E-ISSN: 2997-9439

SemantJournals

American Journal of Education and Evaluation Studies

https://semantjournals.org/index.php/ AJEES

| Research Article

Check for updates

Protection of Personal Medical Data in the Era of Digitalization: Legal Guarantees and Prospects

Imamalieva Diyora

Lecturer at Tashkent State University of Law

Abstract: This article explores the protection of personal medical data in an era defined by digital technologies, global connectivity, and new healthcare paradigms. Given the heightened sensitivity of health information, we analyze existing international frameworks—namely the EU General Data Protection Regulation (GDPR), the Council of Europe's Convention 108, and U.S. regulations such as HIPAA—and discuss how they apply in an environment increasingly shaped by cloud computing, big data analytics, and artificial intelligence. Drawing on leading case law from the Court of Justice of the EU, the European Court of Human Rights, and U.S. courts, we highlight ongoing challenges, including informed consent, data re-identification, cross-border transfers, and cyberattacks targeting healthcare systems. By juxtaposing stringent European data protection models with the more fragmented American healthcare privacy landscape, we identify practical and conceptual gaps that require urgent regulatory attention. Finally, the article suggests possible avenues for greater harmonization and stronger enforcement—ranging from sector-specific standards for AI-driven health analytics to clearer frameworks for data ownership and accountability—aimed at safeguarding individual privacy while facilitating innovation in digital healthcare.

Keywords: digital technologies, GDPR, HIPAA, data protection models, AI-driven health analytics, data ownership and accountability, individual privacy, cloud computing, artificial intelligence.

Introduction

The rapid digital transformation of healthcare systems worldwide has led to an unprecedented volume of medical data being generated, processed, and stored. From electronic health records (EHRs) in hospitals to wearable health trackers, genetic databases, and telemedicine services, personal medical data now proliferate across diverse platforms and jurisdictions. While these technologies promise improved patient outcomes and more efficient healthcare delivery, they also pose serious risks to patient privacy and data security. Unauthorized disclosure, hacking, commercialization of health data, and discriminatory practices based on medical information are just a few of the challenges that have emerged in this new digital environment.Historically, the

confidentiality of medical information has been recognized as a cornerstone of the doctor-patient relationship. Patients often must disclose highly sensitive and private information to healthcare providers to receive proper care; in return, they expect and rely upon stringent confidentiality measures. In many jurisdictions, specific legal and ethical frameworks have long protected this delicate relationship—through professional codes of conduct (e.g., the Hippocratic Oath) and national data protection or privacy laws. However, as digitalization expands the amount of data collected, the ways it can be processed, and the number of entities with access to it, the scope of these legal measures must be reassessed and updated to address new complexities.

Methodology

Health data are classified as a special category of personal data in various jurisdictions, reflecting the recognition that they require a higher level of protection than other forms of personal data. The General Data Protection Regulation (GDPR) in the European Union (EU) explicitly designates health information as "sensitive data" and imposes stricter conditions for processing. In the United States (U.S.), the Health Insurance Portability and Accountability Act (HIPAA) and its implementing regulations create a legal regime that regulates the collection, use, and disclosure of protected health information by specific "covered entities." On the international level, a patchwork of treaties, guidelines, and national laws aims to ensure respect for patient privacy. Yet, the rapid pace of technological innovation outstrips many of these instruments.Recent high-profile data breaches—from ransomware attacks on hospital systems to unauthorized secondary uses of patient data by third-party companies—have reinforced the urgency of robust legal protection. Courts and regulators are grappling with novel questions: Who owns patient data when stored in a cloud environment? What constitutes sufficient de-identification of medical records? How can patients meaningfully consent to secondary uses of their genetic or biometric data? This article explores these issues, outlining existing legal frameworks at the international level, discussing regulatory challenges and gaps, and highlighting prospects for more effective protection of personal medical data.

