Page 3386 - 3396 **DOI:** *https://doij.org/10.10000/IJLMH.1110265*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 8 | Issue 3

2025

Data Privacy in Autonomous Healthcare Systems: A Human Right

SHAIKH SHOHAG HOSSAIN[1] AND SUMAIA SULTANA EMU[2]

ABSTRACT

In an era where digital healthcare systems process the personal health information of billions globally, the fundamental human right to privacy stands as the last guardian between human dignity and digital exploitation. The intersection of data privacy and human rights in healthcare represents a critical challenge where violations constitute fundamental breaches of human dignity, autonomy, and access to care. This research examines autonomous healthcare data privacy through the lens of human rights, analysing how violations of healthcare data privacy constitute fundamental breaches of human rights principles, including dignity, autonomy, non-discrimination, and access to healthcare. The study aims to provide a comprehensive framework for understanding autonomous healthcare data protection as a cornerstone of human rights protection in the digital age. A systematic literature review and doctrinal methodology were employed. The study identified that the right to privacy, enshrined in international human rights instruments such as the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights, provides the foundation for protecting individuals from arbitrary interference with their most sensitive personal information.

Digital and autonomous healthcare system data privacy signifies a fundamental human right essential for protecting human dignity, requiring recognition that data protection is not merely technical but a cornerstone of human rights protection. The integration of autonomous intelligence has introduced new dimensions of human rights challenges that require updated approaches addressing unique risks posed by machine learning systems. In our interconnected world, a violation of privacy anywhere becomes a threat to human dignity everywhere. Future healthcare privacy protection depends on a collective commitment to comprehensive legal frameworks, advanced technological solutions, and strong international cooperation that prioritises human dignity while enabling beneficial uses of health data for improving global health outcomes.

[1] Author is a Lecturer at Department of Law and Assistant Proctor at National University, Bangladesh, and Fellow, MPhil Leading to PhD at Institute of Liberation War and Bangladesh Studies, National University, Bangladesh.

[2] Author is a Lecturer at Department of Law, National University, Bangladesh, and Fellow, MPhil Leading to PhD at Institute of Liberation War and Bangladesh Studies, National University, Bangladesh.

 [ISSN 2581-5369]

Keywords: *Data Privacy, Healthcare, Artificial Intelligence, Autonomous Intelligence, Data Security in Healthcare, Patient Autonomy, Human Rights, International Healthcare Law*

I. INTRODUCTION

In 1948, when the world declared that "no one shall be subjected to arbitrary interference with his privacy," the drafters of the Universal Declaration of Human Rights could hardly have imagined a future where our most intimate health secrets would be exposed with a single cyberattack.[3] Today, as healthcare systems worldwide process the personal health information of billions, the fundamental human right to privacy stands as the last guardian between human dignity and digital exploitation. The intersection of data privacy and human rights in healthcare represents a fundamental aspect of human dignity and autonomy, as privacy serves as a foundational human right that enables the enjoyment of other rights, including healthcare, non-discrimination, and freedom from arbitrary interference. The right to privacy enables our enjoyment of other rights, and interference with our privacy often provides the gateway to the violation of our remaining rights, making healthcare data protection not merely a technical concern but a cornerstone of human rights protection in the digital age.

II. RESEARCH METHODOLOGY

This study employed a systematic literature review and doctrinal methodology. The research methodology incorporated a thematic analysis approach to construct a framework for organizing emerging themes related to healthcare data breaches and human rights violations. This research paper aims to examine data privacy in digital and autonomous healthcare systems through the lens of human rights, analyzing how violations of healthcare data privacy constitute fundamental breaches of human rights principles including dignity, autonomy, non-discrimination, and access to healthcare. The scope encompasses international human rights frameworks that establish privacy as a fundamental right, and the human rights consequences that occur when healthcare data privacy is violated, including emerging threats from artificial intelligence systems.

