PERINATAL JOURNAL

Original Article

Perinatal Journal 2026; 34(1):394-401

https://doi.org/10.57239/prn.26.03410044

The international legal framework for the protection of data privacy in health care

Professor Amer Fakhoury[1*], Professor Mahir Al Banna[2]

[1,2]College of Law, American University in the Emirates, United Arab Emirates, Dubai

Abstract

Collecting and processing sensitive medical data of patients faces a major challenge, especially with the digital transformation that has occurred in the issue of health care services. This sensitive data has become a major challenge considering the developments that have occurred in the way medical services are provided, whether it is telemedicine, electronic health records, or the many applications that have spread on social media sites that provide medical services digitally. Although this major development in health care is directed towards patients, there is a major challenge in how to protect this sensitive data and ensure that this data is not used illegally. Therefore, this research addresses digital transformation in health care as a challenge not only medical but also legal. We need a sufficient arsenal legal system to protect sensitive private data, especially if we know that the international legal framework regulating privacy in the field of health care still needs a lot of work. Therefore, this research focuses on the legal protection of medical data, especially the right to privacy, as stated in international human rights agreements, especially the Universal Declaration of Human Rights issued in 1948. It also highlights the legal duties and obligations of states to take the necessary measures to protect this sensitive data, especially in the era of medical digitization Therefore, this research concludes that it is necessary to note that digital transformation in health care cannot achieve health goals unless it is accompanied by an effective legal arsenal to protect sensitive medical data, so that digital and technological development must be kept pace with respect for the rights, dignity and privacy.

Keywords: Digital transformation, Medical data protection, International law, GDPR, HIPAA, Right to be forgotten

Introduction

There is no doubt that the significant digital development that has occurred in the way healthcare is delivered over the past years, particularly in prenatal care, is one of the most significant developments in the lives of pregnant mothers. But on the other hand, despite the importance of this development and its positive repercussions on the lives of health care recipients, the practical reality has proven that these applications, as well as digital development, may expose the life of the pregnant women to the risk of leaking their sensitive personal information, whether intentionally or unintentionally, which constitutes a major violation of the privacy of the mother and child.[1]

This is indeed what the World Health Organization, one of the main organizations affiliated with the United Nations, has emphasized, confirming that digital health development has become an essential element in strengthening health systems around the world and improving the quality of care provided to pregnant women [2]. However, this digital transformation has been accompanied by the collection and storage of large amounts of sensitive medical information, whether information related to medical examinations, information related to fetal data, data related to the mother's health history, and other data that should never fall into the hands of people who have no connection to the medical file.

Leaking such sensitive data would undermine confidence in these digital applications and would also affect the entire medical system. We must not forget that there is a heavy reliance by patients in many countries, especially third world countries and countries ravaged by wars and conflicts, on these digital applications and platforms, whether in data analysis or in the use of artificial intelligence in pregnancy monitoring. This matter increases the complexity of the issue of privacy protection and raises many questions about the legal challenges that must be taken into consideration.[3]

There is no doubt that the right to privacy is one of the most important rights that a patient must enjoy. This is what many agreements, whether regional or even international, have emphasized. Any violation of such rights constitutes a clear breach of the private

Correspondence: Amer Fakhoury, College of Law, American University in the Emirates, United Arab Emirates, Dubai, **e-mail:** amer.fakhoury@aue.ae,

Received: November 6, 2025 **Accepted:** December 19, 2025

life of the person who has not received medical care. The Universal Declaration of Human Rights of 1948 emphasized the need to protect private life and prevent arbitrary interference with it [4], as did the International Covenant on Civil and Political Rights of 1966, which imposed legal obligations on states regarding the need to protect human private life and thus the special protection of the pregnant mother [5].

Therefore, we find that many countries and international organizations have adopted special standards to protect health data At the top of these systems is what was adopted at the level of the European Union when the European General Data Protection System was adopted, as this system classified health data among the special categories that must be taken into account and given special priority when processing and the necessity of not allowing it to be used except within a narrow and limited scope and with very strict legal guarantees .[6]

Therefore, we find that the World Health Organization has, on more than one occasion, emphasized, when discussing the method of providing maternal health services, the need to integrate two fundamental, inseparable standards: the legal standard and the ethical standard. Therefore, in any digital application and any solutions based on artificial intelligence, both standards must be considered, ensuring data confidentiality and information security and determining legal liability in the event of any violations [7,29]. This applies to sensitive data related to both the pregnant mother and the fetus

Thus, this research addresses the importance of protecting private data in the health care system as a basic human right. It also seeks to highlight the sensitive relationship between the effectiveness of digital prenatal services and the existence of a national and international legal system capable of protecting this data from any breaches and any misuse, whether intentional or unintentional.

