JOURNAL OF HEALTH CARE FINANCE

Summer 2018

The HIPAA Privacy Rule: Flawed Privacy Exposed When Compared with the European Union's General Data Protection Regulation

Clifford J. McKinstry
Chief, Installations Law
HQ Air Mobility Command
Office of the Staff Judge Advocate
Scott AFB, Illinois

Abstract

HIPAA has among its many goals the improvement of health care delivery for those in the United States. One aspect of the grand improvement scheme requires patients to be forthcoming with their personal health information. In many instances that information has made its way into various data bases for storage and retrieval. Protecting that information is a critical factor in instilling in patients the confidence they must have in order to willingly provide their patient data when seeking health care services. How effective HIPAA is in protecting that personal health information is a matter of some debate. Many analysts see the "exceptional" treatment of health data in the United States as flawed, affording at best "confidential" safeguards rather than true privacy protections. The EU, on the other hand, has followed a different track regarding the protection of individual privacy interests, including the protection of individually identifiable health information. This article compares the EU's data privacy approach with the approach of the HIPAA Privacy Rule in the United States. The article concludes that the flaws within HIPAA in the privacy context demonstrate that the need for certain reforms now if "patient privacy" is genuinely a concern for those interested in continuing to improve the American health care system.

Introduction

In an effort to control the flow of personal and sensitive information provided by patients in the course of seeking treatment, receiving care, and providing payment for medical conditions and ailments, the Congress enacted the Health Insurance Portability and Accountability Act of 1996 (HIPAA).[1] HIPAA was considered necessary as an effort to improve the quality of patient healthcare and the means by which that care is delivered. In a nutshell, "HIPAA was created to 'improve the portability and accountability of health insurance coverage' for employees between jobs. Other objectives of the Act were to combat waste, fraud and abuse in health insurance and healthcare delivery. The Act also contained passages to promote the use of medical savings accounts by introducing tax breaks, provides coverage for employees with pre-existing medical conditions and simplifies the administration of health insurance."[2] HIPAA included among its provisions a mandate for what has come to be known colloquially as the Privacy Rule.[3] "The Privacy Rule establishes a Federal floor of safeguards to protect the confidentiality of medical information."[4] Why was such a rule necessary? Simply, and among other things, ". . . without the Privacy Rule patient information held by a health plan could, without the patient's permission, be passed on to a lender who could then deny the patient's application for a home mortgage or a credit card, or to an employer who could use it in personnel decisions."[5]

In the two decades since the passage of HIPAA, there has been a sea change in the manner in which the data travels electronically throughout the world, and, more significantly, in the ways in which that data can be obtained and used by entities for their own benefit—data that includes the private health information of people who have provided it never expecting it to be used for purposes other than treatment and care at the hands of their health care providers. And HIPAA, designed ostensibly to guard that information from those not otherwise entitled to have it, embodies an " . . .idiosyncratic regulatory model [that] has established itself as one of the most disliked (by health care providers) and critiqued (even by privacy advocates) pieces of regulation in the history of health care."[6] Among the most damning critiques of HIPAA is the fact that the mechanisms for safeguarding personally identifiable health information is generally after-the-fact; that is "[h]ealth data protection in this country has exhibited . . . a dependence on downstream data protection models."[7] What that means in practical terms is that the emphasis in health care data is not on restricting the collection of private health information (a characteristic of a system concerned for the real privacy interests of the source of the data), but upon keeping the information collected confidential.[8]

---

[1] Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 100 Stat. 2548 (1996), codified in various sections of the United States Code in Titles 5, 8, 10, 18, 22, 25, 29, 31, 38, and 42.

[2] HIPAA JOURNAL, *HIPAA History*, https://www.hipaajournal.com/hipaa-history/, (June 25, 2018).

[3] *See, generally*, HIPAA, Sec. 264(c)(1), Sec. 264 of Pub. L. 104-191, 110 Stat. 2033-2034 (42 U.S.C. 1320d-2 (note)); and note 28 *infra*.

[4] U.S. Department of Health and Human Services, *Why is the HIPAA Privacy Rule Needed?* Health Information Privacy, https://www.hhs.gov/hipaa/for-professionals/faq/188/why-is-the-privacy-rule-needed/index.html, (June 25, 2018).

[5] Id.

[6] Nicholas P. Terry, *Symposium: Big Data Proxies and Health Privacy Exceptionalism*, 24 HEALTH MATRIX 65, 66 (2014).

[7] Id.

[8] Id. at 69.

The history of data protection (including the protection of a subset of big data[9] involving personal health-related information) in the European Union (EU) has concentrated on upstream or small data[10] protection efforts. That is, restricting the efforts to collect data in the first place.[11] In the EU, the General Data Protection Regulation (GDPR)[12], scheduled for full implementation among the EU member states (and by derivation to all of those doing business which involves personal data moving within, outside of, to, or from the EU) in May 2018, is, by comparison to HIPAA's Privacy Rule, a comprehensive embodiment of the notion of truly effective data privacy protection. Protecting data at the front end of the process is more likely to enable so-called "data subjects"[13]to control their own privacy interests rather than having to depend upon post-disclosure mechanisms restricting additional collection, processing, and use of the data.[14] The fact that health data in the EU is categorized no differently than other data in matters relating to privacy

[9] Definitions of "big data" are numerous. For the purposes of this thesis, "big data" is ". . . a process that is used when traditional data mining and handling techniques cannot uncover the insights and meaning of the underlying data. Data that is unstructured or time sensitive or simply very large cannot be processed by relational database engines. This type of data requires a different processing approach called big data, which uses massive parallelism on readily-available hardware," *Techopedia*, https://www.techopedia.com/definition/27745/big-data, (July 30, 2018).

[10] Like "big data," definitions of "small data" are numerous. For the purposes of this thesis, "small data" is ". . . data use that relies on targeted data acquisition and data mining. It describes a shift in how businesses and other parties look at data use, and is intended to be a counterpoint to the trend toward big data, which revolves around the idea that businesses can use massive amounts of acquired data to pinpoint customer behavior or drive business intelligence in key ways. By contrast, a small data approach involves acquiring specific data sets through less effort, which proponents believe to be a more efficient business practice." Id.

[11] *See*, *generally*, the *Charter of Fundamental Rights of the European Union*, (2000/C 364/01), Article 8: "Protection of personal data 1. Everyone has the right to the protection of personal data concerning him or her. 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. 3. Compliance with these rules shall be subject to control by an independent authority."

[12] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) *Official Journal of the European Union,* Vol. L119, 4/5/2016, 1-88.

[13] General Data Protection Regulation, art. 4(1), Definitions: "'personal data' means any information relating 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, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person," Id. at 33.

[14] General Data Protection Regulation, art. 4(7), Definitions: a data controller is defined as ". . . the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law." A processor is ". . . a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller." The processing of data refers to ". . . any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation (sic), structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction." Id.

protection[15] is an express refutation of the notion of "health privacy exceptionalism"[16] which is prevalent in the United States and embodied in HIPAA. In other words, personal data is data in the EU. Except for the specific circumstances enumerated in the GDPR, it is data that may not be processed under the applicable rules within and among the member states of the EU and, under certain enumerated circumstances, even outside of the EU.

The HIPAA Privacy Rule is an effort to protect data that has made it way to the public domain. It was developed by the Department of Health and Human Services (HHS) because HIPAA required Congress to enact standards regarding the privacy of personally identifiable health information by 1999 and directed HHS to promulgate privacy regulations in the event Congress failed to act by the stated deadline.[17] Congress failed to meet its deadline. HHS followed through on its mandate and issued a Notice of Proposed Rulemaking on November 3, 1999 styled as "Standards for Privacy of Individually Identifiable Health Information."[18] The final rule was issued on December 28, 2000.[19] The purpose of the Privacy Rule is quite simple: ". . . to define and limit the circumstances in which an individual's protected health information may be used or disclosed by others."[20] HHS further clarified its intent: "[w]e are proposing to make the use and exchange of protected health information relatively easy for health care purposes and more difficult for purposes other than health care."[21] The ultimate question is whether the rule accomplishes that objective or whether in creating this downstream effort to protect the privacy of health care-related information, Congress and HHS have essentially failed in their mission. Certainly, when compared to the EU efforts, the Privacy Rule falls far short of the goal to afford genuine protection to the privacy interests of individuals in the context of personal health information.

This thesis demonstrates that concentrating on small data and limiting the flow of PHI that may enter the big data pool, primarily by giving individuals control over what, where, when, why, and

---

[15] Under the GDPR, "personal data" is ". . . any information relating 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, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person." *See* Article 4(1), General Data Protection Regulation, Id. But, Article 9 of the GDPR (Processing of special categories of personal data) includes the following rules with respect to certain kinds of personal data: "(1) Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited." And with respect to the special categories of data, there are 10 enumerated circumstances which allow the processing of the special data. General Data Protection Regulation, art. 9(2)(a) – (2j), Id. at 38-39.

[16] *See*, Nicholas P. Terry, *Protecting Patient Privacy in the Age of Big Data*, 81 UMKC L. REV. 385, 385, Winter, 2012, for a concise explanation of health privacy exceptionalism: "Rightly or wrongly, policymakers have agreed that patient information is deserving of elevated protection compared to other data (so-called health privacy exceptionalism)."

[17] Recommendations with Respect to Privacy of Certain Health Information, Pub. L. 104-191, Section 264(c)(1), , (August 21, 1996), states: "If legislation governing standards with respect to the privacy of individually identifiable health information transmitted in connection with the transactions described in section 1173(a) of the Social Security Act (as added by section 262) is not enacted by the date that is 36 months after the date of the enactment of this Act, the Secretary of Health and Human Services shall promulgate final regulations containing such standards not later than the date that is 42 months after the date of the enactment of this Act. Such regulations shall address at least the subjects described in subsection (b)."

[18] Department of Health and Human Services, Standards for Privacy of Individually Identifiable Health Information, 64 Fed. Reg. 59918, November 3, 1999.

[19] Department of Health and Human Services, Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82462, December 28, 2000.

[20] Standards for Privacy of Individually Identifiable Health Information, *supra* note 18, at 59924.

[21] Id.

how their data is collected and disseminated (as the EU has done through the GDPR), will greatly improve upon patient confidence that their privacy interests are being protected. This focus also serves the goals of HIPAA in collecting such data in the first place. Part I of this thesis discusses HIPAA, the Privacy Rule, the Security Rule, and the Enforcement Rule, and particularly how the Privacy Rule (buttressed by the Security Rule) was designed to serve the interests of patients while safeguarding their privacy interests. Part II examines the history of data privacy in the EU. Part III examines the GDPR, its objectives, and the mechanisms it employs to protect data, eschewing the notion of health data exceptionalism and treating all data with the same degree of protectionism while injecting data subjects with significant control over collection and disclosure. Part IV examines the flaws in the Privacy Rule vis-à-vis affording bona fide protection to patient privacy interests. Part V examines whether the structure of the Privacy Rule matters in the effort to protect health data privacy in the United States. Finally, Part VI offers conclusions and opportunities for change to the Privacy Rule that can instill confidence in those who must provide data in the course of treatment and during the health care operations of their providers, that their privacy interests are protected and their data will not end up in the hands of actors who wish to gain from the use of another individual's most intimate personal information.

