Chapter 4 A comparative analysis with the US legal framework

4.1 Introductory remarks

This Chapter is dedicated to the comparative analysis with the US legal framework. Looking at this framework is of great help in understanding how technical and administrative measures for protecting personal data are implemented in the e-health context. The US system has specific rules in this sector on measures for protecting the informational privacy of patients. Since PbD has been recognised as an international legal concept for the proactive protection of personal data, and it is based on the principles of Fair Information Practices – which were first defined in the US – this investigation aims to compare Article 25 of the GDPR and the HIPAA Privacy and Security Rules, which establish the specific US requirements for healthcare, including the implementation of safeguards to digital medical records.

This comparative analysis is a "micro comparison" since it compares individual legal rules[1300]. This methodology of comparative research requires the definition of a problem and a general hypothesis, and the rules can be compared if they have the same functions[1301]. The comparison aims to re-

1300 *See* Zweigert and Kötz, *Introduzione al diritto comparato*.

1301 *See* Zweigert and Kötz, *op. cit.* On functionalism, including critical aspects, *see* Michaels, "The Functional Method of Comparative Law"; Kischel, *Comparative Law*, pp. 88–101; Valcke, *Comparing law: comparative law as reconstruction of collective commitments*, pp. 194–205; Francesca Bignami. "Formal versus Functional Method in Comparative Constitutional Law". In: *Osgoode Hall Law Journal* 53 (2 2016), pp. 442–471; Samuel, *An Introduction to Comparative Law Theory and Method*, pp. 65–78; Jaakko Husa. "Functional Method in Comparative Law–Much Ado About Nothing?" In: *European Property Law Journal* 2.1 (2013), pp. 4–21; Antonios E. Platsas. "The functional and the dysfunctional in the comparative method of law: some critical remarks". In: *Electronic Journal of Comparative Law* 12.3 (2008); Michele Graziadei. "The functionalist heritage". In: *Comparative Legal Studies: Traditions & Transitions*. Oxford University Press, 2019, pp. 100–127. ISBN: 9780511522260; Jaakko Husa. "Farewell to functionalism or methodological tolerance?" In: *Rabels Zeitschrift für ausländisches und internationales Privatrecht/The Rabel Journal of Comparative and International Private Law* H. 3 (2003), pp. 419–447.

search the similarities and differences and frame the different solutions in common perspectives[1302]. As pointed out by Michaels, "functional equivalence is similarity in difference; it is finding that institutions are similar in one regard (namely in one of the functions they fulfil) while they are (or at least may be) different in all other regards"[1303]. HIPAA is devoted to the protection of identifiable health information by the implementation of organisational and technical measures. DPbD is a more general rule, but it is applicable to personal health data and mandates the implementation of organisational and technical measures, too. Both rules are obligations for the subject who shall comply. The common problem is the need to better protect personal health data in a digital world through safeguards. It is also interesting to understand whether or not an EHR may be used in both EU and US legal frameworks. The preliminary answer is no.

The Chapter begins with a brief overview of information privacy law in the US and privacy principles in US federal law. The goal is to investigate the similarities and differences with the data protection principles of the GDPR in the light of a PbD or DPbD implementation. Then, the Chapter focuses on US health privacy law and the central HIPAA Privacy and Security Rules. Finally, a comparison between DPbD and HIPAA is provided.

4.2 Overview of informational privacy in the US and the FIPS

As noted above, in the US the term "privacy" refers both to the protection of private and family life, i.e. privacy in the EU sense, and the protection of personally identifiable information (PII).

Actually, in US the right to privacy entails different conceptions[1304]: the *right to be let alone*, which was first defined by Warren and Brandeis[1305];

1302 *See* Zweigert and Kötz, *Introduzione al diritto comparato*, p. 49. On the history of legal comparison *see* Pier Giuseppe Monateri. "Il diritto comparato tra disciplina critica, scienza normale e ingegneria politica". In: *Comparare. Una riflessione tra le discipline*. Mimesis Edizioni, 2020, pp. 205–224. ISBN: 9788857567310.

1303 Michaels, "The Functional Method of Comparative Law", p. 371.

1304 *See* the prominent classification by Solove, "Conceptualizing privacy".

1305 In 1890, Warren and Brandeis adopted the expression "right to be let alone" that was firstly used by Judge Cooley in the book *Law of torts*. *See* Thomas M. Cooley. *Law of Torts*. Callaghan & Company, 1888. They interpreted the common law principle of an "inviolate personality" which protected personal writings and productions against publication in any form by invoking the protection of the privacy of an individual from any invasion carried out by

limited access to the self, i.e. the ability to shield oneself from unwanted access by others[1306]; *secrecy*, i.e. the concealment of certain matters from others[1307]; *control over personal information*, i.e. informational privacy[1308]; *person-hood*, i.e. the protection of one's personality, individuality, and dignity[1309]; and *intimacy*, i.e. the control over, or limited access to, one's intimate relationships or aspects of life[1310].

Historically, four US "invasion of privacy" torts protect the right to privacy in US common law: intrusion, disclosure of private facts, false light, and appropriation of name or likeness[1311]. Four different kinds of invasion correspond to four distinct privacy interests of a plaintiff[1312]:

---

the press during the new technological development (e.g. yellow journalism and the Kodak camera), unless one of the legitimate exceptions applied (i.e. consent to the publication, the presence of a public or general interest, and in the case of privileged communication under law of slander and libel). The limitations are described in Warren and Brandeis, "Right to privacy", pp. 214–218. *See* also Chapter 2, Section 2.2.

1306 As Solove pointed out in Solove, "Conceptualizing privacy", pp. 1102–1105, the conception of "limited access" is advanced by several theorists. Among them, Gavison defined limited access as the interaction between secrecy, anonymity, and solitude.

1307 This conception has been developed by the case law on the constitutional right to privacy. *See amplius infra*.

1308 *See infra* the analysis of US informational law.

1309 This conception of privacy has been used by the US Supreme Court. In *Union Pacific Railway Co. v. Botsford*, 141 U.S. 250 (1891), the US Supreme Court ruled that "no right is held more sacred, or is more carefully guarded by the common law, than the right of every individual to the possession and control of his own person, free from all restraint or interference of others, unless by clear and unquestionable authority of law". In *Planned Parenthood v. Casey*, 505 U.S. 833 (1992), the Supreme Court held that "because abortion involves the purposeful termination of potential life, the abortion decision must be recognized as sui generis, different in kind from the rights protected in the earlier cases under the rubric of personal or family privacy and autonomy".

1310 The conception of intimacy goes beyond autonomy and refers to the dimension of a private and close relationship among individuals. *See* Solove, "Conceptualizing privacy", pp. 1121–1124.

1311 The first categorisation of the four torts was provided by William Prosser. "Privacy". In: *Cal. L. Rev.* (48 1960), p. 383. *See* also Daniel J. Solove and Paul M. Schwartz. *Privacy, information, and technology*. Wolters Kluwer Law & Business, 2009. ISBN: 9780735579101, p. 26; Daniel J. Solove and Paul M. Schwartz. *Privacy Law Fundamentals*. International Association of Privacy Professionals, 2019. ISBN: 9781948771252, pp. 17–22, 28–29.

1312 *See* Restatement (Second) of Torts § 652B, 652D, 652E, 652C (1977). *See* also Schachter, *Informational and decisional privacy*, pp. 58–76.

1. Intrusion upon seclusion or solitude, or into the plaintiff's private affairs, meaning someone has intentionally transgressed the plaintiff's right to seclusion by physical trespass or otherwise and this intrusion is highly offensive to a reasonable person. As an example, in *Hamberger v. Eastman* 206 A. 2d 239 (1964) the court applied tort of intrusion for the installation of a secret recording device by the landlord/defendant in the bedroom of a couple/plaintiff;
2. Public disclosure of embarrassing private facts, meaning someone has published or made available facts that are not newsworthy or legitimate matters of public interest and this disclosure is highly offensive to a reasonable person. As an example, in *Barber v. Time, Inc.*, 159 S.W.2d 291 (Mo. 1942) the court held that publishing an article with a picture of a woman, who was in hospital for a particular physical ailment and was not a public figure, was a violation of her right to privacy;
3. Publicity which places the plaintiff in a false light in the public eye, meaning someone has given publicity to the plaintiff's matters that is highly offensive to a reasonable person and in disregard of the falsity of this matter. For instance, when a photograph is published out of context, the person portrayed can give rise to a false light action. In *Wood v. Hustler Magazine, Inc.*, 736 F.2d 1084 (1984) a stolen nude photograph of the plaintiff was published in a pornographic magazine without checking that the consent form was valid;
4. Appropriation of the plaintiff's name or likeliness for personal advantage, meaning someone has appropriated the plaintiff's name or likeness for their own use or benefits. As an example, the violation of the right of publicity was found in *Carson v. Here's Johnny Portable Toilets, Inc.*, 698 F.2d 831 (6th Cir. 1983) where a corporation used the famous catchphrase "here's Johnny" of the star of "The Tonight Show" on portable toilets without consent.

The US Constitution does not mention the right to privacy. Thus, privacy does not appear as a constitutional and fundamental right[1313]. Nonetheless, courts protect this individual right against coercion, violence or threats by their judicial interpretation of certain provisions of the Bill of Rights. In particular, US privacy has evolved from the interpretation

1313 *See* for a comparison with the EU Richards and Hartzog, "Privacy's Constitutional Moment", pp. 45–46.

of the First, Fourth, Fifth, Ninth and Fourteenth Amendments of the Constitution[1314].

1314 Amendment I: "Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances". Amendment IV: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized". Amendment V: "No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a Grand Jury, except in cases arising in the land or naval forces, or in the Militia, when in actual service in time of War or public danger; nor shall any person be subject for the same offence to be twice put in jeopardy of life or limb; nor shall be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation". Amendment IX: "The enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people". Amendment XIV: "Section 1. All persons born or naturalized in the United States, and subject to the jurisdiction thereof, are citizens of the United States and of the State wherein they reside. No State shall make or enforce any law which shall abridge the privileges or immunities of citizens of the United States; nor shall any State deprive any person of life, liberty, or property, without due process of law; nor deny to any person within its jurisdiction the equal protection of the laws. Section 2. Representatives shall be apportioned among the several States according to their respective numbers, counting the whole number of persons in each State, excluding Indians not taxed. But when the right to vote at any election for the choice of electors for President and Vice President of the United States, Representatives in Congress, the Executive and Judicial officers of a State, or the members of the Legislature thereof, is denied to any of the male inhabitants of such State, being twenty-one years of age, and citizens of the United States, or in any way abridged, except for participation in rebellion, or other crime, the basis of representation therein shall be reduced in the proportion which the number of such male citizens shall bear to the whole number of male citizens twenty-one years of age in such State. Section 3. No person shall be a Senator or Representative in Congress, or elector of President and Vice President, or hold any office, civil or military, under the United States, or under any State, who, having previously taken an oath, as a member of Congress, or as an officer of the United States, or as a member of any State legislature, or as an executive or judicial officer of any State, to support the Constitution of the United States, shall have engaged in insurrection or rebellion against the same, or given aid or comfort to the enemies thereof. But Congress may by a vote of two-thirds of each House, remove such disability. Section 4. The validity of the public debt of the United

So, despite the absence of an explicit reference in the Constitution, in the US there is a judicial recognition of a constitutional right to privacy in personal affairs[1315]. In the leading case *Grisworls v. Connecticut* 381 U.S. 479 (1965), the Court held that the Bill of Rights has "penumbras" where the right to privacy can be guaranteed[1316]. As an example, the constitutionally based interest in avoiding disclosure of private facts was held in *Whalen v. Roe* 429 U.S. 589 (1977), where the Supreme Court recognised a "threat to

States, authorized by law, including debts incurred for payment of pensions and bounties for services in suppressing insurrection or rebellion, shall not be questioned. But neither the United States nor any State shall assume or pay any debt or obligation incurred in aid of insurrection or rebellion against the United States, or any claim for the loss or emancipation of any slave; but all such debts, obligations and claims shall be held illegal and void. Section 5. The Congress shall have power to enforce, by appropriate legislation, the provisions of this article". For all the Amendments *see* the website of the US Senate at <senate.org>.

1315 *See* Daniel J. Solove and Paul M. Schwartz. *Information privacy law*. Wolters Kluwer Law & Business, 2011. ISBN: 9780735510401, pp. 247–313.

1316 The "constitutional penumbral theory" was explicitly set by *Grisworls v. Connecticut*, but in Justice Holmes' dissenting opinion of *Olmstead v. United States* 277 U.S. 438 (1928) the judge anticipated that "I am not prepared to say that the penumbra of the Fourth and Fifth Amendments covers the defendant". The prominent dissenting opinion of Judge Brandeis states: "The protection guaranteed by the Amendments is much broader in scope. The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. They recognized the significance of man's spiritual nature, of his feelings, and of his intellect. They knew that only a part of the pain, pleasure and satisfactions of life are to be found in material things. They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the Government, the right to be let alone – the most comprehensive of rights, and the right most valued by civilized men. To protect that right, every unjustifiable intrusion by the Government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment. And the use, as evidence in a criminal proceeding, of facts ascertained by such intrusion must be deemed a violation of the Fifth. Applying to the Fourth and Fifth Amendments the established rule of construction, the defendants' objections to the evidence obtained by wiretapping must, in my opinion, be sustained. It is, of course, immaterial where the physical connection with the telephone wires leading into the defendants' premises was made. And it is also immaterial that the intrusion was in aid of law enforcement. Experience should teach us to be most on our guard to protect liberty when the Government's purposes are beneficent. Men born to freedom are naturally alert to repel invasion of their liberty by evil-minded rulers. The greatest dangers to liberty lurk in insidious encroachment by men of zeal, well meaning but without understanding".

privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files" and ruled a duty to avoid disclosure which "has its roots in the Constitution". *Whalen v. Roe* is a leading case since the Court recognised both decisional privacy and informational privacy while evaluating the validity of the New York State statute on computerisation of schedules of prescription drugs.

Additionally, courts employ a flexible test by balancing the invasion of an individual's privacy against government or public interest (e.g. in searching and punishing crimes), and applying the concept of "reasonable expectation of privacy"[1317]. This concept is based on the Fourth Amendment, which protects against government searches and seizures. In the concurring opinion of *Katz v. United States* 389 U.S. 347 (1967) Justice Harlan analysed the case law and the Fourth Amendment, and stated:

> "My understanding of the rule that has emerged from prior decisions is that there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable'. Thus a man's home is, for most purposes, a place where he expects privacy, but objects, activities, or statements that he exposes to the 'plain view' of outsiders are not 'protected' because no intention to keep them to himself has been exhibited".

The "reasonable expectation of privacy" test is adopted by courts to solve privacy issues and balance competing interests[1318].

Informational or information privacy law in the US involves the rules that protect personal information[1319]. The concept of "personally identi-

---

1317 On this test *see* the leading cases of *Olmstead v. United States* 277 U.S. 438 (1928) (with Brandeis' dissenting opinion); *Katz v. United States* 389 U.S. 347 (1967) (interpreting the Fourth Amendment against unreasonable searches and seizures by the police); *California v. Greenwood* 486 U.S. 35 (1988); *Kyllo v. United States* 533 U.S. 27 (2001) (interpreting the Fourth Amendment against the use of a thermal-imaging device at a private home).

1318 *See ex multis* Daniel J. Solove. "Fourth amendment pragmatism". In: *BCL Rev.* 51 (2010), pp. 1511–1538; Richard A Epstein. "Privacy and the Third Hand: Lessons from the Common Law of Reasonable Expectations". In: *Berkeley Tech. LJ* 24 (2009), pp. 1199–1227; Peter Winn. "Katz and the origins of the reasonable expectation of privacy test". In: *McGeorge L. Rev.* 40 (2009), pp. 1–12; Richard A. Posner. "The uncertain protection of privacy by the Supreme Court". In: *The Supreme Court Review* 1979 (1979), pp. 173–216.

1319 On US informational privacy *see* Westin, *Privacy and Freedom*; Richard A. Posner. "The right of privacy". In: *Ga. L. Rev.* 12 (1977), pp. 393–422; Anita

fiable information" (PII) is not uniformly defined in this legal system, whereas personal data in the EU has a single definition which refers to any information relating to an identified or identifiable person[1320]. It has been pointed out that PII is largely limited to identified information, which is narrower than the EU concept[1321]. Therefore, when the term "information" is used in this book, it will refer to information that directly identifies the individual. However, as will be explained, the notion of identifiable health information is more similar to the EU definition of personal health data than to the concept of PII since it also may embed indirectly identifying information on health.

Informational privacy law is fragmented, and it is a "hodgepodge of various constitutional protections, federal and state statutes, torts, regulatory rules, and treaties"[1322]. Data controllers frequently rely on self-regulations on specific subject matters in defined commercial fields, and they are

---

L Allen. "Coercing privacy". In: *Wm. & Mary L. Rev.* 40 (1998), pp. 723–757; Julie E Cohen. "Examined lives: Informational privacy and the subject as object". In: *Stan. L. Rev.* 52 (1999), pp. 1373–1437; Paul M Schwartz. "Privacy and democracy in cyberspace". In: *Vand. L. Rev.* 52 (1999), pp. 1607–1701; Rotenberg, "Fair information practices and the architecture of privacy (What Larry doesn't get)"; Solove, "Conceptualizing privacy"; Richard C. Turkington and Anita L. Allen. *Privacy Law: cases and materials*. West Group, 2002; Schachter, *Informational and decisional privacy*; Will Thomas DeVries. "Protecting privacy in the digital age". In: *Berkeley Tech. LJ* 18 (2003), pp. 283–311; Daniel J. Solove. "A taxonomy of privacy". In: *U. Pa. L. Rev.* 154 (2005), pp. 477–560; Bamberger and Mulligan, "Privacy on the Books and on the Ground"; Richards and Hartzog, "Taking trust seriously in privacy law"; Anglim, Kirtley, and Nobahar, *Privacy Rights in the Digital Age*; Giovanella, *Copyright and Information Privacy: Conflicting Rights in Balance*, pp. 153–165; Solove and Schwartz, *Information privacy law*; Stephen P. Mulligan, Wilson C. Freeman, and Linebaugh Chris D. *Data Protection Law: An Overview*. Congressional Research Service R45631, 2019; Richards and Hartzog, "Privacy's Constitutional Moment"; Solove and Schwartz, *Privacy Law Fundamentals*.

1320 *See* Schwartz and Solove, "Reconciling personal information in the United States and European Union"; Mark Burdon. *Digital Data Collection and Information Privacy Law*. Cambridge Intellectual Property and Information Law. Cambridge University Press, 2020. ISBN: 9781108283717, pp. 155–170.

1321 *See* Schwartz and Solove, "Reconciling personal information in the United States and European Union", p. 891. The authors claimed that the US definition is too reductionist, whereas the European one is too broad. Therefore, they proposed the new concept of PII 2.0 by differentiating the protection of identifiable and identified information on a harm-based approach.

1322 Solove and Hartzog, "The FTC and the new common law of privacy", p. 587.

self-responsible for complying with them[1323]. Thus, in the US the rules for protecting PII are diffuse and there is not a uniform and omnibus act like the GDPR[1324]. The US approach is mainly sectoral[1325]. The legislator intervenes only on a narrowly targeted basis, when it is necessary[1326]. Even the so-called Privacy Act of 1974 was limited to a specific subject matter, i.e. the information used and disseminated by the federal agencies[1327]. The rationale of this legislative technique is the need to respond promptly to both scandals and regulatory vacuums caused by technological progress and evolution[1328]. So, the statutes are more granular and tailored to a specific field than in a one-size-fits-all regulation[1329].

Additionally, as previously mentioned, the US does not have a national data protection authority, but the FTC case plays a prominent and influential role, since the authority has a mandate on consumer protection under Section 5 of the FTC Act against unfair and deceptive commer-

1323 *See* Klitou, *Privacy-invading technologies and privacy by design. Safeguarding Privacy, Liberty and Security in the 21st Century*, p. 42.

1324 *See* Klitou, *op. cit.*, p. 41.

1325 *See* Kerstin N. Vokinger, Daniel J. Stekhoven, and Michael Krauthammer. "Lost in Anonymization – A Data Anonymization Reference Classification Merging Legal and Technical Considerations". In: *The Journal of Law, Medicine & Ethics* 48.1 (2020), pp. 142–148, pp. 143–144; Feldman and Haber, "Measuring and protecting privacy in the always-on era", p. 201. Conversely, the EU approach is omnibus.

1326 *See* Klitou, *Privacy-invading technologies and privacy by design. Safeguarding Privacy, Liberty and Security in the 21st Century*, p. 40.

1327 Privacy Act of 1974, 88 Stat. 1896. On the Privacy Act *see* Solove and Schwartz, *Information privacy law*, pp. 701–727.

1328 *See* Ugo Pagallo. *La tutela della privacy negli Stati Uniti d'America e in Europa: modelli giuridici a confronto*. Giuffrè Editore, 2008. ISBN: 8814142696, p. 61, which provides several examples of acts responding to scandals (e.g. Watergate and Privacy Act) and progress (e.g. Electronic Communications Privacy Act of 1986).

1329 *See* Michael L. Rustad and Thomas H. Koenig. "Towards a global data privacy standard". In: *Fla. L. Rev.* 71 (2019), pp. 365–453, p. 381.

1330 On the authority of the FTC *see* Solove and Hartzog, "The FTC and the new common law of privacy", p. 587; Kenneth A. Bamberger and Deirdre K. Mulligan. *Privacy on the ground: driving corporate behavior in the United States and Europe*. MIT Press, 2015. ISBN: 9780262029988, p. 48; Rustad and Koenig, "Towards a global data privacy standard", pp. 383–384; Vokinger, Stekhoven, and Krauthammer, "Lost in Anonymization – A Data Anonymization Reference Classification Merging Legal and Technical Considerations", pp. 144–145. *See* also Evan Selinger, Jules Polonetsky, and Omer Tene. *The Cambridge Handbook of Consumer Privacy*. Cambridge University Press, 2018. ISBN: 9781316831960.

cial practices[1330]. This authority recommends the PbD approach[1331] and promotes respect of the FIPs in business practices[1332]. As a result, the protection of the right to privacy has been connected to the promotion of consumer trust, and its regulatory development became consumer-oriented[1333]. In fact, the California Consumer Privacy Act (CCPA) of 2018 protects California consumers' privacy[1334].

In order to apply the PbD principle in the US system, it is necessary to investigate the informational privacy principles which apply there. Given the fragmented framework, there is not a single list of general principles for the processing of information.

