Privacy and integrity of medical information

Herveg, Jean; Hoffman, Sharona

Published in:
The Oxford Handbook of Comparative Health Law

Publication date:
2020

Document Version
Publisher's PDF, also known as Version of record

Privacy and Integrity of Medical Information

Sharona Hoffman and Jean Herveg

The Oxford Handbook of Comparative Health Law
Edited by David Orentlicher and Tamara Hervey

Subject: Law, Medical and Healthcare Law Online Publication Date: Jul 2020
DOI: 10.1093/oxfordhb/9780190846756.013.8

Abstract and Keywords

This chapter explores contemporary regulation of medical privacy in the United States and Europe and its challenges. The need for privacy is a fundamental human necessity. Privacy relates to human beings' ability to maintain their dignity and avoid disclosure of information that might be deemed unpleasant. It is also associated with personal autonomy and informational self-determination. At the same time, however, some degree of data sharing is essential to the appropriate treatment of patients as well as to the proper functioning of society in general and the healthcare system in particular. Thus, privacy cannot be limitless. Hence, this chapter discusses regulatory strengths and shortcomings and highlights gaps in the law. It also suggests further safeguards that policy-makers should implement in order to protect patients and data subjects.

Keywords: privacy, medical privacy, medical data, healthcare, information disclosure, medical information

1 Introduction

Medical privacy is cherished throughout the world. The value of privacy was recognized as early as the 5th century BCE and is included in the Hippocratic Oath. Physicians reciting the oath have traditionally said: "whatsoever I shall see or hear in the course of my profession … if it be what should not be published abroad, I will never divulge, holding such things to be holy secrets."[1] Worldwide, the rule is that healthcare practitioners are bound by the duty not to disclose any information related to their patients, with exceptions applying only in some specific situations. This chapter explores contemporary regulation of medical privacy in the United States and Europe[2] and its challenges. It discusses regulatory strengths and shortcomings and highlight gaps in the law. The authors also suggest further safeguards that policy-makers should implement in order to protect patients and data subjects.

The need for privacy is a fundamental human necessity. Privacy relates to human beings' ability to maintain their dignity and avoid disclosure of information that would be embarrassing, demeaning, or otherwise make others think less of them. Privacy is also associat-

ed with personal autonomy and informational self-determination. Individuals seek privacy in order to control how others perceive them and to avoid abuses that might ensue if their sensitive data were easily available and could be used in harmful ways.[3]

At the same time, some degree of data sharing is essential to the appropriate treatment of patients as well as to the proper functioning of society in general and the healthcare system in particular. Thus, privacy cannot be limitless. At times, medical team members must share patient data in order to provide effective treatment. Health data about individuals are also essential to medical research and to many public health initiatives, such as responses to infectious disease outbreaks. Likewise, institutions may need to review patient data in order to assess and improve the quality of their services. Consequently, government officials must carefully weigh the benefits and risks of privacy versus information exchange in formulating regulatory policies.[4]

In the era of omnipresent social media, one might ask whether individuals still value privacy. Many people, especially the young, routinely post intimate details, including medical information, on Facebook and other platforms for large-scale public consumption. When surveyed, however, overwhelming majorities of respondents indicate that privacy is a priority value for them. Social media users trust in their ability to manage privacy settings and to control access to their data.[5] Privacy, therefore, remains a vital matter in contemporary society.

It is important to understand that three separate terms relate to protecting patients' interests: privacy, confidentiality, and security. *Privacy* focuses on the questions of whether information can be acquired and used, by whom, and under what circumstances, and thus on the patient's rights regarding the use of medical information. *Confidentiality* is the principle that healthcare providers generally must not disclose patient information to third parties without patient authorization. Thus, while privacy is a patient right, confidentiality is a professional obligation. Data *security* refers to mechanisms that prevent unauthorized individuals from accessing patient medical records. These can include passwords, encryption, and other technologies.[6]

In the 21st century, safeguarding privacy has become more challenging than ever before. Medical records no longer take the form of paper files that can be locked away in cabinets. Their replacement, electronic health records (EHRs), can be hacked, easily accessed by unauthorized people through workplace computers, and lost or stolen if they are stored on laptops or USB devices. Medical big data repositories are being developed by numerous government and private entities for purposes of research, public health, quality improvement, and more.[7] These, too, can be hacked or accessed by unapproved personnel. Wearable devices such as Fitbits, Apple Watches, and attachable baby monitors also collect vast amounts of information and raise privacy concerns.[8]

Both the United States and the European Union (EU) have tackled the problem of privacy with major regulatory initiatives. In the United States, safeguards come in the form of the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule, which became effective in 2003.[9] At the level of EU law, medical information confidentiality is ensured

by the notion of data protection. EU data protection law aims to protect citizens' rights over "personal data" in the context of information and communication technologies. The EU has enacted the General Data Protection Regulation (GDPR),[10] recognizing new rights for data subjects, which became applicable on May 25, 2018. HIPAA and GDPR have much in common. Both provide meaningful privacy protections for data subjects and require implementation of sound data security measures. Both carve out reasonable exceptions, such as permitting data use without patient authorization for purposes of judicial proceedings, legal requirements, public health measures, and medical treatment. Both provide patients with access to their own medical records and require covered entities to notify authorities of privacy breaches.

However, the United States and EU regulations diverge in significant ways. For example, the HIPAA Privacy Rule addresses only *protected health information* (PHI). By contrast, the GDPR covers all information concerning identified or identifiable persons and is not limited to healthcare. While HIPAA allows patients to place restrictions on use of their medical information, the GDPR sets up a legal framework in which personal data concerning health may be processed. HIPAA allows healthcare providers to disclose PHI without patient consent to third parties such as insurers and billers for purposes of payment and healthcare administrative functions, while the GDPR might require a patient's consent (e.g., for transmission to the patient's insurance company) and the mandatory disclosure of some information about data processing to the patient. Another important difference is that the GDPR applies to organizations beyond the borders of the EU so long as they process data pertaining to EU citizens and the processing activities relate to the offering of goods or services or the monitoring of behavior that takes place within the EU. Conversely, the HIPAA Privacy Rule's reach outside of the United States is limited to business associates of US covered entities.

The chapter begins with an analysis of privacy and confidentiality. Section 2 addresses both together because they are interrelated principles that are essentially two sides of the same coin. The first section describes and critiques the US HIPAA Privacy Rule, other federal privacy laws, and state confidentiality mandates. The relevant statutory and regulatory provisions establish physicians' duty to maintain patient confidentiality but also outline circumstances in which that duty must be breached and information must be revealed to third parties. The section then addresses how European law (both from the Council of Europe and the EU) approaches medical information privacy and confidentiality and how the main legal rules (on data protection in general) interface with state-level laws about medical professional privilege and secrecy. Section 3 assesses the ways in which health data may lawfully be gathered to ensure data security. In the United States, this is covered by health data security regulations. In the EU context, health data security rules are part of the general rules governing "data processing." The analysis then shifts in Section 4 to the question of *data de-identification*, another tool that is used to protect privacy. Section 5 examines remedies for unauthorized privacy breaches in the United States and EU and the means by which the EU's GDPR is enforced. Section 6 focuses on anti-discrimination laws that prohibit certain uses of health information. In order to avoid privacy harms, regulators must strive both to control access to health data and to man-

age the uses to which they are put once obtained. Thus, anti-discrimination statutes are a useful adjunct to privacy initiatives. The chapter concludes with a discussion of contemporary challenges to regulating privacy, especially in the United States. In particular, it considers the following: (1) growing and ever-evolving data security threats, (2) the proliferation of health data stemming from sources such as social media, and (3) the emergence of predictive health data.

2 Privacy and Confidentiality

2.1 American Law

The word “privacy” does not appear in the US Constitution. However, a variety of celebrated Supreme Court decisions have established that the Constitution encompasses privacy rights.[11] Furthermore, the American Medical Association’s *Principles of Medical Ethics* states that “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.”[12] This principle is reflected in numerous federal and state laws.

Nevertheless, American medical privacy laws and regulations have significant gaps and limitations. Moreover, the Supreme Court has declined to determine whether the Constitution establishes a right to *informational* privacy.[13] Many state laws preceded the enactment of the federal HIPAA regulations, but the latter superseded any state statutes that provided weaker protections.[14] This section examines the substance and scope of US federal and state privacy laws.

2.1.1 The HIPAA Privacy Rule

The HIPAA regulations were promulgated pursuant to the Health Insurance Portability and Accountability Act of 1996 and were amended in accordance with the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009.[15] The HIPAA Privacy Rule governs the disclosure of electronic and hard-copy medical information and allows patients to control their medical records to a degree. The Privacy Rule establishes that, with some exceptions, hospitals, physicians, health insurers, and other covered entities must obtain patients’ permission before disclosing their medical data to others.[16] This is a key confidentiality safeguard for American patients, though it is far from absolute and its limits are discussed in the next sub-section.

Under the HIPAA Privacy Rule, covered entities must also give patients notice of their privacy practices[17] and must allow patients to view their health records and request that they be modified or used restrictively.[18] In addition, covered entities that experience privacy breaches of unsecured data, such as incidents of hacking, must notify affected individuals and the Department of Health and Human Services (DHHS), and, in the case of large breaches, must notify the media as well.[19]

2.1.1.1 The Boundaries of the HIPAA Privacy Rule

While the HIPAA regulations are the most detailed and comprehensive medical privacy regulations in the United States, many critics argue that they fall far short of adequately protecting American patients. The federal regulations' limitations are rooted primarily in three factors: (1) the definition of "covered entity," (2) the numerous Privacy Rule exceptions, and (3) the definition of "protected health information."

The Definition of "Covered Entities." The HIPAA Privacy Rule does not govern many entities and individuals who handle private health information. The regulations define "covered entities" as including health plans, healthcare clearinghouses, and healthcare providers who transmit health information electronically for purposes of HIPAA-relevant transactions and their business associates.[20] Thus, they do not cover employers; marketers; website operators; insurers issuing life, disability, or long-term care policies; and numerous others who may handle large volumes of health information.[21]

There is no doubt that health information is routinely processed and stored by those outside the healthcare industry. Employers, for example, frequently subject applicants and employees to medical inquiries and examinations.[22] They also can obtain records for purposes of workers' compensation claims, wellness programs, reasonable accommodation requests by individuals with disabilities, or Family Medical Leave Act (FMLA) requests.[23]

Patients themselves often willingly disclose data to non-covered entities, such as Fitbit vendors or website operators. For example, WebMD's Symptom Checker asks users to provide details about their age, sex, zip code, e-mail, and symptoms in order to identify their potential health conditions and suggest treatments.[24]

Entities that are not covered by HIPAA remain free of its regulatory obligations. For example, no matter how much health information employers, websites, or marketers possess, they are not required to implement HIPAA's data security measures.

An additional concern is that many US healthcare providers outsource work such as medical transcription, billing, and reading radiological tests (x-rays, computed tomography [CT] scans, magnetic resonance imaging [MRIs]) to workers in developing countries as a cost-saving measure.[25] While the regulations technically cover those engaged in such offshore work as "business associates," in reality, it is extremely unlikely that the US government would be able to reach such individuals for purposes of any enforcement action in case of noncompliance. Therefore, the practice of outsourcing to offshore professionals creates another regulatory gap and exacerbates patients' privacy vulnerabilities.

Regulatory Exceptions. The HIPAA regulations' scope is further limited by numerous exceptions that allow covered entities to disclose health information without patient authorization. First, covered entities may divulge patients' medical information without their permission for purposes of treatment, payment, and healthcare operations.[26] Thus, physicians can consult colleagues or speak to nurses about a patient and can have administrators review records for billing or other office-related purposes without the patients' knowledge. Reportedly, during the course of a typical hospitalization, up to 150 individu-

als may see the patient's records, including doctors, nurses, medical technicians, and billing clerks.[27]

In addition, healthcare providers do not need to obtain patient authorization for disclosures that are (1) required by law; (2) necessary for public health activities; (3) related to victims of abuse, neglect, or domestic violence; (4) required for purposes of health oversight activities; (5) necessary for judicial and administrative proceedings; (6) required for law enforcement purposes; (7) made in order to facilitate cadaveric organ, eye, or tissue donation; (8) provided for medical research purposes (with certain privacy safeguards in place); (9) necessary to avert a serious threat to health or safety; (10) needed for specialized government functions, such as national security and intelligence activities; and (11) authorized by law in order to provide workers' compensation.[28]

In general, the HIPAA exceptions are reasonable and logical. However, Americans must understand that they may have little awareness of who is viewing their medical information and for what purposes it is being used.