I. The Health Insurance Portability and Accountability Act

HIPAA is a statute which accomplishes a number of different objectives. In five titles, HIPAA made sweeping changes to the health care landscape. Title I of the act is styled as "Health Care Access, Portability, and Renewability."[22] It includes provisions that reformed the health insurance business in a fundamental way, most notably by controlling the ability of insurance companies to deny or restrict coverage to insured who changed or lost their jobs.[23] It also established restrictions on the ability of insurance companies to deny coverage based upon pre-existing conditions.[24] Title II of the act is styled "Preventing Health Care Fraud and Abuse: Administrative Simplification; Medical Liability Reform."[25] It contains some of the most significant reforms from a practitioner standpoint and among those who administer health care operations. It includes the requirement for a National Provider Identifier Standard as a ". . . unique health identifier for health care providers and other health care system needs . . . ."[26] It also includes provisions for Transactions and Code Set Standards[27], the Privacy Rule[28], the Security Rule[29], and the Enforcement Rule.[30] Title III of HIPAA is entitled "Tax-Related Health Provisions."[31] This Title covers consumer protection issues, accelerated death benefits, state insurance pools, some IRA distributions when necessary to pay for significant health care costs, and organ and tissue donation information. Title

[22] *See*, generally, Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, § 1, 1996 U.S.C.C.A.N. (110 Stat.) 1936, 1939.
[23] *See*, generally, Health Insurance Portability and Accountability Act of 1996, Pub. L. 104-191, Title I, Sec. 111, Part B, Sec. 2741 et seq.
[24] *See*, generally, Health Insurance Portability and Accountability Act of 1996, Pub. L. 104-191, Tile I, Subtitle A, Part 1, Sec. 101, Part 7, Sec. 701 et seq.
[25] Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, tit. II, 110 Stat. 1936, 1991.
[26] *See*, HIPAA Administrative Simplification: Standard Unique Health Identifier for Health Care Providers, 69 Fed. Reg. 3434 (Jan. 23, 2004).
[27] For a general discussion of the standards and rules under which they operate see Centers for Medicare & Medicaid Services, Regulations and Guidance, HIPAA and ACA, Adopted Standards and Rules.
[28] Privacy of Individually Identifiable Health Information, 45 C.F.R. Part 164, Subpart E.
[29] Security Standards for the Protection of Electronic Protected Health Information, 45 C.F.R. Part 164, Subpart C.
[30] 45 C.F.R. Part 160, Subparts, C, D, and E.
[31] *See*, generally, Health Insurance Portability and Accountability Act of 1996, Pub. L. 104-191, Tile III, Subtitles A-D, §§ 300-371.

IV of HIPAA, styled "Application and Enforcement of Group Health Plan Requirements" imposes conditions on the portability of health insurance, access to health insurance, and conditions on the renewability of plans as well as penalties for insurers who fail to meet the requirements of the law in those areas.[32] And finally, Title V of HIPAA entitled "Revenue Offsets" deals with relatively obscure changes to the Internal Revenue Code.[33]

I(a). The Privacy Rule

HIPAA provides the basic framework by which, among many other things, "individually identifiable health information"[34] (IIHI) is to be gathered, used, maintained, and disseminated in the United States. It is applicable to health plans, health care clearinghouses, and health care providers who transmit health information electronically as contemplated by the statute.[35] The statute provides, among other things, for the adoption of standards for matters under the ambit of the law, defines what is required of those who are covered by the established standards, establishes specific penalties for those who disclose IIHI wrongfully, and includes pre-emption provisions vis-à-vis state law.[36] As Congress established a deadline for additional legislation expounding upon the privacy aspects of IIHI, a deadline which came and went on 21 August 1999, it was left to HHS to develop an administrative rule to implement the provisions of the law as enacted, specifically rules safeguarding the privacy of information given by patients to trusted agents in the course of their interactions with the health care system. That rule was presented in a Notice of Proposed Rulemaking dated November 3, 1999 as *Standards for Privacy of Individually Identifiable Health Information*.[37] The final rule with the same name was issued on December 28, 2000.[38] The latter is known colloquially as the Privacy Rule.

The purpose of the Privacy Rules is to give effect to a person's right to privacy with respect to personal health information.[39] It does that by making the rule applicable to ". . . covered entities,

---

[32] *See*, generally, Health Insurance Portability and Accountability Act of 1996, Pub. L. 104-191, Tile IV, Subtitles A-B, §§ 401-421.

[33] *See*, generally, Health Insurance Portability and Accountability Act of 1996, Pub. L. 104-191, Tile V, Subtitles A-C, §§ 500-521.

[34] 42 U.S.C. § 1320d (6). Individually identifiable health information is ". . . any information, including demographic information collected from an individual, that— (A) is created or received by a health care provider, health plan, employer, or health care clearinghouse; and (B) 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 the past, present, or future payment for the provision of health care to an individual, and— (i) identifies the individual; or (ii) with respect to which there is a reasonable basis to believe that the information can be used to identify the individual."

[35] *See*, generally, 42 U.S.C. § 1320d-1 for the applicability of standards established pursuant to HIPAA. Health care plan is defined at 42 U.S.C. § 1320d (5) as: ". . . a public or private entity that processes or facilitates the processing of nonstandard data elements of health information into standard data elements." Health Care clearinghouse is defined at 42 U.S.C. § 1320d (2) as: ". . . a public or private entity that processes or facilitates the processing of nonstandard data elements of health information into standard data elements." Health care provider is defined at 42 U.S.C. § 1320d (3) as: ". . . a provider of services (as defined in section 1395x(u) of this title), a provider of medical or other health services (as defined in section 1395x(s) of this title), and any other person furnishing health care services or supplies."

[36] All of these provisions of HIPAA are found at 42 U.S.C. Part C – Administrative Simplification, (42 U.S.C. §§ 1320d et seq.).

[37] *See*, *supra* note 18.

[38] *See*, *supra* note 19.

[39] *See*, Standards for Privacy of Individually Identifiable Health Information, *supra* note 19, at 82464, for a discussion of the right to privacy in matters of personal health information as expounded by the United States Supreme Court in *Whalen v. Roe*, 429 U.S. 589 (1977) and the HHS view that the Privacy Rule gives life to that notion of privacy in the HIPAA context.

business associates, and others with respect to ascertaining the compliance by covered entities and business associates with, and the enforcement of, the applicable provisions of this part 160 and parts 162 and 164 of this subchapter."[40] Covered entities are ". . . (1) A health plan. (2) A health care clearinghouse. (3) A health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter."[41] Business associates are essentially entities which do the bidding of covered entities.[42]

The fundamental precept for covered entities and business associates is that they may only use or disclose protected health information (PHI)[43] consistent with the restrictions created by the rule itself. Disclosures and uses that are permitted include: ". . . (i) To the individual; (ii) For treatment, payment, or health care operations, as permitted by and in compliance with § 164.506; (iii) Incident to a use or disclosure otherwise permitted or required by this subpart, provided that the covered entity has complied with the applicable requirements of §§ 164.502(b), 164.514(d), and 164.530(c) with respect to such otherwise permitted or required use or disclosure; (iv) Except for uses and disclosures prohibited under § 164.502(a)(5)(i), pursuant to and in compliance with a valid authorization under § 164.508; (v) Pursuant to an agreement under, or as otherwise permitted by,

[40] 45 C.F.R. § 160.300.

[41] 45 C.F.R. § 160.103

[42] A business associate is defined at 45 C.F.R. § 160.103 in the following manner: "(1) Except as provided in paragraph (4) of this definition, business associate means, with respect to a covered entity, a person who: (i) On behalf of such covered entity or of an organized health care arrangement (as defined in this section) in which the covered entity participates, but other than in the capacity of a member of the workforce of such covered entity or arrangement, creates, receives, maintains, or transmits protected health information for a function or activity regulated by this subchapter, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities listed at 42 CFR 3.20, billing, benefit management, practice management, and repricing; or (ii) Provides, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation (as defined in § 164.501 of this subchapter), management, administrative, accreditation, or financial services to or for such covered entity, or to or for an organized health care arrangement in which the covered entity participates, where the provision of the service involves the disclosure of protected health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person. (2) A covered entity may be a business associate of another covered entity. (3) Business associate includes: (i) A Health Information Organization, E-prescribing Gateway, or other person that provides data transmission services with respect to protected health information to a covered entity and that requires access on a routine basis to such protected health information. (ii) A person that offers a personal health record to one or more individuals on behalf of a covered entity. (iii) A subcontractor that creates, receives, maintains, or transmits protected health information on behalf of the business associate. (4) Business associate does not include: (i) A health care provider, with respect to disclosures by a covered entity to the health care provider concerning the treatment of the individual. (ii) A plan sponsor, with respect to disclosures by a group health plan (or by a health insurance issuer or HMO with respect to a group health plan) to the plan sponsor, to the extent that the requirements of § 164.504(f) of this subchapter apply and are met. (iii) A government agency, with respect to determining eligibility for, or enrollment in, a government health plan that provides public benefits and is administered by another government agency, or collecting protected health information for such purposes, to the extent such activities are authorized by law. (iv) A covered entity participating in an organized health care arrangement that performs a function or activity as described by paragraph (1)(i) of this definition for or on behalf of such organized health care arrangement, or that provides a service as described in paragraph (1)(ii) of this definition to or for such organized health care arrangement by virtue of such activities or services."

[43] PHI is defined at 45 C.F.R. § 160.103 as: " . . . individually identifiable health information: (1) Except as provided in paragraph (2) of this definition, that is: (i) Transmitted by electronic media; (ii) Maintained in electronic media; or (iii) Transmitted or maintained in any other form or medium. (2) Protected health information excludes individually identifiable health information: (i) In education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g; (ii) In records described at 20 U.S.C. 1232g(a)(4)(B)(iv); (iii) In employment records held by a covered entity in its role as employer; and (iv) Regarding a person who has been deceased for more than 50 years."

§ 164.510; and (vi) As permitted by and in compliance with this section, § 164.512, § 164.514(e), (f), or (g)."[44]

The Privacy Rule includes specific prohibitions against disclosure of PHI. Covered entities and business associates may not sell PHI[45]unless there is a specific authorization to do so.[46] But, there are a host of circumstances in which PHI can be used and, in some cases disclosed, without the knowledge and consent of the source of the PHI. Covered entities, for instance, may disclose PHI to their business associates when the relationship between the entities is defined satisfactorily by contracts binding them to one another.[47] Such contracts have to restrict the business associates from unfettered use and unrestricted ability to disclose the PHI.[48] A business associate must have limiting conditions imposed upon it by contract. The contract provisions must be specific and bind the business associate consistent with the restrictions.[49] Group health plans may also reveal PHI to plan sponsors (with restrictions) when determining premium rates or when altering or ending a group plan.[50] There are also a host of occasions when PHI can be disclosed if the subject of the information has an opportunity to object to the release in advance of the proposed use or disclosure. These situations include using and disclosing the information for facility directories,[51]for involvement in treatment or payment of health care costs associated with the person's care to family, close friends, or those with a special nexus to the individual,[52]to family or other people with a special relationship to the person of the person's location, condition, or that the individual

[44] 45 C.F.R. § 164.502(a)(1)
[45] 45 C.F.R. § 164.502(a)(5)(ii)(A).
[46] 45 C.F.R. § 164.508(a)(4).
[47] *See*, 45 C.F.R. §§ 164.504(e)(2), (e)(3), and (e)(5) for the specific requirements of such business arrangements.
[48] 45 C.F.R. § 164.504(e)(2)(i) allows use and disclosure by a business associate ". . . for the proper management and administration of the business associate," and ". . . to provide data aggregation services relating to the health care operations of the covered entity."
[49] 45 C.F.R. § 164.504(e)(2)(ii): " . . . a business associate will: (A) Not use or further disclose the information other than as permitted or required by the contract or as required by law; (B) Use appropriate safeguards and comply, where applicable, with subpart C of this part with respect to electronic protected health information, to prevent use or disclosure of the information other than as provided for by its contract; (C) Report to the covered entity any use or disclosure of the information not provided for by its contract of which it becomes aware, including breaches of unsecured protected health information as required by § 164.410; (D) In accordance with § 164.502(e)(1)(ii), ensure that any subcontractors that create, receive, maintain, or transmit protected health information on behalf of the business associate agree to the same restrictions and conditions that apply to the business associate with respect to such information; (E) Make available protected health information in accordance with § 164.524; (F) Make available protected health information for amendment and incorporate any amendments to protected health information in accordance with § 164.526; (G) Make available the information required to provide an accounting of disclosures in accordance with § 164.528; (H) To the extent the business associate is to carry out a covered entity's obligation under this subpart, comply with the requirements of this subpart that apply to the covered entity in the performance of such obligation. (I) Make its internal practices, books, and records relating to the use and disclosure of protected health information received from, or created or received by the business associate on behalf of, the covered entity available to the Secretary for purposes of determining the covered entity's compliance with this subpart; and (J) At termination of the contract, if feasible, return or destroy all protected health information received from, or created or received by the business associate on behalf of, the covered entity that the business associate still maintains in any form and retain no copies of such information or, if such return or destruction is not feasible, extend the protections of the contract to the information and limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible."
[50] 45 C.F.R. § 164.504(f)
[51] 45 C.F.R. § 164.510(a)
[52] 45 C.F.R. § 164.510(b)(1)(i).