Methodology

This study is a review that examines the multifaced challenges and solutions associated with data privacy in healthcare. It uses a qualitative approach, integrating group building and thematic analysis to explore global health data privacy frameworks, identify vulnerabilities and propose actionable recommendations. The study draws on multiple theoretical perspectives to analyze the complex dynamics of health data privacy, providing a structured basis for understanding patient trust, regulatory compliance and privacy management among health stakeholders. The study created a strong collection of regulatory documents, case studies and scientific articles. The collection included key legal frameworks such as General Data Protection Regulation (GDPR) in Europe and Health Insurance Portability and Accountability Act (HIPAA) in the US. These documents are derived from reputable databases (e.g. PubMed, Scopus, Web of Science, Google Scholar, Wiley and official websites of organizations), official publications and reports prepared by regulatory authorities.

Discussion

The right to data protection is enshrined in international human rights instruments such as the Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR), which protect the rights to privacy, family life, home and correspondence. In particular, the UN Human Rights Committee has interpreted the International Covenant on Civil and Political Rights (General Comment No. 16) to include certain data protection guarantees. The only UN instrument dealing specifically with data protection is the Set of Non-Binding Guidelines for the Regulation of Computerized Personal Data Files, which dates to 1990. The international treaty in this field with the largest number of States parties is Council of Europe Convention No. 108, while many other international organizations (such as the Asia-Pacific Economic Cooperation forum, the General Data Protection Regulation, the Economic Community of West African States and the Organization of American States) have adopted data protection tools, most of which are non-binding [8,30].Despite all this, the status of data protection in public international law remains uncertain due to a number of factors: –International human rights treaties such as the International Covenant on Civil and Political Rights do not specifically mention data protection, and their privacy provisions are so broadly worded that they do not provide much guidance in defining the details of data protection rights. Most other international instruments that specifically address data protection are either regional rather than global or not legally binding [8]

In fact, health data confidentiality means protecting sensitive information, including medical records, personal data and other health-related data, against unauthorized access, misuse or disclosure [9, 10] Laws have been enacted in many countries to improve specific areas, including medical information, health information, financial matters, confidentiality, privacy, e-commerce and cybercrime. Many countries have adopted parts of the European framework, and OECD guidelines have also been widely used in national legislation, even outside OECD countries. Although portions of some may affect certain segments of the health industry, none provides a comprehensive regulatory regime covering all facets of electronics health data. Consequently, no country to date has enacted a single piece of legislation that provides extensive coverage of electronic health care information, and, in most countries, there is no single agency with oversight responsibility for this area. Instead, multiplicity of legislation and regulatory agencies seem to be the rule [11]

This legal framework is generally not focusing on a specific category of patients. For instance, if we try to examine the protection of data privacy of pregnant women, we will find out that is not contained in a single, specific treaty. Instead, it draws on broader international human rights documents and principles that define the rights to privacy, health and non-discrimination, which are then implemented through national laws. As mentioned above, the normative basis of data protection law relies heavily on human rights treaties (ICCPR, CEDAW). The question then arises whether data protection is similarly recognized in international law as a binding legal concept. Balancing technological innovation with strict confidentiality protections is, therefore, critical for safeguarding patient information in an increasingly digitized health landscape [12] So, the current discussion will focus on European (GDPR) and North American VIPAA as models of health data privacy.

