The HIPAA Privacy Rule and the EU GDPR: Illustrative Comparisons

*Stacey A. Tovino**

INTRODUCTION

On August 21, 1996, President Clinton signed the Health Insurance Portability and Accountability Act of 1996 (HIPAA) into law.[1] Over the past two decades, the federal Department of Health and Human Services (HHS) has published several sets of rules[2] implementing the Administrative Simplification provisions within HIPAA[3] as well as the Health Information

* Lehman Professor of Law and Director, Health Law Program, William S. Boyd School of Law, University of Nevada, Las Vegas. I thank Daniel Hamilton, Dean, William S. Boyd School of Law, for his generous financial support of this research project and Emma Babler, Research Librarian, Wiener-Rogers Law Library, for locating many of the sources referenced in this Article. Finally, I thank the organizers, participants, and attendees of the *Seton Hall Law Review* Symposium ("The New EU Data Protection Regulation: Transnational Enforcement and Its Effects on US Businesses") for their comments, questions, and ideas regarding this Article.

[1] Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191, 110 Stat. 1936 (1996).

[2] *See infra* notes 20–35 (referencing several sets of proposed, interim final, and final rules).

[3] HIPAA §§ 261–64 [hereinafter Administrative Simplification Provisions].

Technology for Economic and Clinical (HITECH) Act within the American Recovery and Reinvestment Act (ARRA), signed into law by President Obama on February 17, 2009.[4] These rules include a final rule governing the use and disclosure of protected health information by covered entities and their business associates (Privacy Rule).[5]

On January 25, 2012, the European Commission proposed to protect individuals with regard to the processing of personal data and the free movement of such data.[6] The European Union's (EU's) final General Data Protection Regulation (GDPR) was published in the *Official Journal of the European Union* on May 4, 2016,[7] and will apply beginning May 25, 2018.[8]

This Article compares and contrasts three illustrative concepts and rights in the Privacy Rule and/or the GDPR, including the concepts of authorization and consent, the rights of amendment and rectification, and the right to erasure. Identified similarities reflect the core values of HHS and the EU with respect to maintaining the confidentiality and privacy of personal data and protected health information, respectively. Identified differences reflect the Privacy Rule's original, narrow focus on health industry participants and individually identifiable health information compared to the GDPR's broad focus on data controllers and personal data. Other differences reflect, perhaps, the U.S. health care industry's significant experience with heavy regulation, the health care industry's willingness to accept additional regulation in furtherance of the course of business, and specific concerns about the ways in which employers, insurers, and other institutions have used individuals' health information to their detriment.

This Article proceeds as follows: Part I summarizes the history of the Privacy Rule, including the many proposed rules, interim final rules, final rules, guidance documents, and resolution agreements published by HHS.[9] Part II reviews the Privacy Rule's theory of and approach to health information confidentiality, including the Privacy Rule's three rules of

---

[4] *See* American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, § 13001–24, 123 Stat. 115 (2009) (containing the Health Information Technology for Economic and Clinical Health (HITECH) Act).

[5] Privacy of Individually Identifiable Health Information, 45 C.F.R. §§ 164.500–164.534 (2016).

[6] Commission of the European Communities, Proposal for a Regulation of the European Parliament and of 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), COM (2012) 11 final (Jan. 2012).

[7] Council 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), 2016 O.J. (L 119) 1 [hereinafter EU GDPR].

[8] *Id*. art. 99, ¶ 2 ("It shall apply from 25 May 2018.").

[9] *See infra* Part I.

individual permission, one of which must be satisfied before a covered entity or business associate internally uses or externally discloses an individual's protected health information.[10] Part III compares and contrasts the concepts of authorization and consent under the Privacy Rule and the GDPR, respectively.[11] Part IV focuses on the rights of amendment and rectification in the Privacy Rule and GDPR, respectively.[12] Part V examines the GDPR's right to erasure, also known as the right to be forgotten.[13] This Article concludes by assessing the similarities and differences between these two regulations in these three contexts and explaining the differences with reference to principles of health law that may not broadly apply to non-health industries.

I. HISTORY OF THE HIPAA PRIVACY RULE

As signed into law by President Clinton on August 21, 1996, HIPAA had several purposes, including improving portability and continuity of health insurance coverage in the individual and group markets, combating health care fraud and abuse, promoting the use of medical savings accounts, improving access to long-term care services and insurance coverage, and simplifying the administration of health insurance.[14] The Administrative Simplification Provisions, codified at Subtitle F of Title II of HIPAA,[15] directed HHS to issue regulations protecting the privacy[16] of individually

[10] *See infra* Part II.

[11] *See infra* Part III.

[12] *See infra* Part IV.

[13] *See infra* Part V.

[14] *See* Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191, 110 Stat. 1936, at Preface (1996) ("An Act [t]o amend the Internal Revenue Code of 1986 to improve portability and continuity of health insurance coverage in the group and individual markets, to combat waste, fraud, and abuse in health insurance and health care delivery, to promote the use of medical savings accounts, to improve access to long-term care services and coverage, to simplify the administration of health insurance, and for other purposes."). The Author has reviewed the history of and the regulatory approach taken in the Privacy Rule in a number of prior scholarly articles. *See, e.g.*, Stacey A. Tovino, *Hospital Chaplaincy under the HIPAA Privacy Rule: Health Care or "Just Visiting the Sick?"*, 2 IND. HEALTH L. REV. 51 (2005); Stacey A. Tovino, *Medical Privacy*, *in* GOVERNING AMERICA: MAJOR DECISIONS OF FEDERAL, STATE, AND LOCAL GOVERNMENTS FROM 1789 TO PRESENT (Paul Quirk & William Cunion eds., 2011); Stacey A. Tovino, *HIPAA Privacy for Physicians*, 17 PATHOLOGY CASE REV. 160 (2012); Stacey A. Tovino, *Gone Too Far: Federal Regulation of Health Care Attorneys*, 91 OR. L. REV. 813 (2013); Stacey A. Tovino, *Silence Is Golden . . . Except in Health Care Philanthropy*, 48 U. RICH. L. REV. 1157 (2014); Stacey A. Tovino, *Complying with the HIPAA Privacy Rule: Problems and Perspectives*, 1 LOY. U. CHI. J. REG. COMPLIANCE (2016); Stacey A. Tovino, *Teaching the HIPAA Privacy Rule*, 61 ST. LOUIS U. L.J. (forthcoming 2017). With technical and conforming changes, much of Parts I and II of this Article are reprinted from these prior scholarly articles with the Author's permission.