The Definition of "Protected Health Information" and Data De-identification. A third important limitation relates to the type of information that the privacy regulations protect. PHI is defined as "individually identifiable health information" that is electronically or otherwise transmitted or maintained.[29] However, great volumes of information are stored in de-identified form in databases used for nontreatment purposes such as research, quality assessment, and public health initiatives.[30] De-identified data are entirely exempt from HIPAA coverage and can be disclosed without patient authorization. Data de-identification is explored further in Section 4.

2.1.2 Additional Federal Laws Relevant to Medical Privacy

The HIPAA Privacy and Security Rules are not the only federal laws or regulations to address medical privacy. Several important federal laws include privacy safeguards. For example, the Americans with Disabilities Act (ADA) allows employers to subject applicants and employees to medical inquiries and examinations but mandates that they maintain the confidentiality of medical information and store it separately from other employee records.[31] Likewise, the Family Educational Rights and Privacy Act (FERPA) governs records held by educational institutions, including those containing health data.[32] The Genetic Information Nondiscrimination Act (GINA) prohibits employers and insurers from seeking genetic information in order to ensure the privacy of such data.[33] An additional privacy safeguard is furnished by the federal research regulations, known as the "Common Rule," which mandate that investigators ask research participants for permission to use their identifiable health information.[34] None of these laws includes detailed guidelines as to how data security should be maintained. Nevertheless, professionals handling medical information of any type should be familiar with all relevant privacy regulations.

2.1.3 State Statutory and Common Law Privacy Rights

Medical privacy rights have been codified in the statutes of all of the states and the District of Columbia. To varying degrees, the state law provisions (1) allow patients access to their medical records; (2) restrict data use and disclosure by providers, employers, government agencies, and others; (3) establish legal privileges, such as the psychotherapist–patient privilege; (4) address specific conditions, such as alcohol or substance abuse, cancer, genetic testing, sexually transmitted disease, HIV/AIDS, and mental health; and (5) require breach notification in particular circumstances.[35] Many states have laws that provide stronger privacy protections than HIPAA. For example, they may cover a broader range of entities that handle health information or provide a private cause of action for privacy breaches.[36] Some experts consider the HIPAA Privacy Rule to constitute the floor of privacy protections, with states furnishing additional safeguards.[37]

Like federal law, state laws carve out significant exceptions to their privacy mandates. The states have all established reporting requirements. Generally, healthcare providers must report to state government agencies incidents of particular conditions, such as infectious disease, HIV/AIDS, cancer, and congenital defects, and their reports must include personally identifying details.[38] The government, therefore, has significant collections of patient information.

The states have also adopted “duty to warn” statutes that either permit or require healthcare providers to disclose patient information in particular circumstances. Generally, disclosure to law enforcement authorities and potential victims is required or permitted if a patient appears intent on harming himself or others. Thus, a mental healthcare provider with whom a patient discussed a well-formed plan to engage in violence could not maintain confidentiality with respect to that discussion.[39] Physicians may also be required to disclose private medical information to third parties in order to warn individuals that they are at risk of having been exposed to a disease.[40]

The enactment of many of these statutes followed the well-known ruling in *Tarasoff v. The Regents of the University of California*.[41] The case involved a patient who murdered a woman after disclosing to his psychologist that he intended to do so because she had rejected him as a romantic partner. The Supreme Court of California held that therapists who determine or should recognize that their patients pose a serious risk of violence to others have an obligation to “use reasonable care to protect the intended victim[s] against such dangers,” even at the cost of breaching patient confidentiality.[42]

2.2 European Law: The Organization of the Legal Framework

In Europe, medical information privacy and confidentiality are protected by fundamental rights: the right to respect for private life and the right to data protection. This statement requires some further elaboration. Formally, European law[43] recognizes the “right to private and family life” in the European Convention on Human Rights, a Council of Europe instrument to which 49 European states, including all Member States of the EU, are signatories. The recognition of a right to data protection has been part of the evolution and

development of the data protection rules, both in their adoption in legislation and executive implementation and their judicial interpretation, at the level of Member States, including national courts, and through the case law of the Council of Europe's European Court of Human Rights (in Strasbourg, France) and the EU's Court of Justice (Luxembourg). The right to data protection has thus emerged and been developed as a phenomenon of reciprocal influences between different levels of legislative, executive, and judicial powers in Europe. The result is a relatively complex set of laws, few of which are specifically designed to regulate medical privacy and confidentiality. Overall, therefore, medical information confidentiality and privacy is ensured by data protection rules adopted at the European level and implemented at the Member State level and by medical professional privilege and secrecy rules adopted at the level of each European state. Neither set of rules derogate from the other: each must be applied alongside the other.[44]

2.2.1 Council of Europe Law

The first work on data protection at the European level began at the Council of Europe in the late 1960s, with the adoption of two recommendations on automatic processing of personal data which shaped the first outline of the legal framework for ensuring data protection in Europe. These recommendations concerned databases in the private sector[45] and the public sector.[46] The continuation and development of the Council of Europe's activities in data protection resulted in the adoption of the 1981 Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Treaty no. 108), updated in 2018,[47] as well as numerous sectoral or thematic recommendations, among which are included recommendations on medical data.[48]

Relatively early in time several cases related to data protection were brought before the European Court of Human Rights. Since the *Z v. Finland* judgment in 1997, the European Court of Human Rights Court has repeatedly and consistently proclaimed that

> **(1)** The protection of personal data (and health information are not the least) plays a fundamental role in the exercise of the right to respect for private and family life;
> **(2)** Respecting the confidentiality of health information is an essential principle of the legal system of all Contracting Parties to the Convention; it is essential not only to protect patients' privacy but also to preserve their confidence in the medical profession and health services in general. Without such protection, persons requiring medical care could be discouraged from providing the personal and intimate information necessary to get the appropriate treatment and even to consult a doctor. That could end up jeopardizing their health or, in case of communicable diseases, that of the community.
> **(3)** Domestic legislation should therefore provide appropriate safeguards to prevent the use of personal data and in particular any communication or disclosure of personal data relating to health, which does not comply with the guarantees provided by the Article 8 right to private and family life of the European Convention on Human Rights.

In addition to this assertion of the importance and need to protect personal data for the exercise of the right to respect for private and family life,[49] the European Court of Human Rights has developed a substantial case-law in many areas relevant to data protection. Those most relevant to medical privacy and confidentiality include protection of medical data, medical records, medical records security, access rights (including the right to get a copy), data security, and genetic testing. For example, in the case of *I. v. Finland* (2008), the Court judged that Finland failed to provide a practical and effective protection excluding any possibility of unauthorized access to a medical file.

2.2.2 European Union Law

At the level of the European Community (now the EU), the issue of data protection was formally embraced by the European Parliament on April 8, 1976. It resulted in the adoption, in 1979, of a Resolution on the protection of human rights in the face of the development of technical progress in the field of informatics.[50] Then, after the adoption of the Organisation for Economic Cooperation and Development (OECD) Guidelines for the Protection of Privacy and Transborder Data Flows in 1980, the European Community adopted in 1995 the Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.[51] This was the first binding EU legal instrument on data protection.

The right to data protection was explicitly and formally recognized at the “constitutional” level in EU law in the Charter of Fundamental Rights of the European Union on December 7k 2000, Article 8.[52]

The Treaty on the Functioning of the European Union also recognizes, under its provisions of general application, the right to data protection.[53]

From May 25, 2018, the GDPR ensures data protection in (and in some circumstances beyond) the EU.[54] The GDPR is applicable in 27 countries and concerns directly more than 430,000,000 people within the EU. It also has significant indirect effects, notably in the matter of transfers of personal data to third countries or international organizations.[55]

It is to this extent that any person who comes under the jurisdiction of a Member State[56] has the right to claim the protection of his or her personal data. It is not only an obligation on the part of the healthcare professional or the Member State but also, and above all, a fundamental right which the data subject can claim.[57]

2.2.2.1 The Boundaries of the GDPR: Material Scope

At the level of EU law, the scope of protection for medical information confidentiality and privacy is defined by the scope of the GDPR. The GDPR protects individuals with regard to the “processing” of “personal data,” including personal data related to health. In order to be protected by the Regulation, personal data must be automatically processed, in whole or in part, or at least be included in a paper file.[58] Any use of personal data is a kind of data processing. So is the mere fact of looking at personal data. But to be subject

to the GDPR, the data processing must be, in addition, automated or be part of a paper filing system.

“Personal data” means any information relating to an identified or identifiable natural person (data subject). An identifiable natural person is a human being who can be identified, directly or indirectly, in particular by reference to an identifier. The data subject does not have to be identified. It only has to be *possible* to identify the data subject.[59] The definition of personal data remains substantially unchanged from the earlier Directive, except for the description of the elements likely to help the identification of the data subject.[60]

According to the GDPR and the case-law of the Court of Justice of the EU, the concept of personal data must be interpreted as widely as possible. For instance, IP addresses or codes for medical nomenclature (this refers to the classification of medical acts through specific codes for social security purposes) are personal data.

We could question the relevance of the notion of “personal data,” especially in the context of development of big data and data mining or of artificial intelligence, and argue that the focus should be put on the impact of technologies on the citizen for justifying and developing their regulation, rather than on the personal nature of the data per se.

2.2.2.2 Health Data in the GDPR

Personal data concerning health are a special category of personal data. They are defined in the GDPR as “personal data related to the physical or mental health of a natural person, including the provision of healthcare services, which reveal information about his or her health status.”[61] Personal data concerning health should include all data pertaining to the health status of a data subject which reveal information relating to the past, current, or future physical or mental health status of the data subject. This includes information about the natural person collected in the course of the registration for or the provision of healthcare services, as referred to in Directive 2011/24/EU on cross-border healthcare. Personal data concerning health also include a number, symbol, or particular assigned to a natural person to uniquely identify the natural person for health purposes. It covers information derived from the testing or examination of a body part or bodily substance, including from genetic data and biological samples. It also covers any information on, for example, a disease, disability, disease risk, medical history, clinical treatment, or the physiological or biomedical state of the data subject. The notion of personal data concerning health is regardless of its source (e.g., whether from a physician or other health professional, a hospital, a medical device, or an in vitro diagnostic test).[62]

This definition is very broad to the extent that it covers data which, in themselves, do not relate to the data subject’s health, but from which we could extract information concerning the data subject’s health (such as from data collected when a patient is registered in a hospital: at first sight, these are not related to the patient’s health but are merely administrative information). It also covers data that do not relate to the data subject’s health,

but which could help in finding information concerning the data subject's health (such as a patient's identifier in a national healthcare system).

2.2.2.3 The Link Between Personal Health Data and Genetic Data

In its 2004 working document on genetic data,[63] the Article 29 Data Protection Working Party considered that, in the majority of cases, genetic data were personal data. It added that genetic data may provide to an extent a detailed picture of a person's physical disposition and health condition and therefore could be considered as "data concerning health." However, it added that genetic data may also describe specific forms of a wide range of physical characteristics, and, in this case, genetic data that determine the color of someone's hair, for example, may not be regarded as data directly concerning health.

Today, the GDPR defines genetic data as personal data relating to the inherited or acquired genetic characteristics of a natural person and providing unique information about the physiology or the health of that natural person. In addition, the data must result from the analysis of a biological sample from the natural person in question, in particular chromosomal, deoxyribonucleic acid (DNA), or ribonucleic acid (RNA) analysis, or from the analysis of another element enabling equivalent information to be obtained.[64] It can be deduced that, although they should not be confused, genetic data may qualify as personal data concerning health, depending upon the circumstances.

2.2.2.5 Definition of Personal Data Concerning Health in the GDPR

We should try to keep a strict and objective definition of the notion of personal data concerning health. It should be limited to data containing an element of knowledge about an individual's health status, excluding by that any attempt to cover data that do not contain any information on an individual's health, even if it is possible to deduce personal data concerning health from the information (mainly because of the purpose pursued by the data processing or the context). Furthermore, any data deduced or extracted will automatically be protected under the GDPR by reason of its informational content. In doing so, the data from which information on an individual's health has been deduced or extracted will not be governed by a status which is not appropriate for these data and which does not offer, in reality, any real protection for the data subject. Moreover, it is not sensible to include within the GDPR's definition of health data, those data that are not related to health but from which one can deduce information on the data subject's health. That is for a very simple reason: it is now possible to deduce information relating to an individual's health from a multitude of completely unspecified data. It is therefore better in terms of legal precision to circumscribe the notion to only data which contain information about the data subject's health.

