Przegląd Prawniczy Uniwersytetu im. Adam Mickiewicza | Adam Mickiewicz University Law Review

Vol. 16, 2024
DOI 10.14746/ppuam.2024.16.07

Magdalena Jurczuk,[1] Maria Suprunowicz[2]

Consent in Data Privacy: A General Comparison of GDPR and HIPAA

Abstract: The purpose of this paper is to conduct a general comparison of legal requirements regarding consent under the Health Insurance Portability and Accountability Act (HIPAA) and the General Data Protection Regulation (GDPR). Both regulations aim to protect health data as a special category of personal data, highlighting the importance of obtaining explicit consent or authorization from the data owner before processing or disclosing the information. The article explores the distinct approaches of HIPAA and the GDPR in defining consent and authorization, the requirements for withdrawal or revocation of consent, and the form and language of consent. It also examines the scope of application and the impact on healthcare operations, emphasizing the need for informed and transparent consent practices under both regulations. Furthermore, it examines the differences in the regulatory scopes and the specific measures each framework takes to safeguard personal health information.

Keywords: GDPR, HIPAA, Privacy Rule, consent, authorization, healthcare data, data privacy

1 Magdalena Jurczuk, University of Białystok, Faculty of Law, Białystok, Poland. e-mail: mj77919@student.uwb.edu.pl, https://orcid.org/0009-0003-1348-6097.

2 Maria Suprunowicz, Medical University of Białystok, Faculty of Medicine, Poland, e-mail: suprunowicz.maria@gmail.com, https://orcid.org/0009-0006-6233-3945.

Introduction

As we overcome the complexity of the digital age, the protection of personal health data has emerged as a key focus in the areas of data privacy and healthcare law. The unprecedented integration of technology into healthcare systems has led to the digitization of patient health records and changed the landscape of medical information management. The digitization of medical data requires robust legal and ethical safeguards to ensure the privacy and security of individuals' sensitive health information.[3]

Health data are, by their nature, particularly sensitive in relation to fundamental rights and freedoms, and therefore merit specific protection as the context of their processing, use or disclosure could create significant risks to the fundamental rights and freedoms.[4] At the same time, use of health data can bring great benefits not only in the context of an individual's medical care, but also e.g. in the research of new medical treatment. It should be noted that the right to the protection of personal data is not absolute and is subject to limitations, due to other goods and values protected by law. For example, Recital 4 of the preamble to the GDPR indicates that the processing of personal data should be organized in such a way as to serve humanity, and the right to the protection of personal data should be seen in the context of its social function and weighed against other fundamental rights in accordance with the principle of proportionality.

To protect the privacy of patients, various privacy standards are followed in different regions; these include the Health Insurance Portability and Accountability Act (HIPAA) in the United States and the General Data Protection Regulation (GDPR) in Europe. HIPAA controls the collection and use of medical data in the United States for other related purposes. In the EU, all process-

3 Israel Olawunmi, *Safeguarding Health Data in a Digital Era: A Comparative Study of the GDPR and HIPAA* (2023), 2, https://www.researchgate.net/publication/370934056_SAFEGUARDING_HEALTH_DATA_IN_A_DIGITAL_ERA_A_COMPARATIVE_STUDY_OF_THE_GDPR_AND_HIPAA.

4 Ludmila Georgieva and Christopher Kuner, "Article 9. Processing of Special Categories of Personal Data," in *The EU General Data Protection Regulation (GDPR): A Commentary*, ed. Christopher Kuner et al. (Oxford University Press, 2019), 369.

ing of personal data must be GDPR compliant, and entities that obtain health data from individuals in the EU must meet GDPR guidelines. Organizations that transfer US health-related data to the EU must comply with both rules.[5] This article conducts a comparison of the main elements related to data subject consent under the GDPR and HIPAA regulations. Specifically, it defines the scope of entities obliged to comply, the situations in which consent is required, and the form that consent must take.

Historical Development and General Characteristics of the GDPR and HIPAA

The historical development of the General Data Protection Regulation (GDPR)[6] dates to the 1995 Data Protection Directive,[7] which laid the foundation for data protection regulation in the EU. However, recognizing the need for a more robust and unified approach to data privacy, the European Union embarked on a journey to revamp its data protection framework, culminating in the adoption of the GDPR in 2016. The GDPR represented a significant overhaul of existing data protection laws, aiming to modernize and strengthen data privacy rules to meet the challenges of technological advances and increasing data flows.[8] One of the main goals of the GDPR was to harmonize data protection laws across EU Member States, eliminate regulatory fragmentation, and streamline data privacy requirements for organizations

5 Tian-Fu Lee et al., "Compliance with HIPAA and GDPR in Certificateless-Based Authenticated Key Agreement Using Extended Chaotic Maps," *Electronics* 12, no. 5(2023): 1, https://doi.org/10.3390/electronics12051108.