[15] *See* Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191, §§ 261–64, 110 Stat. 1936 (1996).

[16] Elsewhere, the Author defined and distinguished the concepts of privacy and

identifiable health information if Congress failed to enact comprehensive privacy legislation within three years of HIPAA's enactment.[17] When Congress failed to enact privacy legislation by its deadline, HHS incurred the duty to adopt privacy regulations.[18] The original HIPAA statute clarified, however, that any privacy regulations adopted by HHS must be made applicable only to three classes of individuals and institutions: (1) health plans; (2) health care clearinghouses; and (3) health care providers who transmit health information in electronic form in connection with certain standard transactions (collectively, covered entities).[19]

HHS responded. On November 3, 1999,[20] and December 28, 2000,[21] HHS issued a proposed and final privacy rule ("Privacy Rule") regulating covered entities' uses and disclosures of protected health information (PHI). On March 27, 2002,[22] and August 14, 2002,[23] HHS issued proposed and final

confidentiality for purposes of discussions addressing the legal responsibilities of health industry participants. *See, e.g.*, Stacey A. Tovino, *Functional Magnetic Resonance Information: A Case for Neuro Exceptionalism?*, 34 FLA. ST. U. L. REV. 415, Parts III(J), IV & V (2007). This Article uses the same definitions and distinctions. Privacy refers to an individual's interest in avoiding the unwanted collection by a third party of health or other information about the individual. *Id*. Confidentiality, on the other hand, refers to the obligation of a health industry participant to prevent the unauthorized or otherwise inappropriate use or disclosure of voluntarily given and appropriately gathered health and other information relating to an individual. *Id*. Although the Privacy Rule actually is a health information confidentiality rule—because it sets limits on how health care providers and other covered entities can use and disclose appropriately gathered PHI—the Author uses the phrase "Privacy Rule" and the word "privacy" in this Article because these are the phrases and words selected by HHS and used by the public for the rule and the concepts addressed therein. *See, e.g.*, *Health Information Privacy*, U.S. DEP'T HEALTH & HUM. SERVS., https://www.hhs.gov /hipaa/ (last visited Feb. 13, 2017).

[17] HIPAA § 264 ("If legislation governing standards with respect to the privacy of individually identifiable health information . . . 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 . . .").

[18] *See id*.

[19] *Id*. § 262(a) ("Any standard adopted under this part shall apply, in whole or in part, to the following persons: '(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 referred to in section 1173(a)(1).'"). *See* Standards for Privacy of Individually Identifiable Health Information, 64 Fed. Reg. at 59,918. *See generally* Standards for Privacy of Individually Identifiable Health Information, 64 Fed. Reg. 59,918 & 59,924 (proposed Nov. 3, 1999) (to be codified at 45 C.F.R. pts. 160–64) (explaining that HHS did not directly regulate any entity that was not a covered entity because it did not have the statutory authority to do so).

[20] *Id.*

[21] Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,462 (Dec. 28, 2000).

[22] Standards for Privacy of Individually Identifiable Health Information, 67 Fed. Reg. 14,776 (proposed Mar. 27, 2002) (to be codified at 45 C.F.R. pts. 160–64).

[23] Standards for Privacy of Individually Identifiable Health Information, 67 Fed. Reg. 53,182 (Aug. 14, 2002).

modifications to the Privacy Rule. With the exception of technical corrections and conforming amendments,[24] these rules as reconciled remained largely unchanged between 2002 and 2009.

The nature and scope of the legal duties of confidentiality that applied to covered entities and their business associates (BAs)[25] changed significantly eight years ago. On February 17, 2009, President Obama signed ARRA into law.[26] Division A, Title XIII of ARRA, better known as HITECH, contained certain provisions requiring HHS to modify some of the information use and disclosure requirements and definitions set forth in the Privacy Rule, adopt new breach notification rules, and amend the civil penalty amounts that may be imposed on covered entities and BAs who violate the Privacy Rule.[27]

Since ARRA's enactment, HHS has issued several sets of proposed rules, interim final rules, final rules, and technical corrections both implementing HITECH's required changes to the Privacy Rule as well as responding to other national health information confidentiality concerns. On August 24, 2009, for example, HHS released an interim final rule implementing HITECH's new breach notification requirements.[28] On

[24] *See, e.g.*, Standards for Privacy of Individually Identifiable Health Information, Correction of Effective and Compliance Dates, 66 Fed. Reg. 12,434 (Feb. 26, 2001); Technical Corrections to the Standards for Privacy of Individually Identifiable Health Information Published December 28, 2000, 65 Fed. Reg. 82,944 (Dec. 29, 2000).

[25] Business associates (BAs) are defined to include individual and institutions who: (1) on behalf of a covered entity, but other than in the capacity of a member of the workforce of a covered entity, create, receive, maintain, or transmit PHI for a function or activity regulated by the HIPAA Privacy Rule; and (2) provide, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for the covered entity. *See* Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules, 78 Fed. Reg. 5,566, 5,688 (Jan. 25, 2013) (adopting 45 C.F.R. § 160.103 and providing a new definition of business associate).

[26] *See* American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, § 13001–24, 123 Stat. 115 (2009).