III. CONCEPTUALIZING DATA PRIVACY AND HUMAN RIGHTS

A. Defining data privacy in the autonomous healthcare

Data privacy in autonomous healthcare system must be understood as an extension of the

[3] *Article 12 of The Universal Declaration of Human Rights*, 12, https://www.humanrights.com/course/lesson/articles-12-18/read-article-12.html (last visited Jun. 13, 2025).

fundamental human right to privacy, encompassing both the technical measures used to secure data and the legal and ethical frameworks that govern how healthcare information is collected, stored, processed, and shared in accordance with human rights principles.[4] The human rights foundation of healthcare data privacy recognizes that patients have inherent rights to control access to their personal health information, to provide informed consent for its use, and to be protected from unauthorized disclosure that could violate their human dignity or lead to discrimination.[5] This human rights-based approach to healthcare data privacy acknowledges that violations of medical confidentiality constitute violations of fundamental human rights that can have severe consequences for individual well-being and social justice.

B. Human rights frameworks and data privacy

The foundation of data privacy as a human right can be traced to Article 12 of the Universal Declaration of Human Rights (UDHR), which establishes that "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation," creating a framework that directly applies to healthcare data protection.[6] The International Covenant on Civil and Political Rights (ICCPR) further develops this framework in Article 17, requiring that the gathering and holding of personal information on computers, databases, and other devices must be regulated by law, with effective measures taken to ensure that information concerning a person's private life does not reach unauthorized persons.[7] These human rights instruments establish that privacy is not merely a legal or technical requirement but a fundamental human right that creates obligations for states and healthcare providers to implement comprehensive protections against arbitrary interference with personal health information.[8] The European Court of Human Rights has interpreted these provisions to require that intrusions on privacy must be proportionate to the benefit to society, establishing a human rights framework for balancing healthcare data use with individual privacy protection.

The European Union's General Data Protection Regulation represents a human rights-based

---

[4] Zlatko Delev, *GDPR Considerations for Healthcare: Ensuring Data Protection Compliance*, GDPR LOCAL (Feb. 20, 2024), https://gdprlocal.com/gdpr-considerations-for-healthcare-ensuring-data-protection-compliance/.

[5] Steve Alder, *2024 Healthcare Data Breach Report*, THE HIPAA JOURNAL (Jan. 30, 2025), https://www.hipaajournal.com/2024-healthcare-data-breach-report/.

[6] Article 12 of The Universal Declaration of Human Rights, *supra* note 2.

[7] *Article 17: Privacy, Home, Correspondence; Honour and Reputation*, *in* A COMMENTARY ON THE INTERNATIONAL COVENANT ON CIVIL AND POLITICAL RIGHTS: THE UN HUMAN RIGHTS COMMITTEE'S MONITORING OF ICCPR RIGHTS 458 (Paul M. Taylor ed., 2020), https://www.cambridge.org/core/books/commentary-on-the-international-covenant-on-civil-and-political-rights/article-17-privacy-home-correspondence-honour-and-reputation/5C2A432BF74C4289A49281A9279DAE35.

[8] *Human Rights and Digital Health Technologies - PMC*, https://pmc.ncbi.nlm.nih.gov/articles/PMC7762914/ (last visited Jun. 13, 2025).

approach to healthcare data privacy, treating health data as a special category of personal data that demands stricter protection measures because of its fundamental connection to human dignity and the right to privacy.[9] The World Health Organization has developed comprehensive guidelines for health data protection that explicitly recognize human rights and the right to privacy as fundamental principles in health data governance, demonstrating the global recognition of healthcare data privacy as a human rights issue.[10] WHO's Personal Data Protection Policy emphasizes the application of human rights principles in all aspects of health data management, requiring that data processing activities respect human dignity, autonomy, and privacy while contributing to improved health outcomes.