6 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 (GDPR).

7 Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (Data Protection Directive).

8 European Union Agency for Fundamental Rights and Council of Europe, *Handbook on European Data Protection Law* (Publications Office of the European Union, 2018), 30.

operating in the EU.[9] In addition, the GDPR placed a strong emphasis on allowing individuals to exercise greater control over their personal data.[10] The regulation introduced several key provisions aimed at strengthening individuals' rights regarding their data, including the right to access and rectify personal data, the right to erasure (commonly known as the "right to be forgotten")[11] and the principle of data minimization.[12] These provisions were intended to shift the balance of power in favor of data subjects, allowing them greater control over how their data is collected, processed, and used by organizations.

The GDPR introduced strict requirements for organizations that process personal data, highlighting transparency and accountability in data processing practices. Organizations have been obligated to implement robust data protection measures, conduct privacy impact assessments,[13] and comply with data protection principles as well as data breach notification procedures.[14] The GDPR's enforcement mechanisms, including substantial fines for noncompliance, underscored the importance of complying with data protection laws and upholding individuals' privacy rights. The GDPR's proactive approach to data protection and focus on accountability and transparency[15] have set a precedent for global data privacy standards, influencing data protection practices and regulatory frameworks around the world.[16]

9 Christopher Kuner et al., "Background and Evolution of the GDPR," in *The EU General Data Protection Regulation (GDPR)*, 5.

10 Kuner et al., "Background and Evolution of the GDPR," 20–21.

11 Kuner et al., "Background and Evolution of the GDPR," 22–23.

12 European Union Agency for Fundamental Rights and Council of Europe, *Handbook on European Data Protection Law*, 125.

13 Paweł Fajgielski, „Artykuł 35. Ocena skutków dla ochrony danych," in *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz* (Wolters Kluwer Polska, 2022), 437.

14 Paweł Fajgielski, „Artykuł 33. Zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu," in *Ogólne rozporządzenie o ochronie danych*, 419.

15 Sanjay Sharma, *Data Privacy and GDPR Handbook* (Wiley, 2019), 126, https://doi.org/10.1002/9781119594307.

16 Christopher Kuner, "Article 49. Derogations for specific situations," in *The EU General Data Protection Regulation (GDPR)*, 858.

The Health Insurance Portability and Accountability Act[17] (HIPAA) was enacted by the U.S. Congress in 1996 with the primary goal of addressing data privacy and security issues in the healthcare sector. HIPAA was introduced in response to the growing use of electronic medical records and the need to establish comprehensive standards for protecting individuals' health information.[18] Unlike the GDPR, which has a broader scope with respect to personal data, HIPAA is a U.S. federal law that strictly regulates a type of personal health information in the United States,[19] statutorily referred to as protected health information (PHI).[20] Consequently, HIPAA rules apply to covered entities (e.g. doctors, clinics, psychologists, dentists, health insurance companies, health plans etc.) and business associates.[21] HIPAA consists of several rules, mainly The Privacy Rule and the Security Rule, each of which is designed to protect the confidentiality and integrity of patient health information and ensure the secure handling of electronic health records.[22]

Individually identifiable health information, protected under the Privacy Rule, is information that is a subset of health information, including demographic data collected from an individual, and meets the following criteria: it is cre-

17 U.S. Department of Health and Human Services Office for Civil Rights, "HIPAA Administrative Simplification: Regulation Text: 45 CFR Parts 160, 162, and 164" (2013), accessed June 27, 2024, https://www.hhs.gov/sites/default/files/hipaa-simplification-201303.pdf.

18 Wasim Fathima Shah, "Preserving Privacy and Security: A Comparative Study of Health Data Regulations – GDPR vs. HIPAA," *International Journal for Research in Applied Science and Engineering Technology* 11, no. 8(2023): 2189, https://doi.org/10.22214/ijraset.2023.55551.

19 Israel, *Safeguarding Health Data in a Digital Era*, 5.

20 Protected Health Information (PHI) is any health information that can be used to identify a patient, who relates to physical or mental health, relating to a past, present, or future condition, and includes both living and deceased patients. PHI may be in any form, e.g. oral, paper, or electronic – Lorna Hecker, *HIPAA Demystified: HIPAA Compliance for Mental Health Professionals* (Loger Press, 2016), 7.