[27] *Id.* Elsewhere, the Author critiqued HITECH's imposition of confidentiality requirements directly on BAs and proposed statutory and regulatory changes to HITECH and the HIPAA Privacy Rule, respectively, that would except a class of BAs, including outside counsel, from the confidentiality obligations imposed on other BAs. *See* Stacey A. Tovino, *Gone Too Far: Federal Regulation of Health Care Attorneys*, 91 OR. L. REV. 813, 813–67 (2013). Elsewhere, the Author also critiqued HITECH's loosening of the regulatory provision that governs covered entities' uses and disclosures of protected health information for fundraising purposes. *See* Stacey A. Tovino, *Silence Is Golden . . . Except in Health Care Philanthropy*, 48 U. RICH. L. REV. 1157 (2014). This Article builds on the Author's earlier work in a new dimension; that is, by comparing illustrative provisions in the HIPAA Privacy Rule to the EU GDPR.

[28] Breach Notification for Unsecured Protected Health Information, 74 Fed. Reg. 42,740 (Aug. 24, 2009).

October 30, 2009, HHS released an interim final rule implementing HITECH's strengthened enforcement provisions, including strengthened civil monetary penalties that the federal Office for Civil Rights (OCR) may, for the first time since the enactment of the HIPAA statute, impose directly on BAs who fail to maintain the confidentiality of PHI.[29] On May 31, 2011, HHS released a proposed rule that would modify the HIPAA Privacy Rule's accounting of disclosures requirement.[30] On January 25, 2013, HHS released a final rule modifying the HIPAA Privacy, Security, Breach Notification, and Enforcement Rules in accordance with HITECH ("Final Regulations").[31] On June 7, 2013, HHS released technical corrections to the Final Regulations.[32] On September 16, 2013, HHS released a Model Notice of Privacy Practices designed to assist covered entities in complying with the Final Regulations.[33] On February 6, 2014, HHS released a final rule modifying the Privacy Rule to provide individuals with a right to receive their laboratory test results directly from their testing laboratories.[34] Most recently, on January 6, 2016, HHS released a final rule that modifies the Privacy Rule and permits certain covered entities to disclose PHI to the National Instant Criminal Background Check System.[35]

As of this writing, HHS has also released fifty-one resolution agreements and notices of final determination.[36] In these agreements and notices, covered entities resolve to comply with the Privacy Rule, report to HHS regarding its compliance with the Privacy Rule, pay a resolution amount, and/or pay a civil money penalty.[37] For example, on February 1,

[29] HIPAA Administrative Simplification: Enforcement, 74 Fed. Reg. 56,123 (Oct. 30, 2009).

[30] HIPAA Privacy Rule Accounting of Disclosures Under the Health Information Technology for Economic and Clinical Health Act, 76 Fed. Reg. 31,426 (proposed May 31, 2011) (to be codified at 45 C.F.R. pt. 164).

[31] *See* Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules, 78 Fed. Reg. 5566, 5566 (Jan. 25, 2013).

[32] *See* Technical Corrections to the HIPAA Privacy, Security, and Enforcement Rules, 78 Fed. Reg. 34,264, 34,266 (June 7, 2013).

[33] *Model Notices of Privacy Practices*, U.S. DEP'T HEALTH & HUMAN SERVS., http://www.hhs.gov/hipaa/for-professionals/privacy/guidance/model-notices-privacy-practices/ (last visited Apr. 17, 2017).

[34] CLIA Program and HIPAA Privacy Rule; Patients' Access to Test Reports, 79 Fed. Reg. 7290 (Feb. 6, 2014).

[35] Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule and the National Instant Criminal Background Check System (NICS), 81 Fed. Reg. 382, 396 (Jan. 6, 2016).

[36] *See Resolution Agreements*, U.S. DEP'T HEALTH & HUMAN SERVS., http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/index.html (last visited Apr. 17, 2017).

[37] *See id*.

2017, HHS issued a press release announcing a recent notice of final determination, which imposed a civil money penalty (CMP) on Children's Medical Center of Dallas ("Children's").[38] As background, a workforce member of Children's lost an unencrypted, non-password-protected BlackBerry device that contained the PHI of approximately 3,800 individuals at the Dallas/Fort Worth International Airport.[39] In addition, an unencrypted laptop containing the PHI of 2,462 individuals was stolen from Children's premises.[40] Although Children's had implemented some physical safeguards to protect its laptop storage area, Children's admitted it provided access to the area to workforce personnel not authorized to access PHI.[41] By letter dated January 18, 2017, HHS imposed a $3,217,000.00 CMP on Children's for these two health information confidentiality breaches as well as several other Privacy Rule violations.[42]

II. THE HIPAA PRIVACY RULE'S THEORY OF AND APPROACH TO HEALTH INFORMATION CONFIDENTIALITY

A brief summary of the Privacy Rule's theory and approach to health information confidentiality is necessary before proceeding to Part III, which compares and contrasts the concepts of authorization and consent under the Privacy Rule and the GDPR, respectively.

The Privacy Rule's goal is to balance the interest of individuals in maintaining the confidentiality of their health information with the interests of society in obtaining, using, and disclosing health information to carry out a variety of public and private activities.[43] To this end, the Privacy Rule regulates covered entities' and BAs' uses of, disclosures of, and requests for individually identifiable health information (IIHI)[44] to the extent such

---

[38] Press Release, U.S. Dep't Health & Hum. Servs., Lack of Timely Action Risks Security and Costs Money (Feb. 1, 2017).

[39] *Id*.

[40] *Id*.

[41] *Id*.

[42] Letter from Jocelyn Samuels, Dir., Off. C.R., Dep't Health & Hum. Servs., to Mr. David Barry, Pres., Sys. Clinical Operations, Children's Med. Ctr. 1 (Jan. 18, 2017).