has died,[53]and for disaster relief purposes to public or private entities authorized by law to receive such information.[54]

There are provisions in the law which require covered entities and business associates to account for breaches of protected health information. The so-called Breach Notification Rule requires those who are subject to the rule to notify affected parties in the event of such a breach.[55] The definition of what constitutes a breach is comprehensive: ". . . the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information."[56] The regulation refines the definition by excluding from its coverage certain types of errant disclosures. For instance, good faith, unintentional acquisition or access to PHI, or merely inadvertent disclosures of the same, by an employee of a covered entity or business associate in the course of acting on behalf of the covered entity or business associate, is not a breach under the rule as long as there is no further use or disclosure in contravention of the rule.[57] Also, disclosure of PHI by a covered entity or business associate to an unauthorized person when the covered entity or business associate has a good faith belief that the PHI is not able to be retained by the recipient, does not constitute a breach under the rule.[58] Interestingly, although the Breach Notification Rule presumes that the unauthorized acquisition, use, or disclosure of PHI constitutes a breach, the presumption can be defeated if the offending entity ". . . demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment . . ." of certain factors.[59]

Once a breach has been discovered, it is incumbent upon the covered entity involved to notify each affected individual of the breach.[60] A breach of PHI is considered to have been discovered when the covered entity actually knows of the breach, or should have known of the breach through the exercise of reasonable diligence.[61] Breaches must be disclosed to affected parties expeditiously and in no instance more than 60-days subsequent to the breach's discovery.[62] Breach notifications must contain five basic elements: a description of the breach and when it happened;[63] a description of the information breached;[64] a description of the kinds of things a victim of the breach ought to do in order to protect him/herself from the unauthorized disclosure;[65] a synopsis of the actions

---

[53] 45 C.F.R. § 164.510(b)(5).

[54] 45 C.F.R. § 164.510(b)(4): " . . . [a] covered entity may use or disclose protected health information to a public or private entity authorized by law or by its charter to assist in disaster relief efforts, for the purpose of coordinating with such entities the uses or disclosures permitted by paragraph (b)(1)(ii) of this section. The requirements in paragraphs (b)(2), (b)(3), or (b)(5) of this section apply to such uses and disclosures to the extent that the covered entity, in the exercise of professional judgment, determines that the requirements do not interfere with the ability to respond to the emergency circumstances."

[55] The Breach Notification Rule of HIPAA is found at 45 C.F.R. §§ 164.400-414.

[56] 45 C.F.R. § 164.402.

[57] 45 C.F.R. §§ 164.402(1)(i) and (ii).

[58] 45 C.F.R. § 164.402(1)(iii).

[59] 45 C.F.R. § 164.402(2). The factors include type of PHI and the extent of the disclosure (including the probability that the information will result in re-identification; by looking at who used the PHI or to whom it was disclosed; the actual circumstances under which the disclosure of PHI was made and whether the PHI was actually seen by an unauthorized person or entity; and, finally, the effectiveness of any measures to mitigate the unauthorized disclosure. See 45 C.F.R. §§ 164.402(2)(i)-(iv).

[60] 45 C.F.R. § 164.404(a)(1).

[61] 45 C.F.R. § 164.404(a)(2). The exercise of reasonable diligence on the part of the covered entity involved in a PHI breach does not include the actual knowledge of the person who has committed the breach.

[62] 45 C.F.R. § 164.404(b).

[63] 45 C.F.R. § 164.404(c)(1)(A).

[64] 45 C.F.R. § 164.404(c)(1)(B).

[65] 45 C.F.R. § 164.404(c)(1)(C).

taken by the covered entity to mitigate the potential for harm to the victim of the breach and steps taken by the covered entity to lessen the possibility of future breaches;[66] and contact information for victims to reach out to the covered entity for information about the breach.[67] Notice of a breach ought to be made in writing to a breach victim or electronically if an owner of PHI has previously agreed to that method of notification.[68] The Breach Notification Rule also requires that breach notifications be written in simple language that is readily understandable to one who may be a victim of a breach.[69] Other means reasonably calculated to make contact with a victim of a breach are allowed, and notification to next of kin may be required under circumstances in which a breach victim is deceased.[70]

I(b). The Security Rule

Covered entities and business associates have special responsibilities with regard to electronic PHI (e-PHI) under the HIPAA Security Rule.[71] Electronic protected health information is a subset of the individually identifiable health information which HIPAA is designed to protect. "A major goal of the Security Rule is to protect the privacy of individuals' health information while allowing covered entities to adopt new technologies to improve the quality and efficiency of patient care. Given that the health care marketplace is diverse, the Security Rule is designed to be flexible and scalable so a covered entity can implement policies, procedures, and technologies that are appropriate for the entity's particular size, organizational structure, and risks to consumers' e-PHI."[72]

The statute required the Secretary of HHS ". . . to issue security regulations regarding measures for protecting the integrity, confidentiality, and availability of e-PHI that is held or transmitted by covered entities."[73] Those who are subject to the regulations must
". . . (1) Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits. (2) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information. (3) Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under subpart E of this part. (4) Ensure compliance with this subpart by its workforce."[74]

The Security Rule creates standards on a national scale for the protection of electronic PHI, and covered entities and business associates must establish and put into place administrative, physical, and technical safety mechanisms which guarantee adequate protection for the PHI.[75] The administrative safeguards that covered entities must employ include a process to ensure that

---

[66] 45 C.F.R. § 164.404(c)(1)(D).
[67] 45 C.F.R. § 164.404(c)(1)(E).
[68] 45 C.F.R. § 164.404(d)(1).
[69] 45 C.F.R. § 164.404(c)(2).
[70] 45 C.F.R. §§ 164.404(d)(2) and (3).
[71] Title 45, Subtitle A, Subchapter C, Part 164, Code of Federal Regulations, Security Standards for the Protection of Electronic Protected Health Information, 45 C.F.R. §§ 164.302–164.318.
[72] *See*, "Summary of the HIPAA Security Rule," *Health Information Privacy,* U.S. Department of Health and Human Services, HHS.gov.
[73] Id. A Notice of Proposed Rulemaking was issued on August 12, 1998 and after the required public comment period expired, a Final Rule was issued on February 20, 2003. The Final Rule, Health Insurance Reform: Security Standards, is found at 68 Fed. Reg. 8334 (Feb. 20, 2003).
[74] 45 C.F.R. § 164.306(a).
[75] *See*, "The Security Rule," *Health Information Privacy,* U.S. Department of Health and Human Services, HHS.gov.

security management practices are established and tailored to meet the unique circumstances of the covered entity.[76] They must appoint a person charged with the responsibility of establishing, implementing, and maintaining the security regime employed by the covered entity,[77] restrict access to the e-PHI to those requiring access consistent with their role within the covered entity, and ensure that access is designed to meet the minimum necessary standard established by the Privacy Rule.[78] Covered entities must utilize training programs within their workforce to ensure appropriate restrictions to access to e-PHI consistent with the requirements of the Privacy and Security Rules,[79] and, like any acceptable compliance program within an organization, they must develop and employ sanctions as necessary to enforce the covered entities' policies and procedures.[80] Also, covered entities have to create and implement evaluation mechanisms to ensure that they are meeting the mandates of the Security Rule.[81]

Physical safeguards called for in the Security Rule include restricting access to covered entities' facilities to only those with a need to enter the facilities.[82] And in furtherance of the physical security requirements, covered entities must develop, implement, and maintain appropriate workstation, device, and media controls to restrict use to those which are required for the users and which maintain positive control over the hardware and electronic media which contains e-PHI.[83]

Technical safeguards that are required of covered entities pursuant to the Security Rule include the basic requirement to ". . . [i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights."[84] Other technical safeguards mandated by the rule include audit controls,[85] a requirement to ensure the integrity of the e-PHI,[86] a means of ensuring that those accessing e-PHI are indeed those actually authorized and required to do so,[87] and transmission security measures which protect the integrity of the data as it is being transmitted over an electronic network.[88]

Because the Security Rule applies to a wide variety of entities of varying sizes and complexities, the Rule mandates that those covered entities and business associates conduct risk analyses as a part of their business and management practices.[89] "Risk analysis should be an ongoing process, in which a covered entity regularly reviews its records to track access to e-PHI and detect security incidents, periodically evaluates the effectiveness of security measures put in place, and regularly reevaluates potential risks to e-PHI."[90]

---

[76] 45 C.F.R. § 164.308(a)(1)(i).
[77] 45 C.F.R. § 164.308(a)(2).
[78] 45 C.F.R. § 164.308(a)(3)(i).
[79] 45 C.F.R. § 164.308(a)(3) and 45 C.F.R. 164.308(a)(4).
[80] 45 C.F.R. § 164.308(a)(1)(ii)(C).
[81] 45 C.F.R. §164.308(a)(8).
[82] 45 C.F.R. § 164.310(a).
[83] 45 C.F.R. § 164.310(b), 45 C.F.R. § 164.310(c), and 45 C.F.R. § 164.310(d)(1).
[84] 45 C.F.R. § 164.312(a)(1). Specific implementation specifications imposed by the Security Rule are found at 45 C.F.R. §§ 164.312(a)(2)(i)-(iv). They include standard security measures to ensure positive control over e-PHI data.
[85] 45 C.F.R. § 164.312(b).
[86] 45 C.F.R. § 164.312(c).
[87] 45 C.F.R. § 164.312(d).
[88] 45 C.F.R. § 164.312(e).
[89] 45 C.F.R. § 164.308(a)(1)(ii)(A).
[90] *See*, "Summary of the HIPAA Security Rule," *supra* note 72.

I(c). The Enforcement Rule

The Enforcement Rule was an effort to consolidate compliance and penalty provisions for violations of HIPAA. The rule was first proposed by HHS in 2005[91] and the final rule was issued on February 16, 2006.[92] The rule sought to ". . . complete the Enforcement Rule by (1) making subpart C applicable to all of the HIPAA rules; (2) adopting on a permanent basis most of the provisions of subpart E; and (3) addressing, among other issues, [HHS] policies for determining violations and calculating civil money penalties, how [HHS] will address the statutory limitations on the imposition of civil money penalties, and various procedural issues, such as provisions for appellate review within HHS of a hearing decision, burden of proof, and notification of other agencies of the imposition of a civil money penalty."[93] With respect to enforcement and penalties for violations of HIPAA (including the Privacy Rule and the Security Rule), voluntary cooperation is the preferred method of compliance.[94] And there is provision in the Rule for aggrieved persons to file complaints with the Secretary of HHS and for the Secretary to undertake investigations of those complaints.[95] Covered entities are required to cooperate with investigations and to permit pertinent access to information within the control of the covered entities.[96] Privacy Rule violations under HIPAA fall under the authority of HHS's Office of Civil Rights.[97] For HIPAA violations not related to privacy, enforcement authority rests with the Centers for Medicare & Medicaid Services.[98] Civil monetary penalties of varying degrees of severity are authorized by HIPAA.[99] In addition, there are criminal sanctions available to the Secretary for knowing violations in which individually identifiable health information is either obtained or disclosed in violation of the statute.[100]

II. A Brief History of Data Privacy in the European Union

The origin of privacy protection in Europe since the establishment of what we now know as the European Union can be traced to abuses of collected data on the continent and particularly by Germany after the rise of the National German Socialist Workers Party (NSDAP) in 1933. "During