Research Objectives:

1. Identify and analyze key international legal instruments. We examine the primary international and supranational regulations and guidelines relevant to the protection of personal medical data, with a focus on frameworks such as the EU GDPR, the Council of Europe's Convention 108, and U.S. HIPAA. We also refer to case law from the European Court of Human Rights (ECtHR) and the U.S. Supreme Court to illustrate how courts interpret privacy rights in the medical context.
2. Assess regulatory gaps and challenges in the digital age. We investigate the principal challenges arising from the widespread digitalization of medical data, including issues of interoperability, cross-border data flows, third-party access, big data analytics, and artificial intelligence. Our goal is to highlight where existing regulations may lag behind technological developments.
3. Examine case law and enforcement examples. By referencing both European and U.S. case law, as well as enforcement actions by data protection authorities, we aim to demonstrate how legal principles are applied in practice. Understanding how courts and regulators respond to violations is crucial to gauging the effectiveness of existing frameworks.
4. Propose future directions and best practices. Lastly, the article discusses policy recommendations and prospective pathways for strengthening data protection, suggesting how legal and ethical guidelines might evolve to address emerging trends in healthcare digitalization, such as telehealth, genetic profiling, and AI-driven diagnostics.

International Framework.

The EU has arguably one of the most comprehensive regimes for personal data protection worldwide. The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) sets forth robust requirements for collecting, processing, and transferring personal data, with specific provisions on "special categories" of data, including health data (Article 9 GDPR). Under Article 9, the processing of personal health data is generally prohibited unless one of the narrow exceptions applies—such as explicit consent, the necessity of processing for healthcare purposes, or public interest in the area of public health.

Key principles and obligations consist the following:

Lawful basis and consent: Controllers must have a valid lawful basis for processing health data. Typically, healthcare providers rely on the necessity of processing for the purposes of preventive or occupational medicine, diagnosis, or treatment. In other contexts, particularly research or commercial analytics, explicit and informed consent becomes crucial.

Data minimization and purpose limitation: Even with a lawful basis, controllers are required to minimize the amount of data collected and use it only for specified, legitimate purposes.

Security and accountability: Controllers must implement technical and organizational measures to ensure data security (Article 32 GDPR) and are subject to an accountability obligation (Article 5(2) GDPR). For health data, these measures should reflect the highest standards, given the sensitivity of the information.

Data subject rights: Individuals (patients) have rights including access, rectification, erasure ("right to be forgotten"), and objection to processing. For instance, in Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González (Case C-131/12), the Court of Justice of the EU (CJEU) recognized the right to request delisting of personal data under certain circumstances, though this case involved search engines rather than medical data specifically.

Beyond the EU, the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) and its modernized version Convention 108+ also provide a pan-European basis for data protection. Although not binding in the same manner as the GDPR, Convention 108 sets forth principles of lawful and fair data processing, data quality, and special protection for sensitive data, which includes medical information.

Results

The European Court of Human Rights (ECtHR) has recognized the confidentiality of medical records as a component of the right to respect for private life under Article 8 of the European Convention on Human Rights (ECHR). In Z v. Finland (1997), the Court underscored the importance of protecting the confidentiality of health data, stating that domestic authorities must ensure "effective protection" to avoid "prejudicial consequences for the data subject." Later cases, such as I v. Finland (2008), reiterated the principle, with the Court criticizing insufficient safeguards against unauthorized access to patient records. While these judgments do not prescribe specific legislative models, they establish a broad human rights framework that demands rigorous protection of medical confidentiality.

In the U.S., medical data protection is primarily governed by the Health Insurance Portability and Accountability Act (HIPAA) of 1996 and its implementing regulations, particularly the Privacy Rule and Security Rule. HIPAA applies to "covered entities" (healthcare providers, health plans, and healthcare clearinghouses) and, in many instances, their "business associates" (vendors, service providers). It can be presented in 3 types of rules:

- Privacy rule: Sets standards for how protected health information (PHI) may be used and disclosed. It strictly limits disclosures without patient authorization, except for treatment, payment, or healthcare operations.
- Security rule: Requires administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and availability of electronic PHI (ePHI).
- Breach notification rule: Mandates that covered entities notify affected individuals, the Secretary of Health and Human Services (HHS), and sometimes the media when significant breaches of unsecured PHI occur.

However, HIPAA is criticized for not covering all entities that might handle health data—many health apps, wearable device providers, and consumer genetics companies fall outside its scope. Moreover, individual states have enacted their own privacy and security laws, leading to a fragmented legal landscape. Notably, the California Consumer Privacy Act (CCPA) and its amended version, the California Privacy Rights Act (CPRA), may impose additional obligations on certain businesses handling health data, even if they are not HIPAA-covered entities.