C. The ethical imperative of data privacy in healthcare

The ethical imperative for data privacy in digital and autonomous healthcare systems from fundamental human rights principles including autonomy, dignity, non-discrimination, and justice, which require that healthcare systems respect and protect individual privacy as a matter of human rights compliance. The principle of autonomy, grounded in human rights law, requires that patients have the right to make informed decisions about their healthcare, including decisions about how their personal health information is used and shared, making privacy protection essential for ensuring that healthcare respects human agency and self-determination. Human dignity, another foundational human rights principle, requires that healthcare data practices respect the inherent worth of every individual and protect them from treatment that could undermine their fundamental human value. The human rights framework for healthcare data privacy also encompasses the principle of non-discrimination, requiring that healthcare data practices do not facilitate or enable discrimination based on health status, genetic information, or other protected characteristics, as such discrimination would violate fundamental human rights principles.[11]

IV. THE HUMAN RIGHTS IMPLICATIONS OF DATA BREACHES IN HEALTHCARE

A. Invasion of privacy: legal and ethical perspectives

Healthcare data breaches represent one of the most serious violations of the fundamental human right to privacy, constituting arbitrary interference with private life that is prohibited under international human rights law and causing harm that extends far beyond immediate

[9] Delev, *supra* note 3.
[10] *WHO Personal Data Protection Policy*, https://www.who.int/publications/m/item/who-personal-data-protection-policy (last visited Jun. 13, 2025).
[11] Human Rights and Digital Health Technologies - PMC, *supra* note 7.

 [ISSN 2581-5369]

technical failures.[12] When unauthorized parties access or disclose personal medical records, they violate the fundamental right to privacy enshrined in the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights, creating human rights violations that can have severe and lasting consequences for affected individuals.[13] The invasion of privacy through healthcare data breaches is particularly egregious from a human rights perspective because it involves the most intimate aspects of human life, including medical histories, mental health information, genetic data, and other highly sensitive personal details that are essential to human dignity and autonomy. These violations represent fundamental breaches of the trust relationship between patients and healthcare providers that is essential for protecting human rights in healthcare settings, undermining not only individual privacy but also the broader human rights framework that depends on institutional trustworthiness.[14]

B. Data breaches involving artificial intelligence systems

The emergence of artificial and autonomous intelligence in healthcare has introduced new dimensions of human rights violations through data breaches, as demonstrated by recent incidents where AI systems have inadvertently exposed sensitive patient information.[15] In 2024, Serviceaide, a provider of agentic artificial intelligence-based IT management software, reported a breach affecting more than 483,000 patients when their AI system inadvertently made Catholic Health's patient database publicly available on the web, exposing names, Social Security numbers, medical records, and treatment information.[16] This incident illustrates how AI systems in healthcare can create unique privacy vulnerabilities that compound traditional human rights concerns with new technological risks.[17] The deployment of AI in healthcare without adequate privacy safeguards violates human rights principles by creating new pathways for unauthorized access to sensitive medical information and enabling discrimination based on algorithmic analysis of health data.[18] [19]

C. Discrimination, stigmatization, and marginalization

[12] Article 12 of The Universal Declaration of Human Rights, *supra* note 2.
[13] Article 17, *supra* note 6 at 17.
[14] Human Rights and Digital Health Technologies - PMC, *supra* note 7.
[15] Marianne Kolbasuk McGee, *Agentic AI Tech Firm Says Health Data Leak Affects 483,000*, https://www.bankinfosecurity.com/agentic-ai-tech-firm-says-health-data-leak-affects-483000-a-28424 (last visited Jun. 13, 2025).
[16] *Serviceaide Leak Exposes Records of 500,000 Catholic Health Patients*, https://hackread.com/serviceaide-leak-catholic-health-patients-records/ (last visited Jun. 13, 2025).
[17] *Breaches at Serviceaide, Nationwide Recovery Services Expose Medical Info of More than 500,000 People*, https://therecord.media/breaches-serviceaide-nationwide-medical-info (last visited Jun. 13, 2025).
[18] Human Rights and Digital Health Technologies - PMC, *supra* note 7.
[19] Eduard Kovacs, *480,000 Catholic Health Patients Impacted by Serviceaide Data Leak*, SECURITYWEEK (May 19, 2025), https://www.securityweek.com/480000-catholic-health-patients-impacted-by-serviceaide-data-leak/.