General Data Protection Regulation (GDPR)

The rights of individuals regarding their personal medical data, as part of the European legal framework, aim to ensure the control of individuals over their data while considering the specificities related to their medical nature. Individuals must be informed in a clear and concise manner about the data collected concerning them, the purposes of their use, the retention period, and the potential recipients of the information [13] Already existing, this right is being reinforced by the GDPR. Data subjects can now obtain more information, such as the source of data when these have not been collected directly from them, the details on possible profiling, as well as the guarantees applied in case of data transfer outside the European Union [13] As a matter of fact, EU law must notably preserve the quality and security of these devices while preserving the fundamental freedoms and rights of citizens in compliance with the Charter of Fundamental Rights of the EU, whether it is about the right to social protection (Article 34 of the Charter) or the right to respect for private and family life (Article 7 of the Charter) and the protection of personal data (Article 8 of the Charter) in e-health services requiring a cross-border flow of personal data[14] It is for example in this perspective that since 2011 the Union has adopted a Directive on cross-border health services and the exchange of personal data necessary to access healthcare services provided to a national of a Member State in another EU Member State and their reimbursements by the competent insurance bodies [14]

For the implementation of an adapted legal framework protecting private life at the EU level, the GDPR has included the use of a variety of information and communication technologies (ICT) which brought a very beneficial e-health device [14]

The advantages of ICT in health are also a source of risks for people’s privacy since a large part of the information concerned is qualified as personal health data, therefore sensitive data under EU law. This data circulates between different people and places and is often stored in databases that may concern the individual but also the population. The increasingly large mass of data, the 'big data', both at the individual level, is an example of the complete human genome which today weighs about 2TB (one thousand gigs or one thousand billion bytes) and at the population level, personal data often being gathered in files concerning a large number of individuals, as in health registries or biobanks, files made accessible to authorized health professionals, researchers and other organizations operating in the system of health, also poses a number of challenges regarding the security and confidentiality of data. As unauthorized access by hackers, hackers, but also by commercial companies, in other areas using ICT, the risks related to e-health are those of unscrupulous employers or insurers, even from foreign authorities as recently shown by the PRISM scandal involving the American Security Agency, the NSA, illegally monitoring the communications of several European personalities [15] The text of the GDPR proposal qualifies these operations as a "personal data breach". This is a breach of security resulting in accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access to personal data [14]

In addition to these risks, particular considerations must be taken regarding the processing of personal data relating to people in vulnerable situations, such as pregnant women and children, for which it is necessary to implement special protection measures and design appropriate systems [14] Finally, it is also necessary to consider the questions related to the particularities of certain health information generated and used in an e-health context, such as in the context of access to genetic tests sold on the internet which provide consumers with genetic data that may not only concern the buyer but also his family or descent, which raises a set of ethical questions, particularly when discovering results concerning a genetic disease of a familial nature. All these factors increasing the potential risks of intrusions into the private lives of individuals should be considered in the ongoing reform of EU law on personal data protection and other supervisory work, notably ethical, in e-health [14]

As part of the important reinforcements of people's rights for e-health that the GDPR operates, the notion of free and informed consent (or informed) is clarified, its validation conditions are strengthened. Thus, when national law requires prior consent of the person to the processing of their health data, this must be obtained, possibly in electronic form, with the burden of proof resting on the controller [15]

According to the GDPR, the consent must be informed, given freely and be explicit to give a clear indication of the will of the person concerned. The choice of the person must be exercised through an action characterizing their acceptance of the treatment (e.g., checking a box, signing a paper form – model opt-in) or, in certain cases provided for by law, through significant behavior. Article 25 of the GDPR then specifies that there can be no tacit or passive consent. Consent is said to be limited to the achievement of certain specified purposes and to comply with the principle of proportionality. The adaptations made to people's rights based on current technological possibilities are complemented by an extension of the territorial scope of the GDPR aimed at enforcing the rules it set for operators established outside the borders of the European Union. Paragraph 3 specifies the application of the GDPR when the controller is established in a place where the national legislation of a Member State applies under public international law. Thus, an e-health operator established in the United States could have to comply with EU law when offering its e-health services to persons residing in the territory of the EU, under penalty of prosecution and sanctions [15]

These changes are complemented by a strengthening of the general principles applicable to any processing of personal data, which would include the concept of "Privacy by Design and by Default" enshrined in article 25 of the GDPR, that must be respected by e-health stakeholders. Indeed, Privacy by Design and by Default is a legal concept designed for personal data processing technologies, including health [16] This approach is based on the observation that law alone no longer allows for an effective protection of privacy if we consider the new challenges posed by technological developments and the evolutions of the IT environment but requires a new standard of development. allowing technology to put at the service of law and to ensure protection of privacy through adapted, integrated and innovative processes [14]

