually identifying health information under the new legislation.[267] At the same time they should analyze and record if there are "legal bases for processing the data,"[268] including whether data subject provided consent for processing data for a specific purpose.[269] In this case, it is recommended for entities to review current consent forms and notices for any data processing, and make sure the wording is specific and simple to understand.[270] Similarly, entities should verify that data subjects are able to easily access a withdrawal consent form at any time.[271] For companies processing large volumes of health data, it is important to document how health information is processed, who has access, and whether there is consent to process such personal health information.[272] Companies are recommended to review current policies and procedures, and identify areas that require updates to comply with the amended legislation.[273] Entities should regularly monitor adherence to new policies and procedures, and update them if necessary.[274] Additionally, training should be afforded to highlight HIPAA's new amendments and obligations, and any new policies or procedures established.[275] Training employees on a regular basis will ensure better data protection.

As entities work to map out an inventory of all the health data they are constantly collecting and storing, they should also include proper mechanisms for data subjects to access their personal

---

[264] Terry, *supra* note 180, at 201.
[265] *See* GDPR, *supra* 216, at Art. 5.
[266] *See* Michele DeStefano, *Creating a Culture of Compliance: Why Departmentalization May Not Be the Answer*, 91, 10 HASTINGS BUS. L.J. 71 (Winter 2014). (Discussing compliance function); *see* also Voss and Houser, *Personal Data, supra* note 199, at 333. ("Although compliance and prevention involve assessing current legal risks, prevention involves creating a legal strategy to avoid future legal problems down the road.")
[267] *See* Voss and Houser, *Personal Data, supra* note 199, at 324.
[268] *See Id.* (Discussing GDPR compliance by U.S. companies and explaining how to implement compliance with GDPR).
[269] *See Id.* at 326.
[270] *See* GDPR, *supra* note 216, at Art. 7. (GDPR-Art. 7 sets conditions for consent).
[271] *Id.*
[272] *See* Voss and Houser, *Personal Data, supra* note 199, at 326-27. (Discussing recordkeeping of activities related to data processing under GDPR mandates).
[273] *See* DeStefano, *supra* note 266, at 94.
[274] *See, Id.*
[275] *See Id.*

information, request to amend or delete data, or submit a data transfer request.[276] Most importantly, to ensure strong compliance entities should update any business associate contracts in place and extend additional ones to those entities now subject to the new reformed HIPAA. In this new business associate agreement, covered entities must impose "specified written safeguards on the individually identifiable health information used or disclosed by its business associates,"[277] as identified by the new reformed HIPAA.

VII. Conclusion

Emerging "direct-to-consumer" health products and devices are not addressed by current HIPAA legislation.[278] Healthcare providers should feel comfortable to encourage the use of novel patient-centered technology as it would be highly favorable to improve public health. Unfortunately, gaps and overlaps in the U.S. data privacy laws and regulations have opened a new avenue for third-party entities to obtain sensitive private health information from non-covered health oriented technologies and use it inappropriately for employment decisions or even health, life and other insurance premium purposes.[279] As cogently illustrated in a 2019 article in The New York Times: "The current protocols for exchanging patients' data, for instance, would let people use consumer apps to get different types of information, like their prescription drug history. But it is an all-or-nothing choice. People who authorized an app to collect their medication lists would not be able to stop it from retrieving specific data-like the names of H.I.V. or cancer drugs-they might prefer to keep private." [280] In fact, unauthorized access to sensitive health data by hackers could lead to fraudulent filings of tax returns, fraudulently filing of healthcare claims to insurance companies; or the receipt of other types of benefits such as acquiring free drug prescriptions.[281]

HIPAA's loopholes and lack of a neutral and broad scope, could impair patients' trust in their healthcare providers, and any new technology that could potentially benefit or improve their health.[282] Technology companies currently collecting personal health information across stateliness have expressed legitimate concerns about the complexity of U.S.'s current regulatory environment.[283] Some struggle to grasp HIPAA Rules and understand how and when stricter state privacy laws apply.[284] Unfortunately, HIPAA did not foresee the integration of advanced medical health devices and applications into the healthcare delivery system.

With this new proposal, HIPAA's narrow statutory language should be broadened in its application to lessen health related data privacy issues. Using California's CMIA, CCPA, and the European Union's GDPR as models, the proposed, simpler and comprehensive reformed HIPAA, will help protect the privacy of all types of personal data, regardless of who collects it or how the health information is managed. A uniform and more comprehensive HIPAA should seek to resolve differences among existing state and federal data privacy laws, obligations, responsibilities, and

---

[276] *See* Voss and Houser, *Personal Data, supra* note 199, at 333. (Discussing example of a Seattle-based mobile payments start up Remitly implementing new compliance program).
[277] Jonathan P. Tomes, *20 Plus Years of HIPAA and What Have We Got?,* 78, 22 QUINNIPIAC HEALTH L.J. 39 (2018).
[278] Levy, *supra* note 4, at 8.
[279] FTC Staff Report, *IOTs, supra* note *34, at 48.*
[280] Singer, *When Apps Get Your Medical Data, supra* note 32, at 4.
[281] Tschider, *supra* note 146, at 7.
[282] KOONTZ, *supra* note 1, at 107.
[283] KOONTZ, *supra* note 1, at 116.
[284] *Id.*

legal rights.[285] This new HIPAA federal privacy legislation would prevent confusion among companies doing business across state lines, facing differing and sometimes inconsistent state and federal laws on data privacy and creating a burden to keep up with,[286] consequently hindering innovation. Further, adding a private right of action for inappropriate data use and disclosure will ultimately encourage entities to keep in compliance with the reformed HIPAA legislation.

[285] Nuala O'Connor, *Reforming the U.S. Approach to Data Protection and Privacy,* COUNCIL ON FOREIGN RELATIONS (Jan. 30, 2018) https://www.cfr.org/report/reforming-us-approach-data-protection

[286] Alfred Ng, *US Privacy law is on the horizon. Here's how tech companies want to shape it*, CNET (Sept. 26, 2018) https://www.cnet.com/news/us-privacy-law-is-on-the-horizon-heres-how-tech-companies-want-to-shape-it/