Generally, in the US the processing of PII does not require a legal ground since this legal concept is neither used in the legislation nor developed by the literature. The free flow of information is highly promoted by the courts and the law regulates activities when they may cause harm to individuals[1335]. This is a crucial difference with the EU legal framework, where the grounds are defined in a closed list and lawfulness is the first data protection principle. In the US, the system focuses instead on a procedural notification mechanism called "notice-and-consent" or "notice-and-choice", where consent may be either an opt-in tool for allowing the use or disclosure of information or an opt-out one and the notice provides

1331 *See* Chapter 2, Section 2.2.

1332 An annual report of the FTC collects its enforcement activity on privacy. *See* the document from 2019 at <www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2019/2019-privacy-data-security-report-508.pdf>. Last accessed 06/10/2021.

1333 *See* the interesting analysis connected to the timing of privacy institutionalisation in Bamberger and Mulligan, *Privacy on the ground: driving corporate behavior in the United States and Europe*, pp. 185–186. *See* also Jules Polonetsky, Omer Tene, and Evan Selinger. "Consumer Privacy and the Future of Society". In: *The Cambridge Handbook of Consumer Privacy*. Cambridge University Press, 2018, pp. 1–21. ISBN: 9781316831960.

1334 The Act is included in California Civil Code sections 1798.100 *et seq*. It took effect in 2020. *See* <oag.ca.gov/privacy/ccpa>. Last accessed 06/10/2021. On CCPA *see* Eric Goldman. "An Introduction to the California Consumer Privacy Act (CCPA)". In: *Santa Clara Univ. Legal Studies Research Paper* (2020). *SSRN*: *<papers.ssrn.com/sol3/papers.cfm?abstract_id=3211013&download=yes>*; Nicholas F. Palmieri III. "Who Should Regulate Data: An Analysis of the California Consumer Privacy Act and Its Effects on Nationwide Data Protection Laws". In: *Hastings Sci. & Tech. LJ* 11 (2020), pp. 37–60.

1335 *See* Daniel J. Solove and Paul M. Schwartz. "ALI Data Privacy: Overview and Black Letter Text". In: *UCLA Law Review* 68 (2020), p. 21.

the information on the processing[1336]. The notice element is the common feature of this legal system. In addition, the system usually provides for exceptions to the authorisation/choice requirement.

Traditionally, informational privacy does not specify either the minimisation principle or the purpose specification requirement[1337]. However, in the healthcare context the data minimisation and purpose limitation principles have more importance[1338]. In summary, informational privacy requires not engaging in unfair or deceptive practices, not causing harm to consumers, and following the "notice-and-choice" paradigm[1339].

In this context, the Code of Fair Information Practice provided the principles for the processing of information in automated data systems at the federal level in 1973[1340]. FIPs are the practises which address how personal information should be collected, used, retained, managed, and deleted[1341]. The basic information privacy principles played and continue to play a significant role[1342]. The FIPs provide a starting point for different legal frameworks: they embed "a common language of privacy across countries"[1343]. Several sets of principles can be reconnected under the same term of FIPs, since this common ground is highly flexible.

Following the FIPs of 1973[1344] and using the current legal terms, processing of personal information should not be secret, and the individual should be able to know what information is collected and used by the controller (i.e. notice principle). The same individual should have the right to prevent the use of the information for a different purpose from the one

1336 *See* Burdon, *Digital Data Collection and Information Privacy Law*, p. 142.
1337 *See* Burdon, *op. cit.*, p. 174.
1338 *See* the following Section 4.3.
1339 Richards and Hartzog, "Privacy's Constitutional Moment", p. 19.
1340 On the FIPs *see supra* Chapter 2 Section 2.2.
1341 Anglim, Kirtley, and Nobahar, *Privacy Rights in the Digital Age*, p. 196.
1342 *See* Solove and Schwartz, *Information privacy law*, p. 37; Rotenberg, "Fair information practices and the architecture of privacy (What Larry doesn't get)"; Rubinstein and Good, "Privacy by Design: a Counterfactual Analysis of Google and Facebook Privacy Incidents'"; Richards and Hartzog, "Privacy's Constitutional Moment", pp. 14–20.
1343 Woodrow Hartzog. "The Inadequate, Invaluable Fair Information Practices". In: *Md. L. Rev.* 76 (2016), pp. 952–982, p. 960. In Richards and Hartzog, "Privacy's Constitutional Moment", p. 17, it is argued that "it is fair to say that the FIP model of privacy regulation has been adopted by virtually every country in the world that has decided to take data protection seriously".
1344 The list is provided in Chapter 2, Section 2.2, note no. 95. *See* US Department of Health, *Report of the Secretary's Advisory Committee on Automated Personal Data Systems Records Computers and the Rights of citizens*.

of the collection, unless consent is given (i.e. choice or consent principle). Moreover, the individual should have the right to correct or amend the information (i.e. participation principle). The controller should assure the reliability of information for its intended use and prevent any misuse (i.e. security principle). It has been pointed out that these principles in contemporary terms can be summarised as: transparency, use limitation, access and correction, data quality, and security[1345]. These FIPs were adopted in the Privacy Act of 1974[1346]. The FIPs of 1973 may also be evaluated as a narrower and limited set of principles similar to the GDPR's: fairness, lawfulness, purpose limitation, accuracy, and security.

The US literature frequently refers to the OECD's principles in discussing an evolution of the FIPs to be applied to PII[1347]. In fact, in the US there is no more recent set of comprehensive principles than the Code of the US Department of Health, Education and Welfare. The OECD's Guidelines of 1980 – which were revised in 2013, although the core principles were not emended – are not legally binding, but they have been highly influential in several countries, are broader than CoE's Convention 108, and contain eight basic internationally recognised principles[1348]. Despite the fact that only FIPs of 1973 have been explicitly referred to in the US framework, the OECD principles may be used there by practitioners as a baseline of the PbD approach.

The OECD's Guidelines have been considered the most influential form of FIPs; even though they do not use the term, they rely on the US version of 1973[1349]. The Guidelines are considered a "second generation of

1345 *See* Fred Cate. "The Failure of Fair Information Practice Principles". In: *Consumer Protection in the Age of the Information Economy*. 2006, pp. 343–379. ISBN: 9780754680468, p. 346. The author highlighted that the FIPs were the basis of the Privacy Act of 1974.

1346 *See* e.g. DeVries, "Protecting privacy in the digital age", p. 289.

1347 *See* e.g. Rotenberg, "Fair information practices and the architecture of privacy (What Larry doesn't get)"; Solove, "A taxonomy of privacy", p. 547; Schwartz and Solove, "Reconciling personal information in the United States and European Union", p. 909; Frederik Zuiderveen Borgesius, Jonathan Gray, and Mireille van Eechoud. "Open data, privacy, and fair information principles: Towards a balancing framework". In: *Berkeley Technology Law Journal* 30.3 (2015), pp. 2073–2131, pp. 2102–2107.

1348 A detailed investigation on the Guidelines is provided by Bygrave, *Data privacy law: an international perspective*, pp. 43–51.

1349 Anglim, Kirtley, and Nobahar, *Privacy Rights in the Digital Age*, p. 196. *See* also Hartzog, "The Inadequate, Invaluable Fair Information Practices", p. 958.

FIPs"[1350]. So, a summary of the principles as revised in 2013 is provided in the following Table 4.1[1351].

Table 4.1 OECD privacy principles

PRINCIPLE	DEFINITION
Collection Limitation	The collection of personal data should be limited and data should be obtained by lawful and fair means and, where appropriate, with knowledge or consent
Data Quality	Personal data should be relevant to the purposes, and, to the extent necessary for those purposes, they should be accurate, complete and up-to-date
Purpose Specification	The purposes should be specified no later than at the time of the collection and the subsequent use limited to that purpose or compatible with it
Use Limitation	Personal data should not be disclosed, made available or otherwise used for purposes other than those specified except with the consent of the data subject or by the authority of law
Security Safeguards	Personal data should be protected by reasonable security safeguards against security risks
Openness	There should be a general policy of openness about personal data

1350 Hartzog, *op. cit.*, p. 965.
1351 The definitions of the principles have been condensed from the OECD's Guidelines of 2013.

PRINCIPLE	DEFINITION
Individual Participation	Individuals should have the right to obtain information, erasure, and rectification
Accountability	The data controller should be accountable for complying with measures which give effect to the other principles

Comparing the OECD's principles with the GDPR, it can be argued that some principles are similar[1352]. The OECD's framework does not provide either the legal grounds of processing of the GDPR or other conditions for a lawful processing. It refers to consent only, and does not contain additional safeguards for particular categories of data[1353]. However, the collection limitation principle has a similar rationale as the lawfulness and fairness principles: setting limits to collection activities in the absence of legal conditions[1354]. At the same time, it may be argued that the principle of collection limitation relies too heavily on the notion of consent[1355]. The data quality, purpose specification, use limitation and security safeguard principles are similar to purpose limitation, accuracy and integrity and confidentiality principles, but they are less detailed. The OECD principles do not contain either data minimisation or storage limitation principles. The accountability principle is consistent with the definition of Article 5(2) GDPR. In the OECD's framework there are completely new principles, i.e. openness and individual participation, but they entail safeguards that the GDPR establishes in Chapter III on the rights of the data subject. As a result, other very detailed rules reflect those principles.

1352 In Bygrave, *Data privacy law: an international perspective*, p. 45, the author argued that the OECD Guidelines are even similar to the former version of the CoE principles since the bodies collaborated extensively during the drafting. *See* also the analysis by Paul De Hert. "Data protection as bundles of principles, general rights, concrete subjective rights and rules: piercing the veil of stability surrounding the principles of data protection". In: *Eur. Data Prot. L. Rev.* 3 (2017), pp. 160–179, which comments on the principles and their roles in the legal systems.

1353 This choice is consistent with US law.

1354 On the rationale of fair and lawful processing *see* Bygrave, *Data privacy law: an international perspective*, pp. 146–147.

1355 *See* Anglim, Kirtley, and Nobahar, *Privacy Rights in the Digital Age*, p. 197.

The GDPR provides broader guarantees since it is a specific framework on data protection, whereas the OECD's framework aims to generally provide general internationally recognised principles. So, the application of a PbD or a DPbD approach might differ since the implementation may follow partially different principles. Nonetheless, the core data protection or informational privacy principles may be similar.

Cavoukian often referred to the OECD's version of the FIPs for a PbD approach[1356]. Despite the multiple versions of the FIPs, Cavoukian classified five core principles: purpose specification and use limitation – i.e. reasons for the processing of PII should be identified at or before the time of collection and the use or disclosure should be limited to them – user participation and transparency – i.e. individuals should be empowered – and strong security (confidentiality, integrity, availability)[1357]. These principles may be the starting point for business and management practices.

It should be noted that in the Report of 2012 on PbD the FTC used the notion of FIPs of 1973[1358]. The same authority previously defined five core principles for the protection of online consumers' privacy after reviewing the FIPs, the OECD's of 1980, the DPD's principles, and the Canadian framework: notice or awareness of consumers, choice or consent, access or participation, integrity or security, and enforcement or redress[1359]. The definitions are reported in the following Table 4.2[1360].

1356 *See* e.g. Cavoukian, *Privacy by design: From rhetoric to reality*, p. 12.

1357 *See* Cavoukian, *op. cit.*, pp. 165–166.

1358 *See* Chapter 2 Section 2.2. The authority also made reference to the proposal by Congress on a "Consumer Privacy Bill of Rights" based on the FIPs, which was never approved. The privacy principles in this proposal were: transparency, individual control, respect for context, security, access, accuracy, focused collection, and accountability. *See* the Report by the White House during the Obama administration, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy* of February 2012 at <obamawhitehouse.archives.gov/sites/default/files/privacy-final. pdf>. Last accessed 06/10/2021.

1359 *See* FTC Federal Trade Commission. *Privacy Online: A Report to Congress*. FTC Report, 1998.

1360 The definitions of the principles have been condensed from the FTC's Report of 1998 and Cate, "The Failure of Fair Information Practice Principles", p. 352.

Table 4.2 FTC privacy principles

PRINCIPLE	DEFINITION
Notice/Awareness	Consumers should receive notice of an entity's policy before the collection of PII in order to make informed decisions
Choice/Consent	Consumers should have the opportunity to choose how PII may be used, for secondary use also
Access/Participation	Consumers should have the opportunity to access PII and contest accuracy and completeness
Integrity/Security	PII should be accurate and secure through reasonable steps
Enforcement/Redress	There should be a mechanism in place to enforce the core principles of privacy protection

It has been pointed out that this list is a "remarkable landmark along the evolution of modern FIPS" since the FTC cited the full range of FIP documents, including Directive 95/46, and identified the five principles that those documents have in common[1361]. However, the FTC's principles missed the fundamental collection or use limitation principle, the fairness and the data quality or accuracy principles, and reduced the entire framework to the notion of notice. In particular, the FTC's approach is focused on the concepts of "privacy as control" and "notice-and-choice", where the notice, and the following opt-out or opt-in individual's authorisation, are central.

Hence, the FTC's set of principles guarantees the fewest substantive protections, whereas the OECD Guidelines may be considered to be somewhere in the middle, and the EU's principles entail the widespread protective framework[1362].

While discussing the application of PbD in the US legal framework, two US scholars, Rubinstein and Good, proposed a new formulation of the FIPs which encapsulated other interpretations of the principles so that it

1361 Cate, *op. cit.*, p. 353. Later, the FTC abandoned the enforcement principle.
1362 *See* the comment of *ibid.*

could be used as a set of design principles[1363]. They argued that the FIPs could be considered the foundation of international privacy law and, as they are open-ended principles, could be flexible and with a wide range of application[1364]. The principles are reported here *verbatim*[1365]:

1. "Defined limits for controllers and processors of personal information on the collection, processing, and use of personal data (often referred to as data minimization);
2. Data quality (accurate, complete, and timely information);
3. Limits on data retention;
4. Notice to individual users;
5. Individual choice or consent regarding the collection and subsequent use of personal information;
6. Reasonable security for stored data;
7. Transparent processing systems that affected users can readily understand and act on;
8. Access to one's personal data;
9. Enforcement of privacy rights and standards (including industry self-regulation, organizational measures implemented by individual firms, regulatory oversight and/or enforcement, and civil litigation)".

This formulation of the FIPs takes into account the previous interpretations of the OECD Guidelines and the FTC, by specifying the data quality principle, the importance of the notice and choice, the openness and enforcement principles. Additionally, it is more similar to the GDPR than the OECD's framework since this list of principles includes data minimisation, data retention and transparency. Thus, a PbD implementation with these nine principles in the US system may be more consistent with a DPbD approach whether or not these principles are used in the design stage of technologies and business practices.

The US alignment with the GDPR principles – which is part of the so-called "Brussels Effect"[1366] – is indirectly promoted by the American

1363 *See* Rubinstein and Good, "Privacy by Design: a Counterfactual Analysis of Google and Facebook Privacy Incidents"", p. 1343.

1364 *See* Rubinstein and Good, *op. cit.*, p. 1344.

1365 *See ibid.*

1366 The so-called "Brussels Effect" was coined by Anu Bradford in 2012. *See* lastly Anu Bradford. *The Brussels effect: How the European Union rules the world*. Oxford University Press, 2020. ISBN: 9780190088583. According to Bradford, the EU influenced and influences policies and norms around the world, including legislative initiatives and business behaviours. As reported by Bygrave, the data protection domain is the example *par excellence* of this effect. *See* Lee

Law Institute (ALI), which proposed the following data privacy principles in a law reform project in 2019: transparency, individual notice, consent, confidentiality, use limitation, access and correction rights, data retention and disposal duties, data portability, data security, onward transfer, and accountability and enforcement[1367]. These principles aimed to be consistent with US privacy law and advance it boldly by revitalising the FIPs and by using EU legal categories, like data controller or processor[1368]. The project has been promoted by the two prominent US professors Paul M. Schwartz and Daniel J. Solove[1369].

First of all, the transparency principle follows the traditional "notice-and-choice" US approach by requiring a transparency statement to be used by regulators so that "the data controllers and data processors clearly, conspicuously, and accurately explain the current personal data activities". Then, the individual notice principle entails the need to "inform individuals about how their personal data is being collected, used, and shared" in a privacy notice, and the provision of a heightened notice "for any data activity that is significantly unexpected or that poses a significant risk of causing material harm to data subjects"[1370]. This double notice enhances the individual side of the "notice-and-choice" approach since the subject may be more conscious of what the processing entails and may give a more informed consent. The US system traditionally relies on consent more than the EU system, so the existence of the notice and the following clear consent are necessary, especially where a heightened notice is provided[1371].

A. Bygrave. "The 'Strasbourg Effect' in Data Protection: Its Logic, Mechanics and Prospects in Light of the 'Brussels Effect'". In: *University of Oslo Faculty of Law Research Paper No. 2020–14* (2020). Both the DPD and the GDPR influenced norms worldwide. The *de facto* "Europeanisation" creates a global standard of protection. So, the GDPR had the effect of turning European-style privacy laws at a global level. *See* Richards and Hartzog, "Privacy's Constitutional Moment", p. 4. A paradigmatic example of this effect in the US is the California Consumer Protection Act, which is important since tech and key companies of the digital age are the headquartered in Silicon Valley's State. The CCPA has many similarities with the GDPR, but is more limited in scope. On non-convergence between EU and US data protection laws *see* Fernanda G. Nicola and Oreste Pollicino, "The Balkanization of Data Privacy Regulation". In: *W. Va. L. Rev.* 61 (2020), pp. 60–105.

1367 *See* Rustad and Koenig, "Towards a global data privacy standard", p. 386.

1368 Solove, "Conceptualizing privacy", p. 7.

1369 *See* Solove and Schwartz, "ALI Data Privacy: Overview and Black Letter Text".

1370 Solove, "Conceptualizing privacy", pp. 16–17.

1371 Solove, *op. cit.*, p. 18.

The confidentiality principle is a novelty for the US system that closes a gap in the framework since the concept uses the US notion of the "reasonable expectation of privacy" to protect information "when there is an express or implied promise of confidentiality or a legal obligation of confidentiality"[1372]. As previously noted for the EU legal framework, the duty of confidentiality is particularly important in the e-health sector. So, the introduction of this principle in the FIPs for a PbD approach may be highly recommended.

The use limitation principle refers to the secondary use of PII: the collection does not require a specific legal ground, but the secondary use should seek consent or an exception to allow the processing. So, a lawfulness principle is not included, but the secondary use of information shall be justified. This secondary use is exceptionally allowed for the "fulfilment of a contract to which the data subject is a party", for "the significant advancement of the protection of health or safety of the data subject or other people", and "as in the GDPR, a catch-all for serving a significant legitimate interest without posing a significant risk of material harm to the data subject or others and without being significantly unexpected"[1373]. These scenarios are similar to some legal grounds of the GDPR in Articles 6 and 9.

Moreover, the principles of access and correction include the right to access to PII and the right to request correction of any error in the information to protect its accuracy. The data portability principle has also been included since it is an emerging concept used both in the GDPR and in the California Consumer Privacy Act[1374].

Then, the data destruction principle states that PII "that no longer serves the uses identified in the notice that was provided or other legitimate interests shall be destroyed using reasonable procedures to ensure that it is unreadable or otherwise indecipherable"[1375]. Other limits shall be set to the retention of information, which shall be stored "only for legitimate purposes that are consistent with the scope and purposes of notice provid-

1372 Solove, *op. cit.*, p. 20.
1373 Solove, *op. cit.*, p. 21.
1374 *See* Solove, *op. cit.*, p. 22.
1375 Solove, *op. cit.*, p. 23.

ed to the data subject"[1376]. Nonetheless, a right to erasure is not included in the ALI's principles in spite of the specific provision in the CCPA[1377].

The data security principle has been framed as one of "the most common requirements of data privacy statutes and regulations", which provides reasonable safeguards for protecting information, and the accountability principle requires the development of reasonable and comprehensive privacy programmes[1378]. It should be noted that a PbD principle is not included by the ALI for "not pushing US law too far", but it is specified in the accountability principle description that[1379]:

> "A data controller or data processor shall analyze the privacy and security implications early on in the development of any new product, service, or process. This analysis shall be conducted in a reasonable manner, at a reasonable time, and with a reasonable thoroughness. This analysis shall be documented. A data controller or data processor shall examine how the product, service, or process should be designed to address the privacy or security issues identified in the analysis. The outcome of this examination shall be reflected in the final design of the product, service, or process. Reasonable design choices shall be made. Design choices and the reasoning that supports them shall be documented".

So, the general accountability approach refers to design choices, but it is more organisational than technical in accordance with the vision of the FTC's Report on PbD. At the same time, the risk management, security, contextualised and flexible approach proposed by the ALI project are similar to the considerations previously exposed on Article 25 of the GDPR.

Finally, the ALI's enforcement principle mandates effective, proportionate and dissuasive remedies[1380]. This ALI's project is a prominent effort to reform the FIPs by including OECD's and GDPR's concepts in light of a modern path forward of informational privacy. However, FIPs alone are not sufficient in affecting the design of technologies and business

---

1376 *Ibid.*

1377 CCPA, Cal. Civ. Code § 1798.105. The ALI project does not include a right to erasure or to be forgotten because there is no agreement in the ALI's membership. *See ibid.*

1378 Solove, *op. cit.*, pp. 24–27.

1379 Solove, *op. cit.*, p. 44.

1380 Solove, *op. cit.*, p. 28. All the principles described above are summarised in the Black Letter at Solove and Schwartz, "ALI Data Privacy: Overview and Black Letter Text", pp. 32–46.

practices. As argued by Hartzog, FIPs do not address the structural problems and risks of data processing[1381]. Since they are centred around the concepts of "control over information" and consent ("notice-and-choice"), they are not enough in the digital age where the way in which technologies and practices are designed is crucial. Thus, privacy law should address the design of technologies, and FIPs should be supported and enforced with design-based protection[1382]. Including a PbD principle is pushing US law far towards a more protective and realistic privacy approach.

Having discussed the US legal framework for PII and the principles that can be applied, the next section deals with US rules for the protection of personal health information and for processing electronic health information in the EHRs.

4.3 The US legal framework for health informational privacy and for EHRs

The healthcare domain demands a "deep, culturally significant, and relationship-based" level of protection because of the nature of information involved and of the exceptional possible threats[1383]. In the US several rules regulate health informational privacy or "medical privacy" at both the state and federal level[1384]. The US Constitution does not explicitly grant the

1381 *See* the criticism in Hartzog, "The Inadequate, Invaluable Fair Information Practices". In sum, "FIPs are inadequate because: (1) they have important blind spots regarding the collection, use, and disclosure of personal information that cannot be resolved through more specificity or better implementation; and (2) they fail to address the user bandwidth problem that would persist even if users were given every bit of control imaginable over their data" (at p. 966).