21 Office for Civil Rights (OCR), "Covered Entities and Business Associates," Text, November 23, 2015, accessed June 27, 2024, https://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html.

22 Tim Benson and Grahame Grieve, "Privacy and Consent," in *Principles of Health Interoperability: FHIR, HL7 and SNOMED CT* (Springer Cham, 2021), 368, https://doi.org/10.1007/978-3-030-56883-2_19.

ated or received by a health care provider, health plan, employer, or health care clearinghouse; it 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 it identifies the individual (or with respect to which there is a reasonable basis to believe the information can be used to identify the individual).[23] This regulation is intended to balance the interests of individuals in maintaining the confidentiality of their personal health data in a variety of private and public activities. The fundamental concentration of the Privacy Rule is to regulate the circumstances involving the use and disclosure of PHI by entities subject to it. It covers the use, disclosure, and request for PHI, excluding specific cases such as educational records or employment records.[24] Protecting electronic data is critical for businesses and individuals to build customer trust. The objective of the Security Rule is establishing national safeguards to protect the confidentiality, integrity, and availability of electronic PHI (ePHI) against unauthorized access, use, or disclosure.[25] The HIPAA Security Rule obliges organizations to implement a security management process to identify and investigate risks and subsequently implement security measures to remediate those risks. Mostly, this comprises evaluating threats to patient ePHI, evaluating the adequacy of existing privacy and security measures, assessing potential future threats, and addressing barriers to adoption.[26]

There is no doubt that the shape of both regulations was influenced by the legal system under which they were created. Common law, which originated in England and has since spread to the United States and other former British colonies, is known for its reliance on judicial decisions and the doctrine of

23 Code of Federal Regulations (CFR), "45 CFR § 160.103 Definitions," accessed June 27, 2024, https://ecfr.io/Title-45/Section-160.103.

24 Shah, "Preserving Privacy and Security," 2191.

25 Shah, "Preserving Privacy and Security," 2191.

26 Hecker, *HIPAA Demystified*, 91.

precedent.[27] This system is based on flexibility and case-by-case adjudication, which allows for rapid evolution of the law. In contrast, civil law systems, such as those found in EU Member States, have their origins in Roman law and were primarily shaped by the Napoleonic Code.[28] These systems prioritize written laws over judicial interpretation, with laws being comprehensive and structured to address a wide range of situations in order to promote consistency and foreseeability.[29] The GDPR is structured according to civil law principles, with comprehensive and well-organized statutory provisions that emphasize transparency, accountability, and data minimization in line with the EU Charter of Fundamental Rights.[30] This highlights the close connection between law and human rights in continental legal systems. On the other hand, HIPAA follows a common law approach with a more limited and specific scope of regulation. Unlike the broad application of the GDPR, HIPAA's regulatory focus is on specific sectors,[31] reflecting a common law system's tendency to address issues through targeted and incremental legislative measures. Data privacy laws in the United States are diverse, with separate rules governing various sectors like health care, finance (as outlined in the Gramm-Leach-Bliley Act),[32] and children's online privacy (under COPPA).[33]

27 Časlav Pejović, "Civil Law and Common Law: Two Different Paths Leading to the Same Goal," *Poredbeno Pomorsko Pravo* 40, no. 155(2001): 9.

28 Pejović, "Civil Law and Common Law," 9.

29 Mathias Siems and Po Jen Yap, eds., "Central Themes in Comparative Law," in *The Cambridge Handbook of Comparative Law* (Cambridge University Press, 2024), 232–33, https://doi.org/10.1017/9781108914741.022.

30 Lee A. Bygrave, *Data Privacy Law: An International Perspective* (Oxford University Press, 2014), 58.

31 Richard Stokes, "HIPAA Standards for Privacy of Individually Identifiable Health Information," *Technical Bulletins*, 2002: 2, https://trace.tennessee.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1082&context=utk_mtastech.

32 Edward J. Janger and Paul M. Schwartz, "The Gramm-Leach-Bliley Act, Information Privacy, and the Limits of Default Rules," *Minnesota Law Review* 86, 2001–2002: 1224.

33 Dalia Topelson et al., *Privacy and Children's Data: An Overview of the Children's Online Privacy Protection Act and the Family Educational Rights and Privacy Act* (The Berkman Center for Internet & Society, 2013), 1–2.

Consent Under the GDPR

Health data is sensitive personal information (a special category of personal data) under the GDPR, which requires extra legal protection. Article 9 GDPR states that processing of personal data revealing racial or ethnic origin, political opinions, religious beliefs, 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. The regulation provides exceptions from this rule, including the situation where the data subject has given explicit consent to the processing of those personal data for one or more specified purposes.