---

[91] HIPAA Administrative Simplification; Enforcement, 70 Fed. Reg. 20224 (Apr. 18, 2005).
[92] HIPAA Administrative Simplification; Enforcement, 71 Fed. Reg. 8390 (Feb. 16, 2006).
[93] Id. at p. 8391.
[94] 45 C.F.R. § 160.304: "The Secretary will, to the extent practicable, seek the cooperation of covered entities in obtaining compliance with the applicable requirements of this part 160 and the applicable standards, requirements, and implementation specifications of subpart E of part 164 of this subchapter."
[95] 45 C.F.R. § 160.306(a) and 45 C.F.R. § 160.306(c).
[96] 45 C.F.R. § 160.310.
[97] *See*, Secretarial delegation at 65 Fed. Reg. 82239, 82381 (Dec. 28, 2000).
[98] *See*, Department of Health and Human Services, Centers for Medicare & Medicaid Services, Statement of Organization, Functions, and Delegations of Authority, 68 Fed. Reg. 60694 (Oct. 23, 2003).
[99] The civil penalty structure is tiered. Depending upon the nature of the violation, the covered entities' exercise of reasonable care (or lack thereof), the presence or absence of willful neglect on the part of the covered entities, and whether the covered entities have corrected violations within 30 days of their knowledge of a violation (or within 30 days of when the covered entities ought to have known of a violation), penalties can range from as little as $100 per violation and not to exceed $25,000 in a calendar year, to $50,000 per violation and not to exceed a total of $1,500,000 in a calendar year. See, generally, 42 U.S.C. § 1320d-5 for penalty language.
[100] Criminal penalties under HIPAA are quite straightforward. Knowing violations of the law may result in penalties of $50,000 and a jail term of up to one-year. Acts committed under false pretenses may result in fines of $100,000 and a jail term of up to five-years. Violators who commit an act intending to sell, transfer, or use individually identifiable information in order to gain a commercial advantage, for personal gain, or to cause malicious harm may have imposed upon them a fine of $250,000 and may be imprison for a period not to exceed ten-years. See 42 U.S.C. § 1320d-6 for the criminal provisions applicable to HIPAA violations.

its reign from 1933 to 1945, the Nazi regime used numerous instruments to monitor the public, control behavior and use citizens to monitor their neighbors, colleagues and friends. National Socialism dictated public and private life; all spheres of society and the state had to submit to the *Gleichschaltung*—the policy of achieving rigid and total coordination and uniformity. Total uniformity meant the elimination of democratic structures in favor of the *Führerprinzip*, or the leader principle, which allowed the leader's authority to go unchecked and exist above the law."[101] The Nazis used data in a very efficient manner to control the German population and to achieve its, often nefarious, end state. "The Third Reich . . . systematically abused private data: It maintained a so-called index of Jews that listed the identity of all Jews dating back to their grandparents' generation. In addition, it relied on data collected during the Weimar Republic (1918–1933), including records of homosexuals. Nazi Germany's persecution of Jews and homosexuals proved that no matter the intent of the data-collecting entity, the collection of so much personal information about individuals could be dangerous in and of itself."[102] Other European countries which fell under the German sphere of influence also used data as a means of maintaining control of their populations and in satisfying the demands of Germany for conformity with its extreme racial and political policies.[103]

It was against this backdrop that the newly-formed United Nations promulgated the Universal Declaration of Human Rights in 1948. "The Universal Declaration of Human Rights" (UDHR) is a milestone document in the history of human rights. Drafted by representatives with different legal and cultural backgrounds from all regions of the world, the Declaration was proclaimed by the United Nations General Assembly in Paris on 10 December 1948 (General Assembly resolution 217 A) as a common standard of achievements for all peoples and all nations. It sets out, for the first time, fundamental human rights to be universally protected and it has been translated into over 500 languages."[104] Significantly, Article 12 of that declaration states: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour (sic) and reputation. Everyone has the right to the protection of the law against such interference or attacks."[105]

The Organization for Economic Co-Operation and Development (OECD) created guidelines for the protection of privacy rights in 1980 when it published the "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data."[106] The effort was designed to enable the free flow of data to ensure robust interactions of nations in the commercial spheres while at the same time taking into consideration the personal privacy interests of those whose data might be entered into the many streams of commerce. Eight principles were embedded in the OECD guidelines which sought to protect individual privacy interests. Those principles relate to a limitation on data collection, preserving the quality of the data collected, ensuring that there is a

---

[101] Alvar Freude & Trixy Freude, *Echoes of History: Understanding German Data Protection*, THE BERTELSMAN FOUNDATION, October 1, 2016, http://www.bfna.org/research/echos-of-history-understanding-german-data-protection

[102] Id.

[103] For a general discussion of the treatment of those of the Jewish faith during the Nazi occupation of Holland and the role that data collection and maintenance played in that treatment, see, Linda M. Woolf, *Survival and Resistance: The Netherlands Under Nazi Occupation*, A paper presented at the United States Holocaust Museum, April 6, 1999, http://faculty.webster.edu/woolflm/netherlands.html.

[104] *Universal Declaration of Human Rights*, http://www.un.org/en/universal-declaration-human-rights, August 2, 2018.

[105] *Universal Declaration of Human Rights*, art. 12, Id.

[106] "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data," OECD Home, Directorate for Science, Technology and Innovation, http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

specific purpose behind a data collection effort, limiting the use of the data collected, safeguarding the data, expressions of openness with regard to dealing with personal data, principles regarding accountability for those who control data, and rights associated with those who provide data.[107]

Not to be lost in the development of data protection legislation in the EU is Treaty Number 108 of the Council of Europe known as the "Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data."[108] The purpose of the treaty was simple:
". . . to secure in the territory of each Party for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him ('data protection')."[109] Convention 108 incorporates largely the OECD Guidelines' principles on privacy and along with the OECD Guidelines ". . . form the core of the Data Protection laws of dozens of countries. These rules describe personal information as data that are afforded protection at every step from collection to storage and dissemination."[110]

The principles enumerated in the UDHR, the OECD Guidelines, and Treaty Number 108 greatly influenced the development of the EU's fundamental pronouncement on data privacy and its protection. That pronouncement came in the form of "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data" (DPD).[111] The DPD incorporated all of the ideals of the three documents mentioned above. Its preamble includes 72 recitals which enumerate the reasons for which it was created and cover the first seven and one-half pages of the twenty-page document. With respect to data, the second recital is noteworthy. The DPD states that ". . . data-processing systems are designed to serve man; whereas they must, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably the right to privacy, and contribute to economic and social progress, trade expansion and the well-being of individuals."[112] The DPD, like any pronouncement dealing with emerging technologies and which deals with subjects at a static moment in time, began the process of obsolescence almost immediately upon enactment.

The DPD was an innovation during its development and at its adoption in 1995. But, like many modern-day innovations, progress in the areas that Directive 95/46 sought to manage and control continued apace. The changes that have taken place in the past quarter century, in terms of electronic advancements and global connectivity particularly, have been staggering. Wisely, those behind the DPD recognized that review of the substantive provisions of the pronouncement would be necessary. Article 33 the DPD includes a provision that required the European Commission to review the DPD at periodic intervals and to recommend changes, if necessary, to fulfill the purposes for which the DPD was first promulgated.[113] A number of those reviews took place and

---

[107] "OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, Part Two, Basic Principles of National Application," Paragraphs 7-14, C(80)58/Final, as amended 11 July 2013 by C(2013)79.
[108] Treaty Number 108 of the Council of Europe, "Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data," ETS No. 108, Strasbourg, 1981, https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680078b37
[109] Id. at Ch. I, Art. 1.
[110] David Banisar & Simon Davies, *Article: Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, and Surveillance Laws and Developments*, 18 J. MARSHALL COMPUTER & INFO. L. 1, 11 Fall, 1999.
[111] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.95.
[112] Id at 1.
[113] Id. at 20.

the results highlighted certain aspects of the data protection initiative that required strengthening including the enhancement of individual privacy rights, elevated enforcement efforts, the recognition that the world had become much smaller through advances in technology and thereby making data protection and privacy issues a broader global concern requiring control and regulation, and, of course, the realization that changes would be necessary in order to fulfill the promises of the European Market as an economic force for advancement and change among member states.[114]

Perhaps the preeminent reason behind the need for modification of the DPD came because of the mechanism used by the Commission to enhance and regulate privacy and data concerns in the first place. The issuance of a directive by the European Commission on matters of privacy left open to member states the job of implementing its provisions as each member state saw fit. Leaving implementation decisions to 28 individual member state governments and their associated regulatory arms was an invitation for inconsistent, diverse, and perhaps contradictory implementation and control of data privacy matters within the EU. Enhancement and further harmonization of regulatory efforts consistently throughout the EU clearly became necessary, and the issuance and implementation of a regulation would be among the most logical fixes. Regulations in the EU lay out for member states what is necessary for the consistent application and enforcement of the standards established by a particular regulation.[115]

Technological changes in the past quarter century have also been a driving force in the need to replace the DPD. The development of smart electronic devices, the proliferation of the internet globally, the integration of these and other electronic advances into global commerce, and the rise of big data and the uses to which big data is put, have all dramatically altered the landscape in which all people exist and interact. These changes have made even more important the need to protect the privacy rights of individuals as the data which makes up their lives enters the streams of commerce worldwide making them more susceptible to legitimate and illegitimate uses of their personal information, not infrequently for nefarious and other unwanted purposes.

In any regulatory regime imposed upon users, certainty in terms of standards, requirements, and enforcement is critical. This notion of legal certainty applies also to those whose interests require protection. The DPD, with its diverse implementation throughout the EU and its uncertain application globally, challenged those who use data to establish rules for implementation and compliance, and also challenged those who provide data under various circumstances to ensure the protection of their interests and to vindicate those interests in the event of data breaches.

It is quite obvious that diverse implementation of the DPD resulted in inconsistent development and implementation of enforcement rules for the standards established by and through the DPD. Inconsistency in the application of the DPD globally also made more difficult the environment in which data users and providers operate. The development of a standard legal regime which provides the actors with an established baseline of rules, consistent and uniform interpretation of the rules (to the degree such consistency and uniformity exists in any legal regime), and a consistent and effective means of ensuring enforcement of the rules is crucial for continuing advancement in the area of data privacy protection and in defining the limits of legitimate use of personal data. The EU is confident that the new GDPR will close the gaps noted herein and provide

---

[114] *See, e.g.*,, Commission First Report on the implementation of the Data Protection Directive, (95/46/EC), COM (2003) 265 final, of 15.5.2003., http://eur-lex.europa.eu/LexUriServ/site/en/com/2003/com2003_0265en01.pdf, 1-10; "Communication on the follow-up of the Work Programme for better implementation of the Data Protection Directive," http://ec.europa.eu/justice_home/fsj/privacy/docs/lawreport/com_2007_87_f_en.pdf, 1-100.

[115] For an excellent discussion of the legislative process in the European Union, *see, A Brief Guide to the European Union and Its Legislative Processes*, 8 March 2013, Financial Conduct Authority (UK), Publications, https://www.fca.org.uk/publication/archive/european-union-legislative-process.pdf, 1-41.

the stability required in the application of legal standards for the protection of individual privacy interests of EU citizens and lessen the risk to those who control and process data.[116]

Finally, the transfer of data internationally and across state borders has dramatically altered the landscape within which users and providers operate in the past quarter century. The DPD lacked the kinds of effective rules necessary for the environment in which users, controllers, and processors of data must now act, and uncertainty in the international arena has led the EU to scramble at times under the DPD in order to develop the kinds of safeguards necessary to assure that commerce in and among nations not members of the EU can and will continue to flow.[117] At times under the DPD it has appeared that the uninhibited transfer of goods and services among EU and non-EU nations would be significantly and negatively impacted because of failures to comply with EU privacy principles.

For all of the forgoing reasons and more, the European Commission proposed in 2012 to change the direction of data protection and enhance privacy rights within the EU.[118] Four years later, after much comment, debate, and revision, the Council of the European Union and the European Parliament adopted the GDPR.[119]

III. The General Data Protection Regulation

The GDPR imposes obligations upon those who control and process personal data. And at its root, the GDPR ". . . lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data."[120] But, the GDPR also seeks to protect the rights of natural persons[121]regarding their personal data and the fundamental rights and freedoms of individuals.[122] Its scope, however, is limited to ". . . the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system."[123] The GDPR also asserts that its application is extra-territorial under

---

[116] For a discussion of this concept, see Neil Robinson, Hans Graux, Maarten Botterman, & Lorenzo Valeri, *Review of the European Data Protection Directive*, THE RAND CORPORATION, 2009, Chapter 3, "How does the Directive stand up to current challenges," Section 3.3. "Main Weaknesses," Subsection 3.3.7 "Other Minor Weaknesses," p. 37.

[117] *See*, Shakila Bu-Pasha, *Cross-border issues under EU data protection law with regards to personal data protection*, INFORMATION & COMMUNICATIONS TECHNOLOGY LAW, 26:3, (2017), 213-228, for an excellent discussion of the Safe Harbour Agreement, its demise post-*Schrems I*, and the development of the Privacy Shield as an example of the kinds of chaos wreaked because of the absence of certainty in rules and their application under the Directive.