It should be remembered that data concerning health do not need to come from a health professional, result from an act reserved to health professionals, or arise in the context of health institutions or systems. In addition, data may concern health even when those data are not processed for therapeutic purposes. This is particularly the case with regard to insurance or credit card payments. Moreover, the mere information relating to a physical or psychological aspect of an individual does not necessarily constitute, as such, data con-

cerning health. To gain this last legal qualification, the physical or psychic aspect must teach us something about the health of the data subject. In this sense, data concerning health are all pieces of information relating to the physical or mental health, past, present or future, of a natural person, living or dead.

In practice, all patient data collected in European healthcare settings will fall within the protections of the GDPR either as plain personal data or as a special category of personal data.

2.2.2.6 The Boundaries of the GDPR: Territorial Scope

To be protected by the GDPR, the data processing situation has to fall within its territorial scope. The GDPR applies to the processing of personal data in the context of the activities of an establishment of a data controller[65] or a processor[66] in the EU, regardless of whether the processing takes place in the EU or not.[67] It is thus beyond doubt that the processing of a patient's data carried out by a healthcare professional established in the EU, providing healthcare to a patient in Europe, falls under the scope of the Regulation.

If the data controller or processor is not established in the EU, the Regulation applies to the processing of personal data of data subjects who are in the EU where the processing activities are related to the offering of goods or services to such data subjects in the EU or to the monitoring of data subjects' behavior as far as their behavior takes place within the EU.[68]

But the Regulation does not specify what is meant by a person who is on the territory of the EU. This concept may cover accidental or tourist presence, transit, mere residence, domicile, or principal or secondary establishment in the territory of the EU (i.e., within the territory of a Member State of the EU). Moreover, these notions do not have necessarily the same meaning in all Member States. Finally the Regulation applies to the processing of personal data by a controller not established in the EU but in a place where Member State law applies by virtue of public international law.

The territorial reach of the GDPR is thus wide. It therefore applies in a range of cross-border healthcare contexts involving states outside of the EU.

2.2.2.7 The Boundaries of the GDPR: Personal Scope

Like the earlier Convention of 1981 or the Data Protection Directive of 1995, the GDPR does not explicitly determine its personal scope. However, the Regulation identifies the main actors in data processing. As in the Directive, the data controller is the person who, alone or jointly with others, determines the purposes and means of the data processing[69] and the processor is the one who processes personal data on behalf of the data controller.[70] Doctors, other health professionals, hospitals, and other providers of care all fall into the category of data controller or processor. The Regulation also identifies the recipient,[71] the third party,[72] the representative,[73] the enterprise,[74] and the group of undertakings.[75] There are many controversies about who qualifies as data controller, joint data controller, data processor in hospitals and in the healthcare sector in general.

As with the earlier Directive, the GDPR still does not provide a formal definition of the data subject, even though the latter is supposed to be at the heart of the regulatory system. In any case, the Regulation insists on the point that the protection applies irrespective of the nationality or residence of the data subject.[76] Protection under the GDPR extends to persons who are not nationals of any Member State and who do not reside in the territory of any Member State but whose data are processed by a data controller subject to the Regulation. This approach means that all patients whose personal data are processed in the context of healthcare systems or situations within Member States of the EU are covered by the GDPR's protections.

In any case, all these actors must be properly identified when processing personal data. This can lead to some problems, in particular in the context of Internet platforms for patient's data communication, cloud computing services,[77] or mobile applications (mHealth).[78] Who assumes the role of data controller, joint data controller, or data processor?

2.2.2.8 Substantive/Material Rules of the GDPR on Medical Information Privacy and Confidentiality

The GDPR enumerates common uniform substantive rules and details the principles applicable to all data processing within its scope, including to the processing of personal data concerning health. The principles are not that substantially different from the rules previously laid down by the earlier Data Protection Directive. Seven principles apply to all processing of personal data.

Principles of personal data processing. Personal data must be processed lawfully, fairly, and in a transparent manner in relation to the data subject (principles of *lawfulness, fairness*, and *transparency*).[79] Personal data must be collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes (principle of *purpose limitation*).[80] Further processing for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes should not be considered as incompatible with the initial purposes, provided that it is subject to appropriate safeguards for the rights and freedoms of the data subject. These guarantees must ensure that technical and organizational measures are set in place to ensure compliance with the data minimization principle.[81] Whenever possible, further processing should not, or no more than previously, allow for the identification of the data subject. Personal data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed (principle of *data minimization*). Personal data must be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that are inaccurate in regard to the purposes for which they are processed are erased or rectified without delay (principle of *accuracy*).

Personal data must be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed (principle of *storage limitation*). Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest,

scientific or historical research purposes, or statistical purposes provided that it is subject to appropriate safeguards for the rights and freedoms of the data subject. These guarantees must ensure that technical and organizational measures are set in place to ensure compliance with the data minimization principle.[82] Whenever possible, further processing should not or no more allow for the identification of the data subject.

Personal data must be processed in a manner that ensures an appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage using appropriate technical or organizational measures (principle of *integrity and confidentiality*). Finally, the controller is responsible for compliance with the principles applicable to the processing of personal data. The controller must also, and that is formally new, be able to demonstrate that the data processing is compliant with these principles (principle of *accountability*).[83]

2.2.2.9 Data Processing Lawfulness

The GDPR, Article 6, lists the categories of situations in which it is a priori lawful (i.e., permitted by law) to process personal data.[84] These include where the data subject has given consent for specific purposes, or to protect the vital interests of the data subject or another natural person, or is necessary for a task carried out in the public interest.

At first glance, it would seem that processing of health data is barred by the GDPR. As with personal data revealing racial or ethnic origin, sexual orientation, political opinions, religious or philosophical beliefs, or trade union membership, the processing of data concerning health,[85] genetic data, or biometric data for the purpose of uniquely identifying a natural person is in principle prohibited.[86]

But this general prohibition does not apply to many situations in which health data are processed in the healthcare setting. Article 9.2 of the GDPR lists the categories of situations in which it is lawful to process personal data. This includes where explicit consent is given, to protect the vital interests of the data subject, or processing is necessary for reasons of substantial public interest.

To put it another way, each of these categories is supposed to represent a situation in which the interests involved are in an acceptable balance. The interests to be taken into consideration are those of the data controller, the data subject, and the community. In line with the legitimation mechanisms set up by the earlier Directive, it is of course necessary to verify in each individual case, for each data processing taken and considered separately and individually, whether there is a fair balance among these three kinds of interests. This balance must be done in concreto and not only a priori and in abstracto. In this respect, changing the balance of interests over time (e.g., because of changing understandings of the interests of communities, data subjects, or data controllers arising from new technologies) will have the effect of removing the legitimacy of the data processing for the future. The data processing will have to be stopped unless a solution is found to satisfactorily rebalance the interests involved.

Surprisingly, while one of the objectives of the reform of the legal framework for data protection was to eliminate inconsistencies between Member States regarding the processing of personal data relating to health, the GDPR provides that, in respect of the subsidiarity principle, matters should be dealt with at the most local level at which they can be resolved, and Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data, or data concerning health.[87] It follows that the differences between Member States, which have been strongly condemned, are likely to increase in the matter of personal data related to health.

Furthermore, the GDPR does not lay down criteria for delimiting the territorial scope of the national provisions that Member States might adopt regarding the processing of genetic data, biometric data, or health data.[88]

It remains, of course, that, in any case, without prejudice to the Council of Europe's Treaty No. 108, Member States are bound by the common legal framework that emerges from the case-law of the European Court of Human Rights in the field of data protection and by the rights therefore granted to individuals in terms of data control (situations in which the Court considers that the person is entitled to expect that data will not be disclosed without his or her consent), data access (including access to medical records), or medical records security, for example.

In addition to these Council of Europe and EU-level rules, therefore, medical information privacy and confidentiality is subject to national substantive rules which differ across European states.

2.2.3 State Laws

The protection of health data is integrated in the general framework which has been set up for protecting personal data in Europe. Hence, unlike in the US, the protection of *health* data is not restricted to a specific sector of activities (healthcare), to certain professionals (health practitioners) or institutions (health service providers), or to particular categories of citizens (patients). The European legal context is thus quite distinctive as compared to the usual features of the notion of medical professional privilege or professional secrecy. This raises the issue of the distinction between data protection rules (promulgated at European level) and medical professional privilege or professional secrecy rules (promulgated at national levels). As EU law applies only within the scope of EU competence, and Council of Europe law leaves a significant "margin of appreciation" to states parties, despite the European-level norms there remains room for distinctive approaches to medical privacy and confidentiality through the vector of professional privilege and secrecy law.

The transposition of the 1995 Data Protection Directive[89] into Belgian Law is a good example. To what extent did Belgium's implementation of data protection rules have an impact on professional secrecy rules? More specifically, did the data subject's consent, used as a basis of legitimization for the processing of personal data under data protection

rules, also discharge healthcare practitioners of their duty not to disclose any information about their patients under provision 458 of the Belgian Criminal Code (the latter protecting professional secrecy)? For instance, in this context, might the patient allow the health practitioner to send medical information to the insurance company? In a classical criminal point of view, it was not permissible for a patient to discharge healthcare practitioners from their duty not to disclose information about them except in some situations vested in the law, the case-law, and the legal literature. The issue was even more sensitive in that it was part of a larger discussion about patients' rights at national, European, and international levels and especially about empowering patients in the therapeutic relationship (which could concern the power to master the fate of information protected by professional secrecy).

Nevertheless, the answer was obvious: it had never been the intent of European data protection rules to modify professional secrecy rules. Indeed, the objective of data protection rules was and still is to protect individuals against the development of information and communication technologies and, in particular, to protect them against paper files and automated processing of personal data and to entrust them with new subjective rights. There has never been any intent to interfere with the regulation of healthcare professions or with the (legal and ethical) duties of healthcare practitioners. Two arguments supported this interpretation. First, the Data Protection Directive referred to professional secrecy rules[90] without any hint that it intended to modify them. Therefore, it was already possible to infer from this that professional secrecy rules were separate from data protection rules. Second, the duty to lawfully process personal data[91] was interpreted as meaning that it included the duty to comply with the special rules applicable to the processed data, which refers in this case to professional secrecy rules.[92]

The question is now whether this interpretation is still valid since the adoption of the GDPR. Three reasons suggest that it is. First, the GDPR pursues the same goal as the Directive, though in a more elaborate way. In addition, the GDPR also refers to professional secrecy rules without saying it would impact or modify them.[93] Rather, as in the case of the preceding Directive, the GDPR provides that the ban on processing personal data does not apply to the special categories of personal data (among them those related to health) where those are processed for therapeutic purposes by a health professional subject to the obligation of professional secrecy (under Union or Member State law or rules established by national competent bodies) or, under responsibility of the latter, by another person also subject to an obligation of secrecy (under Union or Member State law or rules established by national competent bodies). Second, Member States are permitted under the GDPR to maintain or introduce further conditions (including limitations) with regard to the processing of genetic data, biometric data, or data concerning health.[94] This national discretion covers the question of maintaining, changing, or adopting new professional secrecy rules. Third, the GDPR explicitly provides that Member States may adopt specific rules to set out the powers of the supervisory authorities in relation to controllers or processors that are subject, under Union or Member State law or rules established by national competent bodies, to an obligation of professional secrecy or other equivalent obligations of secrecy where this is necessary and proportionate to reconcile

the right of the protection of personal data with the obligation of secrecy.[95] Thus, the GDPR has neither the objective nor the effect of modifying existing state-level rules regarding professional secrecy: it refers to them as external rules, and it recognizes the possible application of these external rules, notably when processing personal data related to health for therapeutic purposes.

Hence, to summarize, medical data confidentiality and privacy in Europe is regulated at Council of Europe, EU, and national levels, too.

Author Note

This work has been done with financial support from the EU's Horizon 2020 research and innovation program under Grant Agreement no. 730953 (Inspex) and in part by the Swiss Secretariat for Education, Research, and Innovation (SERI) under Grant no. 16.0136 730953. This contribution only reflects the author's view and does not engage the Commission. It is partially based on a previous publication: J. HERVEG, "Data protection and patient mobility in Europe," in A. DEN EXTER (ed.), CROSS-BORDER HEALTHCARE AND EUROPEAN UNION LAW, Erasmus University Press, 2017, pp. 209–231.

3 Data Security

Personal health data can be a sought-after commodity that brings financial and other benefits to numerous parties. For example, employers are interested in health information because they want workers who will not have absenteeism or productivity problems or generate high health insurance costs. Marketers hope to tailor their advertising efforts to consumers' individualized needs and thus could find certain health details to be a great asset. Even criminals may seek data in order to commit identity theft, credit card fraud, or medical insurance fraud.[96] Consequently, without proper security defenses, medical data may be very vulnerable to hacking, theft, and other abuses. This section examines the legal mechanisms that the United States and EU have implemented to promote data security.