[43] *See* Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,462, 82,464 (Dec. 28, 2000) ("The rule seeks to balance the needs of the individual with the needs of the society."); *id*. at 82,468 ("The task of society and its government is to create a balance in which the individual's needs and rights are balanced against the needs and rights of society as a whole."); *id*. at 82,472 ("The need to balance these competing interests—the necessity of protecting privacy and the public interest in using identifiable health information for vital public and private purposes—in a way that is also workable for the varied stakeholders causes much of the complexity in the rule.").

[44] The Privacy Rule defines "individually identifiable health information" (IIHI) as "information that is a subset of health information, including demographic information collected from an individual, and: (1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and (2) Relates to the past, present, or future

information does not constitute: (1) an education record protected under the Family Educational Rights and Privacy Act of 1974 (FERPA); (2) a student treatment record excepted from protection under FERPA; (3) an employment record held by a covered entity in its role as an employer; or (4) individually identifiable health information regarding a person who has been deceased for more than fifty years.[45] The Privacy Rule calls the subset of IIHI described in the previous sentence "protected health information."[46]

Before using or disclosing PHI, the Privacy Rule requires covered entities and BAs to adhere to one of three different rules depending on the purpose of the information use or disclosure.[47] These rules reflect HHS's desire to appropriately balance the interest of individuals in maintaining the confidentiality of their PHI with a wide range of societal interests in obtaining, using, or disclosing PHI, some of which may have greater societal importance and value than others.[48]

The first rule allows covered entities and BAs to use and disclose PHI with no prior permission from the individual who is the subject of the PHI—but only in certain situations. That is, covered entities may freely use and disclose PHI without any form of prior permission in order to carry out their

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) That identifies the individual; or (ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual." General Administrative Requirements, 45 C.F.R. § 160.103 (2016).

[45] *Id*. (defining "protected health information").

[46] *Id*. (using the phrase "protected health information").

[47] Standard Unique Health Identifier for Health Plans, 45 C.F.R. §§ 164.502–164.514 (2016) (setting forth the use and disclosure requirements applicable to covered entities and business associates).

[48] *See supra* text accompanying note 43.

own treatment,[49] payment,[50] and health care operations[51] activities,[52] as well as certain public benefit activities.[53]

As an example of this first rule, a covered general practitioner (GP) who wishes to consult with a specialist to treat a patient may disclose PHI to the specialist, and the Privacy Rule does not require the patient to give the GP prior authorization for the disclosure.[54] Likewise, a covered hospital that treats a patient may send a bill to the patient's insurer to obtain payment for hospital services rendered without the patient's prior authorization.[55] Similarly, a teaching physician employed by a covered academic medical center may involve medical students, interns, residents, and fellows in patient care, without prior authorization from the patients who are receiving such care, to enable the students and residents to learn to practice medicine.[56] Furthermore, a covered entity that is required by state or other law to disclose PHI to another individual or entity may do so without patient authorization.[57]

---

[49] The Privacy Rule defines "treatment" as:

> [T]he provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another.

Privacy of Individually Identifiable Health Information, 45 C.F.R. § 164.501 (2016).

[50] The Privacy Rule defines "payment" as the activities "undertaken by a health plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan" as well as the activities of a "health care provider or health plan to obtain or provide reimbursement for the provision of health care." *Id*.

[51] The Privacy Rule defines "health care operations" with respect to a list of activities that are related to a covered entity's covered functions. *See id*. (defining health care operations). These activities include, but are not limited to, conducting quality assessment and improvement activities, conducting training programs in which medical and other health care students learn to practice health care under supervision, and arranging for the provision of legal services. *See id*.

[52] *See id*. § 164.506(c)(1) (permitting a covered entity to use or disclose PHI for its own treatment, payment, or health care operations).

[53] Covered entities may use and disclose PHI for twelve different public policy activities without the prior written authorization of the individual who is the subject of the information. *See id*. § 164.512(a)–(l). These public policy activities include, but are not limited to, uses and disclosures required by law, uses and disclosures for public health activities, disclosures for law enforcement activities, uses and disclosures for research, and disclosures for workers' compensation activities. *See id*. § 164.512(a), (c), (b), (f), (i) & (l).

[54] *See id*. § 164.501 (defining "treatment" to include "consultations between health care providers relating to a patient").

[55] *See* Privacy of Individually Identifiable Health Information, 45 C.F.R. § 164.501 (2016) (defining "payment" to include "the activities undertaken by a health care provider . . . to obtain . . . reimbursement for the provision of health care"); *id*. § 164.506(c)(1) (permitting a covered entity to disclose PHI for its own payment activities).

[56] *See id.* § 164.501(c)(1) (defining "health care operations" to include "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").

[57] *See id.* § 164.512(a)(1) (allowing covered entities to "use or disclose protected health

By final illustrative example, a covered entity may disclose a patient's PHI to a law enforcement officer in certain situations, including when the covered entity suspects that the death of the patient may have resulted from criminal conduct.[58] The theory behind these permitted information uses and disclosures is that treating patients, allowing health care providers to obtain reimbursement for providing health care, training medical students and residents, complying with state law, and alerting law enforcement officers to the suspicion of criminal activity outweigh an individual's interest in maintaining complete confidentiality of his or her PHI.

The first rule requires no prior authorization from the individual who is the subject of the information before the information use or disclosure may occur.[59] Under the second rule, a covered entity may use and disclose an individual's PHI for certain activities, but only if the individual is informed in advance of the use or disclosure and has the opportunity to agree to, prohibit, or restrict the use or disclosure.[60] Because the Privacy Rule allows the covered entity to orally inform the individual of (and capture an oral agreement or oral objection to) a use or disclosure permitted by these provisions, this second rule is sometimes referred to as the "oral permission rule," although a more practical written permission also will suffice.