Before exploring the specifics of the topic, it is essential to establish and present the relevant definitions. Article 4(11) GDPR provides the following definition of consent: "consent of the data subject means 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." Moreover, 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.[34] Data concerning health means 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.[35]

The definition of consent provided above demonstrates the conditions which have to be met cumulatively for the consent to become a lawful basis for the processing of personal data:

34 Article 4(1) GDPR.
35 Article 4(15) GDPR.

1) Freely given: The term "free" in this context signifies genuine autonomy and authority for individuals regarding their data. According to the GDPR, consent is considered invalid if the data subject feels pressured to consent, lacks a true choice, or faces negative repercussions for not consenting.[36] Consent should not be coerced, and the data subject should be able to choose whether or not to give consent.[37] Moreover, consent should not be relied upon where there is a clear imbalance between the data subject and controller, in particular, where the controller is a public authority.[38] Consent is not considered voluntary if it cannot be given separately for different personal data processing operations.[39] When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.[40]
2) Specific: Requiring explicit consent coupled with the principle of purpose limitation outlined in Article 5(1)(b) serves as a protection against the potential expansion or ambiguity of reasons for processing data beyond what was originally agreed upon by the data subject during data collection.[41] Articles 5(1)(b) and 6(1)(a) GDPR demand a fairly clear description of the purposes of data processing, therefore supporting in the fulfillment of the specificity criterion.[42] The content of

36 The European Data Protection Board, *Guidelines 05/2020 on Consent under Regulation 2016/679*, 7, accessed November 8, 2024, https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf.
37 Paweł Fajgielski, „Artykuł 4. Definicje," in *Ogólne rozporządzenie o ochronie danych*, 137.
38 Recital 43 GDPR.
39 Fajgielski, „Artykuł 4. Definicje," 137.
40 Article 7(4) GDPR.
41 The European Data Protection Board, *Guidelines 05/2020 on Consent under Regulation 2016/679*, 14.
42 Lee A. Bygrave, Luca Tosoni, "Article 4(11). Consent," in *The EU General Data Protection Regulation (GDPR)*, 183.

the consent statement should correspond to the scope and purpose the consent to data processing; it should not be a vague statement that does not indicate what data is to be processed and for what purpose.[43] On the other hand, recital 32 of GDPR indicates that one consent may cover multiple processing operations if these are undertaken for the same purposes.[44]

3) Informed: This criterion involves ensuring that the data subject is provided with advance knowledge of the parameters of the data processing operation to which they are to consent.[45] Recital 42 of GDPR states that for consent to be informed, the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended. Moreover, controller is responsible for obtaining consent from data subjects by providing clear information that allows them to easily identify the controller and understand the purpose of data processing. The controller must also fulfill additional information duties outlined in Articles 13 and 14 of the GDPR when relying on consent from data subjects.[46]
4) Unambiguous: the expression of consent should not raise doubts about the intention of the person who makes such a statement. If the statement of consent can be interpreted differently and different conclusions can be drawn from it on the subject of consent, doubt may arise as to whether the condition discussed here is met.[47] This criterion is elaborated on in Recital 32 of GDPR, which refers to the need for consent to be provided by a clear affirmative act establishing an un-

43 Dominik Lubasz, "Warunki wyrażania zgody jako przesłanki legalizującej przetwarzanie danych osobowych," *Gdańskie Studia Prawnicze*, no. 4(52)(2021): 69, https://doi.org/10.26881/gsp.2021.4.04.

44 Bygrave and Tosoni "Article 4(11). Consent," 183.

45 Bygrave and Tosoni "Article 4(11). Consent," 184.

46 The European Data Protection Board, *Guidelines 05/2020 on Consent under Regulation 2016/679*,17.

47 Fajgielski, „Artykuł 4. Definicje," 139.

ambiguous indication of the data subject's agreement. D. Lubasz emphasizes that the Regulation does not dictate the specific format or medium in which information must be presented to fulfill the requirement for informed consent. This allows for flexibility in how important information can be communicated, including through written or verbal statements, as well as audio or video recordings.[48] On the other hand, when asking for consent through electronic means, the request should not disrupt the user's ability to use the service. It may be necessary for the data subject to actively indicate consent in order to avoid any confusion. Therefore, it may be acceptable for a consent request to temporarily interrupt the user's experience in order to be effective.[49]