Health Insurance Portability and Accountability Act (HIPAA)

In the US, the US Department of Health and Social services governs the confidentiality of health data by: Law on the portability and liability of health insurance (HIPAA), which imposes measures such as restricting access Procedures and protocols that require encryption and breach notification of electronically protected health information [17] Traditionally, ethical and medical management always includes respecting the confidentiality of the patient’s medical information. However, in the US, legislation regarding social organizations (HIPAA [Health Insurance Portability and Accountability Act], see Pub. L 104-191 (1996)) codified the responsibility of healthcare professionals, care programs, centers that ensure the communication of information between different entities and their associates who electronically transmit health and correlated information (e.g., medical records, billing and eligibility verification). Collectively, these are entities covered by the Health Insurance Portability and Accountability Act (HIPAA) [18]

In fact, the main provision of HIPAA relies on three rules: confidentiality rule which sets standards for the protection of privacy health information (PHI) and grants patients important rights with respect to their medical information. The security rule establishes safeguards that cover entities and their associates is implemented) to protect the confidentiality, integrity, and security of an individual’s identifiable and protected health information (called electronic PHI). As for the third rule, it is called breach notification rule. It requires covered entities to notify affected individuals, the federal government and in some cases the media of a breach of an individual’s unsecured protected identifiable health information [18] Patients can file complaints in case of non-compliance with medical confidentiality concerning them. Complaints can be made directly to the healthcare professional, the Office for Civil Rights at the U.S. Department of Health and Human Services or the privacy officer designated by the institution in accordance with regulations. Although patients do not have the right to initiate a private prosecution under the regulations, they may initiate proceedings under other privacy and confidentiality laws. The Office for Civil Rights regularly imposes civil and criminal penalties for inappropriate disclosure of personal health information. The most reliable solution for healthcare practitioners is to be well-informed about HIPAA regulations, act in good faith, and make reasonable efforts to comply with the guidelines [18]

We can find an effective illustration of the VIPAA implementation in the case of the pop star Britney Spears. In 2008, Spears was admitted to Los Angeles Medical Center (UCLA), where 13 employees were fired for consulting her medical records without her consent. In addition, 6 doctors were also suspended from work [19] The University of California subsequently issued a statement: *“All employees are required to sign confidentiality agreements as a condition of employment and undergo extensive training on privacy and security issues related to HIPAA.”* [19] Failure to ensure the confidentiality and privacy of pregnant women has been identified as a barrier to safe abortions and abortion care. The legal and ethical requirement that a physician maintain patient confidentiality –especially in the case of a controversial and stigmatized procedure such as abortion– is well established [19]

It is important to highlight that the right to privacy gave birth to the right to be forgotten enshrined as an important one among the GDPR provisions as its importance is clearer in the field of health protection data. Indeed, this right may be necessary for people who have mitigated increased health risks, but it may also conflict with the right to memory and legal certainty so, it is important to define ethical and legal standards for deleting health data (the right to be forgotten) and invest in technology that ensures the protection and integrity of information [20]

Revoking personal private data is one of the basic human rights, which has already been sheltered by privacy-preserving regulations like The General Data Protection Regulation (GDPR), The Health Insurance Portability and Accountability Act of 1996 (HIPAA), and the California Consumer Privacy Act in the last twentieth century. Under these regulations, users are allowed to request the deletion of their private data for reasons of confidentiality and security of "their right to be forgotten". However, with the development of data science technologies, machine learning (ML) and deep learning (DL), this fundamental right is often overlooked or violated [21] For example, it was observed that patients' genetic markers leaked from machine learning methods to process genetic data while patients were not aware of it. When users become aware of such risks, they may request that their private data be deleted to protect their privacy [21] at the same time, these regulations will require affected third parties to take immediate action. According to the requirements of these regulations, not only data previously authorized by individuals must be immediately removed from host storage systems, but information associated with it must also be removed from DL models trained on that data, because DL models can store sensitive training data information and thus compromise an individual's privacy [21] Nowadays, healthcare is one of the most promising areas for the deployment of artificial intelligent (AI) systems as so-called intelligent healthcare. ML and DL-based computer-aided diagnosis (CAD)systems in intelligent healthcare accelerate the diagnosis of various diseases and achieve even better results than doctors, such as tumor detection [21] retinal fundus imaging [22] detection and segmentation of COVID-19 lung infections and so on. However, as more patients' data are collected and used for model training in intelligent healthcare, their privacy is exposed to high risk. Therefore, intelligent healthcare is a sector where technology must meet the law, regulations, and privacy principles to ensure that innovation is for the common good to obey those privacy-preserving regulations, methods to revoke personal private data from pre-trained DL models are necessary, hence the importance of the right to be forgotten [21]