3.1 The HIPAA Security Rule

The HIPAA Security Rule is less well-known than the Privacy Rule in the United States but is equally important. It delineates administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of electronic health information (EHI).[97] The administrative safeguard standards include security management processes and workforce security, such as clearance procedures, information access management, security awareness and training, security incident procedures, and contingency plans.[98] Physical safeguards focus on facility access controls, workstation security, and device and media controls.[99] Technical safeguards are procedures to control access to EHI (e.g., en-

cryption), to audit activity related to processing EHI, to protect EHI from improper modification or elimination, and to obtain authentication from those seeking access to EHI.[100]

The HIPAA Security Rule suffers from the same limitations that restrict the scope of the HIPAA Privacy Rule. It covers only health plans, healthcare clearinghouses, healthcare providers who transmit health information electronically for purposes of HIPAA-relevant transactions, and their business associates.[101] Thus, employers, life insurers, educational institutions, marketers, and many others who possess health information do not have to comply with its important data security requirements. Furthermore, because de-identified data do not constitute protected health information,[102] they, too, are not governed by the Security Rule and can be stored in ways that do not comply with its standards.

3.2 Data Security in the GDPR

Security of personal data in the GDPR forms part of a series of new uniform substantive rules to which data controllers and processors are subject. These include, for instance, record keeping, cooperation with supervisory authorities, and privacy impact assessment.

As far as data security is concerned, the data controller and processor must implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk. They must take into account the state of the art; the costs of implementation; and the nature, scope, context, and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons. In assessing the appropriate level of security, they must take into account in particular the risks presented by the data processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored, or otherwise processed.[103] Those measures must be reviewed and updated where necessary. Where proportionate in relation to processing activities, these measures must include the implementation of appropriate data protection policies by the data controller.[104]

Privacy by design imposes obligations on the data controller (and processor) to implement, both at the time of the determination of the means for processing and at the time of the processing itself, appropriate technical and organizational measures (such as pseudonymization) which are designed to implement data-protection principles (such as data minimization) in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of the GDPR and protect the rights of data subjects. In doing so, the data controller has to take into account the state of the art; the cost of implementation; and the nature, scope, context, and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing.[105]

Privacy by default obliges the data controller (and processor) to implement appropriate technical and organizational measures for ensuring that, by default, only personal data that are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the

period of their storage, and their accessibility. In particular, such measures must ensure that, by default, personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.[106] In any case, the data controller and processor must take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller unless required to do so by Union or Member State law.

All this means that hospitals and health practitioners must implement and adapt the general requirements imposed by the GDPR to all data processing. For example, the use of cloud computing by a hospital is not necessarily prohibited by the GDPR. But the implementation of data protection rules could require the use of a public cloud for administrative data and of a private cloud for more sensitive data.

4 Data De-identification, Anonymous Data, and Pseudonymized Data

As noted earlier, bountiful health information is stored in de-identified form in databases that are available to researchers, government officials, and sometimes the public at large.[107] What is de-identified information? The HIPAA Privacy Rule provides detailed guidance. GDPR distinguishes between anonymous data and pseudonymized data.

4.1 De-Identification Under HIPAA

HIPAA states that health information is de-identified if (1) a qualified expert determines that there is only a "very small" risk that the data can be re-identified, and (2) the expert documents his or her analysis.[108] The DHHS issued guidance that recognized several effective de-identification techniques:

- *Suppression*: Redacting particular identifiers before data is disclosed (e.g., zip codes, birthdates, income)
- *Generalization*: Transforming particular information into less specific representations (e.g., indicating a 10-year age range instead of exact age)
- *Perturbation*: Exchanging particular data values for equally specific but different values (e.g., changing patients' ages).[109]

In the alternative, the HIPAA Privacy Rule lists 18 items that should be removed in order to exempt information from HIPAA coverage. These are names; 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 the geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people, and the initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000); 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; telephone numbers; fax numbers; email addresses; social security numbers; medical record numbers; health plan beneficiary numbers; account numbers; certificate/license numbers; vehicle identifiers and serial numbers, including license plate numbers; device identifiers and serial numbers; web universal resource locators (URLs); Internet Protocol (IP) address numbers; biometric identifiers, including finger and voice prints; full face photographic images and any comparable images; and any other unique identifying number, characteristic, or code.[110]

In theory, removal of these 18 elements makes it impossible to connect medical records with patients' names. However, experts have determined that even with redaction of these identifiers, there is a small chance (perhaps 0.01–0.25%), that skilled attackers could re-identify records. They could do so by matching de-identified data to publicly available information, such as voter registration records or news stories about individuals with illnesses or injuries.[111]

In some cases, data analysts may need some of the listed data elements to conduct their analysis. Obtaining consent from thousands or even millions of patients in a database may be prohibitively costly and burdensome. Consequently, the HIPAA Privacy Rule creates a further exemption for three purposes: research, public health, and healthcare operations. It allows covered entities to disclose "limited datasets" for these three uses without patient consent if data recipients sign data use agreements containing specified restrictions and privacy protections. Limited datasets remove most of the 18 listed elements, but they retain dates and geographic locales, though not patients' exact addresses.[112] As valuable as these details are for analysts, they may also make it considerably easier for attackers to re-identify records. By some estimates, the risk of re-identification of limited datasets may be as high as 10–60% depending on what other data are publicly available.[113]

4.2 Anonymous Data and Pseudonymized Data Under the GDPR

The difference between personal data, anonymous data, and pseudonymized data is important. Personal data and pseudonymized data fall under the scope of the GDPR, and all its rules must be respected. Anonymous data are outside the GDPR's scope.

Anonymous data are data for which it is not reasonably possible to make a link with the data subject. It is always a perilous task to decide whether data are anonymous or not in the healthcare sector and especially in the field of scientific research.

Pseudonymized data are data that can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person (cf. Article 4 (5) of the GDPR).

Pseudonymization is a useful form of data processing that can help the data controller meet data security requirements and comply with privacy by design and privacy by default requirements (e.g., the data minimization principle).

5 Mechanisms for Enforcement of Medical Information Confidentiality, Remedies for Privacy Breaches, and Enforcement of Privacy Rights

5.1 American Law

5.1.1 The HIPAA Privacy and Security Rules

The most extensive American privacy regulations, the HIPAA Privacy and Security Rules, do not offer aggrieved individuals a private cause of action. Thus, individuals whose data were disclosed to unauthorized parties cannot sue wrongdoers for damages under federal law. Instead, enforcement is left up to the DHHS Office for Civil Rights (OCR) and state attorneys general offices.[114]

On its website, OCR indicates that between April 2003 and August 2019 it received more than 216,000 HIPAA complaints, and it initiated 979 compliance reviews on its own.[115] Of these, OCR investigated and resolved approximately 27,225 cases, offering technical assistance and requiring privacy practice changes or other corrective action. In addition, OCR reached settlements or imposed civil money penalties in 65 cases, recovering $102,681,582. In the vast majority of cases, OCR found no HIPAA violation.

HIPAA authorizes the government to punish violators with harsh fines and imprisonment.[116] However, robust enforcement depends on adequate staffing. In an era in which many are hostile to “big government,” the federal workforce and its resources will likely shrink rather than grow. In the absence of a threat of private litigation, the HIPAA regulations’ efficacy could be compromised. Some covered entities may calculate that privacy violations are unlikely to be detected and severely punished and thus may be more lax about data security and disclosure than full compliance would require.

5.1.2 State Law

Unlike HIPAA, state common law enables patients to sue healthcare providers for privacy breaches. One tort theory is breach of confidentiality. The elements of this cause of action are (1) the existence of a doctor–patient relationship and (2) a physician’s or medical entity’s disclosure to a third party of confidential information that was gained through this relationship.[117] For example, in the case of *Alberts v. Devine*, the court asserted: “We hold today that a duty of confidentiality arises from the physician–patient relationship and that a violation of that duty, resulting in damages, gives rise to an action sounding in tort against the physician.”[118] Courts have found that the right of confidentiality is rooted in a variety of sources, including privilege statutes protecting physician–patient communica-

tions, licensing statutes prohibiting the disclosure of patient information without authorization, and medical ethics principles articulated in the Hippocratic Oath.[119]

A second tort theory that is available to plaintiffs in limited circumstances is invasion of privacy. Under the common law, the right to privacy can be invaded by "unreasonable publicity given to the other's private life."[120] The tort of invasion of privacy consists of four elements: (a) public disclosure (b) of a private fact (c) that would be objectionable and offensive to a reasonable person and (d) that is not of legitimate public concern.[121]

Courts have also granted relief to those harmed by unauthorized data releases under a number of other theories. These include breach of trust, breach of implied contract, defamation, and negligence.[122] Some state laws provide statutory causes of action as well.[123]

5.1.3 EU Law

To ensure data protection effectiveness, EU law requires Member States to have specific data protection authorities, as well as to provide for specific mechanisms and remedies.

5.1.3.1 Supervisory Authorities

At the level of the Member States, each Member State must provide for one or more independent public authorities to be responsible for monitoring the application of the GDPR in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the EU.[124] Each supervisory authority must act with complete independence in performing its tasks and exercising its powers.[125] The data controller, the processor, and, where applicable, their representatives, must cooperate on request with the supervisory authority.[126]

At the level of the EU, the European Data Protection Board replaces the Working Party on the protection of individuals with regard to the processing of personal data.[127] The Board is composed of the head of one supervisory authority of each Member State and of the European Data Protection Supervisor, or their respective representatives. The Board must act independently when performing its tasks or exercising its powers. In the performance of its tasks or the exercise of its powers, the Board will neither seek nor take instructions from anybody. The Board will draw up an annual report regarding the protection of natural persons with regard to processing in the EU and, where relevant, in third countries and international organizations. The European data protection supervisor will provide the secretariat of the Board.[128]

5.1.3.2 Data Subject's Remedies

Right to lodge a complaint with a supervisory authority. Every data subject has the right to lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual residence, place of work, or place of the alleged infringement if the data subject considers that the processing of personal data relating to him or her infringes the GDPR.[129]

Right to an effective judicial remedy against a supervisory authority. Each natural or legal person shall have the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them.[130] Without prejudice to any other administrative or nonjudicial remedy, each data subject shall have the right to an effective judicial remedy where the supervisory authority which is competent does not handle a complaint or does not inform the data subject within 3 months on the progress or outcome of the complaint.[131]

Right to an effective judicial remedy against a controller or processor. Each data subject shall have the right to an effective judicial remedy where he or she considers that his or her rights under the GDPR have been infringed as a result of the processing of his or her personal data in noncompliance with the GDPR.[132]

Right to compensation and liability. Any person who has suffered material or nonmaterial damage as a result of an infringement of the GDPR has the right to receive compensation from the controller or processor for the damage suffered.[133] Any data controller involved in processing is liable for the damage caused by processing which infringes the GDPR. A processor is liable for the damage caused by processing only where it has not complied with obligations of the GDPR specifically directed to processors or where it has acted outside of or contrary to lawful instructions from the data controller. A data controller or processor is exempt from liability if it proves that it is not in any way responsible for the event giving rise to the damage.

Where more than one data controller or processor, or both a data controller and a processor, are involved in the same processing and where they are responsible for any damage caused by processing, each data controller or processor is liable for the entire damage in order to ensure effective compensation of the data subject.[134]

5.1.3.3 Administrative Obligations of Data Controllers

Notification of personal data breach to supervisory authorities and data subjects. In the case of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored, or otherwise processed (known as “personal data breach”[135]), the data controller must without undue delay and, where feasible, not later than 72 hours after having become aware of it,[136] disclose the personal data breach to the competent supervisory authority.[137] The data controller is exempted from this duty when the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. But, in any case, the data controller must document any personal data breaches, including the facts relating to the personal data breach, its effects, and the remedial action taken. That documentation must enable the supervisory authority to verify the compliance with the obligations applicable to the data controller.

Similarly, the processor must notify the data controller without undue delay after becoming aware of a personal data breach. It must be assumed that it is also required to document any data breaches even if this is not expressly foreseen in the Regulation.

Asymmetrically in relation to the obligation to notify the supervisory authority, the data controller must only disclose the personal data breach to the data subject if the breach is likely to result in a *high* risk to the rights and freedoms of natural persons. This could be the case in the situation in which a hacker publishes online data from a hospital and these data contain information about the health condition of patients. The communication must be done without undue delay. The communication to the data subject must describe in clear and plain language the nature of the personal data breach including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned. It must also contain the name and contact details of the data protection officer or any other contact point where more information can be obtained, the likely consequences of the personal data breach, and the measures taken or proposed to be taken by the controller to address the personal data breach including, where appropriate, measures to mitigate its possible adverse effects.