As mentioned above, Article 9 GDPR mandates "explicit consent" shall be obtained when sensitive personal data is processed. The term "explicit" pertains to how consent is communicated by the individual providing the data. This entails the data subject giving a clear and direct statement of consent. One straightforward method to ensure explicit consent is to confirm consent explicitly in a written format.[50] "Explicit consent" cannot be implied and involves a high degree of precision and definiteness in the declaration of consent, as well as a particular description of the purposes of processing.[51] Thus, Article 9 sets a higher threshold than Article 6 GDPR. As T. Osiej pointed out, the primary legal justification for data processing by medical professionals and healthcare facilities will typically be Article 9(2)(h) of the GDPR. This provision allows for the processing of health data when necessary for activities such as preventive healthcare, occupational medicine, providing healthcare, or social secu-

48 Lubasz, "Warunki wyrażania zgody jako przesłanki legalizującej przetwarzanie danych osobowych," 71.

49 The European Data Protection Board, *Guidelines 05/2020 on Consent under Regulation 2016/679*, 19.

50 The European Data Protection Board, *Guidelines 05/2020 on Consent under Regulation 2016/679*, 20.

51 Christopher Kuner et al., eds., *The EU General Data Protection Regulation (GDPR)*, 377.

rity purposes.[52] The responsibility lies with the controller[53] to prove the data subject has consented to the processing.[54] Usually, the declaration of consent is pre-formulated by the controller, therefore the consent should be provided in a comprehensible and easily accessible form, using clear and plain language.[55]

Moreover, Article 8 states that in relation to providing information services to a child based on consent, the processing will only be lawful under GDPR if the child is at least 16 years old. If the child is under 16, the processing will only be lawful if the consent of the parent (or legal guardian) is provided. The Member States may lower this age requirement; however, it cannot be lower than 13 years for valid consent. Additionally, the controller shall make reasonable efforts to verify parental consent considering the available technology.[56]

The GDPR underlines further conditions of consent in Article 7, in which it mandates that if the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent must be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form. Any part of such a declaration which constitutes an infringement of this Regulation must not be binding. Furthermore, the data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent must not affect the lawfulness of the processing based on consent before its withdrawal. Prior to giving consent,

52 Tomasz Osiej, "Personal Data Protection – Where to Start?," *Ophtha Therapy* 6, no. 1(21) (2019): 52, https://doi.org/10.24292/01.OT.300319.08.

53 Controller means 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 – Article 4(7) GDPR.

54 Processing means 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, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction – Article 4(2) GDPR.

55 Victoria Hordern "Lawful Processing Criteria," in *European Data Protection: Law and Practice*, ed. Eduardo Ustaran (International Association of Privacy Professionals, 2023), 160.

56 Sharma, *Data Privacy and GDPR Handbook*, 134.

the data subject shall be informed about it. It must be as easy to withdraw to give consent. A person providing data may consent to one or multiple purposes, as well as multiple independent consents. As a result, it is important for the controller to be able to clearly identify which consent is being withdrawn in each instance.[57]

It is necessary to mention the proposal for a European Health Data Space which was approved politically by the Council and the European Parliament in the spring of 2024. The objectives of European Health Data Space are as follows: establishing a single market for electronic health record systems, giving citizens control over their health data, and making it easier for data to be shared for the primary use of providing healthcare services throughout the EU. It would also offer a consistent system for using health data for research, innovation, policy-making, and regulatory action (secondary use of data).[58] Regarding electronic health data, the EHDS is in favor of implementing the rights outlined in the GDPR. The EHDS expands on the GDPR's potential for EU legislation pertaining to the use of personal electronic health data for diagnosis, treatment, or the administration of health care systems and services. Moreover the EHDS expands natural persons' right to data portability in the health sector and envisions additional measures to foster interoperability.[59] Building on the GDPR's requirements, natural persons will have more options for digitally accessing and transmitting their electronic health data. It will be mandatory for market participants in the health sector to share electronic health data with third parties chosen by users. Without sacrificing the necessary safety precautions to safeguard natural person rights under the GDPR, the proposal will offer the tools to enforce these rights (via com-

57 Natalia Kalinowska et al., "Badania kliniczne w świetle RODO," *Prawo Mediów Elektronicznych*, no. 3(2018): 5.

58 "European Health Data Space," European Commission, accessed November 8, 2024, https://health.ec.europa.eu/ehealth-digital-health-and-care/european-health-data-space_en.