Under the second rule, a covered entity may conduct five sets of information uses and disclosures once the individual who is the subject of the information has been notified and has either agreed or not objected to the information use or disclosure.[61] These five sets of information uses and disclosures include: (1) certain uses and disclosures of directory information, such as name, location, general condition, and religious affiliation;[62] (2) certain uses and disclosures that would allow other persons to be involved in a patient's care or payment for care;[63] (3) certain uses and disclosures that would help notify, or assist in the notification of, family members, personal representatives, and other persons responsible for the care of the individual's location, general condition, or death;[64] (4) certain uses and disclosures for disaster relief purposes;[65] and (5) certain disclosures to family members and other persons who were involved in the individual's care or payment for

information to the extent that such use or disclosure is required by law and the use or disclosure complies with and is limited to the relevant requirements of such law").

58 *See id*. § 164.512(f)(4).

59 *See supra* notes 54–58 and accompanying text.

60 *See* 45 C.F.R. § 164.510.

61 *See* Privacy of Individually Identifiable Health Information, 45 C.F.R. § 164.510 (2016).

62 *See id.* § 164.510(a).

63 *See id.* § 164.510(b)(1)(i).

64 *See id*. § 164.510(b)(1)(ii).

65 *See id*. § 164.510(b)(4).

health care prior to the individual's death of PHI that is relevant to that person's involvement.[66]

As an illustration of the second rule, the hospital room number and general condition of a patient (e.g., "good," "fair," "poor," "stable") who has given his or her permission or who has not expressed an objection may be disclosed to a visitor who requests directory information about that patient.[67] Likewise, a woman in labor who wishes her partner to be present for her labor and delivery may orally give her permission for her health care providers to involve her partner in her care.[68]

The theory behind requiring at least oral permission for these information uses and disclosures is that the patient has an interest in maintaining the confidentiality of his or her PHI; however, the patient also may have an interest in being visited in the hospital, in obtaining assistance with the patient's health care or payment for health care, and being assisted during a disaster. In addition, the patient's family also may have an interest in visiting the patient in the hospital, assisting the patient with his or her health care and financial needs, and obtaining assistance during a disaster. The required oral permission reflects the individual's interest in maintaining the confidentiality of his or her health information, but the lack of a requirement for a formal written authorization reflects HHS's desire to make it easy for the individual to ask for or agree to receive help.

III. THE CONCEPTS OF AUTHORIZATION AND CONSENT

The third rule—a default rule—requires covered entities and BAs to obtain the prior written authorization from the individual who is the subject of the PHI before using or disclosing the individual's PHI in any situation that does not fit under the first or second rule.[69] Stated another way, in the event that a covered entity or BA would like to use or disclose PHI for a purpose (1) that is not treatment, payment, or health care operations; (2) that does not fall within one of twelve public benefit exceptions; (3) that is not allowed with oral permission or without an objection; and (4) that is not otherwise permitted or required by the Privacy Rule, the covered entity must obtain the prior written authorization from the individual who is the subject of the information.[70]

---

66 *See* Privacy of Individually Identifiable Health Information, 45 C.F.R. § 164.501(b)(5) (2016).

67 *See id.* § 164.510(a)(1), (2).

68 *See id.* § 164.510(b)(1)(i).

69 *See id.* § 164.508(a)(1).

70 *See id.* § 164.508(a)(1).

A. *Definitions, Conceptualizations, Content, and Format*

The Privacy Rule does not formally define "authorization" in a definition regulation; instead, the concept of authorization simply exists as a default rule. The Privacy Rule does, however, specify the form of the authorization required by the third rule, including certain elements and statements that are designed to place the individual on notice of how the individual's PHI will be used or disclosed.[71] These elements and statements include:

> (i) [a] description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion; (ii) [t]he name or other specific identification of the person(s), or class of persons, authorized to make the requested use or disclosure; (iii) [t]he name or other specific identification of the person(s), or class of persons, to whom the covered entity may make the requested use or disclosure; (iv) [a] description of each purpose of the requested use or disclosure; (v) [a]n expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure; (vi) [s]ignature of the individual and date.[72]

The regulations also require: (i) a statement regarding the individual's right to revoke the authorization in writing together with the exceptions to the right to revoke; (ii) a statement regarding the ability or inability of the covered entity or BA "to condition treatment, payment, enrollment, or eligibility for benefits on the authorization;" and (iii) a statement regarding "the potential for information disclosed pursuant to the authorization to be subject to redisclosure by the recipient and no longer be protected by [the Privacy Rule.]"[73] HIPAA-compliant authorization forms also must be written in plain language.[74]

The high level of prior individual permission required by HIPAA's authorization form reflects the value HHS places on an individual's interest in maintaining the confidentiality of his or her PHI compared to other societal interests that are far removed from the core functions of covered entities and BAs. Some of the societal interests include a health care provider's interest in selling the patient's information to a tabloid magazine or a health plan's interest in disclosing the patient's information to a marketing company to allow the company to market its products and services to the individual.[75]

---

[71] *See id*. § 164.508(c)(1), (2).

[72] Privacy of Individually Identifiable Health Information, 45 C.F.R. § 164.508(c)(1) (2016) (listing six core elements).

[73] *Id.* § 164.508(c)(2) (listing three required statements).

[74] *Id*. § 164.508(c)(3).