Healthcare data breaches create serious human rights violations through discrimination, stigmatization, and marginalization that violate fundamental principles of equality and non-discrimination established in international human rights law.[20] When sensitive health information is disclosed without authorization, it can lead to employment discrimination, insurance denials, social ostracism, and other forms of adverse treatment that violate the human rights principles of equal treatment and non-discrimination based on health status. The discrimination potential is particularly acute for individuals with mental health conditions, HIV/AIDS, genetic disorders, or other stigmatized health conditions, creating human rights violations that compound existing vulnerabilities and marginalization. Studies have documented cases where individuals have experienced divorce, job loss, social rejection, and other severe consequences when their health status was inappropriately disclosed, demonstrating how healthcare data breaches can create cascading human rights violations that affect multiple aspects of life.[21] This discrimination not only violates individual rights but also creates broader public health risks by discouraging people from seeking necessary medical care, thereby violating both privacy rights and the right to health.

D. Psychological, social, and economic consequences of data breaches

The psychological impact of healthcare data breaches represents a violation of human rights principles that protect mental health and psychological well-being, as patients often experience increased anxiety, stress, and lasting fear about the security of their medical information. This psychological harm contributes to a reluctance to share future health-related details with providers, creating a cycle of distrust and compromised care that violates both privacy rights and the right to health by undermining the therapeutic relationship.[22] The social consequences of healthcare data breaches include damage to personal relationships, loss of social status, and community ostracism, particularly for individuals with stigmatized health conditions, creating human rights violations that affect social participation and human dignity. Economic consequences can be substantial, ranging from direct financial losses due to identity theft to indirect costs such as lost employment opportunities and increased insurance premiums, demonstrating how privacy violations can create economic human rights violations that affect the right to work and adequate standard of living.

E. Emerging patterns and trends in healthcare privacy violations

Analysis of healthcare data breach trends reveals consistent patterns over the past years, with

[20] Human Rights and Digital Health Technologies - PMC, *supra* note 7.
[21] *Id.*
[22] *Id.*

 [ISSN 2581-5369]

the vast majority of patient records being stolen from third parties rather than directly from hospitals, indicating that human rights violations often occur through complex networks of healthcare-related organizations.[23] The majority of ransomware attacks primarily use social engineering, stolen credentials, and exploitation of unpatched vulnerabilities for initial access, demonstrating the international and systematic nature of threats to healthcare privacy rights.[24] Healthcare data breaches reached an all-time high in 2024, with over 10,000 breaches affecting victims in 94 countries, illustrating the global scope of human rights violations in healthcare data protection and the need for international cooperation to address these threats.[25]

V. CHALLENGES AND LIMITATIONS IN DATA PRIVACY PROTECTION IN HEALTHCARE SYSTEMS

A. Legal and regulatory gaps in healthcare data protection

Significant legal and regulatory gaps persist in digital and autonomus healthcare data protection across global jurisdictions, creating systematic vulnerabilities that enable human rights violations and fail to meet international human rights standards for privacy protection.[26] Many countries lack comprehensive data protection laws specifically tailored to healthcare contexts, instead relying on general privacy legislation that may not adequately address the unique human rights challenges of medical data or provide sufficient protection against discrimination and stigmatization.[27] Even where legal frameworks exist, they often contain loopholes that facilitate human rights violations in healthcare settings, including inadequate protection against unauthorized disclosure, insufficient consent requirements, and weak enforcement mechanisms.[28]

B. Technological and security barriers to data privacy

Healthcare systems face significant technological and security barriers that impede effective protection of human rights in data privacy, as IT systems remain vulnerable to various types of threats that can result in massive violations of privacy rights affecting millions of individuals.[29] The increasing complexity of healthcare technology infrastructure, including

[23] Alder, *supra* note 4.
[24] Sanjay Deo, *Data Breaches Set New Records in 2024*, https://blog.24by7security.com/2024-data-breach-update-0 (last visited Jun. 13, 2025).
[25] *Id.*
[26] World Health Organization Regional Office for Europe, *The Protection of Personal Data in Health Information Systems- Principles and Processes for Public Health* (2021), https://iris.who.int/handle/10665/341374.
[27] Human Rights and Digital Health Technologies - PMC, *supra* note 7.
[28] Alder, *supra* note 4.
[29] Design Admin, *Top 5 Healthcare Cybersecurity Threats in 2024*, CAMBRIDGE COLLEGE OF HEALTHCARE & TECHNOLOGY 5 (Jan. 6, 2025), https://www.cambridgehealth.edu/healthcare-cybersecurity-privacy/healthcare-

electronic health records, telemedicine platforms, and cloud-based storage systems, creates multiple potential points of vulnerability that can enable human rights violations when adequate security measures are not implemented [4]. Healthcare data breaches reached an all-time high in 2024, with over 10,000 breaches affecting victims in 94 countries, demonstrating that technological vulnerabilities continue to create widespread human rights violations despite advances in security technology.[30]