1382 *See* Hartzog, *op. cit.*, pp. 981–982.

1383 Nicolas P. Terry. "Regulatory disruption and arbitrage in health-care data protection". In: *Yale J. Health Pol'y L. & Ethics* 17 (2017), pp. 143–208, p. 197.

1384 *See* Solove and Schwartz, *Information privacy law*, pp. 429–559. On US privacy of health care information *see* Paul M Schwartz. "Privacy and the economics of personal health care information". In: *Tex. L. Rev.* 76 (1997), p. 1; Joy Pritts. *The state of health privacy: an uneven terrain (a comprehensive survey of state health privacy statutes)*. Health Privacy Project, Institute for Health Care Research and Policy, 1999; Turkington and Allen, *Privacy Law: cases and materials*, pp. 221–293; Frank Pasquale and Tara Adams Ragone. "Protecting health privacy in an era of big data processing and cloud computing". In: *Stan. Tech. L. Rev.* 17 (2013), pp. 595–654; Yann Joly and Bartha Maria Knoppers. *Routledge handbook of medical law and ethics*. Routledge, 2016. ISBN: 9781138204126; Sharona Hoffman. "Medical Privacy and Security". In: *The Oxford Handbook of U.S. Health Law*. 2017, pp. 267–288. ISBN: 9780199366521; Frank Pasquale.

federal government authority over health, but a federal system and state systems coexist[1385]. Public health is managed both by the federal system and by the 50 separate states legal systems, where local systems operate under stakeholders' agreements[1386].

Thus, in the US there is a lack of a unified and coordinated healthcare system: the provision of healthcare is managed by "a patchwork of public and private insurance plans", "federal, state, and local governments", and "institutions and individual providers who are often unconnected to one other"[1387]. US citizens usually obtain healthcare coverage through employer health plans or private health insurance plans[1388]. So, contracts are signed between employer, employee, and insurance companies, or between the individual and a private fund or company. It has even been pointed out that since most people receive health benefits at their workplace, employers have a great incentive to weed out employees with expensive healthcare needs so as to pay less for the provision of medical services[1389]. As a result, employers frequently require information about medical history of employees' families or genetic information[1390]. The Genetic Information Nondiscrimination Act (GINA) of 2008 protects against

---

"Health Information Law". In: *The Oxford Handbook of U.S. Health Law*. 2017, pp. 193–212. ISBN: 9780199366521; Christina Munns and Subhajit Basu. *Privacy and healthcare data: 'choice of control' to 'choice' and 'control'*. Taylor & Francis, 2016. ISBN: 9781472426864, pp. 81–98; Daniel J. Solove and Paul M. Schwartz. "Health privacy". In: *Information privacy law*. Wolters Kluwer Law & Business, 2018, pp. 475–602. ISBN: 9781454892755; Vokinger, Stekhoven, and Krauthammer, "Lost in Anonymization – A Data Anonymization Reference Classification Merging Legal and Technical Considerations"; Matthew DeNoncour. *Healthcare technology regulation in the US*. In: *Healthtech, Law and Regulation.* Elgar Commercial Law and Practice, 2020 pp. 80–113. ISBN: 9781839104893.

1385 Margo Edmunds. "Governmental and legislative context of informatics". In: *Public health informatics and information systems*. Springer, 2014, pp. 47–66. ISBN: 9780387227450, p. 50.

1386 *Ibid.* This article defines the US public health system as a three-tiered network of state and local agencies that work in partnership with the federal government.

1387 *See* Sara E. Wilensky and Joel B. Teitelbaum. *Essentials of Health Policy and Law*. Jones & Bartlett Learning, 2019. ISBN: 9781284151619, p. 49.

1388 *See* Joly and Knoppers, *Routledge handbook of medical law and ethics*, p. 56.

1389 Schwartz, "Privacy and the economics of personal health care information", p. 26.

1390 *See* Solove and Schwartz, *Information privacy law*, pp. 540–541.

employers' and insurance companies' discrimination based on genetic tests[1391].

Medical information is collected and used through these insurance plans, during the traditional healthcare provision, and in e-health processing (e.g. apps, Big Data). So, in this legal framework health information may be processed by: employers, who wish to hire an employee in good health; business entities, which manage medical financial funds; drug companies or advertisers and marketers; and healthcare providers and health insurers[1392].

Even in the US system, medical confidentiality is frequently connected to an individual's right to privacy[1393]. The right to privacy limits data collection, whereas confidentiality limits the disclosure of information[1394]. US physicians take the Hippocratic Oath, and must not reveal information and communications under the ethical duty of confidentiality and the physician-patient fiduciary relationship. The American Medical Association's Code of ethics (AMA's Code) explicitly mentions this duty by specifying that physicians shall respect patients' confidences to safeguard their autonomy and trust[1395].

1391 Genetic Information Nondiscrimination Act, Public Law 110–233, 122 STAT. 881. GINA prohibits the collection of information. *See* for a legal critical analysis Bradley A. Areheart and Jessica L. Roberts. "GINA, Big Data, and the Future of Employee Privacy". In: *Yale L.J.* 128 (2018), pp. 710–790.

1392 *See* Sharona Hoffman and Andy Podgurski. "In sickness, health, and cyberspace: protecting the security of electronic private health information". In: *BCL. Rev.* 48 (2007), pp. 331–386, p. 334.

1393 *See* Anglim, Kirtley, and Nobahar, *Privacy Rights in the Digital Age*, pp. 352–354. This article reports that all 50 American States have enacted legislation on medical confidentiality, and the breach of the fiduciary relationship between the physician or medical professionals and the patient. The duty is actually and usually an obligation.

1394 Nicolas P. Terry. "Privacy and the health information domain: properties, models and unintended results". In: *European Journal of Health Law* 10.3 (2003), pp. 223–237, p. 224.

1395 The duty is currently framed as: "A physician shall respect the rights of patients, colleagues, and other health professionals, and shall safeguard patient confidences and privacy within the constraints of the law". *See* AMA website at <www.ama-assn.org/about/publications-newsletters/ama-principles-medical-ethics>. Last accessed 06/10/2021. The Code of Medical Ethics Opinion 3.1.1 AMA specifies that respecting patient privacy means respecting patient autonomy and trust. Patient privacy includes the respect of personal space (i.e. physical privacy), personal data (i.e. informational privacy), personal choices (i.e. decisional privacy), and personal relationships with family members and other intimates (i.e. associational privacy). In the Code of Medical Ethics Opin-

In this context, the primary source of rule is the statutory level, but privacy torts and tort law (i.e. common law) protect medical confidentiality, too. In *McCormick v. England* 494 S.E.2d 431 (S.C. Ct. App. 1997), the holding first states: "breach of confidentiality is a distinct tort from the tort of public disclosure of private facts" (i.e. a privacy tort)[1396]. The duty of confidentiality is based on the existence of a fiduciary relationship between the patient and the physician. As pointed out in *Doe v. Roe* 93 Misc. 2d 201 (1977), "the very needs of the profession itself require that confidentiality exist and be enforced". The same duty persists in the information society where health records are kept in electronic form. In *Doe v. Mills*, 536 N.W.2d 824 (Mic. App. 1995), the court found disclosure of medical information to be a violation of a privacy tort. Breach of confidentiality is recognised as the tort which provides remedy when a professional divulges confidential information unlawfully[1397]. In *Susan S. v. Israels*, 55 Cal.App.4th 1290 (1997) the court recognised a public disclosure of private facts tort for the disclosure of mental health records.

When the Supreme Court held the constitutionally based interest in avoiding disclosure of private facts in *Whalen v. Roe*, the Court recognised the protection of health records and drug records which could be disclosed for state public interest. The Court ruling has been interpreted as the

---

ion 3.2.1, the Association further elaborated on confidentiality of personal information. It pointed out that patients could decide whether and to whom their personal health information is disclosed, but patient's consent might not be required. The disclosure should be restricted to the minimum amount of necessary information, and the patient should receive a notification whenever feasible. Allowed exceptions to the consent should be the disclosure to other healthcare professionals for providing care, to public authorities under explicit law, and to other third parties for a third and independent medical judgement (for patient's safe).

1396 On tort liability for disclosure of patient information *see* Solove and Schwartz, *Information privacy law*, pp. 437–446; Solove and Schwartz, "Health privacy", pp. 483–492.

1397 Solove and Schwartz, *Privacy, information, and technology*, p. 31. It has been pointed out that most states establish a lawful disclosure without individual consent to protect third parties from identifiable harm, to report information for public health purposes under law, and to report a medical emergency. *See* Lawrence O. Gostin, James G. Hodge Jr., and Lauren Marks. "The Nationalization of Health Information Privacy Protections". In: *Tort & Insurance Law Journal* (2002), pp. 1113–1138, p. 1120. On liability concerns of electronic medical record *see* Sharona Hoffman and Andy Podgurski. "E-Health hazards: provider liability and electronic health record systems". In: *Berkeley Tech. LJ* 24 (2009), pp. 1523–1582, which focuses on EHRs and PHRs.

judicial recognition of a right to health informational privacy[1398]. In *Doe v. Southeastern Pennsylvania Transp. Authority* 886 F. Supp. 1186 (E.D. Pa. 1994), the court observed that confidentiality of medical records may fall under the protection of the Fourth Amendment of the Constitution. Disclosure of medical information is not a constitutional privacy violation in itself since disclosure may be reasonably necessary or permissible[1399]. However, courts can protect patients' right to privacy under the Constitution and under certain circumstances. As an example, in *Peninsula Counseling Center v. Rahm* 105 Wn.2d 929 (1986), judge Pearson's dissenting opinion stated that medical information is "of the type which, if disseminated, would tend to cause a reasonable person substantial concern, anxiety, or embarrassment"; therefore, this information should be protected "from compelled disclosure". Once again, a balancing act between public interests and an individual's privacy interest is performed by courts.

A number of states protect medical information in medical confidentiality laws, patient access law, and comprehensive health privacy laws[1400]. In particular, it has been pointed out that state law requirements grant patients access to their medical records, restrict use and disclosure of personal health information, establish privileges for specific categories, institute requirements relating to specific medical conditions, such as alcohol or sexually transmitted disease, and require breach notification in particular circumstances[1401]. Thus, medical confidentiality shall be maintained under statutory, common law and ethical duties[1402].

An important basis for protecting confidentiality in the health context can also be found in the FIPs of 1973 since they were drafted by the US Department of Health with reference to the computerised processing

1398 Healthcare providers could store the information of patients who received prescriptions for drugs that could be illegally abused on the basis of a state procedure and public interest despite the privacy rights of the patients. On this case *see* also the Annotation on the Supreme Court's website at <supreme.justia.com/cases/ federal/us/429/589/>. Last accessed 06/10/2021.

1399 *See* Schachter, *Informational and decisional privacy*, p. 350.

1400 *See* Solove and Schwartz, *Information privacy law*, p. 462; Solove and Schwartz, "Health privacy", p. 506.

1401 Hoffman, "Medical Privacy and Security", p. 274.

1402 *See* e.g. the interesting case of a surgeon with AIDS. In *Estate of Behringer v. Medical Center at Princeton*, 249 N.J. Super. 597 (1991), the holding established a standard of confidentiality on HIV tests and illustrated how to balance privacy against public interest on disclosure.

of medical data by public health agencies[1403]. The Department of Health and Human Services (hereinafter: HHS) is the major operating agency for protecting health and health information of US citizens[1404].

In 1996 the US Congress enacted a federal health regulation: the Health Insurance Portability and Accountability Act of 1996 (hereinafter: HIPAA)[1405]. This Act is a "landmark legislative event" for healthcare in the US[1406]. The primary purpose of this regulation was to permit employees to change jobs without losing the existing conditions in their health plans, and then allow more flexible insurance claims at the federal level[1407]. So, the HIPAA protected the continuity of health insurance when employees changed jobs and sought to avoid discrimination against individual participants in and beneficiaries of group health insurance plans[1408]. It has been pointed out that the HIPAA even envisaged the need to standardise health data to enhance its electronic exchange and improve national healthcare delivery[1409]. The first version of the text did not provide any rules mandating privacy protection for medical data, but the public debate and several privacy advocates claimed a need for it[1410]. Therefore, the Department of Health and Human Services promoted several regulations on privacy and security to be integrated into the HIPAA. Only in 2002, during the Bush administration, was the HIPAA Privacy Rule approved and in 2003 it became effective[1411]. In the same year the Security Rule was published, and it became effective in 2005.

1403 William A. Yasnoff. "Privacy, Confidentiality, and Security of Public Health Information". In: *Public Health Informatics and Information Systems*. Springer, 2014, pp. 155–172. ISBN: 9780387227450, p. 158.

1404 *See* Edmunds, "Governmental and legislative context of informatics", p. 53.

1405 Health Insurance Portability and Accountability Act of 1996 (HIPAA), 110 Stat. 1936 (1996); 45 USC § 1320d-2(b).

1406 Edmunds, "Governmental and legislative context of informatics", p. 56.

1407 *See* Solove and Schwartz, *Information privacy law*, p. 463; Solove and Schwartz, "Health privacy", p. 509.

1408 Schwartz, "Privacy and the economics of personal health care information", p. 40.

1409 Edmunds, "Governmental and legislative context of informatics", p. 56.

1410 On the first version of HIPAA *see* e.g. Francoise Gilbert. "Privacy of Medical Records – The Health Insurance Portability and Accountability Act of 1996 Creates a Framework for the Establishment of Security Standards and the Protection of Individually Identifiable Health Information". In: *N.D.L. Rev.* 73 (1997), pp. 93–108. The author concluded that the Act did not sufficiently address confidentiality issues.

1411 For a comment before the application *see* Peter D Jacobson. "Medical records and HIPAA: is it too late to protect privacy?". In: *Minn. L. Rev.* 86 (2001), pp.

So, the HIPAA requirements for protecting medical information are the Privacy and Security Rules, which are published at 45 Code of Federal Regulations (C.F.R.) parts 160 through 164[1412]. While these provisions are not explicit, they identify personal health information as a category of sensitive information deserving higher protection than common PII[1413].

The HIPAA pre-empts statutory national law unless the latter is more stringent than the former. The more stringent requirement refers to the "ability of the patient to withhold permission and to effectively block disclosure" of personal health information[1414]. So, the law is more stringent when it gives more control to the patient over information. As an example, a more stringent rule is California's Confidentiality of Medical Information Act, which is more comprehensive than the HIPAA[1415]. Other examples may be provided by the case law. In *Creely v. Genesis Health Ventures, Inc.*, 2004 U.S. Dist. LEXIS 25489 (ED Pa Dec. 17, 2004), a

---

1497–1514. The author argued that privacy protection is as necessary as the disclosure and use of PHI for public health purposes. *See* also Joy L. Pritts. "Altered states: state health privacy laws and the impact of the Federal Health Privacy Rule". In: *Yale J. Health Pol'y L. & Ethics* 2 (2001), pp. 327–364, which gave great importance to the right to access and amend health records, and Nathan J Wills. "A tripartite threat to medical records privacy: Technology, HIPAA's privacy rule and the USA Patriot Act". In: *JL & Health* 17 (2002), pp. 271–296, which summarises the requirements by highlighting their rationales and criticising several aspects.

1412 Generally on HIPAA Privacy and Security Rules *see* Burdon, *Digital Data Collection and Information Privacy Law*, p. 175; Hoffman, "Medical Privacy and Security"; Yasnoff, "Privacy, Confidentiality, and Security of Public Health Information"; Edmunds, "Governmental and legislative context of informatics"; Di Iorio and Carinci, "Privacy and health care information systems: where is the balance?"; Janine Hiller et al. "Privacy and security in the implementation of health information technology (electronic health records): US and EU compared". In: *BUJ Sci. & Tech. L.* 17 (2011), pp. 1–39; Dumortier and Verhenneman, "Legal regulations on electronic health records: a prerequisite or an unavoidable by-product? – The legal aspects of electronic health records in Europe and the US analysed"; Gostin, Hodge Jr., and Marks, "The Nationalization of Health Information Privacy Protections"; Tamela J. White and Charlotte A. Hoffman. "The Privacy Standards Under the Health Insurance Portability and Accountability Act: A Practical Guide to Promote Order and Avoid Potential Chaos". In: *W. Va. L. Rev.* 106 (2004), pp. 709–780.

1413 On the same opinion *see* Dumortier and Verhenneman, "Legal regulation of electronic health records: a comparative analysis of Europe and the US", p. 33.

1414 *See* Solove and Schwartz, *Information privacy law*, p. 479.

1415 *See* California Civil Code 56.10 – 56.16. *See* also Anglim, Kirtley, and Nobahar, *Privacy Rights in the Digital Age*, p. 426.

state privacy law was considered more stringent than the HIPAA since it prohibited use or disclosure in circumstances under which such use or disclosure otherwise would have been permitted under the HIPAA. In *United States Ex Rel. Pogue v. Diabetes Treatment Ctrs. of Am.*, 2004 U.S. Dist. LEXIS 21830 (DDC May 17, 2004), Florida law was not pre-empted as more stringent than HIPAA. Moreover, a state law may be more protective than the HIPAA on specific types of health information (e.g. genetic or mental health)[1416].

Where the state law is more stringent than the HIPAA, it shall apply. However, it is difficult to determine whether the state law is more stringent than the HIPAA, as argued by Tomes[1417]. In *Arons v. Jutkowitz*, 9 N.Y.3d 393, 850 N.Y.S. 2d 345, 880 N.E.2d 831, 2007 N.Y. LEXIS 3355 (NY Nov. 27, 2007), the Court ruled that where a state provision has no comparable or analogous federal provision in the HIPAA, or the opposite is the case, there is no possibility of pre-emption because there is nothing to compare and no contrary requirement. As a result, the state provision is effective. Given that the HIPAA does not pre-empt stricter state or local statutory law, it can be argued that the HIPAA represents a minimum set of rules for medical information in the US[1418]. In fact, before the HIPAA state laws were very limited[1419]. The Privacy Rule sets the first national standards for protecting the privacy of health information in the US, by providing a minimum of basic protections[1420].

In summary, the HIPAA Privacy Rule and the Security Rule establish federal standards for protecting personal health information, require appropriate safeguards and set limits and conditions on use and disclosure[1421]. The HIPAA Privacy Rule is based on the FIPs[1422]. It has been claimed that it does not elevate medical privacy to a constitutional right,

1416 *See* on the effects of pre-emption Gostin, Hodge Jr., and Marks, "The Nationalization of Health Information Privacy Protections", pp. 1130–1131.

1417 Jonathan P. Tomes. "20 Plus Years of HIPAA and What Have We Got". In: *Quinnipiac Health L.J.* 22 (2018), pp. 39–106, p. 96.

1418 Yasnoff, "Privacy, Confidentiality, and Security of Public Health Information", p. 160.

1419 *See* Hiller et al., "Privacy and security in the implementation of health information technology (electronic health records): US and EU compared", p. 9; and Pritts, "Altered states: state health privacy laws and the impact of the Federal Health Privacy Rule".

1420 Di Iorio and Carinci, "Privacy and health care information systems: where is the balance?", p. 98.

1421 *See infra* Sections 4.4.1, 4.4.2, 4.4.3.

1422 *See* Richards and Hartzog, "Privacy's Constitutional Moment", p. 19.

but it identifies privacy as the legitimate interest which guarantees protection against unauthorised disclosure of medical information[1423]. The HIPAA is limited in scope. In particular, the scope of HIPAA requirements is limited to covered entities, which is a limited range of health-related entities, healthcare providers and recipients. Covered entities shall apply the rules, and an office of the US Department of Health and Human Services is responsible for checking their compliance. A covered entity may use and disclose personal health information only by respecting the Privacy Rule. The Security Rule mandates administrative, physical and technical safeguards. It even lists technical policies and procedures which are related to access, audit, and integrity controls and it defines standards. Moreover, when a covered entity is implementing the security measures it shall take into account its capabilities, its infrastructure and the cost of implementation. The HIPAA requires a risk analysis, and puts emphasis on organisational measures.

The definition of "personal health information" in the US refers to "individually identifiable health information", meaning a subset of health data that can be referred to an individual and is transmitted or maintained in any form or medium[1424]. As pointed out in *Holman v. Rasak*, 486 Mich. 429, 785 N.W.2d 98, 2010 Mich. LEXIS 1446 (Mich July 13, 2010), the notion can include information orally transmitted to the physician by the patient. Under the HIPAA the definition refers to a particular form of health information, that is "protected health information" (PHI) and is framed as follows[1425].

> "Individually identifiable health information is information that is a subset of health information, including demographic information collected from an individual, and:

1423 White and Hoffman, "The Privacy Standards Under the Health Insurance Portability and Accountability Act: A Practical Guide to Promote Order and Avoid Potential Chaos", p. 712.

1424 In Lauren Newman. "Keep Your Friends Close and Your Medical Records Closer: Defining the Extent to Which a Constitutional Right to Informational Privacy Protects Medical Records". In: *J.L. & Health* 32 (2019), pp. 1–26, the author argues that the Supreme Court's interpretation of what medical information is constitutionally protected is not uniform. Therefore, this article points out that all medical information should be protected by the Constitution to protect individuals against identity theft and data breaches (of medical records, especially).

1425 *See* 45 C.F.R. § 160.103.

> 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 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".

The US notion of PHI is coherent with the OECD's definition of personal health data[1426]. PHI protects both directly and indirectly identifiable health information[1427]. For example, it covers information collected in a medical record, conversations and clinicians' notes, information about the patient in a health insurer's computer system; and billing information about the patient[1428]. PHI refers both to the present and future health status. So, the notion might not be detailed and comprehensive as in the GDPR, but it is broad (e.g. both physical and mental state) and it is open to interpretation as well. It even refers to genetic information, and to the provision of healthcare[1429]. There is neither a reference to the number used for identifying the individual during the healthcare provision nor a mention of information on laboratory tests (or of inferred data[1430]). However, these specifications of the GDPR are established in its Recitals and not in the general definition of the type of data, and the HIPAA includes the identification number in the list of identifiers that can be removed to de-

1426 For the GDPR's and OECD's concepts *see* Chapter 3, Section 3.3.1.

1427 *See* Di Iorio and Carinci, "Privacy and health care information systems: where is the balance?", p. 98.