[75] *See* Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,462, 82,514 (Dec. 28, 2000) ("[C]overed entities must obtain the individual's

Unlike the Privacy Rule, which does not specifically define "authorization," the GDPR defines "consent" as any "freely given, specific, informed and unambiguous indication of the data subject's . . . agreement to the processing of personal data relating to him or her."[76] Under the GDPR, consent is less of a default concept and more of a primary requirement with acceptable alternatives. That is, under the GDPR, the processing of personal data shall be lawful only if and to the extent one of the following applies:

> *(a) the data subject has given consent* . . .; (b) processing is necessary 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; (c) processing is necessary for compliance with a legal obligation to which the controller is subject; (d) processing is necessary in order to protect the vital interests of the data subject or of another natural person; (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; or (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.[77]

With respect to the content of the consent, the GDPR only requires that the data subject be made aware of "the fact that and the extent to which consent is given."[78] For the subject's consent to be considered informed, the GDPR also requires the data subject to be aware of, at least, "the identity of the controller and the purposes of the processing for which the personal data are intended."[79]

According to the GDPR, a consent that is created by the data controller should be provided to the subject "in an intelligible and easily accessible form, using clear and plain language and it should not contain unfair terms."[80] In terms of format, a consent for the processing of personal data—not data concerning health—can be a written statement, as is required by the Privacy Rule for the use or disclosure of PHI under the third rule of individual permission; but it could also be satisfied by an electronic ticking of a box or

authorization before using or disclosing protected health information for marketing purposes.").

[76] EU GDPR, *supra* note 7, art. 4(11).

[77] *Id*. art. 6(1) (emphasis added).

[78] *Id*. pmbl., ¶ 42.

[79] *Id*.

[80] *Id*.

even an oral statement indicating agreement to personal data processing.[81] In comparison, and as discussed in Part II, oral agreement to the use and disclosure of PHI under the Privacy Rule is only permitted in the context of: (1) disclosures of directory information; (2) disclosures to persons involved in patients' care and payment for care; (3) disclosures for notification purposes; (4) disclosures for disaster relief purposes; and (5) disclosures when the individual is deceased.[82]

Notwithstanding the GDPR's loose conceptualization of and format for the consent for the processing of personal data, the GDPR expressly prohibits the processing of personal data concerning health unless the data subject has given "explicit" consent or an exception applies.[83] In addition, the GDPR does allow Member States to maintain or introduce further limitations on the processing of health data,[84] much in the same way states in the U.S. are permitted to have more stringent laws protecting health information confidentiality relative to the Privacy Rule's federal floor.[85]

B. *Conditioning*

To ensure that an individual's prior written authorization for the use or disclosure of his or her PHI under the Privacy Rule is freely given, the Privacy Rule also contains a general "no conditioning" rule. That is, the Privacy Rule generally prohibits covered entities from conditioning treatment, payment, enrollment, or eligibility on an individual's provision of an authorization, although there are three exceptions.[86] As discussed above, an individual who signs an authorization for the use or disclosure of PHI must be notified in the authorization form itself about the "no conditioning" rule, the exceptions to the rule, and the consequences of a refusal to sign an authorization form when conditioning is permitted.[87]

Here, the GDPR is similar although not quite as strong. In other words, the GDPR does have a requirement that consent for the processing of personal data be freely given.[88] In assessing if consent is freely given, the GDPR looks at three factors, including: (1) whether the data subject has

---

81 *Id*. ¶ 32.

82 Privacy of Individually Identifiable Health Information, 45 C.F.R. § 164.510 (2016).

83 EU GDPR, *supra* note 7, art. 9, ¶ 2(a).

84 *Id*. art. 9, ¶ 4.

85 General Administrative Requirements, 45 C.F.R. § 160.203(b) (2016) (stating that the Privacy Rule generally preempts a contrary provision of state law unless the state law is more stringent than the Privacy Rule); *id*. § 160.202 (defining "more stringent").

86 Privacy of Individually Identifiable Health Information, 45 C.F.R. § 164.508(b)(4) (2016). See *infra* note 94 and accompanying text for exceptions.

87 § 164.508(c)(2)(ii)(A), (B).

88 EU GDPR, *supra* note 7, pmbl., ¶ 32; *id*., art. 4, ¶ 11.

genuine, free choice in deciding whether to give consent;[89] (2) whether the data subject is unable to refuse to consent;[90] and (3) whether the performance of a contract is conditioned on the data subject's consent when consent is not necessary for the performance of the contract.[91] The last factor expresses a concern similar to that embodied in the Privacy Rule's "no conditioning" rule, which is the concern that individuals will be asked to cede their rights to data privacy and information confidentiality in order to obtain a desired or necessary service. The difference between the Privacy Rule and the GDPR is the strength of the concern. HHS frames the concept as an outright prohibition with only three exceptions, whereas the GDPR simply assesses conditioning as an element of the voluntariness of consent.

C. *Separation of Presentation*

Another measure of comparison is the regulations' separation of presentation rules. To ensure that individuals who give their prior written authorization know what they are signing and recognize the importance of what they are signing, the Privacy Rule generally prohibits an authorization from being combined with another document.[92] Instead, the Privacy Rule requires an authorization to be presented separately to each individuals for his or her signature.[93] Only three exceptions to this "no combination" rule exist, and these exceptions involve: (1) authorizations combined with research-related documentation; (2) two or more authorizations for the use or disclosure of psychotherapy notes; and (3) two or more authorizations that are not conditioned on treatment, payment, enrollment in a health plan, or eligibility for benefits.[94]

The GDPR expresses similar concerns about the importance of a data subject's understanding his or her consent to data processing. The difference is that the GDPR expressly permits the combination of a consent with another "written declaration which also concerns other matters," but only if the "request for consent [is] presented in a manner which is clearly distinguishable from the other matters."[95] Under the GDPR, then, the consent does not need to be separate, just presented in a manner that is clearly distinguishable.

---

89 *Id.* pmbl., ¶ 42.
90 *Id.*
91 *Id.* art. 7, ¶ 4.
92 45 C.F.R. § 164.508(b)(3) (2016).
93 *See id.* § 164.508(b)(3).
94 *Id.* § 164.508(b)(3)(i)–(iii).
95 EU GDPR, *supra* note 7, art. 7, ¶ 2.