59 "Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the European Health Data Space," EUR-Lex, accessed November 8, 2024, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0197.

mon standards, specifications, and labels). It would support the free flow of health-related personal data and its enhanced protection, as guaranteed by the GDPR.[60]

Consent Under HIPAA

Under the Privacy Rule, except in certain circumstances, such as emergency situations, medical institutions require explicit consent from patients to use or disclose PHI for treatment, payment, or medical operations.[61] This consent often takes the form of written approval, which must be specific and detailed, indicating to whom and for what purpose the information is authorized to be disclosed.[62] HIPAA defers to state law to regulate the age of majority and the rights of parents to act for a child in making health care decisions, and thus, the ability of the parent to act as the personal representative of the child for HIPAA purposes.[63] HIPAA does not provide a legal definition of authorization; however this term should be understood as a consent obtained generally from the patient that permits a covered entity or business associate to disclose or use PHI to an individual or entity for a purpose that would otherwise not be allowed by the HIPAA Privacy Rule.[64]

60 "Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the European Health Data Space."

61 45 CFR §164.508 (a)(1): "Except as otherwise permitted or required by this subchapter, a covered entity may not use or disclose protected health information without an authorization that is valid under this section. When a covered entity obtains or receives a valid authorization for its use or disclosure of protected health information, such use or disclosure must be consistent with such authorization."

62 David M. Parker et al., "Privacy and Informed Consent for Research in the Age of Big Data," *Penn State Law Review* 123, no. 3(2019): 718–19.

63 "At What Age of a Child Is the Parent No Longer the Personal Representative of the Child for HIPAA Purposes?," U.S. Department of Health and Human Services, accessed June 27, 2024, https://www.hhs.gov/hipaa/for-professionals/faq/2093/what-age-child-parent-no-longer-personal-representative-child-hipaa-purposes.html.

64 Steve Alder, "What Is HIPAA Authorization?," The HIPPA Journal, accessed June 27, 2024, https://www.hipaajournal.com/what-is-hipaa-authorization/.

45 CFR §164.508 details the uses and disclosures of protected health information that require an authorization, e.g.:

1) Use or disclosure of PHI otherwise not permitted by the HIPAA Privacy Rule.
2) Use or disclosure of psychotherapy notes.[65]
3) Use or disclosure of protected health information for marketing.[66]
4) Disclosure of protected health information which is a sale of protected health information.

As a general rule, HIPAA prohibits combining an authorization for use or disclosure of protected heath information with any other document to create compound authorization. There are three exceptions to the regulation, concerning research documentation, psychotherapy notes and authorizations that are not conditioned on e.g. treatment, payment, enrollment in a health plan.[67] The Privacy Rule specifies necessary elements of the authorization,[68] including:

1) A description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion.
2) The name or other specific identification of the person(s), or class of persons, authorized to make the requested use or disclosure.
3) The 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.
4) A description of each purpose of the requested use or disclosure.
5) An expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure.
6) Signature of the individual and date.

The regulation also requires: a statement of the individual's right to revoke written approval; a statement of "the ability or inability to condition treatment,

65 Exceptions included in 45 CFR §164.508 (a)(2).
66 Exceptions included in 45 CFR §164.508 (a)(3).
67 45 CFR §164.508 (b)(3).
68 45 CFR §164.508 (c)(1).

payment, enrollment or eligibility for benefits on the authorization." Moreover, HIPAA-compliant approval forms must also be written in plain language.[69] The high level of prior individual authorization required in HIPAA approval forms implicates the value placed on individuals' interest in preserving the confidentiality of their protected health information.

The regulation states that an individual may revoke an authorization provided that the revocation is in writing, except to the extent that the covered entity has taken action in reliance on the authorization; or if the authorization was obtained as a condition of obtaining insurance coverage and another law provides the insurer with the right to contest a claim under the policy or the policy itself.[70]

Conclusion

Both HIPAA and the GDPR recognize that health data is a special category of personal data and take specific measures to adequately protect it, while trying to preserve the ability to effectively treat the patient and operate the health care system. Moreover, both regulations underline the importance of consent and require that before data can be processed or used/disclosed, the consent/authorization of the owner of the information must be obtained. On the other hand, unlike the GDPR, which has a broader scope with respect to personal data, HIPAA is a U.S. federal law that strictly regulates a type of personal health information in the United States, statutorily referred to as protected health information (PHI). As a result, the scope of entities required to comply with HIPAA is much narrower than the GDPR.