1428 *See* Anglim, Kirtley, and Nobahar, *Privacy Rights in the Digital Age*, p. 268.

1429 On genetic information in the US *see* Solove and Schwartz, *Information privacy law*, pp. 526–559. An interesting case on this topic is *Moore v. Regents of the University of California* 793 P.2d 479 (Cal. 1990), where the Court affirms the patient's autonomy over the body but rejects a property-based approach. Genetic information is strictly related to an individual's identity, and it embeds a high discrimination risk.

1430 In Hoffman and Klein, "Explaining explanation, part 1: theoretical foundations", p. 277, "medically inflected data" is considered out of the HIPAA's definition despite the growing ability of prediction of social networks and social media interactions. On the same opinion *see* Terry, "Regulatory disruption and arbitrage in health-care data protection", p. 188.

identify PHI[1431]. Commentators mention the medical record number, the biometric identifiers and the account number among the HIPAA's identifiers[1432]. Thus, legal interpretation may consider a piece of information as PHI or equally "personal health data" despite the differences between the legal frameworks.

Even in the US, personal health information may be collected in HIT and EHR systems to ensure the continuity of patients' care while supporting the diagnosis, managing the treatment, and storing their medical histories[1433]. It has been pointed out that PHI is frequently collected in a record under a unique personal identifier which is associated with the individual and shared among a health network of different entities[1434]. The United States Code defines an EHR as "an electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff"[1435].

The general description of the state of the art of the EHR system is valid for the US legal framework since it uses internationally recognised concepts and standards[1436]. In US EHR systems have the functionalities to support clinical decisions, order entry, and administrative processes, to manage health information and data, and to exchange and integrate PHI from different sources[1437]. Both private medical providers and government agencies store electronic medical records in health information systems that collect demographic, financial, medical, and genetic information, per-

1431 *See* 45 C.F.R. § 160.514(b)(2)(i)(l)(C) and Gostin, Hodge Jr., and Marks, "The Nationalization of Health Information Privacy Protections", p. 1124.

1432 *See* Alexis Guadarrama. "Mind the Gap: Addressing Gaps in HIPAA Coverage in the Mobile Health Apps Industry". In: *Hous. L. Rev. 55* (2018), pp. 999–1025, p. 1007; White and Hoffman, "The Privacy Standards Under the Health Insurance Portability and Accountability Act: A Practical Guide to Promote Order and Avoid Potential Chaos", p. 717.

1433 *See* e.g. Lauren Bair Jacques. "Electronic health records and respect for patient privacy: A prescription for compatibility". In: *Vand. J. Ent. & Tech. L.* 13 (2011), pp. 441–462; Julien, "Electronic Health Records"; Nicolas P. Terry. "Meaningful adoption: What we know or think we know about the financing, effectiveness, quality, and safety of electronic medical records". In: *Journal of Legal Medicine* 34.1 (2013), pp. 7–42.

1434 *See* Anglim, Kirtley, and Nobahar, *Privacy Rights in the Digital Age*, p. 268.

1435 *See* 42 U.S.C. § 17921 (2006).

1436 *See* Chapter 3, Section 3.4.1, where the state of the art has been explained with internationally recognised concepts, from a legal framework perspective.

1437 *See* Julien, "Electronic Health Records".

sonal identifiers (e.g. social security number) and circumstantial elements (e.g. being the victim of a violent crime)[1438].

EHRs are used for care purposes, but they also play an important role for US data-based health research[1439]. Even employers may obtain and use EHRs, but they frequently manage or build PHR systems for their employees[1440]. After the GINA of 2008 employers cannot access the genetic information of employees and their families in the EHR, unless specific authorisation is provided by the individual[1441].

As in the EU, achieving EHR interoperability has been an important goal of US government and stakeholders[1442]. However, the absence of a coordinated national healthcare system may impinge on the creation of a comprehensive network of healthcare providers, pharmacies, and private physicians. In the US a fragmentation of EHRs, and also of the individual's medical history, seems inevitable due to the multilevel and complex healthcare system.

Therefore, the concept of EHR may be frequently mislabelled in the US. When analysing processing in the EHR environment, it will be necessary to evaluate on a case-by-case basis whether "EHR" is used in place of an electronic medical record (EMR) managed only by one provider, i.e. one data controller, or it is used for indicating the record shared among multi-

1438 Gostin, Hodge Jr., and Marks, "The Nationalization of Health Information Privacy Protections", pp. 1117- 1118.

1439 *See* Fred Cate. "Protecting privacy in health research: the limits of individual choice". In: *Calif. L. Rev.* 98 (2010), pp. 1765–1804, p. 1781; Sharona Hoffman and Andy Podgurski. "Balancing privacy, autonomy, and scientific needs in electronic health records research". In: *SMUL Rev.* 65 (2012), pp. 85–144; David M. Parker, Steven G. Pine, and Zachary W. Ernst. "Privacy and Informed Consent for Research in the Age of Big Data". In: *Penn St. L. Rev.* 123.3 (2019), pp. 703–733. Secondary research uses of health data should comply with the HIPAA Privacy Rule.

1440 *See* the prominent analysis by Sharona Hoffman. "Employing e-health: the impact of electronic health records on the workplace". In: *Kan. JL & Pub. Pol'y* 19 (2009), pp. 409–432. Walmart, Intel and BP developed their own PHR systems. Employers may obtain medical information under several statues, such as the Americans with Disabilities Act of 1990 or ADA 42 U.S.C. § 12101.

1441 *See* Hoffman, *op. cit.*, p. 418.

1442 *See* Hoffman, *op. cit.*, pp. 413–414; Julien, "Electronic Health Records", pp. 179–180; Terry, "Regulatory disruption and arbitrage in health-care data protection", pp. 184–186.

ple providers[1443]. Hospitals, physicians, insurers and pharmacies frequently keep their own and separate EMRs[1444].

Anyway, the reasonable expectation of privacy of electronic PHI in EHRs and patient's confidentiality should be protected to safeguard individuals against discrimination, social stigma and misuse[1445]. In particular, it has been pointed out that accessibility, security, accuracy, and interoperability should be considered central issues of EHRs[1446]. Hence, in 2008 the Office of the National Coordinator for Health Information Technology (ONC) released a pivotal document on electronic medical privacy, listing eight principles for establishing a uniform national approach intended to address privacy and security issues of medical informational privacy in the public and private sector[1447]. The ONC's framework was aimed at complementing and working with existing federal, state, and local laws. To come up with the list of principles, the ONC reviewed several other sets of principles, including OECD's and FTC's principles, HIPAA rules and even principles of other legal frameworks (e.g. DPD, PIPEDA). The ONC's principles should apply to "all health care-related persons and entities that participate in a network for the purpose of electronic exchange of

1443 As an example, the Veterans Health Administration developed a portal which allows access to medical information collected in physicians' EHRs. *See* Leslie P Francis. "When patients interact with EHRs: problems of privacy and confidentiality". In: *Hous. J. Health L. & Pol'y* 12 (2011), pp. 171–199, pp. 174–176. So, this is not a typical EHR environment because there is no other provider.

1444 *See* on the fragmentation William Nicholson Price II. "Risk and Resilience in Health Data Infrastructure". In: *Colo. Tech. L.J.* 16 (2017), pp. 65–86, pp. 69–70. *See* also Terry and Francis, "Ensuring the privacy and confidentiality of electronic health records", p. 683. This article clearly differentiates between electronic medical records of individual providers and electronic health records of multiple providers.

1445 *See* Gostin, Hodge Jr., and Marks, "The Nationalization of Health Information Privacy Protections", p. 1118.

1446 On the privacy and confidentiality concerns of EHRs *see* Terry and Francis, "Ensuring the privacy and confidentiality of electronic health records", which suggests an opt-in solution for using the EHR and describes the multiple issues.

1447 ONC Office of the National Coordinator for Health Information Technology. *Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information*. Office of the National Coordinator for Health Information Technology, U.S. Department of Health and Human Services, 2008. *See* the comment by Jacques, "Electronic health records and respect for patient privacy: A prescription for compatibility", p. 460.

individually identifiable health information". Thus, the processing of PHI in EHRs should follow certain principles[1448]:

1. individual access, meaning that the individual should have the timely means of access to PHI and obtain it in a readable form and format;
2. correction, meaning that the individual should have the timely means to contest the accuracy or integrity of PHI, have it amended or dispute a denied request in a documented format;
3. openness and transparency, meaning that policies, procedures, and technologies that directly affect the individual should be open and transparent;
4. individual choice, meaning that the individual should have the opportunity to make an informed decision about the collection, use, and disclosure of PHI;
5. collection, use and disclosure limitation, meaning that PHI should be limited to the extent necessary to fulfil the specified purpose, and not used to discriminate inappropriately;
6. data quality and integrity, meaning that PHI should be complete, accurate and up-to-date to the extent necessary to fulfil the specified purpose, and PHI should not be modified or deleted in an unauthorised manner;
7. safeguards, meaning that PHI should be secured and protected with reasonable administrative, technical, and physical safeguards;
8. accountability, meaning that "these principles should be implemented, and adherence assured, through appropriate monitoring and other means and methods should be in place to report and mitigate non-adherence and breaches".

Overall, these principles may build trust in the electronic exchange of PHI. They are not legally binding, but are used to write policies and interpret the HIPAA[1449]. The ONC's principles established a "a uniform, consistent approach intended to address the privacy and security challenges related to EHRs, independent of any specific institution or legal paradigm"[1450]. Looking at the previous discussion on the FIPs, the ONC's framework

1448 Office of the National Coordinator for Health Information Technology, *Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information*.

1449 *See* Dumortier and Verhenneman, "Legal regulations on electronic health records: a prerequisite or an unavoidable by-product? – The legal aspects of electronic health records in Europe and the US analysed".

1450 Jacques, "Electronic health records and respect for patient privacy: A prescription for compatibility", p. 460.

clearly followed the FIPs of 1973 and the OECD's Guidelines of 1980. It is worth noting that not only should the use and disclosure of PHI be limited in the EHR, but also the collection of information, as argued in Chapter 3 for the EU legal framework[1451].

The Health Information Technology for Economic and Clinical Health Act (hereinafter: HITECH) of 2009 represented a significant privacy law and federal legal regulation for promoting the use of EHRs[1452]. HITECH was included in the American Recovery and Reinvestment Act (ARRA) which sought to encourage the adoption of e-health systems in the US by allocating billions of resources to eligible hospitals and professionals[1453]. In particular, HITECH encouraged the use of EHRs, EMRs and electronic prescriptions to aggregate and distribute PHI. Healthcare providers registered in a subsidy process to receive funds while making a "meaningful use of certified EHR technology"[1454]. HITECH enabled more coordination and alignment within and among states on EHRs to create an interconnected system of healthcare delivery[1455].

In sum, this Act mandated some changes in the HIPAA: it increased penalties, extended the scope of the HIPAA to business associates of covered entities, and required a data security breach notification and a three-year audit trial[1456]. The introduction of the audit trial was an important novelty since it mandated the record of disclosures, which should be

1451 In particular, *see* Chapter 3, Section 3.4.2.

1452 Health Information Technology (HITECH) Provisions of American Recovery and Reinvestment Act of 2009, Title XIII, Subtitle D (Pub. L. 111–5, 123 Stat. 115, significantly codified at 42 U.S.C. § 17937 and 17954).

1453 *See* Dumortier and Verhenneman, "Legal regulation of electronic health records: a comparative analysis of Europe and the US", p. 42; J.A. Magnuson and Patrick W. O'Carroll. "Introduction to public health informatics". In: *Public health informatics and information systems*. Springer, 2014, pp. 3–18. ISBN: 9780387227450, p. 12; Yasnoff, "Privacy, Confidentiality, and Security of Public Health Information", p. 160; Pasquale, "Health Information Law", pp. 203–205.

1454 Terry, "Meaningful adoption: What we know or think we know about the financing, effectiveness, quality, and safety of electronic medical records", p. 15.

1455 Hartley and Jones, *EHR implementation: A step-by-step guide for the medical practice*, p. 6.

1456 *See* Solove and Schwartz, *Information privacy law*, p. 468; Yasnoff, "Privacy, Confidentiality, and Security of Public Health Information", p. 160; Hiller et al., "Privacy and security in the implementation of health information technology (electronic health records): US and EU compared", p. 11.

available to the individual upon request on the basis of a specific right[1457]. The obligation of data breach notification was established both for covered entities and their business associates. Business associates are the third-party vendors with which the covered entities contract. After the HITECH, they are bound to the Privacy Rule by statute of law[1458]. Independent online PHR vendors are still not bound to the rules. However, it has been pointed out that these entities are subject to the FTC Act for their practices[1459].

In 2013, the Department of Health and Human Services released the "Omnibus Final Rule", which implemented the changes of the HITECH Act in the HIPAA's Privacy and Security Rules, as well as in 45 C.F.R.[1460].

HITECH tried to regulate EHR and PHI exchange within this environment by focusing on its standardisation[1461]. It has been reported that healthcare providers were encouraged by the HITECH Act to use certified EHR: this technology was supposed to collect complete and accurate information so that patient care could be improved, providers could better access to medical information, and patients could have been empowered by increased access to their medical records[1462]. Three pillars have been identified for the use of certified EHRs: using this technology in a "meaningful" manner; using the systems for the electronic exchange of health information to improve national quality of healthcare; and using the technology to submit clinical quality and other measures for health[1463].

The HITECH Act conditioned public funding on the "meaningful use" of EHRs: a beneficiary could be funded insofar as the EHR was implemented with defined functional requirements (i.e. basic information, clini-

1457 *See* Yasnoff, "Privacy, Confidentiality, and Security of Public Health Information", p. 160.

1458 *See* Dumortier and Verhenneman, "Legal regulation of electronic health records: a comparative analysis of Europe and the US", p. 48. The author highlights that business associates are bound by statute of law. Therefore, covered entities need to ensure the implementation of the rules by their business associates.

1459 *See ibid.*

1460 Solove and Schwartz, "Health privacy", p. 510. On the Omnibus Rule *See* Hartley and Jones, *EHR implementation: A step-by-step guide for the medical practice*, pp. 88–89.

1461 Dumortier and Verhenneman, "Legal regulations on electronic health records: a prerequisite or an unavoidable by-product? – The legal aspects of electronic health records in Europe and the US analysed".

1462 Magnuson and O'Carroll, "Introduction to public health informatics", p. 13.

1463 Hartley and Jones, *EHR implementation: A step-by-step guide for the medical practice*, p. 6.

cal health information, and medical history)[1464]. In addition to functional requirements, EHRs should follow basic standards on data entry and portability, and the standards defined by "Authorized Testing and Certification Bodies" with reference to the ISO's standards[1465]. The Office of the National Coordinator for Health Information Technology reported that in 2017 nearly 86 % of office-based physicians adopted any EHR, and nearly 80 % adopted a certified record[1466]. However, it is always necessary to concretely evaluate whether the record in use is an EMR or an EHR[1467]. In the US the potential of the EHR is great for enhancing healthcare, but the level of frustration of stakeholders is still high due to the uncoordinated environment[1468].

So, the applicable framework for EHRs and EMRs are primarily the HIPAA, consumer protection guidelines and self-regulatory instruments (e.g. standards, contracts, codes of conduct, and privacy seals)[1469]. In fact, HIPAA Privacy and Security Rules apply to typical healthcare providers (physicians, doctors and pharmacies).

Common law and tort law (public disclosure and intrusion, especially) protect health information in US EHRs too, but this protection is circumscribed[1470]. As previously mentioned, statutory law also regulates medical

1464 *See* Pasquale, "Health Information Law", p. 204.

1465 *See* Pasquale, *op. cit.*, p. 205.

1466 *See* ONC Office of the National Coordinator for Health Information Technology. *Office-based Physician Electronic Health Record Adoption*. 2019.

1467 After the initial phase of ARRA, Terry claimed that there were far more EMRs than EHRs in use. *See* Terry, "Meaningful adoption: What we know or think we know about the financing, effectiveness, quality, and safety of electronic medical records", p. 27.

1468 Katsh and Rabinovich-Einy, "The Internet of On-Demand Healthcare", p. 85.

1469 *See* Dumortier and Verhenneman, "Legal regulation of electronic health records: a comparative analysis of Europe and the US", p. 50. The authors argue that the US the legal framework is less extensive than in Europe, but equally complicated. The right to privacy and the right to avoid disclosure of personal matters have been recognised by courts, but the legal framework protecting them is "a complex patchwork of laws different from state to state and often narrowly targeting a particular population, health condition, data collection effort or specific type of health care organizations". *See* also Jacques, "Electronic health records and respect for patient privacy: A prescription for compatibility".

1470 *See* the reference to case law on electronic health information in Solove and Schwartz, "Health privacy", and Terry and Francis, "Ensuring the privacy and confidentiality of electronic health records", p. 708.

records and medical confidentiality, and it can pre-empt HIPAA requirements where more stringent[1471].

Moreover, 45 C.F.R. § 170 provides the standards, implementation specifications, and certification criteria for EHRs and HITs[1472]. An EHR "edition base" shall include patients' demographics and clinical health information, such as medical history and problem lists[1473]. The main functions are those previously explained in Chapter 3: the integrated view of and access to a patient's information, the clinical decision support system, the clinician order entry, and the health information and communication exchange[1474]. Certification criteria establish whether EHRs meet applicable standards and implementation specifications[1475]. It should be noted that the certification criteria on EHRs provided by the Code are extremely useful for understanding how privacy and security requirements may be framed by a legislator in great detail[1476]. The criteria are divided in required and "optional"[1477]. The privacy and security criteria are specifically defined in 45 C.F.R. § 170.315(d)[1478].

Health information in medical records is also protected by the Privacy Act of 1974, as amended in 2010 at 5 U.S.C. § 552a, and which applies to federal agencies. Under the Privacy Act, individuals have the right to access, and request correction of, medical records maintained by an agency[1479]. The same Act indicates several general requirements for the agen-

1471 *See ibid.*

1472 This section has been revised at 85 FR. 25642, 25639, May 1, 2020, and has been effective since June 30, 2020.

1473 45 C.F.R. § 170.102.

1474 *See* Chapter 3, 3.4.1 in line with 45 C.F.R. § 170.102(2).

1475 The central requirements are 45 C.F.R. § 170.299, which incorporates by reference certain standards, and § 170.315 2015 on edition health IT certification criteria.

1476 *See* e.g. 45 C.F.R. § 170.315, which was amended in 2020.

1477 As an example, in the "computerized provider order entry – medications" criterion at 45 C.F.R. § 170.315(a), it is mandatory to "enable a user to record, change, and access medication orders", whereas it is optional to "include a "reason for order" field".

1478 Chapter 5 will take into account the criteria, safeguards and standards for EHRs that have been adopted by the Code of Federal Regulations.

1479 *See* § 552a of the Privacy Act: "the term "record" means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph". On the access, it is

cies, which shall respect a form of data minimisation principle, guarantee transparency by informing the individuals, preserving accuracy, and implementing policies and administrative, technical and physical safeguards to ensure security and confidentiality of the records[1480]. However, this

established that "each agency that maintains a system of records shall (1) upon request by any individual to gain access to his record or to any information pertaining to him which is contained in the system, permit him and upon his request, a person of his own choosing to accompany him, to review the record and have a copy made of all or any portion thereof in a form comprehensible to him, except that the agency may require the individual to furnish a written statement authorizing discussion of that individual's record in the accompanying person's presence; (2) permit the individual to request amendment of a record pertaining to him and (A) not later than 10 days (excluding Saturdays, Sundays, and legal public holidays) after the date of receipt of such request, acknowledge in writing such receipt; and (B) promptly, either (i) make any correction of any portion thereof which the individual believes is not accurate, relevant, timely, or complete; or (ii) inform the individual of its refusal to amend the record in accordance with his request, the reason for the refusal, the procedures established by the agency for the individual to request a review of that refusal by the head of the agency or an officer designated by the head of the agency, and the name and business address of that official".

1480 *See* § 552a(e): "each agency that maintains a system of records shall (1) maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by executive order of the President; (2) collect information to the greatest extent practicable directly from the subject individual when the information may result in adverse determinations about an individual's rights, benefits, and privileges under Federal programs; (3) inform each individual whom it asks to supply information, on the form which it uses to collect the information or on a separate form that can be retained by the individual (...); (5) maintain all records which are used by the agency in making any determination about any individual with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination; (6) prior to disseminating any record about an individual to any person other than an agency, unless the dissemination is made pursuant to subsection (b)(2) of this section, make reasonable efforts to assure that such records are accurate, complete, timely, and relevant for agency purposes; (7) maintain no record describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual about whom the record is maintained or unless pertinent to and within the scope of an authorized law enforcement activity; (8) make reasonable efforts to serve notice on an individual when any record on such individual is made available to any person under compulsory legal process when such process becomes a matter of public record; (9) establish rules of conduct for persons involved in the design, development, operation, or maintenance of any system of records, or in maintaining any record, and instruct each

Act applies to government agencies only, and not to private healthcare providers[1481].

Furthermore, the FTC's consumer protection applies to companies which process PHI, even in EHRs[1482]. As an example, in 2014 the FTC filed a complaint against the corporation Accretive Health, which offered services to hospital systems, for failing to provide reasonable and appropriate security for consumers' personal information against unauthorised access[1483]. In 2020, the FTC found that the seller of emergency travel

---

such person with respect to such rules and the requirements of this section, including any other rules and procedures adopted pursuant to this section and the penalties for noncompliance; (10) establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained; (...)".

1481 Gostin, Hodge Jr., and Marks, "The Nationalization of Health Information Privacy Protections", p. 1122, which points out the weaknesses of a specific privacy statutory and regulative strategy: "Although existing federal and state privacy statutes and regulations are meaningful and serve valuable ends, they share several weaknesses: (1) like constitutional privacy protections, most statutes apply primarily to government collections, uses, or disclosures of health information, and thus often do not confer protections to health information in the private sector; (2) they fail to address the new challenges to individual privacy arising from the automation of medical records; (3) they collectively represent a patchwork effort to address the privacy and security of specific health information; (4) some kinds of data are treated as superconfidential (e.g., H1V/AIDS), while other data are virtually unprotected, leading to inconsistencies and unfairness; (5) they do not effectively balance competing individual interests in privacy with the need to use the data for the common good; and (6) some state laws prohibit disclosures without informed consent, but make so many exceptions as to negate the prohibition". Then the authors claim the need for a comprehensive approach to health privacy protection.

1482 *See* Dumortier and Verhenneman, "Legal regulations on electronic health records: a prerequisite or an unavoidable by-product? – The legal aspects of electronic health records in Europe and the US analysed", which also refers to PHRs.