[118] *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*, Brussels, 25.1.2012, COM(2012) 11 final, 2012/0011 (COD), C7-0025/12.

[119]Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)(EU), was approved by the Council of the European Union on April 8, 2016 and by the European Parliament on April 16, 2016. It went into effect on May 25, 2016 with full implementation on May 25, 2018.

[120] General Data Protection Regulation, ch. I. art. 1(1), *supra* note 12, at 32.

[121] A natural person is defined as follows: ". . . 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, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person." General Data Protection Regulation, ch. I. art. 4(1), Id. at 33.

[122] General Data Protection Regulation, ch. I. art. 1(2), Id. at 32.

[123] General Data Protection Regulation, ch. I. art. 2(1), Id.

specific circumstances enumerated within the Regulation.[124] This becomes an important aspect of the Regulation for those entities not located within the EU but which seek to do business with EU citizens or which handle data pertaining to EU citizens.

Under the GDPR, controllers and processors are key to matters involving data and privacy. A controller is ". . . the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law."[125] A processor is simply ". . . a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller."[126] Data controllers and processors obviously have to be concerned about personal data. Personal data is: ". . . any information relating to an identified or identifiable natural person ('data subject'). . . ."[127] Processing of data refers to ". . . any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation (sic), structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction."[128]

Three particular kinds of data are singled out in the GDPR. The first is "data concerning health." Data concerning health is ". . . personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status."[129] The second specific form of data is "genetic data." Genetic data is ". . . personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question."[130] And finally, the third unique kind of data is "biometric data." Biometric data is ". . . personal data resulting from specific technical processing relating to the physical, physiological or behavioural (sic) characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data."[131] These types of data are significant in that they are deemed special categories of personal data in which there are restrictions under the GDPR regarding processing. Indeed, the general rule is that the processing of such data is prohibited.[132] The prohibition against processing such data does not apply in a number of circumstances discussed below.

Fundamental to data privacy and protection under the GDPR is the notion that those actors who control or process data do so fairly, lawfully, and with transparency,[133] and it is the controller

---

[124] *See*, General Data Protection Regulation, Ch. I, Id., and "Cross-border issues under EU data protection law with regards to personal data protection," Section 3, *supra* note 117, for an excellent discussion of the extra-territorial application of the General Data Protection Regulation and its predecessor.
[125] General Data Protection Regulation, ch. I, art. 4(7), *supra* note 12, at 33.
[126] General Data Protection Regulation, ch. I, art. 4(8), Id.
[127] General Data Protection Regulation, ch. I, art. 4(1), Id.
[128] General Data Protection Regulation, ch. I, art. 4(2), Id.
[129] General Data Protection Regulation, ch. I, art. 4(15), Id. at 34.
[130] General Data Protection Regulation, ch. I, art. 4(13), Id.
[131] General Data Protection Regulation, ch. I, art. 4(14), Id.
[132] *See*, General Data Protection Regulation, art. 9, Id. at 38, which states: "Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited."
[133] General Data Protection Regulation, ch. II, art. 5(1)(a), Id. at 35.

who is accountable for making sure that it is done in that manner.[134] The notion of transparency takes a prominent role in the GDPR. It is explicitly combined with the notions of fairness and lawfulness in the context of the principles which relate to the processing of data. And while "transparency" is not specifically defined in the GDPR, the GDPR includes in Recital 39 the charge that transparency ". . . requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used. That principle concerns, in particular, information to the data subjects on the identity of the controller and the purposes of the processing and further information to ensure fair and transparent processing in respect of the natural persons concerned and their right to obtain confirmation and communication of personal data concerning them which are being processed."[135]

The word "transparent" appears 17 times in the GDPR, most often in the context of data subjects having knowledge of the actions of controllers and processers vis-à-vis a data subject's personal information, in the context of consent on the part of a data subject prior to a particular use of that subject's data, or in the context of requiring an open process or procedure on the part of controllers and processors as personal data is being gathered, stored, or disseminated. Recital 60 of the GDPR notes that

> . . . [t]he principles of fair and transparent processing require that the data subject be informed of the existence of the processing operation and its purposes. The controller should provide the data subject with any further information necessary to ensure fair and transparent processing taking into account the specific circumstances and context in which the personal data are processed. Furthermore, the data subject should be informed of the existence of profiling and the consequences of such profiling. Where the personal data are collected from the data subject, the data subject should also be informed whether he or she is obliged to provide the personal data and of the consequences, where he or she does not provide such data. That information may be provided in combination with standardised (sic) icons in order to give in an easily visible, intelligible and clearly legible manner, a meaningful overview of the intended processing. Where the icons are presented electronically, they should be machine-readable.[136]

Fair and lawful processing of data is also dependent upon consent of the data subject, or some other legal basis for processing.[137] Consent, inextricably linked to transparency, means ". . . a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement."[138] It is also defined as: ". . . any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her."[139] The GDPR insists that consent be demonstrated by a data controller. Written consent must be based upon a form that is intelligible and accessible and the language used to seek consent has to use simple language with

---

[134] General Data Protection Regulation, ch. II, art. 5(2), Id. at 36.
[135] General Data Protection Regulation, Recital 39, Id. at 7.
[136] General Data Protection Regulation, Recital 60, Id. at 12.
[137] "In order for processing to be lawful, personal data should be processed on the basis of the consent of the data subject concerned or some other legitimate basis, laid down by law, either in this Regulation or in other Union or Member State law as referred to in this Regulation, including the necessity for compliance with the legal obligation to which the controller is subject or the necessity for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract." General Data Protection Regulation, Recital 40, Id. at 8.
[138] General Data Protection Regulation, Recital 32, Id. at 6.
[139] General Data Protection Regulation, art. 4(10), Id. at 34.

obvious meaning.[140] Data subjects have the right to withdraw their consent at any time and they must be informed of that right prior to giving their consent.[141]

Lawful processing can exist only if one of several preconditions has been met. Those conditions include: the specific and focused consent of the data subject has been given,[142] the processing of the data is necessary in order to fulfill the terms of a contract of which the data subject is a party,[143] the data controller is required by law to process the data,[144] it is necessary to protect the vital interests of the data subject or someone else,[145] processing is necessary in order for the controller to fulfill a public interest or it is required in order for the controller to undertake its own official obligations,[146] and where processing is required in order to fulfill legitimate interests of the controller or someone else, unless a fundamental right or freedom of the data subject subsumes the controller's or third party's legitimate interests.[147]

There are general principles enumerated for the processing of data. In addition to lawful, fair, and transparent conditions for processing, data must only be ". . . collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation')."[148] The data collected by a controller must be ". . . adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')(sic)."[149] It must also be accurate and current, and controllers must do all in their power to maintain the accuracy of data.[150] Data also must be ". . . kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational (sic) measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation')."[151] The final principle for processing data requires that all data be processed so as to assure its security, ". . . including protection against unauthorised (sic) or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational (sic) measures ('integrity and confidentiality')."[152]

As noted earlier, there is a general prohibition against the processing of special categories of personal data. But, the GDPR does allow processing of such data under ten distinct circumstances. The most obvious of those circumstances are those in which the data subject has consented to the processing. Even that consent may, however, be null and void if the EU or any member state prohibits a data subject from consenting.[153] Processing of special categories of data is also

[140] General Data Protection Regulation, art. 7(1)-(2), Id. at 37.
[141] General Data Protection Regulation, art. 7((3), Id.
[142] General Data Protection Regulation, art. 6(1)(a), Id. at 36.
[143] General Data Protection Regulation, art. 6(1)(b), Id.
[144] General Data Protection Regulation, art. 6(1)(c), Id.
[145] General Data Protection Regulation, art. 6(1)(d), Id
[146] General Data Protection Regulation, art. 6(1)(e), Id.
[147] General Data Protection Regulation, art. 6(1)(f), Id.
[148] General Data Protection Regulation, art. 5(1)(b), Id. at 35.
[149] General Data Protection Regulation, art. 5(1)(c), Id.
[150] General Data Protection Regulation, art. 5(1)(d), Id.
[151] General Data Protection Regulation, art. 5(1)(e), Id. at 36.
[152] General Data Protection Regulation, art. 5(1)(f), Id.
[153] General Data Protection Regulation, art. 9(2)(a), Id. at 38.

permissible when required by a data controller or in the interest of a data subject in the areas of employment matters, social security, and social protection.[154] The notion of "social protection" appears five times in the GDPR. It is most pointedly described in the context of public health as ". . . for health security, monitoring and alert purposes, the prevention or control of communicable diseases and other serious threats to health."[155] And further in the context of health and public health, ". . . in order to ensure the quality and cost-effectiveness of the procedures used for settling claims for benefits and services in the health insurance system, or for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes."[156]

Processing of special data is also permissible in instances in which it is necessary to protect the interests of the data subject or others when the data subject is incapable of giving his/her consent.[157] In circumstances in which a foundation, a not-for-profit, or some other association provides for adequate safeguards for the information, special data may be processed of members or former members as long as the processing is inextricably tied to the purposes of the entity seeking to process the data and the data is not released outside of the entity, unless the data subject consents to such a release, of course.[158] In instances in which a data subject has put its special data into the public domain, processing is allowed.[159] A judicial exception to the prohibition against the processing of special data exists in instances in which processing is necessary to pursue a claim or to defend against one or when courts are acting as courts as they are required to do so.[160]

A rather more general exception exists allowing processing when there is a "substantial public interest" deserving of vindication.[161] The notion of "substantial public interest" is not defined in the GDPR.[162] A preventive and occupational medicine exception to the no-processing rule exists ". . . for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services. . . ."[163] In instances in which processing of special data is required to assure the health and safety of data subjects, styled as a public interest and therefore impliedly a broad public concern, processing is permitted as long as there are acceptable safeguards for the interests of the data subjects.[164] Finally, the processing of special data is permissible, in limited circumstances, when done in the public interest for the purposes of scientific or historical research, again subject to adequate protection of the fundamental rights of the data subject.[165] The GDPR also allows member states to impose additional conditions upon the processing of genetic, biometric, and health data.[166]

The GDPR provides detailed guidance with respect to the processing of health-related data. Indeed, health data is entitled to a greater degree of protection under the Regulation and can only be processed

---

[154] General Data Protection Regulation, art. 9(2)(b), Id.
[155] General Data Protection Regulation, Recital 52, Id. at 10.
[156] Id.
[157] General Data Protection Regulation, art. 9(2)(c), Id. at 38.
[158] General Data Protection Regulation, art. 9(2)(d), Id.
[159] General Data Protection Regulation, art. 9(2)(e), Id.
[160] General Data Protection Regulation, art. 9(2)(f), Id.
[161] General Data Protection Regulation, art. 9(2)(g), Id.
[162] *See, e.g.*, the British Data Protection Act 2018, specifically Chapter 12, which lists in exhaustive detail the kinds of circumstances under which the conditions for a "substantial public interest" have been met. Similar national laws of other member nations will likely do the same to ensure that processing of data is done lawfully.
[163] General Data Protection Regulation, art. 9(2)(h), *supra* note 12, at 38.
[164] General Data Protection Regulation, art. 9(2)(i), Id.
[165] General Data Protection Regulation, art. 9(2)(j), Id. at 39.
[166] General Data Protection Regulation, art. 9(4), Id.