However, even in the event of a high risk to rights and freedoms, this communication is not always required (e.g., if the hospital has taken all the appropriate measures to mitigate the risks for the data subject). Furthermore, if the data controller has not already communicated the data breach to the data subject, the supervisory authority may, after examining whether this data breach is likely to result in a high risk, require the data controller to communicate or decide that the controller is in one of the situations in which he is exempted from doing so.[138]

Privacy impact assessment. Prior to processing, the data controller must carry out an assessment of the impact of the envisaged processing operations on the protection of personal data[139] where a type of processing, particularly when using new technologies and taking into account the nature, scope, context, and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons. The controller will seek the advice of the data protection officer, where designated, when carrying out a data protection impact assessment.[140]

The data controller will consult the supervisory authority prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk.[141]

If the supervisory authority is of the opinion that the processing would violate the GDPR, especially when the data controller has insufficiently identified or mitigated the risk, the supervisory authority must, within period of up to 8 weeks of receipt of the request for consultation, provide written advice to the controller. In addition where applicable to the processor, the supervisory authority may use any of its investigating powers, remedial powers, advisory powers, or any other power conferred by its national law.[142]

5.1.4 Administrative Fines and Penalties

Depending on the circumstances of each individual case, each supervisory authority may impose effective, proportionate, and dissuasive administrative fines[143] in addition to or in place of corrective measures.[144]

Member States must lay down the rules on other penalties applicable to infringements of the GDPR, in particular for infringements that are not subject to administrative fines. They must take all measures necessary to ensure that these penalties are implemented (and enforced). Such penalties must be effective, proportionate, and dissuasive.[145]

To date, we are witnessing an increase in the number of infringements of the GDPR investigated by supervisory authorities, including in the healthcare sector.

6 Anti-Discrimination Laws

Despite the law's best efforts to protect privacy, individuals' health information is routinely seen by a multitude of entities and persons. Some parties may want to use medical data to their own advantage in ways that do not serve data subjects' best interests. Thus, employers, financial institutions, marketers, and others with financial agendas might use medical data to make adverse decisions that deprive individuals of various opportunities or exploit their vulnerabilities.[146] Consequently, American law includes point-of-use legislation that prohibits particular parties from using medical data to discriminate against data subjects. In Europe, although EU law prohibits discrimination in some contexts (notably employment) on a number of forbidden grounds, health status is not one of those grounds. Thus, most relevant anti-discrimination laws are at the state level, with protection at the EU level occurring through the application of more general data protection rules.

6.1 American Law

Most notably, the ADA establishes a far-reaching anti-discrimination mandate. The ADA prohibits a large variety of parties from engaging in disability-based discrimination. Title I of the statute applies to employers with 15 or more employees. Title II relates to public services, including any instrumentalities of state and local governments. Title III governs "public accommodations and services provided by private entities," such as banks, insurance offices, private educational institutions, sales establishments, and more.[147] Thus, entities that possess identifiable health information and are aware of individuals' disabilities may not use the data for discriminatory purposes. For example, an employer may not reject a qualified applicant just because it is aware that the applicant has a history of cancer, diabetes, or epilepsy.

The Rehabilitation Act of 1973 was the first federal disability discrimination law, but its reach is more limited than the ADA's because it focuses on federal entities. It prohibits programs operated by federal agencies, programs receiving federal financial assistance, federal employers, and federal contractors from discriminating against individuals be-

cause of their disabilities.[148] The Rehabilitation Act coexists with the ADA, which does not cover the executive branch of the federal government.

GINA prohibits employers and health insurers (but not others) from discriminating based on genetic information.[149] Recall that employers and health insurers cannot intentionally seek genetic data, including family health histories, about individuals.[150] Moreover, if they happen to possess genetic data, they must not use it to make adverse decisions regarding data subjects.[151]

Section 1557 of the Affordable Care Act (ACA) is another provision that bans disability-based discrimination. It covers any health program or activity that is funded and/or administrated by the US #DHHS and any health insurance marketplace insurers.[152]

Also relevant is the Fair Housing Act. This law prohibits discrimination in the sale, rental, and financing of housing based on disability and other protected categories.[153]

Almost all states have also adopted statutory anti-discrimination mandates that protect individuals with disabilities.[154] Many are very similar to federal law, but some offer additional protections, such as covering employers with fewer than 15 workers.

6.2 EU Law

EU law prohibits discrimination on various protected grounds, including disability, in certain contexts, particularly employment.[155] However, in general, when it comes to using health data to discriminate, people in Europe must look to their own country’s law for protection. Some national legislation bans or restricts the use of medical information under certain circumstances (insurance, credit, employment, school, etc.). For instance, “medical condition” is a prohibited ground of discrimination under the French Labor Code. At the EU level, the main protection against discrimination coming from the use of medical data must be found in data protection rules.

First, as explained earlier, personal data must be processed lawfully and for a legitimate purpose. The latter means that no one may process data in order to unlawfully discriminate against data subjects. Moreover, personal data must be adequate, relevant, and limited to what is necessary in relation to the legitimate purposes for which they are processed (this refers to the principle of data minimization). And personal data must be protected against unauthorized or unlawful processing. The data controller is responsible for compliance with these obligations, which should, at least in principle, prevent discrimination against data subjects.

It must be reiterated that the assessment of the legitimacy of data processing is sensitive to other aspects of the implementation of data protection, such as the level of confidentiality and security of the data processing, the level of control exercised by the national supervisory authority, the degree of necessity of the purpose pursued, and so on.

It is also important to remember that Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data, or data concerning health. Therefore, medical information privacy and confidentiality is subject to national substantive rules, which differ across European states.

7 Contemporary Legal Challenges

7.1 Data Security

As hackers and other cybercriminals become increasingly sophisticated, new data security threats arise with dizzying speed. For example, healthcare providers must now worry about “ransomware attacks” by which hackers encrypt data and demand ransom in exchange for decryption keys, thereby denying users access to their own data until they comply with payment demands. The scope of this threat became clear in the wake of the May 2017 “WannaCry” ransomware attack that crippled the British National Health Service and many other providers around the globe.[156]

The HIPAA Security Rule details many administrative, physical, and technical safeguards. But its recommendations are not exhaustive because its authors could not possibly anticipate every risk that would arise in the future. Moreover, the Security Rule deliberately leaves implementation mechanisms to the discretion of covered entities.[157] In fact, a provision entitled “Flexibility of Approach” states: “Covered entities may use any security measures that allow the covered entity to reasonably and appropriately implement the standards and implementation specifications.”[158]

A flexible approach reduces covered entities’ compliance burdens. Moreover, the approach recognizes the ever-changing nature of technology and its need to continuously evolve to respond to new forms of cybersecurity threats.

Yet, alongside its benefits, flexibility can raise significant risks in the regulatory context. It can leave covered entities with anemic and inadequate guidance on how to comply with legal requirements. Resource-poor healthcare providers who do not have sophisticated information technology departments might be at a particular disadvantage. They would be well-advised to consult security experts and adopt best industry practices, but some may have other priorities in light of tight budgets.[159]

Because attackers are quick to exploit newly discovered vulnerabilities in software systems, it is critical that covered entities diligently assess and respond to these risks. It is also essential that regulators tirelessly follow cybersecurity threats and periodically reevaluate the HIPAA Security rule to determine whether and how regulations should be revised.

7.2 Data Subjects' Rights to Their Medical Information

Under the HIPAA Privacy Rule, patients have a right to inspect and obtain copies of their medical records other than psychotherapy notes. Access requests can be denied under particular circumstances, such as the existence of a reasonable likelihood that seeing the data will result in harm to the patient or another party.[160] In addition, patients may ask that their health records be amended or used restrictively, though covered entities may deny the requests for legitimate reasons specified in the regulations (e.g., the records are accurate and should not be changed).[161]

The question of the patient's access to medical information in Europe finds a first answer in patient's rights legislation but also under data protection law. And where the old Data Protection Directive formally recognized three rights (right of access, right to object to data processing, and right not to be subject to individual automated decisions), the GDPR grants data subjects eight rights (right to information, right of access, right to rectification, right to erase, right to limit treatment, right to data portability, right to object to data processing, and right not to be subject to automated individual decisions).[162]

In particular, the right to data portability[163] means that, where the data are processed on the basis of the data subject's consent or a contract and by automated means, the data subject has the right to request and receive in a structured, commonly used, and machine-readable format the data he or she has provided to the data controller. The data subject is then entitled to forward these data to another data controller. The data subject may also ask the first controller to send them directly to another data controller if technically feasible.[164] This right inevitably brings to mind the situation in which the patient's medical record is shared between healthcare professionals to ensure the continuity of care. The implementation of this newly formalized right may therefore not be a problem in the health sector as long as it is extended to data not provided by the patient.[165]

That being said, the real challenge is to know how these rights will really and effectively prosper in light of the debates around cloud computing services, big data, and mobile applications and whether this formal increase in the number of rights will improve data protection and benefits for data subjects. Doubt is permitted. There should be more information for the public on the way mobile applications work and more transparency about algorithmic governance in healthcare contexts. For example, public authorities and bodies should disseminate more information about the numerous actors and data flows occurring behind the screens of smartphones that gather health (and other) data.[166]

7.3 The Proliferation of Health-Related Data

It is a mistake to think that personal health information is restricted to patients' electronic health records. A large number of private and public sector entities are creating data resources for "secondary use" (i.e., use for non-treatment purposes). Such purposes include research, public health initiatives, healthcare institutions' quality assessment and improvement efforts, and more. Health information resources are often termed "big da-

ta," which means large collections of data characterized by their high volume, variety, and velocity (the speed with which they are produced and grow).[167]

National, regional, and local government agencies, as well as private enterprises, have launched big data initiatives. The National Institutes of Health describe their *All of Us* program as follows: "The All of Us Research Program is a historic effort to gather data from one million or more people living in the United States to accelerate research and improve health. By taking into account individual differences in lifestyle, environment, and biology, researchers will uncover paths toward delivering precision medicine."[168]

A federal-state-industry partnership sponsored by the Agency for Healthcare Research and Quality has developed the Healthcare Cost and Utilization Project, which created the State Inpatient Databases (SID). The SID contain hospital discharge records that are available for purchase in some states.[169]

Another example, this from the private sector, is IBM Watson Health. This project "brings together individual clinical research and social data from a diverse range of health sources creating a secure cloud-based data sharing hub."[170]

Big data collections often consist of de-identified EHRs. Under the HIPAA Privacy Rule, covered entities can disclose fully de-identified information without patient consent, and information distributed by noncovered entities is not subject to any disclosure constraints. Thus, many patients will never discover that their records have been incorporated into a database and are being used by third parties. As noted earlier, the risk of re-identification can never be completely eliminated no matter how thoroughly identifiers are expunged.

More startlingly, when some identifiers are retained (e.g., by entities not covered by HIPAA), the risk of re-identification increases dramatically. In fact, it is estimated that up to 87% of the US population could be uniquely identified based on three items alone: gender, zip code, and date of birth.[171] In the pre-HIPAA era, Latanya Sweeney, now a Harvard professor, became famous for having identified Massachusetts Governor William Weld's records based on "anonymized" hospital discharge data that she matched to voter registration information when she was a graduate student in 1996.[172]

Health information databases are not the only source of data that could be available to others without patients' knowledge. There is an abundance of what one scholar calls "medically inflected data."[173] Data miners seeking individuals' health data have no shortage of sources available to them. Supermarket loyalty cards, credit card transactions, web browsing histories, social media interactions, phone call records, and other data fall outside the jurisdiction of the HIPAA Privacy Rule, but they can reveal a great deal about individuals' health. For example, experts analyzed the Facebook "likes" of approximately 60,000 volunteers and were able to discern "sexual orientation, ethnicity, religious and political views, personality traits, intelligence, happiness, use of addictive substances, parental separation, age, and gender."[174] The risk to privacy is also demonstrated by a 2012 *Forbes* magazine article entitled "How Target Figured Out a Teen Girl Was Pregnant

Before Her Father Did.”[175] Target was able to determine that the teenager was pregnant based on her purchases and began sending her coupons for baby goods.

Who might be interested in information related to individuals’ health? The list includes employers, lenders, marketers, advertisers, and anyone else with a stake in a person’s economic future. To illustrate, employers seek workers who will be healthy, productive, and not generate high health insurance costs. Lenders want borrowers who are healthy enough to work and pay back their loans. Marketers wish to tailor their advertising to fit customers’ needs and desires. Consequently, a growing industry of data miners and data brokers offers a wealth of personal information for sale.[176]

In the contemporary world virtually no one can escape the disclosure of personal details. Health data are no exception. Legislators must ensure that HIPAA and other privacy laws do not ignore emerging data trends and are updated to provide appropriate privacy protections.[177]

7.4 Predictive Health Information

Thus far, the chapter has largely addressed data that reveal something about individuals’ current health status. However, certain types of data may be indicators of future illnesses, even for people who appear to be perfectly healthy at the present time.