1483 Accretive Health, F.T.C. No. C-4432 (2014), available at <www.ftc.gov/enforcement/cases-proceedings/ 122–3077/accretive-health-inc-matter>. Last accessed 06/10/2021. According to the FTC, "Accretive Health created unnecessary risks of unauthorized access or theft of personal information by: a. Transporting laptops containing personal information in a manner that made them vulnerable to theft or other misappropriation; b. Failing to adequately restrict access to, or copying of, personal information based on an employee's need for information; c. Failing to ensure that employees removed information

membership plans SkyMed International Inc. failed to provide reasonable security for the collected health information of members' records[1484]. The FTC's framework is an important baseline for protection against the entities that are not subject to the HIPAA since they are not covered entities[1485]. The FTC Act protects against entities engaged in a commercial activity, and not non-profit and governmental entities; nonetheless, it has been highlighted that the FTC can generally settle larger fines than the HIPAA[1486]. The FTC's scope covers unfair and deceptive practices. It may be argued that the PbD approach may be a recommended practice in this field on the basis of the FTC's actions. In fact, in the Report of 2012 the FTC referred to the healthcare sector by pointing out that its framework on consumer protection did not overlap with the HIPAA, but it is meant to encourage best practices among healthcare companies[1487].

---

from their computers for which they no longer had a business need; and d. Using consumers' personal information in training sessions with employees and failing to ensure that the information was removed from employees' computers following the training". Moreover, in 2011 a data breach involving the information of 23,000 patients occurred.

1484 SkyMed International Inc., F.T.C. No. C-1923140 (2020), available at <www.ftc.gov/enforcement/ cases-proceedings/1923140/skymed-international-inc-matter>. Last accessed 06/10/2021. In particular, SkyMed: "a. failed to develop, implement, or maintain written organizational information security standards, policies, procedures, or practices; b. failed to provide adequate guidance or training for employees or third-party contractors regarding information security and safeguarding consumers' personal information; c. stored consumers' personal information on Respondent's network and databases in plain text, without reasonable data access controls or authentication protections; d. failed to assess the risks to the personal information stored on its network and databases, such as by conducting periodic risk assessments or performing vulnerability and penetration testing of the network and databases; e. failed to have a policy, procedure, or practice for inventorying and deleting consumers' personal information stored on Respondent's network that is no longer necessary; and f. failed to use data loss prevention tools to regularly monitor for unauthorized attempts to transfer or exfiltrate consumers' personal information outside of Respondent's network boundaries". The investigation showed that 130,000 cloud records were publicly available online for at least five months.

1485 *See* Guadarrama, "Mind the Gap: Addressing Gaps in HIPAA Coverage in the Mobile Health Apps Industry", p. 1011, which refers to mobile health application industry.

1486 Solove and Schwartz, "Health privacy", p. 533.

1487 *See* the Report at p. 16–17. *See* Chapter 2, note no. 116.

EHR privacy is also explicitly protected by ethical confidentiality rules. According to AMA's Code of Medical Ethics Opinion 3.3.1, US physicians have an ethical obligation of confidentiality to manage medical records appropriately[1488]. Appropriate management entails a "clear policy prohibiting access to patients' medical records by unauthorised staff", and an information retention which respects patients' future health care needs. Medical records should be made available to patients on request, to subsequent physicians or other authorised person where necessary, and on the basis of law. The record may be transferred on request, and the physician should not refuse, but a reasonable fee may be asked. This is a sort of right to data portability. During the processing, the storage of the records should be safe, and when they have to be discarded, they should be destroyed completely. A notification on how to access the medical record and for how long it will be available should be received by the patient (i.e. information retention).

Opinion 3.3.2 of the AMA explicitly refers to electronic records by recommending that physicians choose an electronic system "that conforms to acceptable industry practices and standards". The system should be able to restrict data entry and access only to authorised users, routinely provide monitoring and auditing tools, implement security measures to ensure data security and integrity, as well as policies and practices "to address record retrieval, data sharing, third-party access and release of information, and disposition of records"[1489]. The patient could request a notice on how

1488 *See* this opinion and the following one at <www.ama-assn.org/delivering-care/ethics/ management-medical-records>. Last accessed 06/10/2021. *See* also Francis, "When patients interact with EHRs: problems of privacy and confidentiality", which reports the valuable concepts of the AMA's Opinions on EHRs.

1489 The other "Breach of Security in Electronic Medical Records" Opinion 3.3.3 further elaborates on the concept of security. In particular, it specifies: "when used with appropriate attention to security, electronic medical records (EMRs) promise numerous benefits for quality clinical care and health-related research. However, when a security breach occurs, patients may face physical, emotional, and dignitary harms. Dedication to upholding trust in the patient-physician relationship, to preventing harms to patients, and to respecting patients' privacy and autonomy create responsibilities for individual physicians, medical practices, and health care institutions when patient information is inappropriately disclosed. The degree to which an individual physician has an ethical responsibility to address inappropriate disclosure depends in part on his or her awareness of the breach, relationship to the patient(s) affected, administrative authority with respect to the records, and authority to act on behalf of the practice or institution. When there is reason to believe that patients'

confidentiality and integrity of information are protected. So, as in the EU, the access and security of electronic medical records are central issues to be addressed with both administrative and technical safeguards. The AMA's opinions are consistent with HIPAA requirements.

Overall, it can be argued that the protection of health information privacy and EHRs remains fragmented since the US healthcare system is managed by different entities, whose e-health technologies are often mutually incompatible and not interoperable[1490]. However, the HIPAA Privacy and Security Rules are specific health information requirements, which are dedicated to the protection of the e-health sector and whose implementation seeks organisational and technical safeguards. In order to investigate the similarities and differences between US and EU approaches to protecting identifiable health information, the next Section focuses on HIPAA Privacy and Security Rules in detail.

4.4 Analysing the HIPAA Privacy and Security Rules

The analysis of the HIPAA Rules will be divided into three sections. The first section deals with the general requirements on applicability, while the

---

confidentiality has been compromised by a breach of the electronic medical record, physicians should: (a) Ensure that patients are promptly informed about the breach and potential for harm, either by disclosing directly (when the physician has administrative responsibility for the EMR), participating in efforts by the practice or health care institution to disclose, or ensuring that the practice or institution takes appropriate action to disclose. (b) Follow all applicable state and federal laws regarding disclosure. Physicians have a responsibility to follow ethically appropriate procedures for disclosure, which should at minimum include: (c) Carrying out the disclosure confidentially and within a time frame that provides patients ample opportunity to take steps to minimize potential adverse consequences. (d) Describing what information was breached; how the breach happened; what the consequences may be; what corrective actions have been taken by the physician, practice, or institution; and what steps patients themselves might take to minimize adverse consequences. (e) Supporting responses to security breaches that place the interests of patients above those of the physician, medical practice, or institution. (f) Providing information to patients to enable them to mitigate potential adverse consequences of inappropriate disclosure of their personal health information to the extent possible".

1490 Nicholson Price II, "Risk and Resilience in Health Data Infrastructure". The author concludes the analysis on the healthcare system by suggesting the creation of a centralised data-driven infrastructure of medical technologies.

second and third sections are dedicated to the Privacy Rule and Security Rule respectively.

4.4.1 General requirements

The HIPAA seeks to guarantee medical privacy by "data type" and "by custodian type"[1491]. The Privacy Rule protects individually identifiable health information, defined as "protected health information" (PHI), regardless of the form in which the information is stored, whereas the Security Rule protects the sub-set of this category of information which is in electronic form (e-PHI)[1492]. These rules are based on the principle of technological neutrality and follow the FIPs. De-identified health information does not fall under the HIPAA, if the anonymisation respects some standards and other implementation specifications[1493].

1491 Terry, "Regulatory disruption and arbitrage in health-care data protection", p. 205.

1492 *See* 45 C.F.R. § 160.501 and Solove and Schwartz, *Information privacy law*, p. 465.

1493 On de-identified health information and HIPAA Privacy Rule, and a comparison of anonymisation with the GDPR *see* Elizabeth A. Brasher. "Addressing the Failure of Anonymization: Guidance from the European Union's General Data Protection Regulation". In: *Colum. Bus. L. Rev.* (2018), pp. 209–253, pp. 220–223. *See* also Hoffman and Podgurski, "Balancing privacy, autonomy, and scientific needs in electronic health records research", pp. 95–97. PHI is fully de-identified when 18 items are removed (45 C.F.R. § 164.514(b)(2)(i)): "(A) Names; (B) All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census: (1) The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and (2) The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000. (C) All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older; (D) Telephone numbers; (E) Fax numbers; (F) Electronic mail addresses; (G) Social security numbers; (H) Medical record numbers; (I) Health plan beneficiary numbers; (J) Account numbers; (K) Certificate/license numbers; (L) Vehicle identifiers and serial numbers, including license plate numbers; (M) Device identifiers and serial numbers; (N) Web Universal Resource Locators (URLs); (O) Internet Protocol (IP) address num-

The HIPAA applies to "covered entities", namely health plans, health care clearinghouses and healthcare providers that transmit any health information in electronic form in connection with a transaction format defined by the Act, and their business associates[1494]. The definitions of covered entities are the following[1495]:

> "Health care clearinghouse means a public or private entity, including a billing service, repricing company, community health management information system or community health information system, and "value-added" networks and switches, that does either of the following functions:
> 1. Processes or facilitates the processing of health information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction;
> 2. Receives a standard transaction from another entity and processes or facilitates the processing of health information into nonstandard format or nonstandard data content for the receiving entity".
> "Health care provider means a provider of services (as defined in section 1861(u) of the Act, 42 U.S.C. 1395x(u)), a provider of medical or health services (as defined in section 1861(s) of the Act, 42 U.S.C. 1395x(s)), and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business".
> "Health plan means an individual or group plan that provides, or pays the cost of, medical care (as defined in section 2791(a)(2) of the PHS Act, 42 U.S.C. 300gg-91(a)(2))".

A healthcare clearinghouse is a recipient of PHI that processes and aggregates medical information[1496]. Examples of clearinghouses include billing services, repricing companies, value-added networks, and banks[1497]. A

---

bers; (P) Biometric identifiers, including finger and voice prints; (Q) Full face photographic images and any comparable images; and (R) Any other unique identifying number, characteristic, or code...".

1494 *See* 45 C.F.R. § 160.102 on applicability.

1495 *See* 45 C.F.R. § 160.103. There are also "hybrid entities" which are less regulated than covered entities since their purpose is not the provision of care or only components of an entity process health information.

1496 White and Hoffman, "The Privacy Standards Under the Health Insurance Portability and Accountability Act: A Practical Guide to Promote Order and Avoid Potential Chaos", p. 718.

1497 *See* Rebecca Herold and Kevin Beaver. *The practical guide to HIPAA privacy and security compliance*. CRC Press, 2015. ISBN: 9781439855591, p. 12.

healthcare provider is the typical healthcare entity, such as physician, hospital, nurse, pharmacist, or medical technician[1498]. So, a healthcare provider may be either an individual or an organisation that provides personal care, including related billing service[1499]. Both private entities (e.g. health insurance company) and government organisations (e.g. Medicaid[1500]) that provide for the cost of medical care fall under the definition of health plans[1501]. So, health insurance insurers and government- and state-funded programmes are health plans subject to the HIPAA.

Since HITECH, the HIPAA applies to business associates of covered entities, which process information on their behalf[1502]. So, business associates can include a health information organisation that provides transmission services of PHI, and offers PHR on behalf of a covered entity, and a

1498 White and Hoffman, "The Privacy Standards Under the Health Insurance Portability and Accountability Act: A Practical Guide to Promote Order and Avoid Potential Chaos", p. 718, which includes "doctors, nurses, therapists, hospitals, medical technicians, nursing homes, rehabilitations centers, psychologists, pharmacists, and therapists".

1499 Herold and Beaver, *The practical guide to HIPAA privacy and security compliance*, p. 12.

1500 On this initiative *see* Wilensky and Teitelbaum, *Essentials of Health Policy and Law*, pp. 233–248. Medicaid is the federal public health insurance programme for indigent people. *See* also the official website at <www. medicaid.gov/>. Last accessed 06/10/2021.

1501 *See* Gostin, Hodge Jr., and Marks, "The Nationalization of Health Information Privacy Protections", p. 1126.

1502 *See* 45 C.F.R. § 160.102(b). According to 45 C.F.R. § 160.103 business associate of a covered entity means "a person who: (i) on behalf of such covered entity or of an organized health care arrangement (as defined in this section) in which the covered entity participates, but other than in the capacity of a member of the workforce of such covered entity or arrangement, creates, receives, maintains, or transmits protected health information for a function or activity regulated by this subchapter, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities listed at 42 CFR 3.20, billing, benefit management, practice management, and repricing; or (ii) provides, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation (as defined in § 164.501 of this subchapter), management, administrative, accreditation, or financial services to or for such covered entity, or to or for an organized health care arrangement in which the covered entity participates, where the provision of the service involves the disclosure of protected health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person".

subcontractor that creates, receives, maintains, or transmits PHI[1503]. Even EHR system vendors may be included in this definition if they are third parties that offer the EHR systems under a contract with the healthcare providers. As another example, lawyers, accountants and billing companies are usually contractors of covered entities whose work involves the use and disclosure of PHI[1504]. Business associate agreements and contracts between the covered entity and its business associates will define the safeguards that the latter shall provide for information disclosed by the former[1505].

The HIPAA has come under criticism by commentators who have pointed out that significant health-related activities do not fall under the definition of covered entity[1506]. In fact, the definition of covered entity has been criticised as too narrow[1507]: many subjects that process health information operate outside the HIPAA's conditions, leaving a large gap[1508]. EHR and EMR providers are subject to HIPAA Privacy and Security Rules. Nonetheless, it has been pointed out that employers utilising employer health plans and PHRs or EHRs are not covered entities while administering the plans, but the HIPAA's requirements may apply to health plans that disclose

1503 *See* 45 C.F.R. § 160.103(3).

1504 *See* Gostin, Hodge Jr., and Marks, "The Nationalization of Health Information Privacy Protections", p. 1126, which was published before the HITECH but referred to examples of business associates. *See* also White and Hoffman, "The Privacy Standards Under the Health Insurance Portability and Accountability Act: A Practical Guide to Promote Order and Avoid Potential Chaos", p. 719, which includes "malpractice insurers, accountants, certain vendors, lawyers, and collection agencies". Herold and Beaver, *The practical guide to HIPAA privacy and security compliance*, p. 13 points to these sectors: "legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services".

1505 *See* Tomes, "20 Plus Years of HIPAA and What Have We Got", p. 78, which discusses the cost of the drafting activity.

1506 *See* Solove and Schwartz, *Information privacy law*, p. 473; Dumortier and Verhenneman, "Legal regulation of electronic health records: a comparative analysis of Europe and the US"; Hoffman and Klein, "Explaining explanation, part 1: theoretical foundations", pp. 275–276; Hoffman, "Medical Privacy and Security", p. 275; Terry, "Regulatory disruption and arbitrage in health-care data protection"; Guadarrama, "Mind the Gap: Addressing Gaps in HIPAA Coverage in the Mobile Health Apps Industry".

1507 *See* also Hoffman and Podgurski, "In sickness, health, and cyberspace: protecting the security of electronic private health information", p. 334.

1508 Anglim, Kirtley, and Nobahar, *Privacy Rights in the Digital Age*, p. 270; Guadarrama, "Mind the Gap: Addressing Gaps in HIPAA Coverage in the Mobile Health Apps Industry"; Solove and Schwartz, "Health privacy", p. 514.

PHI to employers pursuant to a confidential agreement[1509]. So, employers are bound by the HIPAA Privacy Rule only to the extent that they act as insurers, i.e. they provide the plans as health plans[1510]. Online health services (e.g. apps, m-health, Google Health) are frequently excluded[1511]. Websites, mobile apps, and other e-health services shall not comply with HIPAA requirements[1512]. Future regulation may extend the definition to the emerging subjects of the e-health domain, or it may cover protected health information regardless of the entity that processes it[1513].

1509 *See* Gostin, Hodge Jr., and Marks, "The Nationalization of Health Information Privacy Protections", p. 1126, which refers to 45 C.F.R. § 164.504(f)(l)(1), (2).

1510 Hoffman, "Employing e-health: the impact of electronic health records on the workplace", p. 424. In the case *Beard v. City of Chicago*, 2005 U.S. Dist. LEXIS 374 (ND Ill Jan. 10, 2005), it is ruled that under the HIPAA the definition of PHI excludes PHI in employment records held by a covered entity in its role as employer.

1511 Dumortier and Verhenneman, "Legal regulation of electronic health records: a comparative analysis of Europe and the US", pp. 34–35; Terry, "Regulatory disruption and arbitrage in health-care data protection", pp. 181–184. Google Health is building an EHR tool to connect different healthcare providers. The tool will store EMRs, connect providers, organise PHI, aggregate health information and use AI. *See* the first presentation at <www.youtube.com/watch?v=P3SYqcPXqNk>. Last accessed 06/10/2021. Other services in the G Suite are related to healthcare. Cloud Healthcare API allows "easy and standardized data exchange between healthcare applications and solutions built on Google Cloud". *See* the information on the product at <cloud.google.com/healthcare>. Even this tool uses analytics and AI applications.

1512 On the concerns of online health networking *see* Patricia Sanchez Abril and Anita Cava. "Health privacy in a techno-social world: a cyber-patient's bill of rights". In: *Nw. J. Tech. & Intell. Prop.* 6 (2007), pp. 244–277. From 2007 to 2019, Microsoft HealthVault collected PHI as web-based portals. This tool was more similar to a PHR than an EHR.

1513 *See* the analysis in Guadarrama, "Mind the Gap: Addressing Gaps in HIPAA Coverage in the Mobile Health Apps Industry", p. 1019. The HIPAA should be extended by federal legislative action. Moreover, other self-regulative initiatives should start from the developers of health applications. In Hoffman and Klein, "Explaining explanation, part 1: theoretical foundations", p. 285, it is suggested that Texas's definition of covered entity may be used since it is more inclusive. *See* TEX. HEALTH & SAFETY CODE ANN. 181.001(b)(2) (West): "Covered entity means any person who: (A) for commercial, financial, or professional gain, monetary fees, or dues, or on a cooperative, nonprofit, or pro bono basis, engages, in whole or in part, and with real or constructive knowledge, in the practice of assembling, collecting, analyzing, using, evaluating, storing, or transmitting protected health information. The term includes a business associate, health care payer, governmental unit, information or computer management entity, school, health researcher, health care facility,

4.4.2 The HIPAA Privacy Rule

Generally, it has been argued that the HIPAA Privacy Rule requires covered entities to give patients notice of privacy practices and protects EHRs from illegal use or disclosure of PHI[1514]. The term "use" may include the employment, application, utilisation and examination of PHI[1515]. A disclosure is a release, transfer, or provision of access in any manner outside the covered entity[1516]. The HIPAA mandates some duties at the organisational and technical level for uses and disclosures. The implementation of the safeguards is an obligation subject to civil and criminal sanctions.

As previously mentioned, the legal ground for processing is not a traditional legal category in the US. Data processing is generally permitted, and the approach of "notice-and-control" usually applies (at least) on the basis of the consent of the individual. Nonetheless, the HIPAA provides a general rule on use and disclosure of PHI, that prohibits processing, except when it is explicitly permitted by the rules[1517]. So, despite the absence of explicit grounds and of the lawfulness principle, the HIPAA indirectly provides the conditions for a "lawful processing". Where the purpose is treatment, payment and healthcare operations, consent is not necessary. However, the individual's authorisation is necessary for other specified purposes and secondary uses, but some exceptions may apply. The HIPAA's exceptions are comparable with the grounds of Article 9 GDPR, and they can be summarised here[1518].

---

clinic, health care provider, or person who maintains an Internet site; (B) comes into possession of protected health information; (C) obtains or stores protected health information under this chapter; or (D) is an employee, agent, or contractor of a person described by Paragraph (A), (B), or (C) insofar as the employee, agent, or contractor creates, receives, obtains, maintains, uses, or transmits protected health information". As a result, the definition of covered entity may be related to the nature of information, instead of a closed list of categories of the subject.

1514 Terry and Francis, "Ensuring the privacy and confidentiality of electronic health records", p. 714.

1515 Herold and Beaver, *The practical guide to HIPAA privacy and security compliance*, p. 72.

1516 Herold and Beaver, *op. cit.*, p. 73.

1517 *See* 45 C.F.R. § 160.502.

1518 The HIPAA defines the exceptions in great detail. The following paragraphs will summarise the exceptions by defining the contexts of processing where consent is not required, and without listing every condition established in 45 C.F.R. § 164.512. The comparison with the EU law is not new. Before the GDPR Dumortier and Verhenneman, "Legal regulation of electronic health

The HIPAA frequently refers to disclosure of PHI to other subjects that can be considered recipients. The potential disclosures are categorised by the literature as "required" and "permissive". The former category includes the disclosure to the patient or his/her representative, and the disclosure for audit or other enforcement purposes, while the latter refers to all other disclosures (e.g. for treatment or on the basis of statutory law). Permissive disclosure may or may not require patient's consent. As a result, it has been claimed that the healthcare provider has more control than the individual over what PHI will be disclosed to recipients or what PHI will remain confidential[1519].

First of all, HIPAA provisions allow processing when information is disclosed directly to the individual, or when the purpose of the use or disclosure is treatment, payment or a healthcare operation. Under the HIPAA "treatment" means "the 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", the "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"[1520]. In particular, the treatment, payment and healthcare operation purpose embes the following five scenarios[1521]:

1. "A covered entity may use or disclose protected health information for its own treatment, payment, or health care operations;
2. A covered entity may disclose protected health information for treatment activities of a health care provider;
3. A covered entity may disclose protected health information to another covered entity or a health care provider for the payment activities of the entity that receives the information;

---

records: a comparative analysis of Europe and the US", p. 49, highlighted that the exceptions for research or for treatment are comparable to the exemptions for the prohibition on the processing of personal health data in the EU. *See* also Dumortier and Verhenneman, "Legal regulations on electronic health records: a prerequisite or an unavoidable by-product? – The legal aspects of electronic health records in Europe and the US analysed".

1519 *See* Hiller et al., "Privacy and security in the implementation of health information technology (electronic health records): US and EU compared", p. 15; Munns and Basu, *Privacy and healthcare data: 'choice of control' to 'choice' and 'control'*, p. 93.

1520 *See* 45 C.F.R. § 164.501.