The GDPR provides the definition of consent as "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

69 45 CFR §164.508 (c)(2), (3).
70 45 CFR §164.508 (b)(5).

to the processing of personal data relating to him or her" but at the same time recognizes that for protection of healthcare data this standard is not sufficient. Thus, "explicit consent" must be obtained prior to the data processing. This aligns with the comprehensive nature of civil law and aims to provide broad data protection across various contexts. Although consent is included in the HIPAA's Privacy Rule, it is not as fundamental as it is in the GDPR. HIPAA does not provide a legal definition of authorization; however, this term should be understood as consent obtained generally from the patient that permits a covered entity or business associate to disclose or use PHI to an individual or entity for a purpose that would otherwise not be allowed by the HIPAA Privacy Rule. In addition, the GDPR sets out general rules that consent should meet, without explicitly prejudging its specific content. On the other hand, HIPAA indicates the substantive elements of authorization, e.g. the name of the person to whom the covered entity may make the requested use/disclosure, or an expiration date that relates to the individual or the purpose of the use or disclosure. As opposed to consent under the GDPR, which can be given in other ways than in writing, authorization under the HIPAA must be in writing. The HIPAA's focus on the healthcare sector is a specific application of common law, allowing for different consent standards in other sectors governed by separate laws.

The GDPR and HIPAA also regulate the rights of withdrawal/revocation of consent/authorization. The GDPR grants individuals the explicit right to withdraw consent at any time, emphasizing individual rights and autonomy in civil law. This requirement ensures that withdrawing consent is just as simple as giving it, giving individuals greater control over their personal data. Moreover, the European regulation states that the data subject must be informed about his or her right of withdrawal. On the other hand, HIPAA requires a statement of the individual's right to revoke written approval and that an individual may revoke an authorization provided that the revocation is in writing. The HIPAA approach does not prioritize the right to withdraw consent as much as the GDPR. Individuals are able to revoke authorization in specific

situations, but the process has more restrictions in terms of its reach and use. This approach is based on a practical common law perspective that focuses on the operational requirements of healthcare providers and insurers, while also taking into account patient privacy and practical considerations. Neither law directly specifies the age of majority at which the data subject can lawful consent/authorization, instead referring to EU Member State laws/US state laws.

Regarding the form of consent, the GDPR allows combining request for consent with other written documents if it is presented in a manner which is clearly distinguishable from the other matters. Conversely, HIPAA generally prohibits combining an authorization for use or disclosure of protected heath information with any other document to create compound authorization. In this regard, therefore, it is a stricter regulation that aims to increase data subject awareness and transparency of use/disclosure of information. Both the GDPR and HIPAA underline the necessity of providing consent/authorization in plain language, which supports the conclusion that under both regulations, not only the European one, the consent should also be informed.

References

Alder, Steve. "What Is HIPAA Authorization?" The HIPPA Journal. Accessed June 27, 2024. https://www.hipaajournal.com/what-is-hipaa-authorization/.

Benson, Tim, and Grahame Grieve, "Privacy and Consent." In *Principles of Health Interoperability: FHIR, HL7 and SNOMED CT*. Springer Cham, 2021. https://doi.org/10.1007/978-3-030-56883-2_19.

Bygrave, Lee A. *Data Privacy Law: An International Perspective*. Oxford University Press, 2014.

Bygrave, Lee A., and Luca Tosoni. "Article 4(11). Consent." In *The EU General Data Protection Regulation (GDPR): A Commentary*, edited by Christopher Kuner, Lee A. Bygrave, Christopher Docksey, and Laura Drechsler. Oxford University Press, 2019.

EUR-Lex. "Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the European Health Data Space." Accessed November 8, 2024. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0197.

European Commission. "European Health Data Space." Accessed November 8, 2024. https://health.ec.europa.eu/ehealth-digital-health-and-care/european-health-data-space_en.

The European Data Protection Board. *Guidelines 05/2020 on Consent under Regulation 2016/679*. Accessed November 8, 2024. https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf.

European Union Agency for Fundamental Rights, and Council of Europe. *Handbook on European Data Protection Law*. Publications Office of the European Union, 2018.

Fajgielski, Paweł. „ Artykuł 4. Definicje." In *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz*. Wolters Kluwer Polska, 2022.

Fajgielski, Paweł. „Artykuł 33. Zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu." In *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz*. Wolters Kluwer Polska, 2022.

Fajgielski, Paweł. „Artykuł 35. Ocena skutków dla ochrony danych." In *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz*. Wolters Kluwer Polska, 2022.

Georgieva, Ludmila, and Christopher Kuner. "Article 9. Processing of Special Categories of Personal Data." In *The EU General Data Protection Regulation (GDPR): A Commentary*, edited by Christopher Kuner, Lee A. Bygrave, Christopher Docksey, and Laura Drechsler. Oxford University Press, 2019.

Hecker, Lorna. *HIPAA Demystified: HIPAA Compliance for Mental Health Professionals*. Loger Press, 2016.

Hordern, Victoria. "Lawful Processing Criteria." In *European Data Protection: Law and Practice*, edited by Eduardo Ustaran. International Association of Privacy Professionals, 2023.