Shortcomings

Although there are strong legal frameworks, the increasing integration of electronic health records and digital tools has greatly increased the risk of data breaches and unauthorized access [23] Notable examples include the hacking of Anthem Inc. in the US, which exposed 79 million people to electronic personal health information (ePHI), and the WannaCry ransomware attack on the UK's National Health Service (NHS), which disrupted vital healthcare services [24, 25] Similarly, a breach of Singapore's SingHealth system put the personal data of 1.5 million patients at risk [26] while incidents in sub-Saharan Africa such as the hacking of the COVID-19 test results portal of the Ghana Health Service and the breach of medical data south-African of 2020 highlight challenges related to inadequate encryption and resource constraints[27,28] These cases highlight that even with well-established regulations and systemic and technological shortcomings can jeopardize data privacy. The approach of protecting personal data from the design stage and by default turns out to be a double-edged sword in the context of strict and complex regulations to read for non-initiated, especially if one considers the potential cost of the measures and the extent of the ethical and legal questions surrounding e-health activities which are not addressed by the GDPR, we could only fear a curb or the flight of some entrepreneurs outside the EU. At worst, there was a massive abandonment of the European market [14]

There are still many questions about the impact of these rules on the field of health and research. Specific issues related to e-health require specific developments sometimes outside the framework of the GDPR.

Conclusion

The findings confirm that effective protection of health data requires multi-stakeholder engagement, combining government monitoring with technological advances such as artificial intelligence and civil society engagement. While emerging technologies provide new opportunities for penetration detection and interoperability, they also raise ethical concerns about consent, independence, and ownership of the data that must be processed. Addressing health data privacy challenges requires globally harmonized regulations, advanced technological tools, and international cooperation. Strengthening frameworks, improving IT infrastructure, and using semantic models and ontologies are essential to protect sensitive data, ensure compliance, and enhance public confidence in digital health systems.

References

1.World Health Organization. WHO recommendations on antenatal care for a positive pregnancy experience. Geneva: World Health Organization; 2016.

2.World Health Organization. WHO guideline: recommendations on digital interventions for health system strengthening. Geneva: World

Health Organization; 2019.

3.Kruse CS, Smith B, Vanderlinden H, Nealand A. Security techniques for the electronic health records. J Med Syst. 2017;41(8):127.

4.United Nations. Universal Declaration of Human Rights. 1948; Article 12.

5.United Nations. International Covenant on Civil and Political Rights. 1966; Article 17.

6.European Union. General Data Protection Regulation (EU) 2016/679; Article 9.

7.World Health Organization. Ethics and governance of artificial intelligence for health. Geneva: World Health Organization; 2021.

8.Kittichaisaree, K. & Kuner, K. "The Growing Importance of Data Protection in Public International Law" 2015 www.ejiltalk.org/the-growing-importance-of-data-protection-in-public-international-law/

9. Marques, IC., and Ferreira. JJ. Digital transformation in health: Asystematic review of 45 years of evolution. Health Technol (Berl) 2020; 10: 575–586.

10. Keshta, I and Odeh, A. Security and privacy of electronic health records: Concerns and challenges. Egypt Inf J 2021; 22: 177–183. https://www.msdmanuals.com/fr/professional/sujets-sp%C3%A9ciaux/probl%C3%A8mes-m%C3%A9dico-l%C3%A9gaux/confidentialit%C3%A9-et-hipaa-health-insurance-portability-and-accountability-act

11.Rodrigues, R., Wilson, S., Schanz, S. "The Regulation of Privacy and Data Protection in the Use of Electronic Health Information: An International Perspective and Reference Source on Regulatory and Legal Issues Related to Person-Identifiable Health Databases", Pan American Health Organization 2001.