1521 45 C.F.R. § 160.506(c).

4. A covered entity may disclose protected health information to another covered entity for health care operations activities of the entity that receives the information, if each entity either has or had a relationship with the individual who is the subject of the protected health information being requested, the protected health information pertains to such relationship, and the disclosure is: (i) for a purpose listed in paragraph (1) or (2) of the definition of health care operations; or (ii) for the purpose of health care fraud and abuse detection or compliance;
5. A covered entity that participates in an organized health care arrangement may disclose protected health information about an individual to other participants in the organized health care arrangement for any health care operations activities of the organized health care arrangement".

So, the first hypothesis may be compared with Art. 9(2)(h) GDPR (the "healthcare exception") since both rules allow for processing where the covered entity/data controller has the provision of care or treatment as a purpose. The covered entity is directly the healthcare provider, but the HIPAA's rules do not refer to a contract with a professional or to a statutory law, as the GDPR does. The covered entity may use and disclose PHI on the basis of the HIPAA directly. The duty of confidentiality specified by Article 9(3) GDPR for this exception is not included in the HIPAA, but in US medical confidentiality may be granted by ethical codes and by statutory laws[1522].

The other scenarios reported above refer to disclosures to subjects that are related to the provision of care or to the payment of services. Applying these rules to the EHR environment, it seems that the processing is permitted without any consent or authorisation by the individual, if the transmission of e-PHI among healthcare providers in the network is necessary for treatment purpose.

It should also be noted that the HIPAA includes the insurance sector in these exceptions since health insurers and health plans can be covered entities. This is an important difference with the GDPR, where processing for insurance purposes is not allowed under the "healthcare exception" since it shall seek the explicit consent of the data subject[1523].

For other purposes, uses and disclosures, the covered entities shall seek the patient's valid authorisation, i.e. the patient's consent, or the authorisation of a personal representative, unless one of the explicit exceptions

1522 *See infra* Section 4.3.
1523 *See* the argument in Chapter 3, Section 3.3.2.

applies[1524]. In the HIPAA individual consent is an opt-in authorisation, and the use, disclosure, and secondary use shall be consistent with this authorisation[1525]. A valid authorisation shall be written in plain language and limited in time, and shall identify certain core elements, such as the type of PHI, the purpose of the use and disclosure, and the name of the entities involved (e.g. the various recipients)[1526]. The authorisation shall be signed by the individual who shall be informed of the "the right to revoke the authorization in writing", unless some exceptions apply[1527]. The covered entity shall also provide the individual with a copy of the authorisation. Where the authorisation is not valid, the covered entity may be sanctioned[1528].

It has been pointed out that the concept of authorisation under the HIPAA Privacy Rule is similar to consent under the GDPR[1529]. In particular, similarities may include: "the expression of concern relating to clarity" and the need to separate authorisation and consent from other documentation; the prohibition of conditioning services on the basis of authorisation/consent; the existence of the right to revoke an authorisation in the US and the right to withdraw consent in the EU; and the particular attention to marketing purposes[1530]. Both the HIPAA and the GDPR require a free expression of will explicitly dedicated to health information and separated from consent to the medical treatment. Unlike the GDPR, the HIPAA establishes a specific written form for the authorisation, and is more detailed and directive than the GDPR on content of this authorisation[1531].

1524 *See* 45 C.F.R. § 160.508.

1525 *See* Burdon, *Digital Data Collection and Information Privacy Law*, p. 175. The consistency is specified in 45 C.F.R. § 164.508(a).

1526 Solove and Schwartz, "Health privacy", p. 515. The elements are listed in 45 C.F.R. § 164.508(c).

1527 *See* 45 C.F.R. § 164.508(c)(i)(2).

1528 *See* e.g. *Martin v. Rolling Hills Hosp., Llc*, 2020 Tenn. LEXIS 154 (Tenn Apr. 29, 2020), where the court specified that "under federal law, a medical authorization is not HIPAA compliant if the authorization has not been filled out completely, with respect to a core element". In this case, the defendants demonstrated that the authorisation of the hospital lacked three core elements required by the HIPAA.

1529 Stacey A Tovino. "The HIPAA Privacy Rule and the EU GDPR: illustrative comparisons". In: *Seton Hall L. Rev.* 47 (2017), pp. 973–994, p. 992.

1530 *Ibid.*

1531 *Ibid.*

According to the HIPAA, consent is necessary for any use or disclosure of psychotherapy notes (except in some authorised cases), for marketing purposes, and for the sale of PHI. Whether the purpose of the processing activities is marketing or commercial, the patient's authorisation is always required. The HIPAA defines marketing by listing activities of the covered entities or third parties that fall under this categorisation[1532]. It is interesting that HIPAA classifies these three binding consent requests. The GDPR simply requires explicit consent without defining concrete contexts. Here the rationale seems to be on the one hand the need to better protect psychotherapy notes, which are highly sensitive, and on the other hand, the opportunity to better safeguard PHI where the purpose of the use and disclosure becomes merely commercial. Clearly, the binding authorisation is problematic if the individual is not sufficiently informed of the risks of the use and disclosure of medical information[1533].

Several exceptions allow primary and secondary uses of PHI without a patient's authorisation. Firstly, use and disclosure may directly be required by law[1534]. Secondly, under the "public health exception" public health authorities and agents can process PHI without the consent of the individual for public health purposes, including preventing and controlling diseases, reporting information to defined authorities, and workplace surveillance[1535]. The public health exemption is established on the basis of the experience of public health agencies, which have to accomplish mandated activities, such as disease surveillance, outbreak investigation, and other public health purposes[1536]. It has been reported that healthcare providers have been reluctant to share information with public health authorities so as not be sanctioned under the HIPAA; however, this compliance concern is caused by a general lack of understanding of the rules, since public agen-

1532 *See* 45 C.F.R. § 164.501.

1533 For considerations on informational asymmetry and nudging, *see* Chapter 2, Section 2.3.

1534 As an example, the publication of death records sought by historical societies were considered permissible under Nebraska's public records statute in the case *State Ex Rel. Adams County Historical Soc'y v. Kinyoun*, 277 Neb. 749, 765 N.W.2d 212, 2009 Neb. LEXIS 80 (Neb May 15, 2009).

1535 *See* Yasnoff, "Privacy, Confidentiality, and Security of Public Health Information", p. 160; Gostin, Hodge Jr., and Marks, "The Nationalization of Health Information Privacy Protections", p. 1115. *See* for more details, 45 C.F.R. § 164.512(a) – (b).

1536 Edmunds, "Governmental and legislative context of informatics", p. 57.

cies may even be considered covered or hybrid entities[1537]. This exception is similar to the "public health" ground of the GDPR, but the HIPAA establishes more detailed conditions for its applicability[1538].

In the employment sector, the covered healthcare provider may disclose PHI to the employer in some circumstances, i.e. to conduct an evaluation on medical surveillance of the workplace, or to evaluate a work-related illness or injury[1539]. The entity may also disclose information to comply with laws on workers' compensation programmes or other similar benefit programmes for work-related injuries or illness[1540]. These exceptions demonstrate the need to use PHI in the context of employment, but they are different from the GDPR's employment basis because in the HIPAA's provision the controller/covered entity and the employer are different subjects. As explained, employers are usually out of the HIPAA's scope of application. Thus, the GDPR's ground of Art. 9(2)(b) is very different since it is based on the assessment of the working capacity from the employer to its employee and the on the basis of social security and social protection law. Conversely, the HIPAA refers to the disclosures operated by a covered entity to an employer for defined purposes.

Another permitted exception is the disclosure on victims of abuse, neglect or domestic violence, where PHI is communicated to a government authority, including a social service or protective services agency, which is authorised by law to receive this category of information[1541]. This particular exception is not provided by the GDPR, but it may be established by Member States under Article 9(4) GDPR.

The "judiciary and administrative proceedings exception" allows the use of PHI by a covered entity in a legal proceeding, and the "law enforcement exception" allows the disclosure of PHI to law enforcement officials pursuant to a court order, subpoena or other legal order[1542]. The HIPAA defines the particular information that can be disclosed in these contexts, such as demographic data, the type of injury and the description of medical conditions.

1537 *See* Yasnoff, "Privacy, Confidentiality, and Security of Public Health Information", p. 1.
1538 *See* 45 C.F.R. § 164.512(a).
1539 *See* 45 C.F.R. § 160.512(b)(v).
1540 *See* 45 C.F.R. § 164.512(l).
1541 *See* 45 C.F.R. § 164.512(c).
1542 Gostin, Hodge Jr., and Marks, "The Nationalization of Health Information Privacy Protections", p. 1115. *See* 45 C.F.R. § 164.512(e) – (f).

The provisions for these exceptions are actually very detailed. From a comparison of these requirements with Art. 9(2)(f) of the GDPR it is clear that the GDPR is more limited than the HIPAA. In fact, the HIPAA permits disclosure for law enforcement purpose in cases where EU Directive (EU) 2016/680 applies (and not the GDPR).

PHI can be used for "health research" purposes where one of the three following conditions apply: when an Institutional Review Board (IRB) or a privacy board provides explicit authorisation in this sense after a specific procedure, when PHI is de-identified, or when the individual provides explicit and written authorisation[1543]. The HIPAA does not specify whether use and disclosure may be permitted for archiving purposes in the public interest, or for scientific, historical or statistical purposes as in the GDPR, nor does it require a law as a legal basis. Looking at this exception, the procedure of the institutional or privacy board or the de-identification process may provide some guarantees for individual rights.

The emergency treatment exception (i.e. vital interest ground) is not provided by the HIPAA, but disclosure of PHI is permitted if the covered entity believes in good faith that it is necessary "to prevent or lessen a serious and imminent threat to the health or safety of a person or the public", and the recipient is "reasonably able to prevent or lessen the threat"[1544]. Moreover, specialised government functions often need the disclosure of PHI, such as in the case of military and veterans' activities. So, the HIPAA permits processing where some defined functions should be performed by public entities[1545]. This exception may be considered similar to the public interest ground where a specific statute defines the purpose of the processing and the disclosure.

The following table summarises the comparison between the HIPAA's exceptions detailed above and the legal grounds for processing of the GDPR described in Chapter 3, Section 3.3.2. As shown in this Table 4.3, many legal bases have similar conditions as the HIPAA, but none are identical.

1543 *See* 45 C.F.R. § 164.512(i), § 164.514(a) and § 164.508(a)(1). *See* Cate, "Protecting privacy in health research: the limits of individual choice", p. 1788, which contests the concept of a patient's authorisation because of potential abuse.

1544 *See* 45 C.F.R. § 164.512(j). Notably, the rules on privacy notice specify that in an emergency treatment situation the notice shall be delivered as soon as reasonably possible, implying that this situation occurs in the treatment, payment and healthcare context.

1545 *See* 45 C.F.R. § 164.512(k).

Table 4.3 Summary of the comparison between GDPR grounds and HIPAA rules

LEGITIMATE BASIS (EU), RULE/ EXCEPTION (US)	GDPR	HIPAA
Consent	Explicit consent, Art. 9(2)(a) (e.g. apps)	Valid authorisation, explicitly for marketing and psychotherapy notes § 164.508
Employment use	Obligation and rights in the field of employment, social security, social protection law, Art. 9(2)(b)	Work-related illness or injury or work-related surveillance by the employer, and workers compensation § 164.512(b)(v)- (l)
Vital interest	Vital interest, Art. 9(2)(c)	Uses and disclosures to avert a serious threat to health or safety § 164.512(j)
Data made public	Art. 9(2)(e)	Not provided
Data on abuse	Not provided	Information on abuse, neglect, domestic violence, § 164.512(c)
Legal use	Legal claim use, Art. 9(2)(f)	Judicial and administrative proceedings, law enforcement purpose, § 164.512(f)
Public interest	Substantial public interest, Art. 9(2)(g)	Specialised government functions, § 164.512(k)

LEGITIMATE BASIS (EU), RULE/ EXCEPTION (US)	GDPR	HIPAA
Healthcare exception	Preventive or occupational medicine, assessment of the working capacity, medical diagnosis, medical treatment, management of health services and systems subject to conditions provides by law, Art. 9(2)(h)	Treatment, payment, healthcare provision
Contract with healthcare professional	Execution of a contract with healthcare professional, Art. 9(2)(h)	Not provided
Public health	Public interest in public health, Art. 9(2)(i)	Public health activities, health oversight activities, serious threats to health or safety, § 164.512(b)(1)
Research	Archiving in public interest, scientific, historical research, statistic, Art. 9(2)(j)	After a privacy board's decision § 164.512(i)

Under the previous circumstances, the covered entity shall implement policies and procedures to limit the amount of information to be disclosed. The "minimum necessary rule" is a sort of minimisation principle that has been introduced in the HIPAA where it is specified that covered entities shall make reasonable efforts to limit PHI to "the amount reasonably necessary to achieve the purpose of the disclosure"[1546]. Hence, a covered entity shall use and disclose the minimum amount of PHI to the extent it is necessary to fulfil the intended purpose or carry out any function[1547]. To this end, the covered entity should evaluate its practices and

1546 *See* 45 C.F.R. § 164.514(d).

1547 *See* Dumortier and Verhenneman, "Legal regulation of electronic health records: a comparative analysis of Europe and the US", p. 49, which point

limit unnecessary or inappropriate access to, and disclosure of, protected health information[1548]. Implementing policies and procedures for routine disclosures may limit the PHI disclosed to the amount reasonably necessary to achieve the purpose[1549]. It can be argued that the HIPAA provides a form of information minimisation related to medical confidentiality[1550]. This rule is flexible, like the data minimisation principle. It may even enhance patient autonomy and promote trust in the healthcare system[1551]. However, this requirement does not apply to treatment purposes and to a few other exceptions, such as disclosure with the individual's authorisation or disclosure required by law[1552].

As regards an individual's rights, the HIPAA Privacy Rule includes: the right to receive a privacy notice; where applicable, the right to request restriction and to receive confidential communications; the right to access (i.e. right to inspect and obtain a copy) and the right to rectification of PHI (i.e. right to amend); the right to obtain a record of when and why PHI has been shared with others for certain purposes (i.e. right to receive an accounting of disclosures); and the right to file a complaint to the Health and Human Services' Office of Civil Rights[1553]. Commentators define these rights as fair information practices for health consumers[1554].

---

out that this rule was introduced after the ARRA in 2009. *See* also Terry, "Regulatory disruption and arbitrage in health-care data protection", p. 99.

1548 Terry, *op. cit.*

1549 Hartley and Jones, *EHR implementation: A step-by-step guide for the medical practice*, p. 103.

1550 *See* Burdon, *Digital Data Collection and Information Privacy Law*, p. 175.

1551 Gostin, Hodge Jr., and Marks, "The Nationalization of Health Information Privacy Protections", p. 1131.

1552 *See* Solove and Schwartz, *Information privacy law*, p. 467, which reports § 164.502(b)(1). As regards EHRs and medical records, it is further specified that for all uses, disclosures, or requests to which the "minimum necessary rule" applies, a covered entity "may not use, disclose or request an entire medical record, except when the entire medical record is specifically justified as the amount that is reasonably necessary to accomplish the purpose of the use, disclosure, or request". *See* 45 C.F.R. § 164.514(d)(5). *See* also Herold and Beaver, *The practical guide to HIPAA privacy and security compliance*, pp. 95–98.

1553 Hiller et al., "Privacy and security in the implementation of health information technology (electronic health records): US and EU compared", pp. 13–14.

1554 *See* e.g. Gostin, Hodge Jr., and Marks, "The Nationalization of Health Information Privacy Protections", p. 1128.

Unlike the GDPR, the patient's rights to erasure, to portability, and to not be subject solely to an automated decision are not granted[1555].

Firstly, the individuals have the right to receive a notice of privacy practice which shall contain certain information and be written in plain language[1556]. As previously mentioned, the individual shall be informed of the right to revoke the authorisation while providing consent[1557]. After that, the notice shall be given to the individual and also be available on request later[1558]. The HIPAA even mandates the statement that shall be used as the header of the notice: "this notice describes how medical information about you may be used and disclosed and how you can get access to this information. Please review it carefully"[1559]. Moreover, the content of the notice shall include several details, including a description of the uses and disclosures and of each purpose, a statement on the individual's rights and how they can be exercised, references to covered entities' duties (e.g. on notifying a breach), and contact details[1560]. The notice can be provided electronically.

Secondly, individuals have the right to request restriction to the use and disclosure of information[1561]. However, this option is significantly limited[1562]. The right to request restriction applies in few conditions because, despite the ability to request limitation of the use of PHI during a treatment, payment or healthcare operation, the covered entity may or may not agree to the restrictions[1563]. This entity shall restrict the use

1555 Some comparative considerations on the existing rights will be provided in the next section.

1556 *See* 45 C.F.R. § 164.520. *See* also the list of binding statements in Herold and Beaver, *The practical guide to HIPAA privacy and security compliance*, pp. 102–103.

1557 Solove and Schwartz, "Health privacy", p. 515, which emphasises this right.

1558 Hartley and Jones, *EHR implementation: A step-by-step guide for the medical practice*, p. 94, suggests seeking professional advice from a counsel to write the notice and then providing the notice at the first visit to the healthcare facility.

1559 *See* 45 C.F.R. § 164.520(b)(1)(i). An example of compliant structure of an HIPAA privacy notice is provided in Herold and Beaver, *The practical guide to HIPAA privacy and security compliance*, pp. 153–158.

1560 *See* the binding elements in 45 C.F.R. § 164.520(b)(1)(ii). In 45 C.F.R. § 164.520(b)(2), HIPAA lists the optional elements.

1561 *See* 45 C.F.R. § 164.502, § 164.522.

1562 *See* the discussion in Hiller et al., "Privacy and security in the implementation of health information technology (electronic health records): US and EU compared", p. 15; Munns and Basu, *Privacy and healthcare data: 'choice of control' to 'choice' and 'control'*, p. 92.

1563 45 C.F.R. § 164.522(a).

and disclosure for payment purposes only. Interestingly, the individual also has the right to request confidential communication of PHI (i.e. an accommodation of communication preferences) from the covered entity by alternative means where it is reasonable[1564].

The right to access to health information also applies in the US. In particular, individuals have the "right to inspect" (i.e. access) their medical record and obtain a copy of it "in a designed record set"[1565]. However, this right has several limitations, and is not absolute[1566]. It does not apply to psychotherapy notes or to "information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding". In other cases, the covered entity may deny the access request on the basis of "nonrenewable grounds for denial": if the covered entity is a correctional institution and the information may jeopardise the health, safety, security, custody, or rehabilitation of the individual or of others; while the information is used in the course of a research; if the information is collected in a record subject to the Privacy Act; and if the information is obtained from another entity under the duty of confidentiality[1567]. The HIPAA also lists renewable grounds for denial by including the following cases: if a licensed healthcare professional evaluates that access is "reasonably likely to endanger the life or physical safety of the individual or another person"; and if the PHI makes reference to another person or the request for access is made by the individual's personal representative, and a licensed health care professional evaluates that access may cause harm as reported in the first cases[1568]. As a result, the discretion of the covered entity is combined with a professional judgement.

Where the right of access is applicable, the form and format of access are requested directly by the individual, even electronically, and the request shall be satisfied in a timely manner[1569]. So, in an EHR environment the

---

1564 45 C.F.R. § 164.522(b).

1565 *See* 45 C.F.R. § 164.524(a)(1).

1566 On this right *see* e.g. Hartley and Jones, *EHR implementation: A step-by-step guide for the medical practice*, pp. 124–127.

1567 *See* 45 C.F.R. § 164.524(a)(2).

1568 *See* 45 C.F.R. § 164.524(a)(3). The individual has the right to have the denial reviewed by another licensed healthcare professional designated by the covered entity. The covered entity shall give access to the other accessible information and write the denial in plain language by explaining the basis for the denial and by describing how the individual may complain to the entity pursuant to a procedure.

1569 *See* 45 C.F.R. § 164.524(c). The covered entity has 30 days to satisfy the request. The individual may agree to a summary of PHI in place of the entire designed

individual may request to receive the data electronically. Notably, the individual has the right to "transmit the copy of protected health information directly to another person designated": this is a sort of right to portability[1570]. The HIPAA Privacy Rule allows patients access to their PHI, but this right does not include a right to establish the provenance of the data and the purpose for which it is used, as in the EU. A right to concealment is not explicitly provided[1571]. However, commentators suggested the possibility of establishing a right to flag particularly sensitive information as "confidential" to keep it secret from the healthcare network[1572].

Moreover, the individual has the right to correct inaccurate or missing PHI maintained in a record set[1573]. After the request, the covered entity has 60 days to identify the record, provide the amendment and inform the individual[1574]. The covered entity may deny its applicability in whole or in part, but may explain the basis for denial in written form[1575].

As regards the right to receive "an accounting of disclosures", it is a particular right of the HIPAA that applies to the information disclosed in the six years prior to the request[1576]. However, disclosures for carrying out treatment, payment and healthcare operations are excluded, as well as other eight circumstances[1577]. As a result, the right is again highly

---

record set. The covered entity may charge the individual for the request. The fee shall be reasonable, and cost based.

1570 *See* 45 C.F.R. § 164.524(c)(3)(ii).

1571 *See* this right in the EU system at Chapter 3, Section 3.4.2.

1572 *See* Jacques, "Electronic health records and respect for patient privacy: A prescription for compatibility", p. 461.

1573 *See* 45 C.F.R. § 164.526(a).

1574 *See* 45 C.F.R. § 164.526(b) and (c).

1575 *See* 45 C.F.R. § 164.526(d).

1576 *See* 45 C.F.R. § 164.528(a).

1577 The cases are listed by 45 C.F.R. § 164.528(a)(1): "An individual has a right to receive an accounting of disclosures of protected health information made by a covered entity in the six years prior to the date on which the accounting is requested, except for disclosures: (i) To carry out treatment, payment and health care operations as provided in § 164.506; (ii) To individuals of protected health information about them as provided in § 164.502; (iii) Incident to a use or disclosure otherwise permitted or required by this subpart, as provided in § 164.502; (iv) Pursuant to an authorization as provided in § 164.508; (v) For the facility's directory or to persons involved in the individual's care or other notification purposes as provided in § 164.510; (vi) For national security or intelligence purposes as provided in § 164.512(k)(2); (vii) To correctional institutions or law enforcement officials as provided in § 164.512(k)(5); (viii) As part of a limited data set in accordance with § 164.514(e); or (ix) That occurred prior to the compliance date for the covered entity".

limited. Anyway, the written accounting of disclosures shall contain specific elements established by the HIPAA, including the date, the contact details of the recipients, a brief description of the PHI and the basis for disclosure[1578].