D. *Rights of Revocation and Withdrawal*

Under the Privacy Rule, an individual generally has the right to revoke an already-given authorization at any time so long as the revocation is in writing.[96] The Privacy Rule provides two exceptions to this right to revoke, addressing situations in which: (1) the covered entity has already acted in reliance on the authorization, including by using or disclosing PHI before the revocation was received; and (2) an authorization was obtained as a condition of obtaining insurance coverage and other law provides the insurer with the right to contest a claim under the policy or the policy itself.[97] The Privacy Rule implements the right to revoke by requiring all authorizations to contain a statement adequate to place the individual on notice of the individual's right to revoke the authorization, the exceptions to the right to revoke, and a description of how the individual may revoke his or her authorization.[98]

The GDPR has a similar concept known as withdrawal. That is, the GDPR requires the data subject to be allowed to withdraw his or her consent at any time unless personal data has already been processed pursuant to the prior consent.[99] Like the Privacy Rule, the GDPR also requires subjects to be informed of their right to withdraw their consent prior to giving consent.[100]

Where the GDPR is more stringent than the Privacy Rule is with respect to the ease of withdrawal. The GDPR requires it to be as easy for the data subject to withdraw his or her consent as it is for the subject to give consent.[101] HIPAA covered entities, on the other hand, frequently make it *more* difficult for individuals to revoke their authorizations than to give their authorization. For example, many covered hospitals require revocations to be sent to the hospital through regular U.S. mail or presented in person to the hospital's Privacy Officer or other health information manager,[102] although they make their authorizations readily available for online completion and

96 45 C.F.R. § 164.508(b)(5).

97 *Id.* § 164.508(b)(5)(i), (ii).

98 *Id.* § 164.508(c)(2)(i)(A), (B).

99 EU GDPR, *supra* note 7, pmbl., ¶ 42 (stating that consent is not freely given if the individual is unable to withdraw consent); *id.* art. 7, ¶ 3 ("The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.").

100 *Id.* art. 7, ¶ 3.

101 *Id.*

102 *See, e.g.*, *Protected Health Information (PHI) Release Authorization*, U. MED. CTR. 1, https://www.umcsn.com/Common/Documents/authorization_disclose_health_info.pdf (last visited Apr. 17, 2017) ("Revocation must be made in writing and presented or mailed to the UMC Health Information Management Department at the following address: *1800 W. Charleston Blvd., Las Vegas, Nevada 89102*.") (emphasis in original).

submission.[103]

E. *Marketing*

Another point of comparison is that of marketing. If a communication falls within the Privacy Rule's definition of marketing,[104] the Privacy Rule prohibits a covered entity or BA from using or disclosing an individual's PHI for marketing unless the individual signs a specific authorization form noting that the purpose of the use or disclosure is marketing and stating whether any remuneration associated with the marketing exists,[105] unless an exception to the marketing authorization requirement applies.[106]

The GDPR is similar in terms of its dislike for what it calls "direct marketing," requiring the processing of personal data for direct marketing to be "explicitly brought to the attention of the data subject," requiring it to be "presented clearly and separately from any other information," giving the data subject a clear right to object to the processing of his or her personal data for direct marketing, and actually setting forth a prohibition against marketing following such an objection.[107]

---

[103] *See, e.g.*, *Authorization for Release of Health Information Pursuant to HIPAA, OCA Official Form No.: 960*, N.Y. ST. DEP'T HEALTH, http://www.nycourts.gov/forms/hipaa_fillable.pdf (last visited Apr. 17, 2017) (offering a fillable, electronic HIPAA-compliant authorization form).

[104] Privacy of Individually Identifiable Health Information, 45 C.F.R. § 164.501 (2016) (defining marketing as the making of a communication about a product or service that encourages recipients of the communication to purchase or use the product or service; excluding from the definition of marketing communications made for purposes of: (1) Providing refill reminders or otherwise communicating about a drug or biologic that is currently being prescribed for the individual, but only if any financial remuneration received by the covered entity in exchange for making the communication is reasonably related to the covered entity's cost of making the communication; (2) For the following treatment and health care operations purposes, except where the covered entity receives financial remuneration in exchange for making the communication: (A) For treatment of an individual by a health care provider, including case management or care coordination for the individual, or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to the individual; (B) To describe a health-related product or service (or payment for such product or service) that is provided by, or included in a 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; or (C) For case management or care coordination, contacting of individuals with information about treatment alternatives, and related functions to the extent these activities do not fall within the definition of treatment).

[105] *Id.* § 164.508(a)(3)(i), (ii).

[106] *Id.* § 164.508(a)(3)(i)(A), (B).

[107] EU GDPR, *supra* note 7, pmbl., ¶ 7; *id*. art. 21, ¶¶ 2, 3.

IV. RIGHTS OF AMENDMENT AND RECTIFICATION

Under the Privacy Rule, an individual generally has the right to have a covered entity amend PHI or a record about the individual for as long as the PHI is maintained in the designated record set.[108] There are several exceptions to this right. For example, a covered entity is permitted to deny a request for amendment if the information is, indeed, accurate and complete,[109] or if the covered entity that is being asked to amend the information did not create the information.[110] Thus, the right is best framed as a right to have amended incorrect or incomplete PHI by the creator of the PHI. Individuals must be told of this right through their covered entities' notices of privacy practices (NOPP).[111]

The GDPR has a rectification provision that is almost identical to the Privacy Rule's amendment provision. That is, the GDPR gives data subjects the right to obtain rectification of inaccurate personal data from the controller without undue delay and "the right to have incomplete personal data completed, including by means of providing a supplementary statement."[112] The EU states in the Preamble to the GDPR that, "[e]very reasonable step should be taken to ensure that personal data which are inaccurate are rectified or deleted."[113] Like the NOPP requirement, the GDPR also requires data controllers, at the time when personal data are obtained and even when personal data are not obtained, to provide the data subject with information regarding his or her right to request rectification.[114]

V. RIGHT TO ERASURE

One area where the Privacy Rule and the GDPR are very different is with respect to the GDPR's right to erasure, also called the right to be forgotten.[115] This right gives data subjects the ability to obtain from the controller the erasure of personal data concerning him or her without undue delay when one of the following illustrative, but not exhaustive, grounds applies:

> (a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; . . . (c) the data subject objects to processing . . . and

---

108 Privacy of Individually Identifiable Health Information, 45 C.F.R. § 164.526(a)(1) (2016).

109 *Id*. § 164.526(a)(2)(iv).