One notable Supreme Court decision addressing medical data—though from a commercial speech perspective—is Sorrell v. IMS Health Inc. (2011), 564 U.S. 552. The Court invalidated a Vermont statute restricting the sale, disclosure, and use of pharmacy records that revealed prescriber-identifying information. While the Court focused on free speech concerns, the case underscores the complexities of regulating commercial use of prescription data in the U.S. healthcare market.

Globally, there is no single binding treaty that comprehensively regulates health data protection. However, instruments like the OECD Privacy Guidelines (updated in 2013) and the World Medical Association (WMA) International Code of Medical Ethics offer guidance. The WHO also issues guidelines on digital health strategies, emphasizing data protection as a key component of any large-scale health program.

Regulatory Challenges in the Digital Age.

As medical data proliferate, healthcare stakeholders increasingly leverage big data analytics and artificial intelligence (AI) to gain insights—predictive modeling for disease outbreaks, personalized treatment recommendations based on genomic data, and more. While these technologies promise breakthroughs in patient care, they also raise data protection challenges, such as:

- Informed Consent and Transparency: Often, patients are unaware that their medical records may be subject to analytics or shared with third parties for secondary uses (e.g., research, product development). GDPR requires “explicit consent” for processing sensitive data, but the broad scope of AI-driven analytics often blurs the original purpose for which consent was obtained.
- De-identification and Re-identification Risks: Techniques like pseudonymization and anonymization can reduce privacy risks, yet advanced data mining methods can “re-identify” individuals by combining multiple datasets. In the context of DNA or other biometric data, the risk of re-identification is especially salient.
- Bias and Discrimination: AI models can inadvertently embed biases if trained on skewed datasets. In the healthcare context, this could lead to discriminatory outcomes, e.g., underdiagnosis of conditions prevalent in minority groups or over-prioritizing resources for majority populations.

Discussions

Healthcare data often cross borders—for instance, when stored on cloud servers in different countries or shared among multinational research consortia. However, varying data protection

regimes complicate these transfers. Under the GDPR, personal data can only be transferred outside the EU/EEA if the receiving country ensures an "adequate level" of protection, or if contractual and other safeguards (Standard Contractual Clauses, Binding Corporate Rules) are in place. This can be burdensome for global healthcare providers, research institutions, and telemedicine platforms that operate in multiple jurisdictions.A major legal development in this area was the Schrems II (Case C-311/18) decision of the CJEU in 2020, which invalidated the EU-U.S. Privacy Shield framework due to concerns over U.S. surveillance laws. Healthcare entities that relied on Privacy Shield for transatlantic data transfers had to pivot to other mechanisms. This ruling highlights how national security and surveillance laws can conflict with the privacy imperatives of protecting health data, further complicating cross-border collaboration in medical research. Even within single jurisdictions, healthcare data protection can be fragmented. In the U.S., HIPAA applies only to covered entities and certain associates, leaving many consumer-facing health applications unregulated at the federal level. State laws might fill some gaps, but the result is inconsistent protection. Similarly, while the GDPR is comprehensive for EU Member States, healthcare is often a shared competence, meaning local laws implementing it can introduce variations. Enforcement gaps: Regulators such as Data Protection Authorities (DPAs) in the EU and the Office for Civil Rights (OCR) under HHS in the U.S. oversee compliance. While large fines can be imposed for violations (GDPR fines can reach up to 4% of a company's global turnover), enforcement often lags behind new technologies. Startups may not prioritize compliance due to limited resources or uncertainty about how regulations apply to novel applications (e.g., direct-to-consumer genetic testing, mental health apps). Healthcare systems have become prime targets for cybercriminals due to the high value of medical records on black markets. Ransomware attacks can paralyze hospital operations, risking patient safety. The shift to telemedicine—accelerated by the COVID-19 pandemic—further increases the attack surface as more communication occurs over the internet. Regulatory Response: GDPR (Article 32) and HIPAA (Security Rule) both mandate "appropriate technical and organizational measures" to safeguard personal health information. However, the standards are often principle-based, leaving it to covered entities to determine what is "appropriate." This flexibility can lead to inconsistent adoption of security measures, particularly by smaller providers or new digital health startups. Some jurisdictions, like France, have introduced stricter rules for telemedicine platforms and higher certification standards for health data hosting. But globally, cybersecurity remains one of the most pressing and under-addressed regulatory challenges in healthcare.