The HIPAA Privacy Rule protects confidentiality of PHI and grants these individual rights. In addition to the Privacy Rule, the Security Rule adds protection to a subset of PHI, that is electronic protected health information.

4.4.3 The HIPAA Security Rule

The Security Rule covers e-PHI protection by providing administrative, physical and technical safeguards[1579]. The Rule mandates effective procedures to avoid improper disclosure of PHI and regular risk assessments to plan remedial actions[1580]. It has been pointed out that the goals of the Security Rule revolve around the confidentiality, integrity, and availability of electronic PHI, i.e. the central concepts of security or CIA triad[1581]. In particular, the rationale of the Security Rule is protecting the confidentiality, integrity and availability of e-PHI at a reasonable and appropriate level[1582].

The Security Rule is also designed to be technologically neutral[1583]. The approach is highly scalable and flexible, but it also mandates the implementation of specific standards[1584]. The legislative technique of providing a list of specific standards has the virtue of giving guidance and specificity,

---

1578 *See* 45 C.F.R. § 164.528(b).

1579 *See* Solove and Schwartz, *Information privacy law*, p. 468.

1580 Yasnoff, "Privacy, Confidentiality, and Security of Public Health Information", p. 160; Ryan M. Krisby. "Health care held ransom: modifications to data breach security & the future of health care privacy protection". In: *Health Matrix* 28 (2018), pp. 365–401.

1581 Herold and Beaver, *The practical guide to HIPAA privacy and security compliance*, p. 206. On confidentiality, integrity, and availability *see* Chapter 1, Section 2.5.1.

1582 *See* Hoffman and Podgurski, "In sickness, health, and cyberspace: protecting the security of electronic private health information", p. 336.

1583 *See* Hartley and Jones, *EHR implementation: A step-by-step guide for the medical practice*, p. 149.

1584 The standards for all e-PHI are defined in 45 C.F.R. § 162.308, § 164.310, § 164.312, § 164.314 and § 164.316.

but important safeguards may be omitted, or they may not be updated over time[1585].

The HIPAA provides a comprehensive security approach that covers both the technical and organisation levels. The general rules on security are divided into four general requirements[1586]:

1. implementing administrative, technical and physical safeguards to ensure confidentiality, integrity and availability of processed e-PHI (i.e. created, received, maintained or transmitted e-PHI);
2. implementing technical and physical safeguards to protect e-PHI against reasonably anticipated threats to its security or integrity;
3. safeguarding e-PHI against unauthorised use or disclosure;
4. ensuring that not only the covered entity, but also its employees and workforce, comply with the Rule.

The three categories of safeguards – administrative, physical, and technical – should work together to limit privacy and security risks[1587]. As mentioned above, the approach is flexible. In fact, it is specified that "covered entities and business associates may use any security measures that allow the covered entity or business associate to reasonably and appropriately implement the standards and implementation specifications" defined in the rules[1588]. The implementation of reasonable and appropriate measures is highly contextual since the covered entity shall take into account its size, complexity, and capabilities, technical infrastructure, hardware and software security capabilities, the costs of implementation of the security measures, and the probability of risks of security breaches[1589].

Hence, no one-fits-all approach is provided by the Security Rule. Actually, the requirement of reasonable and appropriate measures can be

1585 *See* the comment by Solove and Schwartz, "ALI Data Privacy: Overview and Black Letter Text", p. 24. An example of requirement with the list of standards is 45 C.F.R. § 162.1302. This requirement defines the standards for referral certification and authorisation transaction. Interestingly, the standards are divided according to time period and are frequently updated.

1586 *See* 45 C.F.R. § 164.306. *See* also Hoffman and Podgurski, "In sickness, health, and cyberspace: protecting the security of electronic private health information", p. 339; Klitou, *Privacy-invading technologies and privacy by design. Safeguarding Privacy, Liberty and Security in the 21st Century*, p. 272; Dumortier and Verhenneman, "Legal regulation of electronic health records: a comparative analysis of Europe and the US", p. 34.

1587 *See* Krisby, "Health care held ransom: modifications to data breach security & the future of health care privacy protection", p. 372.

1588 45 C.F.R. § 164.306(b)(1).

1589 45 C.F.R. § 164.306(b)(2). *See* also § 164.530(i)(1).

considered a "tacit acknowledgement that perfection is not achievable and that the goal of protecting the privacy of patient health information, while important, justifiably may be balanced against other constraints and imperatives", as ruled in *Bereston v. Uhs of Del., Inc.*, 2018 D.C. App. LEXIS 83 (DC Mar. 8, 2018).

The Security Rule establishes administrative, physical, technical and organisational safeguards within their implementation specifications, which can be "required" or "addressable"[1590]. The safeguards or "standards" and the "required" implementation specifications shall always be implemented as binding tools, whereas the "addressable" implementation specifications leave covered entities some discretion[1591]. The "addressable" specification is not optional, but the entity can assess whether it is reasonable and appropriate, and where not, a more reasonable and appropriate specification may be implemented in its place as an equivalent alternative[1592]. The decision shall be the outcome of a risk analysis[1593]. The measures shall be maintained, reviewed and modified continuously since the measures shall always ensure reasonable and appropriate protection of e-PHI[1594].

Administrative safeguards include organisational and management measures, meaning policies and procedures[1595]. This category of safeguards covers nearly two-thirds of implementation requirements under the Security Rule[1596]. The security management process is central in preventing, detecting and containing security breaches[1597]. In fact, the Security Rule requires both a risk analysis and several risk managements practices[1598]. In particular, the covered entity shall conduct a risk analysis by assessing the

1590 45 C.F.R. § 164.306(d).
1591 *See* Krisby, "Health care held ransom: modifications to data breach security & the future of health care privacy protection", p. 372.
1592 45 C.F.R. § 164.306(d).
1593 *See* Hartley and Jones, *EHR implementation: A step-by-step guide for the medical practice*, p. 151.
1594 45 C.F.R. § 164.306(e).
1595 45 C.F.R. § 164.304: "Administrative safeguards are administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's or business associate's workforce in relation to the protection of that information".
1596 Eric C. Thompson. *Building a HIPAA-Compliant Cybersecurity Program*. Apress, 2017. ISBN: 9781484230602, p. 47.
1597 45 C.F.R. § 164.308(a)(1)(i).
1598 A table on the administrative requirements is provided by Herold and Beaver, *The practical guide to HIPAA privacy and security compliance*, pp. 214–225.

potential threats and it shall then implement sufficient security measures to reduce the risks to a "reasonable and appropriate level"[1599].

The Office of the National Coordinator for Health Information Technology (ONC) and the Health and Human Services' Office for Civil Rights (OCR) developed a useful downloadable Security Risk Assessment (SRA) Tool to conduct a compliancy assessment[1600]. Other "required" administrative measures are the so-called "sanction policy" and the "information system activity review". The former mandates appropriate sanction policies against workforce members who fail to comply with the administrative procedures, while the latter requires the implementation of procedures for regularly reviewing the records of the information system activity, such as audit logs, access reports, and security incident reports[1601].

Access and authorisation mechanisms for limiting the access of the workforce to e-PHI are provided under the category of "addressable" administrative specifications[1602]. Access to and sharing of e-PHI should be limited through reasonable and appropriate precautions, such as authorisation policies and procedures. In particular, the suggested implementation specifications are: security reminders, procedures for protection from malicious software, log-in monitoring, and password management. Therefore, hospital employees who are not responsible for treatment shall not have access to health information[1603]. Employees should be trained in security policies and procedures, and shall be sanctioned for any violation[1604]. These considerations apply to e-PHI in the EHRs. So, it has been argued that the workforce should also be trained to use EHRs correctly by following "good practices that respect patient privacy"[1605]. In fact, another "addressable" administrative specification is "security awareness and training"[1606].

1599 45 C.F.R. § 164.308(a)(1)(ii)(A) and (B).

1600 *See* the official website and the tool at <www.healthit.gov/topic/privacy-security-and-hipaa/ security-risk-assessment-tool>. Last accessed 06/10/2021.

1601 45 C.F.R. § 164.308(a)(1)(ii)(C) and (D).

1602 45 C.F.R. § 164.308(a)(3) and (4).

1603 *See* Dumortier and Verhenneman, "Legal regulation of electronic health records: a comparative analysis of Europe and the US", p. 34, which argues that this aspect of the Privacy Rule is comparable with the EU proportionality principle.

1604 Yasnoff, "Privacy, Confidentiality, and Security of Public Health Information", p. 160.

1605 Jacques, "Electronic health records and respect for patient privacy: A prescription for compatibility", p. 461.

1606 45 C.F.R. § 164.308(a)(5)(i) – (ii).

Furthermore, the HIPAA Security Rule establishes that the covered entity shall implement policies and procedures to address security incidents, report the breaches, and then mitigate the effects of an occurred incident[1607]. Contingency plans are necessary to respond promptly to emergencies. To ensure protection during an emergency situation, a data backup plan, a disaster recovery plan, and an emergency mode operation plan are explicitly "required" in advance[1608]. Instead, testing and revision procedures of the plans and an assessment on specific characteristics are just "addressable" measures. However, a periodical evaluation of the plans is always binding[1609].

The administrative safeguards that are defined as "organisational" specifications refer to business associate contracts and to other arrangements[1610]. Business associates that create, receive, maintain, or transmit e-PHI on the covered entity's behalf shall ensure satisfactory safeguards of compliance. To this end, the contract or agreement shall specify the implementation specifications of the business associates and indicate the permitted use and disclosure of PHI[1611]. Some organisational requirements even establish a regime for the mentioned contract or agreements between the covered entity and its business associate (or another sub-contractor), and for groups of health plans[1612].

Other administrative requirements are defined in the Privacy Rule[1613]. Covered entities shall designate a privacy official, who is responsible for privacy policies and procedures, and a contact person, who receives privacy complaints. This contact person can be the same official, or not[1614]. The privacy official reports directly to management and this subject is responsible for the implementation of the HIPAA compliance programme[1615]. The workforce members shall be trained on policies and procedures to protect PHI and to limit unlawful uses and disclosures.

1607 45 C.F.R. § 164.308(a)(6). Examples of security policies are provided by Herold and Beaver, *The practical guide to HIPAA privacy and security compliance*, pp. 239–248.

1608 45 C.F.R. § 164.308(a)(7).

1609 45 C.F.R. § 164.308(a)(8).

1610 45 C.F.R. § 164.308(b).

1611 On business associate contracts and use and disclosure of PHI *see* 45 C.F.R. § 164.505(e), which describes the elements of the contracts in details.

1612 45 C.F.R. § 164.314.

1613 45 C.F.R. § 164.530.

1614 *See* Solove and Schwartz, "Health privacy", p. 514.

1615 *See* Hartley and Jones, *EHR implementation: A step-by-step guide for the medical practice*, pp. 91–92, which reports several of the official's activities.

Training all workforce members on privacy and security is an ongoing formal and informal process[1616]. So, physicians are included, and they should be trained on patients' privacy rights, policies, procedures and administrative, physical and technical safeguards[1617]. The covered entity shall have and apply sanctions to employees who do not comply with the rules[1618].

Any harmful effect in violation of administrative requirements shall be mitigated to the extent practicable. The mitigation requirement does not specify what actions should be taken to resolve harm, but the covered entity shall seek a solution in the first phase of a complaint (e.g. on a privacy breach). Documenting and retaining information for six years on safeguards, policies, and procedures are important administrative requirements[1619]. It has been suggested that HIPAA documentation should include: privacy policies and procedures, privacy notices, authorisations, patient requests (e.g. on rights), dispositions of complaints and documentation of other actions, and documentation of activities and designations[1620].

Physical safeguards refer to measures necessary for securing the buildings and the equipment, for protecting against the risks posed by natural and environmental causes and unauthorised intrusion[1621]. Storage back-up, secure planning, access control and validation mechanisms, and privacy records are provided under the category of "addressable" physical specifications[1622]. The workstations of the workforce should be secured to perform their functions in a safe environment, including the hardware and the software employed. The only "required" physical safeguards are a

---

1616 *See* Hartley and Jones, *op. cit.*, p. 95. An example of external training is provided by Professor Daniel Solove in his blog at <teachprivacy.com/hipaa-training/>. Last accessed 06/10/2021. Covered entities may choose in the catalogue different types of training and may receive a final certification.

1617 *See* Hartley and Jones, *op. cit.*, p. 96.

1618 45 C.F.R. § 164.530(e). In Hartley and Jones, *op. cit.*, p. 97, there are some examples of sanctions: verbal reminder, privacy retraining, reminder in the employee's personnel file, suspension, and termination.

1619 45 C.F.R. § 164.530(j).

1620 *See* further in Hartley and Jones, *EHR implementation: A step-by-step guide for the medical practice*, p. 96.

1621 45 C.F.R. § 164.304: "Physical safeguards are physical measures, policies, and procedures to protect a covered entity's or business associate's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion". *See* also Krisby, "Health care held ransom: modifications to data breach security & the future of health care privacy protection", p. 373.

1622 45 C.F.R. § 164.310(a) – (d).

"disposal" – which mandates "policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored" – and a "media re-use" – which refers to the "procedures for removal of electronic protected health information from electronic media before the media are made available for re-use"[1623].

The concept of technical safeguards includes "the technology and the policy and procedures for its use that protect electronic protected health information and control access to it"[1624]. The HIPAA requires the use of unique user identification names or numbers, and emergency access procedures[1625]. Automatic log-off after a specific period of inactivity of the system, encryption and decryption mechanisms, audit log controls, authentication mechanisms, and secure communications channels are all "addressable" measures. So, encryption is explicitly included as a reasonable and appropriate measure by the Security Rule.

Given these three categories of safeguards, the implementation specifications shall always be documented in written form[1626]. This documentation shall be retained for six years, made available to the workforce that should implement the measures, and updated periodically.

Then, the ARRA included the breach notification rule in the Security Rule. In particular, the breach notification rule mandates the notification of the breach to every individual affected by the data breach in a specific written form[1627]. The notification shall be made without unreasonable delay and no later than 60 days after the discovery of the occurred breach. The HIPAA enumerates the elements of the notification in extensive de-

1623 45 C.F.R. § 164.310(d)(2).
1624 45 C.F.R. § 164.304.
1625 45 C.F.R. § 164.312.
1626 45 C.F.R. § 164.316.
1627 For the definition of the breach *see* 45 C.F.R. § 164.402; for the rules on the notification *see* 45 C.F.R. § 164.404.
1628 The required elements in 45 C.F.R. § 164.404 are: "(A) a brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known; (B) a description of the types of unsecured protected health information that were involved in the breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved); (C) any steps individuals should take to protect themselves from potential harm resulting from the breach; (D) a brief description of what the covered entity involved is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches; and (E) contact procedures for in-

tail[1628] Even the media (e.g. television or websites), the OCR, and the business associate can receive a notification under specific circumstances[1629].

HIPAA Privacy and Security Rules contain obligations for the covered entities. The Health and Human Services' Office of Civil Rights enforces these Rules if a covered entity is not complaint with them. Actually, the individual does not have the right to sue covered entities for violations, but the option to file a complaint with the Office[1630]. As pointed out in the case law – *Rigaud v. Garofalo*, 2005 U.S. Dist. LEXIS 7791 (ED Pa May 2, 2005), *Orr v. Carrington*, 2019 U.S. Dist. LEXIS 5407 (2019), *Paris v. Herring*, 2019 U.S. Dist. LEXIS 205964 (2019) – courts can dismiss patients' claims for lack of subject matter. In *Montgomery v. Cuomo*, 291 F. Supp. 3d 303, 317 n.42 (W.D.N.Y. 2018) the court held that "only the Secretary of Health and Human Services or other government authorities may bring a HIPAA enforcement action. There is no private right to sue for a HIPAA violation". So, only the OCR may investigate and impose civil penalties if a covered entity fails to comply with the HIPAA[1631].

---

dividuals to ask questions or learn additional information, which shall include a tollfree telephone number, an e-mail address, Web site, or postal address. (2) plain language requirement. The notification required by paragraph (a) of this section shall be written in plain language".

1629 *See* 45 C.F.R. § 164.406, § 164.408, § 164.410.

1630 *See* 45 C.F.R. § 164.306, which provides the right to file a complaint and the specific conditions: "(a) Right to file a complaint. A person who believes a covered entity or business associate is not complying with the administrative simplification provisions may file a complaint with the Secretary. (b) Requirements for filing complaints. Complaints under this section must meet the following requirements: (1) A complaint must be filed in writing, either on paper or electronically. (2) A complaint must name the person that is the subject of the complaint and describe the acts or omissions believed to be in violation of the applicable administrative simplification provision(s). (3) A complaint must be filed within 180 days of when the complainant knew or should have known that the act or omission complained of occurred, unless this time limit is waived by the Secretary for good cause shown. (4) The Secretary may prescribe additional procedures for the filing of complaints, as well as the place and manner of filing, by notice in the Federal Register". On the OCR's enforcement activities *see* e.g. Roger Hsieh. "Improving HIPAA Enforcement and Protecting Patient Privacy in a Digital Healthcare Environment". In: *Loy. U. Chi. LJ* 46 (2014), pp. 175–223.

1631 *See* 45 C.F.R. § 164.306 on the compliance review of the Office, § 164.310 on the cooperation duties of the covered entity and business associates, § 160.402, § 160.404, § 160.408 on civil penalties, and the following paragraphs for the procedure and subpoena.

As reported by the OCR, individuals most often complain about impermissible uses and disclosures of protected health information, lack of safeguards, lack of patient access to PHI, lack of administrative safeguards of e-PHI, and use or disclosure of more than the minimum necessary PHI[1632]. The Office also reported that the most common types of covered entities to be sanctioned are general hospitals, private practices and physicians, outpatient facilities, pharmacies and health plans. The OCR often concludes resolution agreement with covered entities that have violated the HIPAA. As explicitly stated in every agreement, this kind of settlement is not an admission, concession, or evidence of liability, but a way to resolve a "potential violation" of HIPAA requirements. As an example, in *Parkview Health System, Inc. Resolution Agreement and Corrective Action Plan* the entity agreed to pay a resolution amount and comply with a Corrective Action Plan for having left "71 cardboard boxes of medical records unattended and accessible to unauthorised persons on the driveway"[1633]. In 2020, the health insurance plan Premera Blue Cross paid over 6 million dollars to settle a data breach that affected 10 million individuals had been caused by a cyberattack[1634]. The entity did not conduct an "accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI", and it did not implement "security measures sufficient to reduce risks and vulnerabilities to a reasonable appropriate level", meaning the plan potentially violated 45 C.F.R. § 164.308(a)(1)(ii)(A) and 164.308(a)(1)(ii)(B)[1635].

The literature has considered the absence of a private cause of action a great limitation of legal protection of PHI[1636]. It has been argued that the HIPAA has several deficiencies. In sum, the HIPAA does not apply to the new emerging private sector on e-health, individuals do not have a right

1632 *See* Office for Civil Rights (OCR) at <www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-highlights/index.html>. Content last reviewed on 15 December 2020. Last accessed 06/10/2021.

1633 *See* Solove and Schwartz, "Health privacy", pp. 526–531, which also provides the New York Presbyterian Hospital Resolution Agreement and Corrective Action Plan.

1634 The Premera Blue Cross (PBC) Resolution Agreement and Corrective Action Plan is available at <www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/premera/index.html>. Last accessed 06/10/2021.

1635 *See* p. 2 of the mentioned agreement.

1636 *See* Hoffman and Klein, "Explaining explanation, part 1: theoretical foundations", p. 278, which reports that a private cause of action was provided by California's Confidentiality of Medical Information Act. *See* also Terry, "Regulatory disruption and arbitrage in health-care data protection".

to verify in detail how the information has been used under the rules, the HIPAA gives little guidance on the concrete implementation and on how to achieve compliance, and finally it has an insufficient enforcement mechanism[1637].

It may at first be recommended that the regulatory scope of the protection of medical information be extended beyond the "custodian-type" paradigm and to all health information. As regards the limited guidance on implementation, the HIPAA's flexible approach seems broad as it omits reference to clear guidelines on technical protection[1638]. However, it should be noted that the rules are very detailed. This level of detail goes beyond the protection of informational privacy in the US. At the same time, encryption and other technical safeguards are simply "addressable" during the transmission of e-PHI. Neither a state-of-the-art criterion nor broader reference to other processing activities (e.g. storage, aggregation) are included. It has been pointed out that the HIPAA needs more efficient and stringent storage and backup requirements[1639]. Nonetheless, many specific standards and implementation requirements have been specified in the Security Rule and the level of administrative and organisational safeguards seems very high. Finally, the enforcement mechanism might be amended to provide a private cause of action, as in the EU legal framework. At the same time, the OCR guarantees independent enforcement at the administrative level, which might be considered similar to the enforcement of a DPA in a Member State.

After this analysis of the HIPAA Privacy and Security Rules, the upcoming final section will provide a comparison with the EU legal framework, with particular reference to the data protection by design obligation.

4.5 A comparison between HIPAA and DPbD in the e-health context

This section presents a comparison between HIPAA Privacy and Security Rules and the DPbD requirement of the GDPR applied to the e-health

1637 *See* Hoffman and Podgurski, "In sickness, health, and cyberspace: protecting the security of electronic private health information", p. 337.

1638 *See* Krisby, "Health care held ransom: modifications to data breach security & the future of health care privacy protection", pp. 383–384. *See* also Hoffman and Podgurski, "In sickness, health, and cyberspace: protecting the security of electronic private health information", p. 353.

1639 *See* Krisby, "Health care held ransom: modifications to data breach security & the future of health care privacy protection", pp. 384–385.

care sector, and to EHRs especially. In particular, the elements of the comparative analysis are presented in the following order: the scope of application and the rationale of the norms, the object and the recommended measures, and the underlying principles and rights.

The HIPAA is devoted to the protection of PHI, e-PHI, PHRs, EMRs and EHRs by the implementation of defined policies, procedures, and technical specifications. DPbD is a more general rule, but it is applicable to personal health data and to EHRs, and it mandates the implementation of organisational and technical measures, as well, without defining them. Both rules contain obligations subject to sanctions. Despite some similarities this analysis will show that an EHR may not be used in both EU and US legal frameworks since the DPbD principle goes beyond a set of measures to be implemented. An explicit legal recognition of PbD in the US law may bring these frameworks closer together[1640]. However, HIPAA requirements may still be considered useful examples of measures for DPbD guidelines for EHRs.