> . . . where necessary to achieve those purposes for the benefit of natural persons and society as a whole, in particular in the context of the management of health or social care services and systems, including processing by the management and central national health authorities of such data for the purpose of quality control, management information and the general national and local supervision of the health or social care system, and ensuring continuity of health or social care and cross-border healthcare or health security, monitoring and alert purposes, or for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, based on Union or Member State law which has to meet an objective of public interest, as well as for studies conducted in the public interest in the area of public health.[167]

The drafters of the GDPR specifically called for consistent circumstances under which the processing of health data would be permitted under the Regulation and emphasized need for the protection of the fundamental rights of data subjects in such circumstances.[168]

Among the more interesting aspects of the GDPR is Article 17.[169] Article 17 is styled as the "Right to erasure ('right to be forgotten')."[170] There are six circumstances under which a data subject may demand and a controller must erase personal data. Those circumstances are: the data is no longer needed for the purposes for which it was gathered or processed,[171] consent to processing has been revoked,[172] the data subject objects to processing consistent with the requirements of the Regulation,[173] when the data has been processed contrary to law,[174] a Member State law which exercises jurisdiction over a controller requires erasure,[175] or in special circumstances involving the data of a child.[176] This right to be forgotten can be a challenge for a controller. Nonetheless, ". . . [w]here the controller has made the personal data public and is obliged . . . to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data."[177] And there are a limited set of circumstances under which a controller is not obligated to erase data. Those circumstances include processing necessary for the freedom of expression and information dissemination in that context, processing required consistent with the national laws of member states in the public interest (when that authority resides with the controller), public health interests require processing, vital and social statistical purposes require processing in the public interest, and processing required to establish, exercise, or defend a legal claim.[178]

Transnational application of the GDPR will be of some significance for controllers and data processors. The territorial scope of the Regulation is defined in Article 3. First, the Regulation applies to processing of personal data by a controller or processor establishment within the EU, regardless of whether the processing itself takes place within the EU.[179] The notion of

---

[167] General Data Protection Regulation, Recital 53, Id. at 10.
[168] Id.
[169] General Data Protection Regulation, art. 17, Id at 43.
[170] Id.
[171] General Data Protection Regulation, art. 17(1)(a), Id.
[172] General Data Protection Regulation, art. 17(1)(b), Id. at 44.
[173] General Data Protection Regulation, art. 17(1)(c), Id.
[174] General Data Protection Regulation, art. 17(1)(d), Id.
[175] General Data Protection Regulation, art. 17(1)(e), Id.
[176] General Data Protection Regulation, art. 17(1)(f), Id.
[177] General Data Protection Regulation, art. 17(2), Id.
[178] General Data Protection Regulation, art. 17(3)(a)-(e), Id.
[179] General Data Protection Regulation, art. 3(1), Id. at 32.

establishment is explained throughout the Regulation, but particularly in Recital 36 wherein the definition of "main establishment" is found: a controller's main establishment

> . . . in the Union should be the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union, in which case that other establishment should be considered to be the main establishment. The main establishment of a controller in the Union should be determined according to objective criteria and should imply the effective and real exercise of management activities determining the main decisions as to the purposes and means of processing through stable arrangements. That criterion should not depend on whether the processing of personal data is carried out at that location. The presence and use of technical means and technologies for processing personal data or processing activities do not, in themselves, constitute a main establishment and are therefore not determining criteria for a main establishment.[180]

A processor's "main establishment" is

> . . . the place of its central administration in the Union or, if it has no central administration in the Union, the place where the main processing activities take place in the Union. In cases involving both the controller and the processor, the competent lead supervisory authority should remain the supervisory authority of the Member State where the controller has its main establishment, but the supervisory authority of the processor should be considered to be a supervisory authority concerned and that supervisory authority should participate in the cooperation procedure provided for by this Regulation. In any case, the supervisory authorities of the Member State or Member States where the processor has one or more establishments should not be considered to be supervisory authorities concerned where the draft decision concerns only the controller. Where the processing is carried out by a group of undertakings, the main establishment of the controlling undertaking should be considered to be the main establishment of the group of undertakings, except where the purposes and means of processing are determined by another undertaking.[181]

But, greatly expanding upon the jurisdiction of the GDPR, the Regulation is applicable to the processing of personal data irrespective of where the controller or processor is established when the processing of the data involves offering goods and services to data subjects located in the EU (even if no payment is required of the data subject) or if the behavior of data subjects within the EU is being monitored.[182] Article 3 also makes the Regulation applicable in instances in which the law of a member state is applicable through general principles of international law to a controller's processing of personal data in those instances in which the controller is not established within the EU.[183]

The GDPR uses significant sanctions to enhance compliance and to punish controllers and processors who violate the terms of the Regulation.[184] Chapter VIII of the Regulation enumerates

---

[180] General Data Protection Regulation, Recital 36, Id. at 6.

[181] Id. at 7.

[182] General Data Protection Regulation, art. 3(2), Id. at 33.

[183] General Data Protection Regulation, art. 3(3), Id. at 32. Recital 25 refers to member states' diplomatic and consular facilities as examples of this extra-territorial applicability.

[184] Recital 148 expresses the sentiment as follows: "In order to strengthen the enforcement of the rules of this Regulation, penalties including administrative fines should be imposed for any infringement of this Regulation, in addition to, or instead of appropriate measures imposed by the supervisory authority pursuant to this Regulation." General Data Protection Regulation, Recital 148, *supra* note 12, at 27. Recital 149 takes the sanction sentiment a step further: "Member States should be able to lay down the rules on criminal penalties for infringements of this Regulation, including for infringements of national rules adopted pursuant to and within the limits of this Regulation. Those criminal penalties may also allow for the deprivation of the profits obtained through

remedies available to aggrieved parties, discusses the liabilities of controllers, processors, and others for violations of the Regulation, and lists the penalties which may be imposed for violations of the GDPR. Most significant in the Regulation is a private right of action for aggrieved data subjects.[185] Data subjects have the option to proceed against supervisory authorities, controllers, and processors of their data.[186] Data subjects may also have certain entities act on their behalf in order to vindicate their rights under the Regulation, and those entities may also act *sua sponte* on behalf of aggrieved data subjects if authorized to do so by a particular member state.[187] Aggrieved parties who have ". . . suffered material or non-material damage as a result of an infringement of [the] Regulation shall have the right to receive compensation from the controller or processor for the damage suffered."[188] The notion of "material" is not specifically defined within the Regulation, but references to "physical, material, or non-material" breach sprinkled throughout the Regulation give some insight as to meaning.[189] Liability for controllers and processors is joint and several under the Regulation.[190]

The GDPR provides for the imposition of fines consistent with Article 83 of the Regulation, and in accordance with Article 84 allows member states to establish and impose other penalties upon those who violate the Regulation.[191] Fines are intended to be ". . . effective, proportionate and dissuasive."[192] The maximum fine depends upon the Article of the GDPR violated, but for controllers and processors deemed to have infringed the rights of data subjects the maximum fine is €10,000,000, or up to two-percent of the annual turnover for the year preceding in the case of a larger undertaking, whichever is greater.[193] Infringements deemed more serious under the

---

infringements of this Regulation. However, the imposition of criminal penalties for infringements of such national rules and of administrative penalties should not lead to a breach of the principle of ne bis in idem, as interpreted by the Court of Justice." General Data Protection Regulation, Recital 149, *supra* note 12, at 27.

[185] "Without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement if the data subject considers that the processing of personal data relating to him or her infringes this Regulation." General Data Protection Regulation, art. 77(1), *supra* note 12, at 80.

[186] General Data Protection Regulation, art. 78 & art. 79, Id. at 80.

[187] General Data Protection Regulation, art. 80, Id. at 81.

[188] General Data Protection Regulation, art. 82(1), Id.

[189] For instance, Recital 75 of the GDPR discusses the kinds of risks to the rights and freedoms of people which may result from data processing as: ". . . physical, material or non-material damage, in particular: where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation (sic), or any other significant economic or social disadvantage; where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data; where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures; where personal aspects are evaluated, in particular analyzing (sic) or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behavior (sic), location or movements, in order to create or use personal profiles; where personal data of vulnerable natural persons, in particular of children, are processed; or where processing involves a large amount of personal data and affects a large number of data subjects." General Data Protection Regulation, Recital 75, Id. at 15.

[190] General Data Protection Regulation, art. 82, Id. at 81.

[191] Other penalties under Article 84 appear to be intended for ". . . infringements which are not subject to administrative fines pursuant to Article 83, and shall take all measures necessary to ensure that they are implemented. Such penalties shall be effective, proportionate and dissuasive." General Data Protection Regulation, art. 84(1), Id. at 83.

[192] General Data Protection Regulation, art. 83(1), Id. at 82.

[193] General Data Protection Regulation, art. 83(4)(a), Id.

Regulation warrant fines of up to €20,000,000, or up to four-percent of the annual turnover for the year preceding in the case of a larger undertaking, whichever is greater.[194]

IV. The Flawed Privacy Rule

Juxtaposing the Privacy Rule and the GDPR, it is evident that the two data protection efforts are similar in many respects and yet fundamentally different in approach and effect. Beginning with the proposition that personal health data is a commodity which is valuable,[195]private, and deserving of protection, both regulations focus on what is necessary to maintain the value of the data, to keep it private, and to protect it from release against the wishes of the data subject. The Privacy Rule focuses on how to accomplish these tasks after the data has been collected. There is a presumption that the data is in the public domain and the dominant theme in the United States is to protect it where it is stored and to manage it so as to prevent it from getting where it ought not to be. In the EU, however, member states have concentrated on keeping data away from the public domain at the outset. That is accomplished most graphically by the demands placed upon controllers and processors to make data subjects aware of what will be done with data if the owner decides to provide the information sought. So the data subject, about whom the data is sought, controls whether the data ends up in the hands of a controller, largely without precondition.

Of particular note, in the EU personal health data is data. It is not covered, as in the United States, by its own body of statutory and regulatory rules. It is treated in virtually the same fashion as any other data is treated under the EU regulatory scheme. HIPAA segregates health data from the data universe and creates a special set of rules for how to deal with it. Unlike the GDPR, HIPAA doesn't really afford a patient an opportunity to effectively control the migration of his/her data into the Big Data universe. Indeed, it gives less credence to a data subject by simply assuming that PHI will be provided during the course of treatment (in most instances) and that whatever happens next to the PHI will be done only with the best interests of the patient in mind.[196] In the EU, affirmative consent and transparency are required with respect to a data subject agreeing to provide data (including health data) in the first place. Furthermore, special categories of data (of which health data is a part) are prohibited from processing unless the data subject specifically agrees to that processing.[197] Logic dictates that a system designed to keep data away from others is bound to be a more effective means of controlling data than one which only imposes controls after data has entered the domain of data writ large.

---

[194] General Data Protection Regulation, art. 83(5), Id.

[195] *See,* Ira S. Rubinstein, *Big Data: The End of Privacy or a New Beginning,* 3 INTERNATIONAL DATA PRIVACY LAW, 74, 76 (2013), ("All of the biggest Internet companies—Google, Facebook, Amazon, eBay, Microsoft, and Yahoo!—are engaged in Big Data in one form or another and treat data as a major asset and source of value creation.").

[196] For instance, the HHS model "Notice of Privacy Practices," is a five-page document enumerating the rights of patients regarding their PHI. In the section indicating that a patient has the right to ask his/her provider not to share data or to limit the use of the data, the following confidence-building language appears: "You can ask us not to use or share certain health information for treatment, payment, or our operations. We are not required to agree to your request, and we may say 'no' if it would affect your care. If you pay for a service or health care item out-of-pocket in full, you can ask us not to share that information for the purpose of payment or our operations with your health insurer. We will say 'yes' unless a law requires us to share that information." *See* the *Model Notice of Privacy Practices*, https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/npp_fullpage_hc_provider.pdf , at 2. The Privacy Rule almost immediately requires providers to notify a patient that he/she can ask that PHI not be used, but that the provider can override that request.

[197] General Data Protection Regulation, art. 9(2)(a), *supra* note 12, at 38.