Janger, Edward J., and Paul M. Schwartz. "The Gramm-Leach-Bliley Act, Information Privacy, and the Limits of Default Rules." *Minnesota Law Review* 86, 2001–2002: 1219–61.

Kalinowska, Natalia, Bartłomiej Oręziak, and Marek Świerczyński. "Badania kliniczne w świetle RODO." *Prawo Mediów Elektronicznych*, no. 3(2018): 4–15.

Kuner, Christopher. "Article 49. Derogations for specific situations." In *The EU General Data Protection Regulation (GDPR): A Commentary*, edited by Christopher Kuner, Lee A. Bygrave, Christopher Docksey, and Laura Drechsler. Oxford University Press, 2019.

Kuner, Christopher, Lee A. Bygrave, and Christopher Docksey. "Background and Evolution of the GDPR." In *The EU General Data Protection Regulation (GDPR): A Commentary*, edited by Christopher Kuner, Lee A. Bygrave, Christopher Docksey, and Laura Drechsler. Oxford University Press, 2019.

Kuner Christopher, Lee A. Bygrave, and Christopher Docksey, eds. *The EU General Data Protection Regulation (GDPR): A Commentary*. Oxford University Press, 2019.

Lee, Tian-Fu, I-Pin Chang, and Guo-Jun Su. "Compliance with HIPAA and GDPR in Certificateless-Based Authenticated Key Agreement Using Extended Chaotic Maps." *Electronics* 12, no. 5(2023): 1108. https://doi.org/10.3390/electronics12051108.

Lubasz, Dominik. "Warunki wyrażania zgody jako przesłanki legalizującej przetwarzanie danych osobowych." *Gdańskie Studia Prawnicze*, no. 4(52) (2021): 62–79. https://doi.org/10.26881/gsp.2021.4.04.

Olawunmi, Israel. *Safeguarding Health Data in a Digital Era: A Comparative Study of the GDPR and HIPAA*. 2023. https://www.researchgate.net/publica-

tion/370934056_SAFEGUARDING_HEALTH_DATA_IN_A_DIGITAL_ERA_A_COMPARATIVE_STUDY_OF_THE_GDPR_AND_HIPAA.

Osiej, Tomasz. "Personal Data Protection – Where to Start?" *Ophtha Therapy* 6, no. 1(21)(2019): 51–54. https://doi.org/10.24292/01.OT.300319.08.

Parker, David M., Steven G. Pine, and Zachary W. Ernst. "Privacy and Informed Consent for Research in the Age of Big Data." *Penn State Law Review* 123, no. 3(2019): 703–33.

Pejović, Časlav. "Civil Law and Common Law: Two Different Paths Leading to the Same Goal." *Poredbeno Pomorsko Pravo* 40, no. 155(2001): 7–32.

Shah, Wasim Fathima. "Preserving Privacy and Security: A Comparative Study of Health Data Regulations – GDPR vs. HIPAA." *International Journal for Research in Applied Science and Engineering Technology* 11, no. 8(2023): 2189–99. https://doi.org/10.22214/ijraset.2023.55551.

Sharma, Sanjay. *Data Privacy and GDPR Handbook*. Wiley, 2019. https://doi.org/10.1002/9781119594307.

Siems, Mathias, and Po Jen Yap, eds. "Central Themes in Comparative Law." In *The Cambridge Handbook of Comparative Law*. Cambridge University Press, 2024. https://doi.org/10.1017/9781108914741.022.

Stokes, Richard. "HIPAA Standards for Privacy of Individually Identifiable Health Information." *Technical Bulletins*, 2002: 1–16. https://trace.tennessee.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1082&context=utk_mtastech.

Topelson, Dalia, Christopher Bavitz, Ritu Gupta, and Irina Oberman. *Privacy and Children's Data: An Overview of the Children's Online Privacy Protection Act and the Family Educational Rights and Privacy Act*. The Berkman Center for Internet & Society, 2013.

U.S. Department of Health and Human Services. "At What Age of a Child Is the Parent No Longer the Personal Representative of the Child for HIPAA Purposes?" Accessed June 27, 2024. https://www.hhs.gov/hipaa/for-profes-

sionals/faq/2093/what-age-child-parent-no-longer-personal-representative-child-hipaa-purposes.html.

U.S. Department of Health and Human Services Office for Civil Rights. *HIPAA Administrative Simplification: Regulation Text: 45 CFR Parts 160, 162, and 164*. 2013. Accessed June 27, 2024. https://www.hhs.gov/sites/default/files/hipaa-simplification-201303.pdf.