Researchers are aggressively searching for predictive health information. For example, a study published in 2014 suggested that physicians could use blood tests to predict imminent dementia.[178] Investigators found that people who suffered from cognitive impairment when their blood was drawn or within a few years of the test had lower levels of 10 phospholipids. Data algorithms can also forecast certain diseases before their symptoms are apparent. Researchers have used algorithms to analyze EHR and insurance claims data to predict clinical depression, diabetes, and heart failure.[179]

Data that are not explicitly medical in nature can be illuminating as well. Smoking and childlessness are known to generate health risks.[180] Researchers have found that people who shop in bicycle stores are generally in good health, and those who vote in midterm elections are healthier than those who do not.[181] By contrast, individuals with low credit scores may not have the financial means to fill prescriptions and obtain good medical care and thus are vulnerable to poor health.

One can learn a great deal about people’s health from their smoking status, parental status, purchases, voting patterns, and credit scores. Yet such information remains outside the scope of the HIPAA Privacy and Security Rules if it is not contained in a medical record.

Moreover, Americans are not protected against discrimination based on predictions of illness in later years. The ADA covers only individuals who (1) have a physical or mental impairment that substantially limits one or more major life activities, (2) have a record of such an impairment, or (3) are regarded as currently having such an impairment.[182] It

therefore does not reach healthy individuals who are subject to discrimination because they are suspected of being at risk of *future* health problems. Consequently, under the ADA, nothing would stop employers, lenders, educational institutions, or others from rejecting applicants because of anticipated medical conditions. Almost no other anti-discrimination law (with the exception of GINA, which governs only genetic information) is broad enough to prohibit discrimination based solely on predictive data.

As prognostic abilities improve, third parties may increasingly seek predictive data from data brokers. They will be valuable for anyone who has a stake in others' health as an employer, lender, advertiser, etc. Once the information is in such parties' possession, they are free to use it as they see fit. This includes making adverse decisions about individuals in order to avoid business risks and save costs.

Consequently, the privacy laws are not the only legislation that may need to be amended in order to be aligned with current technological and medical capabilities. The ADA and other anti-discrimination laws, which focus only on current disabilities, also require revision. It is inevitable that some personal health-related information will fall into the hands of others without patient consent. Patients would be well-served by protections that limit the uses to which such information can be put. American law should uniformly prohibit discrimination based on predictive health information.

By contrast, with sectoral or point-of-use legislation, the GDPR provides a comprehensive framework regulating the processing of all personal data. However, there is room for some national legislation in addition to the GDPR rules, even if the limits of Member States freedom are not always straightforward in the matter of data protection. It is also important to recall that the GDPR rules must be analyzed, implemented, and interpreted in light of Convention no. 108+ and all the sectorial recommendations adopted by the Council of Europe in the matter of data protection.

8 Conclusion

With the enactment of the HIPAA Privacy and Security Rule early in the 21st century, American law took a leap forward in the area of medical privacy. However, contemporary privacy and anti-discrimination laws still contain significant gaps and limitations. Much regulatory work remains to be done to ensure that Americans enjoy comprehensive legal protections.

In Europe, the GDPR has consolidated the previous applicable rules from Directive 95/46/EC. Furthermore, it has expanded and developed certain requirements, and it has also created some new obligations for data controllers and data processors. But the GDPR does not provide a specific set of rules for the processing of personal data concerning health, except the rules for lifting the ban on their processing (Article 9 of the GDPR). The consequence is that processing of health data is mainly subject to the general regime put into place by the GDPR, with some special rules about when it is lawful to process health data. In fact, the real challenge lies more in making the GDPR an effective tool for

protection of citizens' rights when it comes to the processing of personal data related to them. Today, this challenge should focus on how to inform data subjects about their rights and on the way new information and communication technologies work, including new actors in data flows in eHealth and mHealth. This is all the more true when considering mobile health applications and big data in the context of scientific and medical research. As in the United States, there is more regulatory work to be done.

Notes:

(1.) Ian E. Thompson, *The Nature of Confidentiality*, 5 J. MED. ETHICS 57, 57 (1979).

(2.) The notion of professional privilege in healthcare has never been harmonized in Europe. The notion is specific to each European state. Its material and personal scope may vary from state to state, as well as its legal effects. In general, breach of professional secrecy may lead to criminal prosecution of immediate contract termination for the practitioner concerned. Undue use or even possession of information protected by professional privilege may also be a criminal offence.

(3.) BRUCE SCHNEIER, DATA AND GOLIATH: THE HIDDEN BATTLES TO COLLECT YOUR DATA AND CONTROL YOUR WORLD 126–127 (W.W. Norton 2015).

(4.) SHARONA HOFFMAN, ELECTRONIC HEALTH RECORDS AND MEDICAL BIG DATA: LAW AND POLICY 116–124 (Cambridge University Press 2016).

(5.) Id. at 138; David J. Kaufman et al., *Public Opinion About the Importance of Privacy in Biobank Research*, 5 AM. J. HUM. GENET. 85 (2009), 645; Bernard Debatin et al., *Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences*, 15 J. COMPUTER-MEDIATED COMM. 1 (2009) 86, 100.

(6.) COMM. ON HEALTH RESEARCH & THE PRIVACY OF HEALTH INFO.: THE HIPAA PRIVACY RULE, IOM, BEYOND THE HIPAA PRIVACY RULE: ENHANCING PRIVACY, IMPROVING HEALTH THROUGH RESEARCH 76 (Sharyl J. Nass et al. eds., 2009).

(7.) Sharona Hoffman & Andy Podgurski, *The Use and Misuse of Biomedical Data: Is Bigger Really Better?* 39 AM. J. L. MED. 497, 503–515 (2013).

(8.) Janice Phaik Lin Goh, *Privacy, Security, and Wearable Technology*, 8 LANDSLIDE (2015).

(9.) 45 C.F.R. §§ 160.101–534 (2018).

(10.) Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119 4 May 2016 p. 1.

(11.) See Griswold v. Connecticut, 381 U.S. 479, 483, 485–486 (1965) (asserting that "the First Amendment has a penumbra where privacy is protected from governmental intrusion"); Roe v. Wade, 410 U.S. 113, 153 (1973) (determining that the right to privacy en-

compasses a woman's decision to terminate her pregnancy, subject to appropriate state regulation).

(12.) American Medical Association, *AMA Code of Medical Ethics: AMA Principles of Medical Ethics* (revised 2001), https://www.ama-assn.org/sites/default/files/media-browser/principles-of-medical-ethics.pdf.

(13.) National Aeronatutics and Space Administration v. Nelson, 131 S.Ct. 746, 756–757 (2011).

(14.) U.S. Department of Health and Human Services, Does the HIPAA Privacy Rule Preempt State Laws?, https://www.hhs.gov/hipaa/for-professionals/faq/399/does-hipaa-preempt-state-laws/index.html (last reviewed July 26, 2013).

(15.) 42 U.S.C. §§ 1320d–1320d-9 (2010); Health Information Technology for Economic and Clinical Health (HITECH) Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (ARRA), Pub. L. No. 111–115 (Feb. 17, 2009).

(16.) 45 C.F.R. §§ 164.508–.510 (2018).

(17.) 45 C.F.R. § 164.520(a) (2018).

(18.) 45 C.F.R. §§ 164.520, 164.522 (2018).

(19.) 45 C.F.R. §§ 164.400–.408 (2018). The media must be notified if a breach involves "more than 500 residents of a State or jurisdiction." Id. at § 164.408. Unsecured protected health information means information "that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a [specified] technology or methodology," such as encryption.

(20.) 45 C.F.R. §§ 160.102–160.103 (2018); 42 U.S.C. §17934 (2010).

(21.) Sharona Hoffman & Andy Podgurski, *In Sickness, Health, and Cyberspace: Protecting the Security of Electronic Private Health Information*, 48 B.C. L. REV. 331, 337 (2007).

(22.) 42 U.S.C. §12112(d) (2010).

(23.) Sharona Hoffman, *Employing E-Health: The Impact of Electronic Health Records on the Workplace*, 19 SPG KAN. J.L. & PUB. POL'Y 409, 409–410 (2010).

(24.) WebMD, *WebMDsymptomchecker*, http://symptoms.webmd.com/#introView.

(25.) Nir Kshetri & Dholakia Nikhilesh *Offshoring of Healthcare Services: The Case of the Indian Medical Transcription Offshoring Industry*, 25 J. HEALTH ORG. & MANAGEMENT 94, 94 (2011).

(26.) 45 C.F.R. §164.506 (2018).

(27.) Judy Foreman, *At Risk of Exposure: In the Push for Electronic Medical Records, Concern Is Growing About How Well Privacy Can Be Safeguarded*, L.A. TIMES, June 26, 2006, http://articles.latimes.com/2006/jun/26/health/he-privacy26.

(28.) 45 C.F.R.§§ 164.502–512 (2018).

(29.) 45 C.F.R. § 160.103 (2018).

(30.) Hoffman & Podgurski, *supra* note 7, at 506–515.

(31.) 42 U.S.C. § 12112(d)(4)(B) (2010).

(32.) 20 U.S.C. § 1232g (2010).

(33.) Genetic Information Nondiscrimination Act of 2008, Pub. L. No. 110–223, 122 Stat. 881 (2008) (codified as amended in scattered sections of 29 and 42 U.S.C.).

(34.) 45 C.F.R. §§ 46.102(f) & 46.116 (2018).

(35.) AMERICANS HEALTH LAWYERS ASSOCIATION, STATE HEALTHCARE PRIVACY LAW SURVEY (2013); LawAtlas, Public Health Departments and State Patient Confidentiality Laws Map, http://lawatlas.org/preview?dataset=public-health-departments-and-state-patient-confidentiality-laws.

(36.) CAL. CIV. CODE §§56-56.06 and 1798.84(b) (2018); TEX. HEALTH & SAFETY CODE ANN. § 181.001(b)(2) (2015).

(37.) Mary Butler, *Is HIPAA Outdated? While Coverage Gaps and Growing Breaches Raise Industry Concern, Others Argue HIPAA Is Still Effective*, 88 J. AHIMA 14–17 (April 2017), https://bok.ahima.org/doc?oid=302073#.XPLIP4hKg2w.

(38.) Joy L. Pritts, *Altered States: State Health Privacy Laws and the Impact of the Federal Health Privacy Rule*, 2 YALE J. HEALTH POL'Y, L. & ETHICS 325, 335 (2002); LawAtlas, Public Health Departments and State Patient Confidentiality Laws Map, http://lawatlas.org/preview?dataset=public-health-departments-and-state-patient-confidentiality-laws.

(39.) Ahmad Adi & Mohammad Mathbout, *The Duty to Protect: Four Decades After Tarasoff*, AM. J. PSYCH. RESIDENTS' J. 1–8 (Apr. 2018), https://ajp.psychiatryonline.org/doi/pdf/10.1176/appi.ajp-rj.2018.130402.

(40.) *See* Bradshaw v. Daniel, 854 S.W.2d 865 (Tenn. 1993).

(41.) Tarasoff v. Regents of University of California, 17 Cal. 3d 425 (Cal. 1976).

(42.) Id. at 431. See also AMERICAN LAW INSTITUTE, RESTATEMENT THIRD OF THE LAW, TORTS: LIABILITY FOR PHYSICAL AND EMOTIONAL HARM, § 41 (2010).

(43.) In the strict sense, European law refers to the law originating from the EU institutions and bodies. In a broader sense, it also refers to the law emanating from the Council of Europe. In this section, we refer to the broad notion of European law.

(44.) This means, notably, that, in this extent, professional secrecy rules may not oppose the data subject's right of access under data protection law.

(45.) Council of Europe, Resolution (73) 22.

(46.) Council of Europe, Resolution (74) 29.

(47.) This Convention has been revised, and the Convention 108+ was adopted by the Committee of Ministers on May 18, 2018, at its 128th meeting.

(48.) Recommendation 97(5) on the protection of medical data is also under revision (see doc. T-PD(2018)06).

(49.) On the basis of which it could already be argued that each state has a positive obligation to protect personal data.

(50.) OJ 5 June 1979 no. C 140/34.

(51.) OJ L 281 23 November 1995 p. 31 (take into account the consolidated text).