Another significant difference between health data protection efforts in the United States and Europe is that once a patient provides data to a health provider in the United States, it may not be removed from a data base simply at the request of the patient. The GDPR includes the novel "right to be forgotten."[198] That right imposes upon controllers the obligation to erase data that it may have on a data subject under one of six circumstances. The most notable of those circumstances is simply that in which a ". . . data subject withdraws consent on which the processing is based . . . and where there is no other legal ground for the processing."[199] The GDPR even goes so far as to make a controller liable for chasing data that was once in its control to the extent that is technically feasible.[200] The erasure obligation of the controller is not absolute, of course. But, it does place upon the controller an obligation to refute the desire of the data subject to be forgotten and makes that demand absolute except in those limited circumstances noted in the Regulation.[201] HIPAA and the Privacy Rule have no such provisions. At best under HIPAA, a patient has the right to demand correction of data, and if the data is incorrect, it must be amended to rectify the error.[202] But, access to PHI contained in records under HIPAA is not absolute. Covered entities can deny access to PHI in a variety of circumstances,[203] and, once examined and correction or modification is requested, covered entities can deny a request to amend in a variety of circumstances, including the fact that the PHI wasn't created by the covered entity,[204] when it is not included as a part of a "designated record set,"[205]when access is not allowed under the rules, or because it is correct.[206]

Another important distinction between HIPAA and the GDPR in the context of health data is the ability of third parties to access data, despite the Privacy Rule, for the purposes of marketing activities. For instance, any health data that doesn't identify a person and in a situation in which it is not reasonable to believe that a person can be identified from the information, the Privacy Rule concludes that the information is not "individually identifiable health information."[207] The term "marketing" is defined in a very straight forward manner: ". . . to make a communication about a product or service that encourages recipients of the communication to purchase or use the product or service."[208] However, what is not defined as "marketing" is also significant. For instance, marketing does not include a communication which describes ". . . a health-related product or service (or payment for such product or service) that is provided by, or included in a

[198] General Data Protection Regulation, art. 17(1), Id. at 43.
[199] General Data Protection Regulation, art. 17(1)(b), Id.at 44.
[200] General Data Protection Regulation, art, 17(2), Id.
[201] General Data Protection Regulation, art, 17(3), Id.
[202] See, 45 C.F.R. § 164.525 & 45 C.F.R. § 164.526.
[203] There are a host of circumstances under the Privacy Rule whereby access to an individual's PHI can be denied. Those circumstances include: psychotherapy notes, data that is compiled in anticipation of litigation, PHI that is included in records that are covered by the Privacy Act (5 U.S.C. 552a), *et cetera*. 45 U.S.C. § 164.524 includes a complete enumeration of the circumstances in which a denial of access can be made.
[204] 45 C.F.R. § 164.526(a)(2)(i).
[205] 45 C.F.R. § 164.526(a)(2)(ii). A "designated record set" is a term of art under the Privacy Rule. It is "(1) A group of records maintained by or for a covered entity that is: (i) The medical records and billing records about individuals maintained by or for a covered health care provider; (ii) The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or (iii) Used, in whole or in part, by or for the covered entity to make decisions about individuals. (2) For purposes of this paragraph, the term record means any item, collection, or grouping of information that includes protected health information and is maintained, collected, used, or disseminated by or for a covered entity." 45 C.F.R. § 164.501.
[206] 45 C.F.R. § 164.526(a)(2)(iv).
[207]45 C.F.R. § 164.514(a). The latter provision establishes one of the standards required by HIPAA for individually identifiable health information and the circumstances in which it can be used and disclosed.
[208] 45 C.F.R. § 164.501.

plan of benefits of, the covered entity making the communication, including communications about: the entities participating in a health care provider network or health plan network; replacement of, or enhancements to, a health plan; and health-related products or services available only to a health plan enrollee that add value to, but are not part of, a plan of benefits."[209]

Thus, supplying one's PHI to the company or companies that are a part of the "health care operations" of the provider from whom one gets one's health care and treatment services is not marketing under the Privacy Rule despite the fact that what the company or companies are doing with that information is targeting the owner of the PHI for the express purposes of marketing their products to the one whose PHI has been provided.[210] Therefore, for data which falls into the latter category there are no restrictions at all as far as the Privacy Rule is concerned. Also included in the section pertaining to requirements for using and disclosing PHI is reference to the concept of a "limited data set."[211] And among the permitted uses to which the information in a limited data set may be put is ". . . for the purposes of research, public health, or health care operations."[212] As noted, health care operations is a wide universe under the Privacy Rule. In the area of research

---

[209] Id.

[210] "Health care operations" is defined quite broadly under the rule at 45 C.F.R. § 164.501: ". . . (1) Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; patient safety activities (as defined in 42 CFR 3.20); population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment; (2) Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers, training of non-health care professionals, accreditation, certification, licensing, or credentialing activities; (3) Except as prohibited under §164.502(a)(5)(i), underwriting, enrollment, premium rating, and other activities related to the creation, renewal, or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to claims for health care (including stop-loss insurance and excess of loss insurance), provided that the requirements of §164.514(g) are met, if applicable; (4) Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs; (5) Business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the entity, including formulary development and administration, development or improvement of methods of payment or coverage policies; and (6) Business management and general administrative activities of the entity, including, but not limited to: (i) Management activities relating to implementation of and compliance with the requirements of this subchapter; (ii) Customer service, including the provision of data analyses for policy holders, plan sponsors, or other customers, provided that protected health information is not disclosed to such policy holder, plan sponsor, or customer. (iii) Resolution of internal grievances;
(iv) The sale, transfer, merger, or consolidation of all or part of the covered entity with another covered entity, or an entity that following such activity will become a covered entity and due diligence related to such activity; and
(v) Consistent with the applicable requirements of §164.514, creating de-identified health information or a limited data set, and fundraising for the benefit of the covered entity."

[211] 45 C.F.R. § 164.514(e). According to the regulation, "A limited data set is protected health information that excludes the following direct identifiers of the individual or of relatives, employers, or household members of the individual: (i) Names; (ii) Postal address information, other than town or city, State, and zip code; (iii) Telephone numbers; (iv) Fax numbers; (v) Electronic mail addresses; (vi) Social security numbers; (vii) Medical record numbers; (viii) Health plan beneficiary numbers; (ix) Account numbers; (x) Certificate/license numbers; (xi) Vehicle identifiers and serial numbers, including license plate numbers; (xii) Device identifiers and serial numbers; (xiii) Web Universal Resource Locators (URLs); (xiv) Internet Protocol (IP) address numbers; (xv) Biometric identifiers, including finger and voice prints; and (xvi) Full face photographic images and any comparable images." 45 C.F.R. § 164.514(e)(2).

[212] 45 C.F.R. § 164.514(e)(1).

implicating privacy interests of individuals and their PHI, some commentators have decried the effectiveness of HIPAA and the Privacy Rule saying, ". . . the HIPAA Privacy Rule does not protect privacy as well as it should, and that as currently implemented, the Privacy Rule impedes important health research."[213] Hardly a rousing endorsement for the mechanism designed to, among other things, improve health care outcomes in the United States.

Contrast these expansive exceptions and unique definitions regarding marketing under HIPAA with the GDPR. A data subject whose data falls under the GDPR can consent to the processing of that data, including for the purposes of marketing. However, generally, without consent, the processing of special categories of personal data (which includes data related to health) is prohibited.[214] Of the ten exceptions to the general processing prohibition noted in Article 9, none of those exceptions fits a purely marketing-related situation. Recital 47 of the GDPR does note that ". . . [t]he processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest."[215] Nowhere in the discussion of "legitimate interests" in Recital 47 is a marketing exception for health data carved out. Indeed, the Recital notes that ". . . the existence of a legitimate interest would need careful assessment including whether a data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place. The interests and fundamental rights of the data subject could in particular override the interest of the data controller where personal data are processed in circumstances where data subjects do not reasonably expect further processing."[216] Thus, unlike HIPAA, the GDPR is unlikely to consider the processing of health data for the purposes of marketing to be legitimate absent the specific consent of the data subject.

A significant shortcoming in HIPAA also appears in the context of enforcement. The statute provides for a number of different enforcement options, in the civil context and in instances in which criminal violations of the statute have occurred. Civil violations of the Privacy Rule and the Security Rule are managed by HHS through its Office of Civil Rights (OCR).[217] Criminal violations of HIPAA are handled by the Department of Justice after referral from the OCR. Other violations of HIPAA (non-Privacy Act, non-Security Act, and non-criminal) are managed by the Centers for Medicare and Medicaid Services (CMS) by delegation of authority from the Secretary of HHS.[218] What HIPAA lacks, however, is a provision which gives individuals a private right of action under the statute. Many have tried to find such a right in the law and have been rebuked.[219] Simply put, private actions to enforce HIPAA must rely upon state court remedies which implicate HIPAA and the rules established thereunder. For instance, in *Byrne v. Avery Center for Obstetrics and Gynecology PC*, 327 Conn. 540, (2018), the Connecticut Supreme Court concluded that a

---

[213] Sharyl J. Nass, Laura A. Levit, & Lawrence O. Gostin, Editors, IOM (Institute of Medicine), 2009, *Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health Through Research*, Washington, DC: THE NATIONAL ACADEMIES PRESS, 1-320, 15.

[214] General Data Protection Regulation, art. 9(1), *supra* note 12, at 38.

[215] General Data Protection Regulation, Recital 47, Id. at 9.

[216] Id.

[217] 42 U.S.C.1320d-5(a)(1).

[218] *See*, *supra* footnotes 97 & 98 for discussion of these delegations of authority.

[219] The cases indicating that no such right exists are legion: *Walker v. Gerald*, No. 05-6649, 2006 WL 1997635 (E.D. La. June 27, 2006); *Agee v. United States*, 72 Fed. Cl. 284 (2006); *Poli v. Mountain Valleys Health Ctrs., Inc.*, No. 2:05-2015-GEB-KJM, 2006 WL 83378 (E.D. Cal. Jan. 11, 2006); *Univ. of Colo. Hosp. Auth.*, 340 F. Supp. 2d 1142 (D. Colo. 2004); *Johnson v. Quander*, 370 F. Supp. 2d 79 (D.D.C. 2005); *Cassidy v. Nicolo*, No. 03-CV-6603-CJS, 2005 WL 3334523 (W.D.N.Y. Dec. 7, 2005); *Means v. Ind. Life & Accident Ins. Co.*, 963 F. Supp. 1131 (M.D. Ala. 1997); *Wright v. Combined Ins. Co. of Am.*, 959 F. Supp. 356 (N.D. Miss. 1997); *O'Donnell v. Blue Cross Blue Shield of Wyo.*, 173 F. Supp. 2d 1176 (D. Wyo. 2001).

plaintiff is owed a common law duty of confidentiality by virtue of the relationship he/she has with a physician, and consistent with its decision in 2014 involving the same parties, that "HIPAA and its implementing regulations may be utilized to inform the standard of care applicable to such claims arising from allegations of negligence in the disclosure of patients' medical records . . . ."[220] *Byrne* is significant in that it signals clearly that HIPAA does not preempt a plaintiff from pursuing a defendant for violations of HIPAA standards in an appropriate state court. It is far from conclusive at this point though that such a standard will be recognized in all state courts.

The GDPR, on the other hand, includes in Article 82 an "individual right to compensation and liability."[221] Specifically, the Regulation states: "Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered."[222] What is more, an aggrieved data subject has the ability to appoint another entity to represent his/her interests in pursuit of the Article 82 compensation claim.[223] The right to compensation is reiterated in Recital 146 of the Regulation wherein the authors of the GDPR spell out with specificity the obligations of controllers and processors for damages incurred by an aggrieved data subject.[224] Actions for compensation should be brought where the controller or the processor has an establishment as defined by the Regulation or in the courts of the Member State where the data subject lives.[225] It remains to be seen the extent to which aggrieved data subjects will avail themselves, either personally or through surrogates, of remedies for privacy violations under the GDPR, but the mechanisms are in place to cause controllers and data processors to heed to strictures of the Regulation vis-à-vis safeguarding the personal data of those who choose to allow its release into the Big Data world.

---

[220] *Byrne v. Avery Ctr. for Obstetrics & Gynecology, P.C.*, 314 Conn. 433, 459, 102 A.3d 32, 49 (2014).
[221] General Data Protection Regulation, art. 82, *supra* note 12, at 81.
[222] General Data Protection Regulation, art. 82(1), Id.
[223] "The data subject shall have the right to mandate a not-for-profit body, organisation or association which has been properly constituted in accordance with the law of a Member State, has statutory objectives which are in the public interest, and is active in the field of the protection of data subjects' rights and freedoms with regard to the protection of their personal data to lodge the complaint on his or her behalf, to exercise the rights referred to in Articles 77, 78 and 79 on his or her behalf, and to exercise the right to receive compensation referred to in Article 82 on his or her behalf where provided for by Member State law." General Data Protection Regulation, art. 80(1), Id.
[224] Recital 146 of the General Data Protection Regulation notes that: "The controller or processor should compensate any damage which a person may suffer as a result of processing that infringes this Regulation. [2]The controller or processor should be exempt from liability if it proves that it is not in any way responsible for the damage. [3]The concept of damage should be broadly interpreted in the light of the case-law of the Court of Justice in a manner which fully reflects the objectives of this Regulation. [4]This is without prejudice to any claims for damage deriving from the violation of other rules in Union or Member State law. [5]Processing that infringes this Regulation also includes processing that infringes delegated and implementing acts adopted in accordance with this Regulation and Member State law specifying rules of this Regulation. [6]Data subjects should receive full and effective compensation for the damage they have suffered. [7]Where controllers or processors are involved in the same processing, each controller or processor should be held liable for the entire damage. [8]However, where they are joined to the same judicial proceedings, in accordance with Member State law, compensation may be apportioned according to the responsibility of each controller or processor for the damage caused by the processing, provided that full and effective compensation of the data subject who suffered the damage is ensured. [9]Any controller or processor which has paid full compensation may subsequently institute recourse proceedings against other controllers or processors involved in the same processing." General Data Protection Regulation, Recital 146, Id. at 27.
[225] See General Data Protection Regulation, art. 79(2), Id. at 80.