First of all, it has been specified above that the concept of PHI and personal health data are not equal. Nonetheless, the GDPR's definition of "data concerning health" and the HIPAA's definition of e-PHI both protect the "medical data" of the past, current and future health status, and other data related to health, such as genetic information, and the identifiers or the numbers assigned to healthcare services[1641]. A prominent US scholar suggested using the GDPR's definition of "data concerning health" for a new federal law on health informational privacy[1642]. Terry claimed the need to include any identifiable health information under the HIPAA to broaden its scope[1643].

Both the HIPAA and DPbD do not apply to anonymous and anonymised data, where the process of anonymisation is effective. In fact, the HIPAA dedicates several requirements to de-identification of PHI in order to allow its use and disclosure (e.g. for research purposes). Article 25 of the GDPR does not mention anonymisation since this activity takes personal data out of the scope of the GDPR, where its rules do not apply[1644]. In addition, neither rule applies to raw data. Actually, the discussion on

1640 On the FTC's Report on PbD and the proposal for a Consumer Bill of Rights *see* Chapter 2, Section 2.2.

1641 *See* respectively Article 4(15) GDPR and 45 C.F.R. § 160.103.

1642 *See* Terry, "Regulatory disruption and arbitrage in health-care data protection", p. 205.

1643 *See ibid.*

1644 *See* Recital 26 of the GDPR.

"quasi-health data" is not feasible in the HIPAA context since health apps and wearable devices are out of its scope[1645]. In the US the protection of observed, complex, and predicted health information might be guaranteed by other rules, including the FTC Act, which may apply to HIT companies where that information identifies the individual.

The HIPAA is domain-limited since only defined health entities, as well as their uses and disclosures of PHI, fall under its application[1646]. The HIPAA does not apply to all the data controllers that process identifiable health information. In fact, the focus is the entity rather than the information; as a result, this framework is fragmented "by custodian type" and it defines sector-specific duties[1647]. Instead, DPbD obligation is generally applicable to data controllers that process personal data according to the material and territorial scope of the GDPR[1648].

Despite the fact that the HIPAA always refers to "use and disclosure" and not to "processing", it may be argued that they are examples of data processing activities by looking at Article 4(2) GDPR. The term "use" of the HIPAA Privacy Rule may subsume "recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use" of the GDPR. The term "disclosure" may instead subsume "disclosure by transmission, dissemination or otherwise making available" of information to recipients[1649]. The HIPAA might not include "alignment or combination, restriction, erasure or destruction" and "collection"[1650]. The GDPR definition of data processing is evidently broader than the activities specified in the HIPAA, where the scope is focused on the disclosure of information in particular. Indeed, in the EHR context it has been claimed that "HIPAA can be interpreted as based on the assumption that health information will be collected from the individual; its focus is on the subsequent protection, use, and sharing of that information", whereas "the EU framework begins with detailed considerations about whether the information may be col-

1645 On the definition of "personal health data" *see* Chapter 3, Section 3.3.1.
1646 45 C.F.R. § 160.102.
1647 *See* Terry, "Regulatory disruption and arbitrage in health-care data protection", p. 164.
1648 *See* Chapter 2, Section 2.4.1.
1649 *See infra* the definitions of use and disclosure reported in Section 4.4.2.
1650 Terry in Terry, "Regulatory disruption and arbitrage in health-care data protection", p. 162 argues that the HIPAA leaves a narrow set of requirements to data collection.

lected and how to protect patients in the original collection process"[1651]. This is a significant difference between the two frameworks since only the GDPR concerns the full life cycle of processing activities.

Moreover, the GDPR provides some rules on personal health data, but it remains a uniform and general regulation, which is sector-neutral. The different sectorial approach of the HIPAA is consistent with the nature of the US legal system and the US informational privacy regulatory framework, where the sectorial regulation is typical. In the US the legal framework is less comprehensive and harmonised than in the EU. At the same time, the HIPAA is more detailed than other statutory laws at the national and federal level by providing "relatively robust protections against unauthorized uses of health information", which are more consistent when compared to other sectors[1652].

This federal law on health information pre-empts less stringent local and statutory law, but it can be pre-empted by other more stringent national statutes[1653]. As outlined in Chapter 3, Member State law may provide more detailed rules for the e-health care sector and EHRs in light of their competence on public health[1654]. So, even in the EU there might be more stringent rules on health data protection. In the US framework many resources have been allocated to e-health improvement in recent decades, and the HIPAA is guiding healthcare providers in the slow adoption of EHRs[1655]. As pointed out above, the US health environment is highly fragmented. Thus, a more uniform and coordinated environment like in the Member States (and in the EU) may ease the use of EHRs in this legal system.

In the US the relationship of a covered entity with its business associate is regulated through a contract or an agreement for ensuring compliance with the rules when the information is used by the business associate on behalf of the entity. The need for a contractual agreement is similar to the contract between the data controller and the processor[1656]. The business associate shall directly implement the HIPAA requirements, including the

1651 Hiller et al., "Privacy and security in the implementation of health information technology (electronic health records): US and EU compared", p. 31.
1652 *See* Terry, "Regulatory disruption and arbitrage in health-care data protection", p. 162.
1653 45 C.F.R. § 160.202.
1654 In particular, *see* Sections 3.3 and 3.4.2.
1655 *See* HITECH at note no. 1452.
1656 The respective requirements are Article 28 of the GDPR and 45 C.F.R. § 164.505(e).

Security Rule. By contrast, as explained above, the DPbD requirement is not specifically addressed to processors or technological developers[1657]. Third parties shall not comply with Article 25 of the GDPR. This represents a limitation of the DPbD principle. Even so, the obligation to implement measures on the data controller may have an indirect impact on the processor according to Recital 78 of the GDPR.

As regards the rationale of the rules, the goal of the HIPAA Privacy Rule 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"[1658]. DPbD is a general obligation of the controller that seeks the implementation of technical and organisational measures for protecting principles and rights of the data subjects by design. Even DPbD requires balancing controller's interests with the necessity to protect data subjects by defining some criteria. Both the HIPAA Security Rule and DPbD aim at protecting information/data through a set of measures ensuring accountability with the law. Despite the absence of a PbD requirement in the US legal frameworks, the HIPAA has been included in the examples of rules that give an important role to technical means for protecting privacy[1659].

However, DPbD goes beyond a set of standards or implementation specifications. It is an example of *regulation by design*. The GDPR covers the design phase of the data processing and its concrete activities. Notably, the timing of the HIPAA provisions never refers to the phase before the use or disclosure of PHI or e-PHI. It may be argued that the HIPAA compliance programme and safeguards should be projected in advance, but it does not explicitly refer to the design of practices and technologies.

Article 25 of the GDPR is open. By contrast, the HIPAA defines, enumerates and lists the categories of safeguards in a detailed and complex way[1660]. Nonetheless, the language of the rules requires interpretation in both cases. The HIPAA, like DPbD, does not mandate a one-size-fits all ap-

1657 *See* Chapter 2, 2.4.1.

1658 Tovino, "The HIPAA Privacy Rule and the EU GDPR: illustrative comparisons", p. 979.

1659 *See* Klitou, *Privacy-invading technologies and privacy by design. Safeguarding Privacy, Liberty and Security in the 21st Century*, p. 272.

1660 On the complexity of the HIPAA's rules *see* Guarda, *Fascicolo sanitario elettronico e protezione dei dati personali*, pp. 86–90.

proach, but a case-by-case approach[1661]. As a matter of fact, the implementation of measures is a never-ending approach in both legal frameworks. Overall, in both frameworks the measures shall be maintained during the activities and be revised periodically. As a result, the cost of implementation of these rules has a significant impact both on controllers and on covered entities[1662].

It may be pointed out that the physical, administrative and technical safeguards of the HIPAA embed specifications that can be considered "technical and organisational measures" under the GDPR. The adjective "appropriate" is used in Article 25 of the GDPR and in the HIPAA in a partially different way. In the EU, "appropriate" entails a discretion on choosing any measure that can implement data protection principles, whereas in the US the adjective is used to evaluate and potentially adopt the "addressable" specified safeguards, while the "required" safeguards shall always be implemented[1663]. Both the HIPAA and DPbD mention the context of the activities, the concrete characteristics of the data controller/covered entity, the costs of implementation and the risk level in the criteria to be taken into account while defining the measures[1664]. Thus, the approaches of the rules are scalable, flexible, and even technically neutral.

Despite the absence of the state of the art criterion in the Security Rule, the HIPAA explicitly provides standards to be adopted in some specific areas, for EHRs especially[1665]. As a result, the state of the art is often directly defined by the legislator[1666]. Where not defined, it should be claimed that HIPAA does not include an "effective criterion" for the measures, but only the "appropriate" one. So, it may be argued that the HIPAA does not require an implementation of rules and principles in "an effective manner".

Comparing the organisational requirements set by the GDPR for processing a large amount of sensitive data with the HIPAA requirements, it can be noted that under both regulations the subjects shall maintain a record on the activities, notify or communicate a data breach, carry out a

1661 *See* Tomes, "20 Plus Years of HIPAA and What Have We Got", p. 91 for HIPAA, and Chapter 2, Section 2.4.2 for DPbD.

1662 *See* on the costs of HIPAA the detailed investigation by Tomes, *op. cit.*, which suggests a reform of the HIPAA to find "a more cost-effective way to protect privacy". On the cost of DPbD, *see* Chapter 2, Section 2.4.3.

1663 On the GDPR's criteria *see* Chapter 2, Section 2.4.6.

1664 *See* on DPbD Chapter 2, Section 2.4.4 and 2.4.3.

1665 On EHR standards *see* also 45 C.F.R. § 170 amended in 2020.

1666 On defining the state of the art of DPbD *see* Chapter 2, Section 2.4.3.

risk assessment, and designate a DPO/privacy official[1667]. Indeed, the risk assessment is considered a required organisational measure for protecting personal health data/PHI both in the EU and in the US. While Article 25 mandates taking into account the risks during the implementation of the measures and Article 32 of the GDPR establishes a separate duty on security, the HIPAA uses the risk assessments as an "administrative safeguard" and embeds security measures. The HIPAA enumerates several policies and procedures that are crucial in the e-health context[1668].

Despite some similarities at the organisational level, the HIPAA does not require an appropriate design of the technologies and of the business practices from the development stage of the technology processing e-PHI. The HIPAA is more detailed than the EU rules on security and measures for the system[1669]. Actually, the HIPAA includes technical specifications that may be subsumed as DPbD measures if they are implemented before the processing in a designed stage of the EHR. Some HIPAA Security Rule requirements may be considered examples of measures for a DPbD implementation in the EHR since they are targeted towards the e-health context and include several detailed safeguards suggested by Article 29 Working Party and by the EC[1670]: mechanisms and limits for identification and authentication, access control, audit control, secure network communication, and encryption[1671]. Nevertheless, the HIPAA Security Rule focuses on the use or disclosure phase only and classifies these measures as "addressable safeguards".

Furthermore, the GDPR refers to certification as a tool for complying with DPbD and DPbDf obligations. In the HIPAA certification is a means for ensuring the "meaningful use" of EHRs. As regards the enforcement of the rules, an entity that violates the HIPAA may face civil and criminal

1667 For the GDPR *see* Chapter 3, Section 3.3.3.

1668 *See infra* in Section 4.4.3 the references to the organisational safeguards.

1669 Hiller et al., "Privacy and security in the implementation of health information technology (electronic health records): US and EU compared", p. 35.

1670 *See* Article 29 Working Party, *Working Document on the processing of personal data relating to health in electronic health records (EHR)*, European Commission, *Commission Recommendation (EU) 2019/243 of 6 February 2019 on a European Electronic Health Record exchange format*, and Chapter 3, Sections 3.4.2 and 3.4.3.

1671 Interestingly, in the technical safeguards HIPAA explicitly mentions encryption, while the GDPR used only the neutral term of pseudonymisation. *See* Chapter 2, Section 2.4.2.

penalties[1672], whereas DPbD may be enforced through the GDPR's administrative fine process, and judicial and non-judicial remedies. Anyway, the absence of a private cause of action is evidently a great limitation of the HIPAA.

This comparison takes into account the principles and rights involved in Article 25 GDPR and HIPAA Rules. As discussed in Chapter 2, DPbD obligation refers to principles and rights of the GDPR and the EU Charter[1673]. Generally, the HIPAA does not refer to informational principles or FIPs. From the text, it is clear that it applies a sector-based confidentiality and disclosure-centred model[1674]. US scholars have pointed out that the HIPAA is based on FIPs[1675]. Other principles have been defined by the ONC on EHRs[1676].

The previous Section has discussed and compared the different grounds for the use and disclosure of PHI and the possible similarities with GDPR. Both the HIPAA and GDPR establish multiples grounds or exceptions which go beyond the authorisation/consent of the individual/data subject. It should be remembered that the principle of lawfulness, except for the choice or consent, and other "GDPR-lite" principles (e.g. fairness) are not included in the FIPs[1677].

Looking at the HIPAA requirements, it may be argued that the detailed rules on privacy notice and the right to receive an accounting of disclosures may enhance transparency between the covered entity and the individual. Notably, the ONC's principles for processing PHI in EHRs include openness and transparency as crucial principles for processing medical information and the individual choice principle states that the individual should have the opportunity to make informed decisions about the use and disclosure of PHI. Only in a transparent context, a decision may be informed. As explained for the DPbD obligation, the language is important for easing comprehension and transparency[1678]. Even the HIPAA in-

1672 *See* the practical table on HIPAA violation and penalties in Tomes, "20 Plus Years of HIPAA and What Have We Got", p. 98.
1673 Chapter 2, Section 2.4.8.
1674 Nicolas P. Terry. "Protecting patient privacy in the age of big data". In: *UMKC L. Rev.* 81 (2012), pp. 385–415, p. 406.
1675 *See* Richards and Hartzog, "Privacy's Constitutional Moment", p. 19.
1676 *See infra* note no. 1448.
1677 *See infra* Section 4.2.
1678 *See* Chapter 2, Section 2.4.8.

troduces a "plain language" requirement for notification and information to the individual and for the individual's authorisation[1679].

According to the ONC's principles, PHI should be limited to the extent necessary to fulfil the specified purpose, and not used to discriminate inappropriately. The purpose limitation principle is not directly provided in the HIPAA. However, the HIPAA indirectly restricts the purposes by listing the possible disclosures. The "minimum necessary rule" of the HIPAA limits how much PHI can be used or disclosed. Hence, PHI should be limited to the minimum necessary to accomplish the envisaged purpose. The rationale of this rule is similar to the data minimisation principle, which is embedded in the concept of DPbD and DPbDf[1680]. The HIPAA derogates the minimum rule where it establishes that it does not apply to the disclosures related to treatment purposes, individual's consent, or disclosure required by law[1681]. It seems that the data minimisation principle does not have any derogation in the GDPR. However, as previously explained[1682], the data minimisation principle in the e-health environment means that the system should collect all the data necessary for treatment purposes. In particular, EHRs should be as comprehensive as possible to support healthcare provision[1683]. The same concept is included in the derogation for treatment purpose of the HIPAA.

The right to amend of the HIPAA is an expression of the accuracy principle. This GDPR concept has been recognised by the ONC in two different principles. The ONC's principle of "correction" states that the individual should have the timely means to contest the accuracy or integrity of PHI, have it amended or dispute a denied request in a documented format. "Data quality and integrity" recommends that PHI be complete, accurate and up-to-date to the extent necessary to fulfil the specified purpose, and that PHI should not be modified or deleted in an unauthorised manner.

Both DPbD and HIPAA give great importance to security and its principles of integrity, confidentiality and availability. In most cases the reasonable HIPAA administrative, technical, and physical safeguards require security measures and policies since the Security Rule obviously aims to

---

1679 *See* 45 C.F.R. § 164.404(c)(2), § 164.508(i)(3), § 164.512(e)(1)(ii), § 164.520(b)(1).

1680 *See* Chapter 1, Section 2.4.8.

1681 *See* Tomes, "20 Plus Years of HIPAA and What Have We Got", p. 99 on 45 C.F.R. § 164.502(b), § 164.514(d).

1682 *See* Chapter 3, Section 3.4.2.

1683 *See* Chapter 2, Section 3.4.3.

enhance security of e-PHI. It may be claimed that this Rule is dedicated to electronic information only. However, it surely applies to the EHR environment.

The last principle of accountability is included in the ONC's principles and it may be argued that it is implied in the HIPAA requirements on documentation, on the privacy officer, on mitigation and civil and criminal penalties. Nonetheless, the lack of a private action and the limits of the enforcement exposed above, and the absence of a data protection authority, force an effective accountability on the covered entity.

Under the HIPAA, an individual's rights are more limited than under GDPR. The following Table 4.4 summarises the rights provided by the two frameworks.

Table 4.4 GDPR vs. HIPAA rights

GDPR RIGHTS	HIPAA RIGHTS
Right to be informed	Right to receive a notice
Right to access	Right to inspect and obtain copy of PHI
Right to rectification	Right to amend
Right to erasure	Not provided
Right to restriction	Right to request restriction
Right to data portability	Right to transmit a copy of PHI
Right to object	Not provided
Right to have human intervention	Not provided
Not provided	Right to request confidential communication
Not provided	Right to receive an accounting of disclosures

The right to be informed and the right to receive a notice of privacy practice guarantee that the data subject or the individual obtains the information on processing in plain language. HIPAA requirements on notice are very detailed. The elements of a privacy policy in the EU and a privacy notice in the US are different[1684]. It is worth noting that the

1684 *See* Articles 13 and 14 of the GDPR and 45 C.F.R. § 164.520.

HIPAA contains more (required and optional) elements than the GDPR. However, a long and complex privacy notice seems difficult to read and be understood by individuals.

The right to access is granted by both legal frameworks[1685]. The HIPAA Privacy Rule and Article 15 of the GDPR entail the right to obtain a copy of PHI/personal data and to make the request electronically. It should be noted that in the HIPAA several circumstances limit this right[1686]. Nonetheless, where applicable, the right to inspect even allows the transmission of PHI to a third party which is a limited version of the right to data portability[1687]. The possibility of knowing who accessed the EHR – that has been suggested for EHR in the EU[1688] – may be guaranteed by the HIPAA under the right to receive an accounting of disclosures[1689].

The HIPAA provides the right of revocation of the individual's authorisation and the right to amend information which are almost identical to the right to withdraw consent and right to rectification of GDPR[1690]. Nonetheless, it should be specified that the covered entity is not required to implement the changes[1691]. In the HIPAA there are not rights equal to the rights to object and to have human intervention. As mentioned, in the e-health context the right to object of GDPR is not easily applicable and the right to have human intervention applies in automated processing activities[1692]. Despite the absence of a right to erasure in the HIPAA, it is important to remember that in the e-health context and EHRs this right

1685 Article 15 of the GDPR and 45 C.F.R. § 164.524(a).

1686 Terry argued that all data should be accessible upon request. *See* Terry, "Regulatory disruption and arbitrage in health-care data protection", p. 205.

1687 45 C.F.R. § 164.524(c). Lynskey reported the HIPAA requirement as an example of an international instrument of the right to data portability in Lynskey, "Chapter III Rights of the Data Subject (Articles 12–23). Article 20. Right to data portability", p. 501.

1688 *See* Chapter 3, Section 3.4.2.

1689 The individual may receive information of the disclosure of PHI in the network. However, this information does not refer to the professional who accessed the EHR as an employee of the covered entity.

1690 *See* the comparison in Tovino, "The HIPAA Privacy Rule and the EU GDPR: illustrative comparisons", p. 990.

1691 Hiller et al., "Privacy and security in the implementation of health information technology (electronic health records): US and EU compared", p. 32. The covered entity may provide a denial.

1692 *See* Chapter 3, Section 3.3.3.

is difficult to apply[1693]. Health information shall be retained for clinical reasons, billing records, and other public purposes[1694].

In summary, the next Table 4.5. compares the two rules as discussed here.

Table 4.5 Synthesis of the comparison between DPbD and HIPAA

CRITERIA	DPbD – GDPR	HIPAA – US
Legal system	EU	US
Legal nature	Principle and obligation	Multiple obligations and duties
Theoretical framework	Data protection	Informational privacy
Embedded principles	GDPR principles and EU Charter	Not explicitly provided
Embedded rights	Arts. 12–22 GDPR and Charter	45 C.F.R. § 164
Timing	Full life cycle of processing	Use and disclosure
Flexibility	Yes	Yes
Technical neutrality	Yes	Yes
Subjects	Data controller primarily	Covered entities and business associates

1693 *See* the arguments in Chapter 2, Section 3.4.2.

1694 *See* Tovino, "The HIPAA Privacy Rule and the EU GDPR: illustrative comparisons", pp. 992–993, which provides some concrete examples: "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".

CRITERIA	DPbD – GDPR	HIPAA – US
Security	Separate duty	Included

The US framework has more detailed technical and organisational specifications than GDPR and is focused on health information. Both EU and US laws protect identifiable personal health information, but in the US the regulation is binding only for covered entities. The European data protection framework applies to all kinds of processing of personal data and to the full life cycle of processing activities of the data controllers. In comparison to the EU, rights and principles in the US appear more limited. Despite the level of detail, it has been argued that US healthcare protection should move beyond the HIPAA and provide an additional framework for protecting medical informational privacy, including the collection of information[1695]. To this end, healthcare entities should apply the FIPs[1696].

Adopting the FTC's approach of privacy by design will improve the patient's medical privacy[1697]. A new federal law on health information might integrate the FIPs as general protective principles and might also give the FTC the enforcement power to act as a data protection authority even beyond the scrutiny of unfair practices[1698]. An effective and appropriate application of PbD or DPbD solutions may strengthen the dialogue between these legal frameworks.

Notwithstanding the different structures of legal protection in the EU and in the US, the applicable rules for the health information domain of these legal systems share the need to enhance the safeguards and control over the design of EHRs and medical records. Regulators on both sides of the Atlantic mandate organisational and technical measures to be implemented in a case-by-case approach. So, after the theoretical investigation of these four Chapters on data protection by design, the legal framework and the e-health care sector, and the comparison with the US, the next Chapter will discuss the technical tools for designing data protection in order to provide the instruments for the elaboration of the guidelines.

1695 *See* Terry, "Regulatory disruption and arbitrage in health-care data protection".
1696 *See* Terry, *op. cit.*, p. 169.
1697 *See* Terry, "Protecting patient privacy in the age of big data", p. 405.
1698 This opinion is pointed out by Terry, "Regulatory disruption and arbitrage in health-care data protection", p. 201.