(52.) Charter of fundamental rights of the EU, 2016/C 202/02. See Working Party on the Protection of Individuals with Regard to the Processing of Personal Data *Recommendation 4/99 on the inclusion of the fundamental right to data protection in the European catalogue of fundamental rights* WP 26 7 September 1999.

(53.) See Article 16 TFEU.

(54.) Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119 4 May 2016 p. 1.

(55.) On the Regulation, *see*: S GUTWIRTH, R LEENES, & P. DE HERT (ed.), REFORMING EUROPEAN DATA PROTECTION LAW, Law, Governance and Technology Series, Issues in Privacy and Data Protection, volume 20 (Springer, 2015).

(56.) In the meaning of the first Article of the European Convention on Human Rights to which Article 52 of the Charter of Fundamental Rights of the EU refers.

(57.) On the right to data protection, *see*: G. GONZALEZ FUSTER, THE EMERGENCE OF PERSONAL DATA PROTECTION AS A FUNDAMENTAL RIGHT OF THE EU, Law, Governance and Technology Series, Issues in Privacy and Data Protection, volume 16 (Springer, 2014); B. van der Sloot, "Legal Fundamentalism: Is Data Protection Really a Fundamental Right ?" in R. LEENES, R. van BRAKEL, S. GUTWIRTH, & P. DE HERT, DATA PROTEC-

TION AND PRIVACY: (IN)VISIBILITIES AND INFRASTRUCTURES, Law, Governance and Technology Series, Issues in Privacy and Data Protection, volume 36 (Springer, 2017), 3.

(58.) The filing system means any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized, or dispersed on a functional or geographical basis (Article 4.6 of the Regulation).

(59.) Article 4.1 of the Regulation.

(60.) Such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

(61.) Article 4.15 of the Regulation.

(62.) Recital 35 of the Regulation.

(63.) Article 29 Data Protection Working Party Working, Document on Genetic data, 17 March 2004, WP 91.

(64.) See Recital 34 of the Regulation.

(65.) The [data] controller means the natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller, or the specific criteria for its nomination may be provided for by Union or Member State law (Article 4.7 of the Regulation). See Article 29 Data Protection Working Party *Opinion 1/2010 on the concepts of "controller" and "processor"* WP 169 16 February 2010.

(66.) The processor means a natural or legal person, public authority, agency, or other body which processes personal data on behalf of the controller (Article 4.8 of the Regulation).

(67.) Article 3.1 of the Regulation.

(68.) Article 3.2 of the Regulation.

(69.) Article 4.7 of the Regulation. See Article 29 Data Protection Working Party *Opinion 1/2010 on the concepts of "controller" and "processor"* WP 169 16 February 2010.

(70.) Article 4.8 of the Regulation.

(71.) The "recipient" means a natural or legal person, public authority, agency, or another body to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the

applicable data protection rules according to the purposes of the processing (Article 4.9 of the Regulation).

(72.) The “third party” means a natural or legal person, public authority, agency, or body other than the data subject, controller, processor, and persons who, under the direct authority of the controller or processor, are authorized to process personal data (Article 4.8 of the Regulation).

(73.) The “representative” means a natural or legal person established in the Union who, designated by the controller or processor, represents the controller or processor with regard to their respective obligations (Article 4.8 of the Regulation).

(74.) The “enterprise” means a natural or legal person engaged in an economic activity, irrespective of its legal form, including partnerships or associations regularly engaged in an economic activity (Article 4.8 of the Regulation).

(75.) The “group of undertakings” means a controlling undertaking and its controlled undertakings (Article 4.8 of the Regulation).

(76.) See Recital no. 14. In any case, this protection is expressly excluded for legal persons (see Recital no. 14). The Regulation is, however, once again ambiguous. Indeed, it states that “*This Regulation does not cover the processing of personal data which concerns legal persons and in particular undertakings established as legal persons, including the name and the form of the legal person and the contact details of the legal person*.” This last sentence seems to imply a form of derogation, which would mean that there could be some form of protection for other data related to enterprises. In theory, this would be wrong, but this recital brings unnecessary doubt.

(77.) See Article 29 Data Protection Working Party *Opinion 05/2012 on Cloud Computing* WP 196 1 July 2012.

(78.) See Article 29 Data Protection Working Party *Opinion 02/2013 on apps on smart devices* WP 202 27 February 2013.

(79.) See Article 29 Data Protection Working Party *Guidelines on Transparency under Regulation 2016/679* WP 260 rev.01 11 April 2018.

(80.) See Article 29 Data Protection Working Party *Opinion 03/2013 on purpose limitation* WP 203 2 April 2013.

(81.) These measures may include pseudonymization, to the extent that these purposes can be achieved in this way. Pseudonymization means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person (Article 4.5 of the Regulation).

(82.) Id.

(83.) See Article 29 Data Protection Working Party *Opinion 3/2010 on the principle of accountability* WP 173 13 July 2010

(84.) See Article 6 of the Regulation and the possibility of special arrangements for processing imposed by law or carried out in the public interest or in the exercise of official authority by the controller and the flexibility of the criterion for the compatibility of further data processing. See Article 29 Data Protection Working Party *Guidelines on Consent under Regulation 2016/679* WP 259 rev.01 10 April 2018.

(85.) The definition of health data is discussed *supra*, at 2.2.2.5.

(86.) Article 9.1 of the Regulation.

(87.) Article 9.4 of the Regulation.

(88.) Article 9.4 *in fine* of the Regulation.

(89.) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

(90.) See Recital 33 of the Directive 95/46/EC and Article 8.3.

(91.) Article 6.1. a) of Directive 95/46/EC.

(92.) *See*: J. HERVEG, M.-N. VERHAEGEN, & Y. POULLET, *Les droits du patient face au traitement informatisé de ses données dans une finalité thérapeutique: les conditions d'une alliance entre informatique, vie privée et santé*, 2 REVUE DU DROIT DE LA SANTÉ, 56–84 (2002–2003); C. DE TERWANGNE, «Les cabinets d'avocats et la loi sur la protection des données à caractère personnel », in CABINETS D'AVOCATS ET TECHNOLOGIES DE L'INFORMATION: BALISES ET ENJEUX (Bruxelles, Academia-Bruylant, 2005), Cahiers du CRID, no. 26, p. 156.

(93.) See Article 9.3 of the Regulation on the processing of special categories of personal data.

(94.) Article 9.4 of the Regulation.

(95.) See Article 90 of the Regulation. These rules are only applicable to personal data received or collected by the data controller or data processor in an activity subjected to this obligation of secrecy.

(96.) HOFFMAN, *supra* note 4, at 59–60.

(97.) 45 C.F.R. §§ 164.302 -.318 (2018).

(98.) 45 C.F.R. § 164.308 (2018).

(99.) 45 C.F.R. § 164.310 (2018).

(100.) 45 C.F.R. § 164.312 (2018).

(101.) 45 C.F.R. §§ 160.102–160.103 (2018); 42 U.S.C. §17934 (2010).

(102.) 45 C.F.R. § 160.103 (2018).

(103.) See Article 32 of the Regulation.

(104.) See Article 24 of the Regulation. The application of an approved code of conduct or approved certification mechanisms may serve as a means of demonstrating compliance with the obligations of the data controller.

(105.) On this, see Article 25.1 of the Regulation. An approved certification mechanism may serve as an element to demonstrate compliance with these requirements.

(106.) See Article 25.2 of the Regulation. Again, an approved certification mechanism can serve as an element to demonstrate compliance with these requirements.

(107.) HOFFMAN, *supra* note 4, at 168–175; *supra* Part I.A.1.a.

(108.) 45 C.F.R. § 164.514(b)(1) (2018).

(109.) *Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule*, U.S. DEP'T OF HEALTH & HUMAN SERVS. (Nov. 26, 2012), http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/De-identification/guidance.html#guidancedetermination (noting that techniques such as suppression and generalization are often used in combination).

(110.) 45 C.F.R. § 164.514(b)(2)(i) (2018). In addition, information will not be considered de-identified if an entity has "actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information." Id. at §164.514(b)(2)(ii).

(111.) NAT'L COMM. ON VITAL & HEALTH STATISTICS, REPORT TO THE SECRETARY OF HEALTH AND HUMAN SERVICES ON ENHANCED PROTECTIONS FOR USES OF HEALTH DATA: A STEWARDSHIP FRAMEWORK FOR "SECONDARY USES" OF ELECTRONICALLY COLLECTED AND TRANSMITTED HEALTH DATA 36 n.16 (2007), http://bok.ahima.org/PdfView?oid=76869 ; Sharona Hoffman & Andy Podgurski, *Balancing Privacy, Autonomy, and Scientific Needs in Electronic Health Records Research*, 65 SMU L. REV. 85, 105–107 (2012).

(112.) 45 C.F.R. §§164.514(e)(1)-(4) (2018).

(113.) Kathleen Benitez & Bradley Malin, *Evaluating Re-identification Risks with Respect to the HIPAA Privacy Rule*, 17 J. AM. MED. INFORMATICS ASS'N 169, 169 (2010).

(114.) 45 C.F.R. §160.306 (2018); 42 U.S.C.A. § 1320d-5(d) (2010).

(115.) US Department of Health & Human Services, Enforcement Highlights, https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-highlights/index.html (last reviewed on November 9, 2017).

(116.) 42 U.S.C.A. §§ 1320d-5–1320d-6 (2010).

(117.) Neil M. Richards & Daniel J. Solove, *Privacy's Other Path: Recovering the Law of Confidentiality*, 96 GEO. L.J. 123, 157 (2007).

(118.) Alberts v. Devine, 479 N.E.2d 113, 120 (Mass. 1985)

(119.) Peter A. Winn, *Confidentiality in Cyberspace: The HIPAA Privacy Rules and the Common Law*, 33 RUTGERS L.J. 617, 654–655 (2002).

(120.) Newkirk v. GKN Armstrong Wheels, Inc., 168 F.Supp.3d 1174, 1201 (N.D. Iowa 2016).

(121.) *See* Diaz v. Oakland Tribune, 188 Cal. Rptr. 762, 766 (Cal. Ct. App. 1983).

(122.) *Confidentiality and Privacy of Personal Data*, in INSTITUTE OF MEDICINE, HEALTH DATA IN THE INFORMATION AGE: USE, DISCLOSURE, AND PRIVACY 149 (Molla S. Donaldson & Kathleen N. Lohr, Eds. 1994).

(123.) Id.; Sharona Hoffman & Andy Podgurski, *E-Health Hazards: Provider Liability and Electronic Health Record Systems*, 24 BERKELEY TECH. L. J. 1523, 1558–1560 (2009).

(124.) See Article 51 of the Regulation on the principle of independence and Article 55 on the issue of the competence of the supervisory authority (cf. Article 4.22 of the Regulation for the definition of the *supervisory authority concerned*). It is expressly provided that the supervisory authorities are not competent to review the processing operations carried out by the courts in the exercise of their judicial function (Article 55.3 of the Regulation). The duties and powers of the supervisory authorities are detailed in Articles 57 and 58 of the Regulation.

See Article 29 Data Protection Working Party *Guidelines for identifying a controller or processor's lead supervisory authority* WP 244 rev.01 5 April 2017.

(125.) See Article 52 of the Regulation.

(126.) Article 31 of the Regulation. The application of an approved Code of Conduct or an approved certification mechanism may serve as an element to demonstrate compliance with date processing security requirements.

(127.) See Article 68 of the Regulation. Article 70 lists its missions.

(128.) The European Data Protection Supervisor is also the supervisory authority for EUROPOL.

(129.) It is not easy to argue that this right exists in the case of a breach of a rule which would be imposed by a Member State within the scope of the discretion which would be accorded to the state for the implementation of a particular provision of the Regulation. See Article 80 on the question of the representation of data subjects.

(130.) Directive 95/46/EC already provided that Decisions by the supervisory authority which give rise to complaints may be appealed against through the courts (Article 28.3, *in fine*). See Article 78.1 of the Regulation. Proceedings against a supervisory authority must be brought before the courts of the Member State where the supervisory authority is established. Where proceedings are brought against a decision of a supervisory authority which was preceded by an opinion or a decision of the Board in the consistency mechanism, the supervisory authority shall forward that opinion or decision to the court (Article 78.4 of the Regulation).

(131.) See Article 78.2 of the Regulation. Proceedings against a supervisory authority must be brought before the courts of the Member State where the supervisory authority is established. Where proceedings are brought against a decision of a supervisory authority which was preceded by an opinion or a decision of the Board in the consistency mechanism, the supervisory authority shall forward that opinion or decision to the court (Article 78.4 of the Regulation).