V. Does the Structure of HIPAA Really Matter?

A focus on the protection of privacy under HIPAA is certainly a worthwhile endeavor by any objective standard of analysis. That the GDPR appears to give that protection more bite, in terms of enforcement, control of data by data subjects, and ultimately the right to have data removed from the data bases of controllers and processors, ought not to result in a mark of failure for HIPAA and the Privacy Rule. The challenge for health data protection in the United States going forward lies at the crossroads between Big Data and health data. As alluded to earlier, Big Data is a growing force in the burgeoning information and data world. Big Data in a nutshell is ". . . a more powerful version of knowledge discovery in databases or data mining, which has been defined as 'the nontrivial extraction of implicit, previously unknown, and potentially useful information from data'."[226] So-called "data mining" is the process by which Big Data becomes useful to commercial and non-commercial interests in the information age. It is aptly described as allowing ". . . firms to discover or infer previously unknown facts and patterns in a database. It relies not on causation but on correlations that arise from the application of non-public algorithms to large collections of data. Consequently, the newly discovered information is not only unintuitive and unpredictable, but also results from a fairly opaque process."[227] In less obtuse language, this means that through the process of data mining many of the protections built into the Privacy Rule (and to a lesser extent also built into the GDPR), are destined to be defeated or circumvented to the disadvantage of those most interested in the privacy of their health information data.

HIPAA and the GDPR both seek to create mechanisms which limit the ability of those not intended to receive data from obtaining health-related information (and other personal information in the case of the GDPR) and using it to their advantage or the advantage of their clients. The disadvantage to the HIPAA regime is that there exists a presumption that the information enters the Big Data world in the first place. All of its HIPAA's efforts to restrict the flow of that information come after the fact. On the other hand, the GDPR affords data subjects the opportunity to prevent their data from entering the Big Data stream in the first place. That kind of restriction is the only sure means of preventing health data from falling prey to the efforts of data mining specialists. And furthermore, the GDPR also enables data subjects to exercise their "right to be forgotten," a right which does not exist in HIPAA or its Privacy Rule.

The significance of health data entering electronic information steams cannot be lost. Big Data at its essence ". . . challenges the very foundations of [privacy protection laws] . . . by enabling re-identification of data subjects using non-personal data, which weakens anonymization as an effective strategy, thereby casting doubt on the fundamental distinction between personal data and non-personal data. [Big Data] also greatly exacerbates the dignitary harms associated with amassing information about a person—what Professor Daniel Solove refers to as aggregation. With its massive scale, continuous monitoring from multiple sources, and sophisticated analytic capabilities, [Big Data] makes aggregation more granular, more revealing, and more invasive."[228] Therefore, restricting the flow of personal health data at the front end of the process by which patients (data subjects) encounter the monolithic health care industry is the only truly effective means today of protecting privacy in that arena. And while the GDPR goes much further than

[226] *Big Data: The End of Privacy or a New Beginning, supra* note 194, at 76 (footnote omitted).
[227] Id.
[228] Id. at 77 (footnotes omitted).

HIPAA in both front-end control and after-the-fact data extraction by data subjects, Big Data still looms large as efforts to mine data systems continue to defeat privacy protections.[229]

To get a sense for how big Big Data is and the difficulty of aligning the privacy interests of individuals with the commercial and personal interests at stake with the "internet of things" (IoT),[230]one need only examine how quickly the IoT universe is growing. "One report estimates that the digital universe will grow nearly 20 times during 2015–25 to 180 zettabytes (or 180 x 1021 bytes – 180 trillion gigabytes). To put this number in perspective, a single zettabyte could store the equivalent of 2 billion years of music or Tolstoy's War and Peace 323 trillion times."[231] This growth puts into perspective HIPAA and the Privacy Rule, created in 1996 and 2000 respectively (with modifications to the latter in 2002). Stating the obvious, things have changed dramatically in the last 22 years, most particularly in the world of the IoT. While the GDPR as the successor to the DPD has been developed deliberately over the past decade with an eye toward adapting and changing to meet the times, HIPAA and the Privacy Rule appear to be fundamentally behind the times. And perhaps the fact that the United States treats private health information differently than other data is partially to blame for the shortcomings of HIPAA and the Privacy Rule. "By 2015, 25 billion devices are projected to be connected to the Internet; this number could double to 50 billion devices by the end of the decade. Simply going about our everyday lives creates a vast trail of 'digital exhaust' that can reveal much about us."[232] It is highly unlikely that digital exhaust was even contemplated when HIPAA and the Privacy Rule were conceived, whereas the authors of the GDPR were certainly cognizant of it and Big Data's emerging presence as that regulation was being developed. Indeed, the concepts of consent, transparency, erasure, and even the private right of action under the GDPR are much better suited to safeguard the privacy interests of individuals under that legal regime than the concepts embedded in HIPAA and the Privacy Rule.

So the structure of the mechanisms designed to protect health information do matter. In May 2014, the Executive Office of the President concluded as much in a White Paper dealing with the impacts of Big Data across a multitude of societal data points. Specifically in the health care arena,

---

[229] Rubinstein calls into question the ability of any privacy protection law to successfully stave off the efforts of Big Data to manipulate data that is in the electronic stream of information. Anonymization, for instance, which plays a role in the protection efforts of the Privacy Rule (see 45 C.F.R. § 164.514 for the Privacy Rule's discussion of de-identification of PHI), has proven to be a less than effective means of protecting personal health information, and data minimization (the belief that controlling the amount of information that flows into electronic data streams) ". . . is inimical to the underlying thrust of [Big Data], which discovers new correlations by applying sophisticated analytic techniques to massive data collection, and seeks to do so free of any *ex ante* restrictions. Because data minimization requirements would cripple Big Data and its associated economic and social benefits, regulators should expect to see this requirement largely observed in the breach." Id. at 78 (footnotes omitted).

[230] The term "the internet of things" was first used by Kevin Ashton, a technologist and co-founder of the Auto-ID Center at the Massachusetts Institute of Technology, in 1999. It is ". . . the concept of basically connecting any device with an on and off switch to the Internet (and/or to each other). This includes everything from cellphones, coffee makers, washing machines, headphones, lamps, wearable devices and almost anything else you can think of. This also applies to components of machines, for example a jet engine of an airplane or the drill of an oil rig." Jacob Morgan, *A Simple Explanation of the Internet of Things,* FORBES, May 13, 2014, https://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/#46546b971d09. Succinctly, "[t]he IoT is a giant network of connected 'things' (which also includes people). The relationship will be between people-people, people-things, and things-things." Id.

[231] Christopher Smart, *Regulating the Data that Drive 21st-Century Economic Growth The Looming Transatlantic Battle*, Research Paper for the US and Americas Programme, CHATHAM HOUSE, June 2017, at. 5, https://www.chathamhouse.org/sites/files/chathamhouse/publications/research/2017-06-28-regulating-data-economic-growth.pdf

[232] Joseph Jerome, *Symposium: Big Data: Catalyst for a Privacy Conversation*, 43 Ind. L. Rev. 213, 215, 2014.

and recognizing the preference in the United States for sector-specific laws and implementing rules regarding data protection and privacy, the authors concluded that "[t]he complexity of complying with numerous laws when data is combined from various sources raises the potential need to carve out special data use authorities for the health care industry if it is to realize the potential health gains and cost reductions that could come from big data analytics. At the same time, health organizations interact with many organizations that are not regulated under any of these laws. In the resulting ecosystem, personal health information of various kinds is shared with an array of firms, and even sold by state governments, in ways that might not accord with consumer expectations of the privacy of their medical data."[233] Unfortunately, in the United States these results occur despite the specific protections of the health data privacy law and rules.

The key distinction between HIPAA and the GDPR vis-à-vis personal health data is the mechanism used to deal with the subject. A casual reader of HIPAA will readily conclude that the statute and its implementing rules emphasize control of disclosure of information already collected. "Although frequently described in terms of 'privacy' and 'privacy law,' the legal protections applied to patient health information by the common law, state statutes, or the HIPAA federal standards have very little to do with either."[234] Patients effectively lose control of their information once disclosed and the obligations of those to whom that information is disclosed has everything to do with confidentiality and little to do with privacy. Today ". . . the modern law of health 'privacy' resides in the far narrower, disclosure-centric doctrine captured in cases, statutes, and regulations dealing with breach of confidence. A patient exercises his right of privacy (as recognized by the ethical domain) when he chooses to provide information to his physician (albeit a 'right' that is illusory if it is a condition of treatment). Thereafter, dissemination of that information by the physician is limited by ethical and legal standards of confidence. Today, when courts and regulators speak of medical 'privacy' they are usually in error, mislabeling obligations of 'confidentiality.'"[235] This concept is significant because the positioning of data in a place where it is available makes the protections afforded by HIPAA less relevant. The law's and the implementing regulations' relevance is diminished because ". . . some traditional health information circulates in what may be termed a HIPAA-free zone. Further, the very concept of health sector specific regulation is flawed because health related or medically inflected data frequently circulates outside of the traditionally recognized health care sector."[236] This, then, makes true efforts to restrict data collection, like those of the GDPR, far more effective than efforts to control the dissemination of data after the fact, as in HIPAA and its implementing rules. In the end, legal structure matters a great deal.

VI. Conclusion

HIPAA and its Privacy Rule have been noble efforts to enhance the health care of patients in the United States essentially by modernizing the methods of health care delivery. In order to achieve that enhancement, health information technology improvements have been

[233] Executive Office of the President, *Big Data: Seizing Opportunities, Preserving Values*, (2014) at 23, https://obamawhitehouse.archives.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf, July 30, 2018.
[234] Testimony of Nicholas P. Terry Before the National Committee on Vital Health Statistics (NCVHS), Subcommittee on Privacy, Hearings on Privacy and Health Information Technology, *Electronic Health Records and Privacy*, August 16-17, 2005, https://www.ncvhs.hhs.gov/wp-content/uploads/2014/05/050816p1.pdf, at 6.
[235] Id.
[236] *See*, *Protecting Patient Privacy in the Age of Big Data*, *supra* note 16, at 3.

institutionalized (most notably through the promotion of and development efforts behind electronic medical records). The protection of the privacy interests of patients under HIPAA, however, has been subordinated to the interests of those who believe that disclosure of information is a necessary precursor to health care improvement efforts. To give consideration to patient privacy interests in the United States, the notion of healthcare information exceptionalism has become the model for patient privacy protection. The European Union has approached patient privacy interests differently. The now fully implemented GDPR treats private health information as it treats other data, with an emphasis on *allowing* a data subject to prevent the disclosure of the information in the first place. And by preventing that information from making its way into electronic data bases, data subjects are more effectively in control of their privacy interests and less dependent upon the actions of others to prevent the further disclosure and use of patient data. Through efforts at transparency, consent, erasure, and effective enforcement, the European Union has sought to impose a privacy model with some fidelity. HIPAA and its Privacy Rule will need to grow and mature as long as the confidentiality model prevails in the realm of private health data protection. As true today as it was six years ago when written, "[a]s EMRs and other HIT initiatives continue to generate vast pools of patient data and data analysis is hyped as the savior of health care, the necessity for a reformed privacy model will increase."[237] And the flaws that exist within HIPAA and its Privacy Rule demonstrate that the need for such reform is now if patient privacy is genuinely a concern for those interested in continuing to improve the American health care system.

[237] Id. at 30.