110 *Id*. § 164.526(a)(2)(i).

111 *Id*. § 164.520(b)(1)(iv)(D).

112 EU GDPR, *supra* note 7, art. 16.

113 *Id*. pmbl., ¶ 39.

114 *Id*. art. 13, ¶ 2(b); *id.* art. 14, ¶ 2(c).

115 *Id*. art. 17.

> there are no overriding legitimate grounds for the processing; . . .
> (d) the personal data have been unlawfully processed;
> (e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject.[116]

The GDPR further requires controllers to establish modalities, including electronic request modalities, that facilitate the exercise of the right to erasure of personal data.[117]

The Privacy Rule not only does not contain a right to erasure, but it also does not modify federal and state medical record and other record retention requirements. For example, the federal Medicare Conditions of Participation require Medicare-participating hospitals to maintain hospital medical records for five years.[118] Many state medical practice acts require physicians licensed in those states to maintain their own medical records for a set period, such as seven years.[119] In addition to federal and state medical record retention requirements, there exist other health compliance record retention requirements. For example, the Privacy Rule requires covered entities to maintain documentation required by the Privacy Rule for six years from the date when the documentation was created or was last in effect, whichever is later, even if the patient or insured no longer has contact with the covered entity.[120]

The GDPR does have exceptions to the right to erasure that address situations in which retention is: (1) necessary to comply with a legal obligation under Union or Member State law; (2) desirable for public health reasons; or (3) desirable for scientific archiving reasons.[121] These three illustrative exceptions somewhat map on to the medical record and HIPAA documentation maintenance requirements discussed immediately above. Again, however, note the difference in approach. That is, general federal and state health law and the Privacy Rule require the *maintenance* of medical records and HIPAA documentation for a certain period of time. The GDPR requires *erasure* except when an exception applies.

---

116 *Id*. art. 17(1)(a), (c), (d) & (e).

117 *Id*. pmbl., ¶ 59.

118 Conditions of Participation for Hospitals, 42 C.F.R. § 482.24(b)(1) (2016).

119 *See, e.g.*, 22 TEX. ADMIN. CODE § 165.1(b)(1) (2016).

120 Privacy of Individually Identifiable Information, 45 C.F.R. § 164.530(j)(2) (2016).

121 See EU GDPR, *supra* note 7, art. 17, ¶ 3, for a list of all the exceptions to the right to erasure.

CONCLUSIONS

This Article has compared and contrasted the Privacy Rule and the GDPR in three contexts, including authorization and consent, amendment and rectification, and erasure. There are many similarities between the concepts of authorization under the Privacy Rule and consent under the GDPR. Obvious similarities include: (1) the expression of concern relating to clarity and separation of presentation of the authorization under the Privacy Rule and consent under the GDPR; (2) the prohibition of conditioning services on an authorization under the Privacy Rule and the assessment of such conditioning with respect to the voluntariness of consent under the GDPR; (3) the right of an individual to revoke an authorization under the Privacy Rule and to withdraw a consent under the GDPR; and (4) significant concerns relating to the use and disclosure of PHI for marketing under the Privacy Rule and the processing of personal data for direct marketing under the GDPR.

The terminology, organization, and presentation of these concerns, prohibitions, and rights in the Privacy Rule and the GDPR certainly are different. The most notable difference—and the best illustration of such a difference—is the Privacy Rule's heavy-handed regulation of the content of the authorization, including the six core elements and three required statements that must be in every authorization.

It would be tempting to say that the Privacy Rule is, across the board, more detailed and directive than the GDPR. For example, the Privacy Rule contains a strong prohibition against combining authorizations with other documents, whereas the GDPR allows consent to be presented in the context of a written declaration concerning other matters so long as the request for consent is presented in a manner that is clearly distinguishable from such other matters. However, the GDPR does contain greater particularity and regulatory rigidity in some contexts, including its requirement relating to the ease of consent withdrawal.

With respect to the rights of amendment and rectification of inaccurate or incomplete data, the Privacy Rule and the GDPR are very similar. The regulatory language—amendment versus rectification—is the biggest difference. A significant difference, however, lies in the GDPR's right to erasure and the lack of comparable language in the Privacy Rule. In general, federal and state health law, including the Privacy Rule, require retention of medical records, billing records, compliance records, and other records for at least five years, if not longer. There are important clinical reasons for these record retention requirements. Clinicians need to know, for example, whether a patient is allergic to a drug or has had an adverse drug reaction in the past, and older medical records are critical in terms of providing this information and preventing drug and other injuries.

Health insurers, too, need to maintain billing and payment records for purposes of determining whether patients have satisfied their annual deductibles, have met their annual out-of-pocket maximums and, if President Trump repeals the Affordable Care Act, whether insureds or applicants for insurance have preexisting health conditions that could make them ineligible for insurance coverage of a future illness.

Health oversight agencies, including the Centers for Medicare and Medicaid Services, the Office for Civil Rights, and the Drug Enforcement Agency, also need billing and other administrative records to identify health care fraud and abuse, to detect privacy violations, and to become aware of problematic prescription patterns.

In summary, the obligation to maintain and the ability to produce health-related records upon request is critical to the smooth functioning of the health care delivery system as well as the health care financing system, helping to explain some of the key differences between the GDPR and the Privacy Rule, especially with respect to erasure.