A more conceptual but increasingly salient question is: Who "owns" patient data? In many jurisdictions, patients retain certain rights over their data, while healthcare providers or insurers may "control" the data for treatment and billing. With the advent of data-driven business models—like genomic sequencing companies that monetize large genetic databases—tensions emerge between commercial interests and patient autonomy.

Some argue that patients should receive compensation or at least more robust control over how their data is monetized, while others maintain that the value stems from the analytics and infrastructure provided by commercial entities. Legally, the notion of "ownership" varies: the GDPR confers "data subject rights," not ownership per se. In the U.S., courts have historically ruled that individuals do not hold a property right in tissue samples or genetic information once it is voluntarily provided, as in Moore v. Regents of the University of California (1990). Nonetheless, new legislation like the CPRA in California broadens consumer rights in certain data contexts, hinting at an evolving paradigm where individuals might gain more power to control, delete, or share health data.

Conclusion.

The digital era offers exciting prospects for healthcare—improved diagnostics, personalized medicine, and global research collaborations—yet it also challenges traditional notions of privacy

and data protection. Personal medical data, by its very nature, demands the highest levels of legal and ethical safeguards. As the volume, variety, and velocity of these data continue to grow, regulators, courts, and the healthcare industry must adapt or risk eroding public trust.

From an international standpoint, the GDPR sets a high watermark for comprehensive data protection, particularly for sensitive data such as health information. It illustrates how legal frameworks can evolve to address new technologies while maintaining fundamental rights. The U.S. approach, anchored by HIPAA, presents significant contrasts, especially as many health-related data streams now originate from non-HIPAA-covered entities. Meanwhile, courts—whether the ECtHR in Europe or state and federal courts in the U.S.—have increasingly recognized the right to privacy of one's medical information, bolstering demands for stronger safeguards.

Several critical challenges remain. The fragmentation of laws and the jurisdictional mismatch in cross-border data flows create compliance hurdles and potentially expose data to weaker legal regimes. Rapid developments in AI and big data analytics raise questions of consent, re-identification, and algorithmic bias. Cybersecurity threats loom large, as healthcare systems continue to be prime targets for ransomware and data theft. Finally, questions of data ownership, compensation, and ethical commercialization remain unresolved, revealing broader societal debates about how personal health information should be governed.

Looking forward, more harmonized global standards—potentially building on the modernized Convention 108+ or collaborative efforts between the EU, U.S., and other major economies—could help address cross-border complexities. Regulators might also adopt risk-based, sector-specific guidelines for advanced analytics and AI in healthcare, ensuring robust protections for sensitive health information. A heightened focus on transparency, patient control, and accountability could preserve trust in digital health innovations. In sum, while the path ahead is complex, establishing stronger legal guarantees and forward-looking regulatory regimes is essential for realizing the full promise of digital healthcare—safely and ethically.

REFERENCES:

1. Regulation (EU) 2016/679 (General Data Protection Regulation).
2. Council of Europe, Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data (and Convention 108+).
3. Health Insurance Portability and Accountability Act (HIPAA), Pub. L. No. 104-191, 110 Stat. 1936 (1996).
4. California Consumer Privacy Act (CCPA) (2018), amended by the California Privacy Rights Act (CPRA) (2020).
5. Google Spain SL and Google Inc. v AEPD and Mario Costeja González (Case C-131/12).
6. Data Protection Commissioner v Facebook Ireland Ltd, Maximillian Schrems (Case C-311/18, "Schrems II").
7. Z v. Finland, 25 February 1997, Application No. 22009/93.
8. I v. Finland, 17 July 2008, Application No. 20511/03.
9. Sorrell v. IMS Health Inc., 564 U.S. 552 (2011).
10. Moore v. Regents of the University of California, 51 Cal.3d 120 (1990).
11. OECD, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (2013).
12. World Medical Association, *WMA International Code of Medical Ethics* (last revised 2022).
13. World Health Organization, *Guidelines on Digital Health Interventions* (2019).