(132.) See Article 79.1 of the Regulation. Proceedings against a controller or a processor must be brought before the courts of the Member State where the controller or processor has an establishment. Alternatively, such proceedings may be brought before the courts of the Member State where the data subject has his or her habitual residence, unless the controller or processor is a public authority of a Member State acting in the exercise of its public powers.

(133.) Court proceedings for exercising the right to receive compensation must be brought before the courts competent under the law of the Member State where the data controller or processor has an establishment. Alternatively, such proceedings may be brought before the courts of the Member State where the data subject has his or her habitual residence, unless the controller or processor is a public authority of a Member State acting in the exercise of its public powers.

(134.) See Article 82 of the Regulation. Where a controller or processor has, in accordance with paragraph 4, paid full compensation for the damage suffered, that controller or processor shall be entitled to claim back from the other controllers or processors involved in the same processing that part of the compensation corresponding to their part of responsibility for the damage.

(135.) Article 4.12 of the Regulation. See Article 29 Data Protection Working Party Working *Document 01/2011 on the current EU personal data breach framework and recommendations for future policy developments* WP 184 5 April 2011, *Opinion 03/2014 on Per-*

sonal Data Breach Notification WP 213 25 March 2014, and *Guidelines on Personal data breach notification under Regulation 2016/679* WP 250 rev.01 6 February 2018.

(136.) See Article 33 of the Regulation. Where the notification to the supervisory authority is not made within 72 hours, it has to be accompanied by reasons for the delay. Where, and in so far as it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

(137.) The notification must at least describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned, and the categories and approximate number of personal data records concerned; communicate the name and contact details of the data protection officer or other contact point where more information can be obtained; describe the likely consequences of the personal data breach; and describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

(138.) Article 34 of the Regulation.

(139.) *See*: D. WRIGHT & P. DE HET (ed.), PRIVACY IMPACT ASSESSMENT, Law, Governance and Technology Series, volume 6 (Springer, 2012); and Article 29 Data Protection Working Party *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679* WP 248 4 April 2017.

(140.) See Article 35 of the Regulation. A single assessment may address a set of similar processing operations that present similar high risks. The controller shall seek the advice of the data protection officer, where designated, when carrying out a data protection impact assessment (leaving open the question of the obligation to do so when the controller had no obligation [formally or in the framework of technical and organizational measures] to designate one but still did it).

The supervisory authority must establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment. The supervisory authority must communicate those lists to the European Data Protection Board. The supervisory authority may also establish and make public a list of the kind of processing operations for which no data protection impact assessment is required. The supervisory authority shall communicate those lists to the European Data Protection Board. Prior to the adoption of the lists, the competent supervisory authority will apply the consistency mechanism where such lists involve processing activities which are related to the offering of goods or services to data subjects or to the monitoring of their behavior in several Member States or may substantially affect the free movement of personal data within the Union.

Compliance with approved codes of conduct by the relevant controllers or processors must be taken into due account in assessing the impact of the processing operations per-

formed by such controllers or processors, in particular for the purposes of a data protection impact assessment.

Where appropriate, the data controller must seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations.

(141.) When consulting the supervisory authority pursuant to paragraph 1, the controller shall provide the supervisory authority with (Article 36.3 of the Regulation):

(1.) where applicable, the respective responsibilities of the controller, joint controllers, and processors involved in the processing, in particular for processing within a group of undertakings;
(2.) the purposes and means of the intended processing;
(3.) the measures and safeguards provided to protect the rights and freedoms of data subjects pursuant to this Regulation;
(4.) where applicable, the contact details of the data protection officer;
(5.) the data protection impact assessment;
(6.) and any other information requested by the supervisory authority.

(142.) See Article 58 of the Regulation.

(143.) On all of this and in particular the factors to be taken into account in each individual case, see Article 83 of the Regulation.

(144.) See the list of corrective measures in Article 58.2, a) to h), and j) of the Regulation. See also Article 29 Data Protection Working Party *Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679* WP 253 3 October 2017. Public bodies enjoy a special regime.

(145.) See Article 84 of the Regulation.

(146.) Sharona Hoffman, *Big Data and the Americans with Disabilities Act*, 68 HASTINGS L. J. 777, 778 (2017).

(147.) 42 U.S.C. §§ 12111–12189 (2010).

(148.) 29 U.S.C. §§ 791-794(a) (2010).

(149.) Genetic Information Non-Discrimination Act, Pub. L. No. 110–233, 122 Stat. 881 §§ 201(4) & 202(a) (2008); 29 U.S.C. § 1182 (2010); 42 U.S.C. §2000ff-1(a) (2010). Genetic information is defined as including (i) an individual’s genetic tests, (ii) the genetic tests of an individual’s family members, and (iii) the manifestation of a disease or disorder in an individual’s family members. 42 U.S.C. §§ 2000ff (4)(A) (2010).

(150.) 29 U.S.C. § 1182 (c) & (d) (2010); 42 U.S.C. § 2000ff-1(b) (2010).

(151.) 29 U.S.C. § 1182 (a) & (b) (2010); 42 U.S.C. § 2000ff-1(a) (2010).

(152.) 42 U.S.C. §18116 (2010).

(153.) 42 U.S.C. 3604 (2010).

(154.) National Conference of State Legislatures, State Laws on Employment-Related Discrimination, July 2015, http://www.ncsl.org/documents/employ/Discrimination-Chart-2015.pdf; Stephen A. Rosenbaum, Disability Rights and Public Accommodations: State-by-State (2011), http://adasoutheast.org/publications/ada/public_accommodations_disability_rights_state-by-state_Final.pdf.

(155.) Council Directive 2000/78/EC of 27 November 2000, establishing a general framework for equal treatment in employment and occupation. Official Journal (EC) L 303/16 of 2 Dec. 2000.

(156.) I. Glenn Cohen et al., *Your Money or Your Patient's Life? Ransomware and Electronic Health Records*, 167 ANNALS INTERN. MED. 587 (2017).

(157.) 45 C.F.R. § 164.306 (b) (2018).

(158.) 45 C.F.R. § 164.306(b)(1) (2018).

(159.) SHARONA HOFFMAN, ELECTRONIC HEALTH RECORDS AND MEDICAL BIG DATA: LAW AND POLICY 69–70 (Cambridge University Press 2016); Hoffman & Podgurski, *supra* note 21, at 350–354.

(160.) 45 C.F.R. § 164.524 (2018)

(161.) 45 C.F.R. §§ 164.524 and 164.526 (2018).

(162.) See the limits which may be imposed on these rights by Union law or by the law of the Member State to which the controller or processor is subject, by means of legislative measures, in accordance with Article 23 of the Regulation. These limits are permissible only if they respect the essence of fundamental rights and freedoms and are necessary and proportionate measures in a democratic society to guarantee one of the objectives listed in this provision. See Article 29 Data Protection Working Party *Guidelines on Transparency under Regulation 2016/679* WP 260 rev.01 11 April 2018 and *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679* WP 251 rev.01 6 February 2018.

(163.) Article 29 Data Protection Working Party *Guidelines on the right to data portability* WP 242 rev.01 5 April 2017.

(164.) See Article 20 of the Regulation. This right is without prejudice to the right to erasure or to be forgotten. That right does not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. In addition, it cannot adversely affect the rights and freedoms of others.

(165.) See, e.g., Article 4.2 (f) of Directive 2011/24/EC of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare (see the consolidated text), which provides that *in order to ensure continuity of care, patients who have received treatment are entitled to a written or electronic medical record of such treatment and access to at least a copy of this record in conformity with and subject to national measures implementing Union provisions on the protection of personal data, in particular Directives 95/46/EC and 2002/58/EC*.

(166.) Recently, the *British Medical Journal* has published a very interesting study on the data flows behind mobile health applications (Q. Grundy, K. Chiu, F. Held, A. Continella, L. Bero, & R. Holz. *Data sharing practices of medicines related apps and the mobile ecosystem: traffic, content, and network analysis*, 364 BMJ 1920 (2019). These kind of studies should be more encouraged, and they should receive more coverage from the news media.

(167.) Gil Press, *12 Big Data Definitions: What's Yours?*, FORBES, Sept. 3, 2014, https://www.forbes.com/sites/gilpress/2014/09/03/12-big-data-definitions-whats-yours/#6301d92913ae.

(168.) National Institutes of Health, *All of Us Research Program* (last visited Dec. 21, 2017), https://allofus.nih.gov/.

(169.) Healthcare Cost and Utilization Project, *Overview of the State Inpatient Databases (SID)* (last modified Apr. 18, 2017), http://www.hcup-us.ahrq.gov/sidoverview.jsp.

(170.) Margaret Bays, *IBM Watson Health: How Does it Work?* IBM DEVELOPER WORKS (June 15, 2017), https://www.ibm.com/developerworks/community/blogs/e3ec7365-1b09-44f2-906f-19826275860f/entry/IBM_Watson_Health_How_Does_it_work?lang=en.

(171.) Hoffman & Podgurski, *supra* note 112, at 105; Latanya Sweeney, *Simple Demographics Often Identify People Uniquely*, Carnegie Mellon University, Data Privacy Working Paper 3. Pittsburgh (2000), https://dataprivacylab.org/projects/identifiability/paper1.pdf.

(172.) Kathleen Benitez & Bradley Malin, *Evaluating Re-identification Risks with Respect to the HIPAA Privacy Rule*, 17 J. AM. MED. INFORMATICS ASS'N 169, 169 (2010).

(173.) Nicolas P. Terry, *Big Data Proxies and Health Privacy Exceptionalism*, 24 HEALTH MATRIX 65, 77 (2014).

(174.) Michal Kosinskia,1, David Stillwella, & Thore Graepel, *Private Traits and Attributes Are Predictable from Digital Records of Human Behavior*, 110 PNAS 5733, 5733 (2013), http://www-psych.stanford.edu/~knutson/bad/kosinski13.pdf.

(175.) . Kashmir Hill, *How Target Figured Out a Teen Girl Was Pregnant Before Her Father Did*, FORBES (Feb. 16, 2012), https://www.forbes.com/sites/kashmirhill/2012/02/16/

how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/#7c4f90266668 (discussing Target's practice of data-mining its customers' purchasing records in order "to figure out what you like, what you need, and which coupons are most likely to make you happy").

(176.) Sharona Hoffman, *Citizen Science: The Law and Ethics of Public Access to Medical Big Data*, 30 BERKELEY TECH. L. J. 1741, 1773–1780 (2016).

(177.) For recommendations see HOFFMAN, *supra* note 4, at 73-79 and 148-51.

(178.) Alison Abbott, *Biomarkers Could Predict Alzheimer's before It Starts*, NATURE, March 9, 2014, http://www.nature.com/news/biomarkers-could-predict-alzheimer-s-before-it-starts-1.14834.

(179.) Mohana Ravindranath, *IBM Used Predictive Analytics to Find Patients at Risk of Heart Failure*, WASH. POST, February 20, 2014, https://www.washingtonpost.com/business/on-it/ibm-used-predictive-analytics-to-find-patients-at-risk-of-heart-failure/2014/02/20/9b0ddb3c-9a47-11e3-b88d-f36c07223d88_story.html; Arthur Allen, *Big Brother Is Watching Your Waist*, POLITICO, July 21, 2014, http://www.politico.com/story/2014/07/data-mining-health-care-109153; Susan H. Babey et al., *Prediabetes in California: Nearly Half of California Adults on Path to Diabetes*, UCLA Center for Health Policy Research Health Policy Brief (March 2016), http://healthpolicy.ucla.edu/publications/Documents/PDF/2016/prediabetes-brief-mar2016.pdf.

(180.) Sharona Hoffman, *Big Data and the Americans with Disabilities Act*, 68 HASTINGS L. J. 777, 784–785 (2017).

(181.) Rachel Emma Silverman, *Bosses Tap Outside Firms to Predict Which Workers Might Get Sick*, WALL ST. J., February 17, 2016, https://thebenefitblog.com/2016/02/19/bosses-tap-outside-firms-to-predict-which-workers-might-get-sick/.

(182.) 42 U.S.C. § 12102 (2010).

Sharona Hoffman

Edgar A. Hahn Professor of Law, Professor of Bioethics, Co-Director of Law-Medicine Center, Case Western Reserve University School of Law; B.A., Wellesley College; J.D., Harvard Law School; LL.M. in Health Law, University of Houston; S.J.D. in Health Law, Case Western Reserve University. Author of Electronic Health Records and Medical Big Data: Law and Policy (Cambridge University Press 2016). For further information see https://sharonahoffman.com/.

Jean Herveg

University of Namur, Faculty of Law, CRIDS (Research Centre on Information, Law & Society), Head of the LIS Department (Liberties in the Information Society); Member of the Bar of Brussels.