12.Conduah, A., Ofoe , S., Siaw-Marfo, D. "Data privacy in healthcare: Global challenges and solutions" Digital Health, Vol. 11, 11-19, 2025 DOI: 10.1177/20552076251343959 journals.sagepub.com/home/dhj

13.Gauthier-M. Régulation juridique de la « médecine numérique » : évolutions, enjeux et défis de l'utilisation des données de santé. (2024) www.village-justice

14.Chassang, G. "La protection des données personnelles en matière de santé. E-santé, droit de l'Union Européenne et protection de la vie privée des personnes : vers l'émergence d'un techno droit spécifique au travers de la proposition de règlement général sur la protection des données personnelles ? Revue de Lamy Droit de l'immatériel, 2014, Suppl. au no 108, hal-04590547

15.Granmar, CG. Global applicability of the GDPR in context. Int Data Privacy Law 2021; 11: 225–244. 11. Hiramatsu K, Barrett A and Miyata Y. PhRM

16.Hedley, A. "Privacy as a factor in residential buildings and site development: an annotated bibliography", in Issue 32 of Bibliography, National Research Council of Canada. Division of Building Research, 1966.

17.Cohen D. HIPAA Reform or a patchwork scheme: A look at preemption, scope, and the inclusion of a Private Right of Action in a New Federal Data Privacy Law. 2020

18.Pope, T. "Confidentialité et HIPAA (Health Insurance Portability and Accountability Act), August 2025 https://www.msdmanuals.com/fr/professional/sujets-sp%C3%A9ciaux/probl%C3%A8mes-médico-légaux/confidentialité-et-hipaa-health-insurance-portability-and-accountability-act

19.Ornstein, C. Hospital to punish snooping on Spears. Los Angeles Times (2005) https://www.latimes.com/archives/la-xpm-2008-mar-15-me-britney15-story.html

20.Queiroz de Barros, I., & Fernandes, S. "Right to be forgotten in healthcare: a scoping review" Revista Gaucha de Enfermagem 46, 1-13, 2025 DOI: 10.1590/1983-1447.2025.20250085.en

21.Juexiao, Z., Li, H., Liao, X., Li, Z., Longxi, Z., Xin, G., Zhang, B., & Wenjia, H. "A unified method to revoke the private data of patients in intelligent healthcare with audit to forget" nature Communications, February 2023. https://doi.org/10.1038/s41467-023-41703-x

22.Poplin, R. et al. Prediction of cardiovascular risk factors from retinal fundus photographs via deep learning. Nat. Biomed. Eng. 2, 158–164

(2018).

23.Zhou, L. et al. A rapid, accurate and machine-agnostic segmentation and quantification method for CT-based COVID-19 diagnosis. IEEE Trans. Med. Imaging 39,2638–2652 (2020). 16. Zhou, L. et al. An interpretable deep learning workflow for discovering subvisual abnormalities in CT scans of COVID-19 inpatients and survivors. Nat. Mach. Intell. 4, 494–503 (2022).

24.Shankar, N and Mohammed, Z. Surviving data breaches: a multiple case study analysis. J Comp Int Manage 2020; 23: 35–54.

25.Morse, A. Investigation: WannaCry cyber-attack and the NHS. Report by the National Audit Office; 2024.

26.Al Shkeili, K. Is the medical information of political elites at increasing risk from strategically motivated cyberattacks? [unpublished manuscript]; 2020.

27.Ghana Health Service. COVID-19 test results exposure case. Accra: Ghana Health Service; 2024 June 2. Available from https://ghs.gov.gh/.

28.Van Niekerk B. An analysis of cyber-incidents in South Africa. Afr J Inf Commun 2017; 20: 113–132.

29 Zhao, Y., Shin, C., & Ompok, C. C. (2025). Job Satisfaction, Work Engagement, and OCB in Preschool Teachers: A Review of Mediating Mechanisms. Journal of Management Practices, Humanities and Social Sciences, 9(4), 232-243.

30. Jam, F. A., Ali, I., Albishri, N., Mammadov, A., & Mohapatra, A. K. (2025). How does the adoption of digital technologies in supply chain management enhance supply chain performance? A mediated and moderated model. Technological Forecasting and Social Change, 219, 124225.