C. AI-Specific challenges in privacy protection

Machine learning systems in healthcare face unique privacy challenges that require specialized approaches to protect human rights, as traditional security measures may be insufficient to address adversarial attacks, membership inference attacks, and other AI-specific threats to patient privacy.[31] The development of privacy-preserving machine learning techniques remains an active area of research, with ongoing challenges in implementing federated learning, differential privacy, and other protective measures while maintaining the utility of AI systems for healthcare applications.[32] AI systems can introduce new forms of bias and discrimination that violate human rights principles, particularly when training data contains historical biases or when algorithmic decision-making processes lack transparency and accountability.[33] The complexity of AI systems makes it difficult for patients to understand how their data is being processed and used, potentially undermining informed consent requirements and violating human rights principles of autonomy and self-determination.

VI. RECOMMENDATIONS FOR STRENGTHENING DATA PRIVACY IN HEALTHCARE

A. Reforming and enhancing legal frameworks for data protection

Comprehensive legal reform is essential for strengthening human rights protection in healthcare data privacy, requiring countries to develop legislation that aligns with international human rights standards while ensuring that privacy rights are effectively protected and enforced.[34] Legal frameworks should explicitly recognize healthcare data protection as a fundamental human rights issue, including specific provisions that treat healthcare data as requiring enhanced protection because of its connection to human dignity, autonomy, and non-discrimination. Legislation should establish independent oversight bodies

cybersecurity-privacy-information/top-5-healthcare-cybersecurity-threats-in-2024/.
[30] Deo, *supra* note 23.
[31] Admin, *supra* note 28 at 5.
[32] Human Rights and Digital Health Technologies - PMC, *supra* note 7.
[33] *supra* note 15.
[34] Europe, *supra* note 25.

with the authority to investigate human rights violations, impose meaningful penalties, and provide effective remedies to individuals whose privacy rights have been violated.[35]

B. Implementing privacy-preserving AI technologies

Healthcare organizations should invest in advanced privacy-enhancing technologies that protect human rights by ensuring that patient data security is maintained while preserving the utility of health information for medical care and research that serves the public good.[36] Federated learning, differential privacy, homomorphic encryption, and secure multi-party computation represent key technologies for protecting patient privacy in AI systems while enabling healthcare organizations to benefit from machine learning capabilities.[37] These privacy-preserving techniques allow healthcare organizations to train AI models on sensitive data without exposing individual patient information, thereby protecting human rights while advancing medical knowledge and improving patient care.[38]

C. Improving transparency, patient consent, and informed consent processes

Healthcare organizations must implement transparency and consent processes that genuinely embody human rights principles of autonomy and self-determination, ensuring that patients have meaningful control over their personal health information and can make informed decisions about its use. Consent processes should be designed to reflect human rights principles by being specific, informed, and granular, allowing patients to consent to particular uses of their data while withholding consent for others, thereby respecting individual autonomy and control. Digital consent management systems should be implemented to make it easier for patients to review and modify their consent preferences over time, ensuring that consent remains meaningful and reflects ongoing respect for human rights principles of self-determination.

D. Promoting international collaboration for universal data privacy standards

International collaboration is essential for developing universal standards for digital and autonomous healthcare system data privacy that protect human rights regardless of where individuals receive care, requiring harmonization of data protection laws across jurisdictions to ensure consistent human rights protection.[39] This includes working through international organizations such as WHO to develop and promote global standards for health data

[35] WHO Personal Data Protection Policy, *supra* note 9.
[36] Human Rights and Digital Health Technologies, *supra* note 7.
[37] Admin, *supra* note 28 at 5.
[38] Human Rights and Digital Health Technologies, *supra* note 7.
[39] WHO Personal Data Protection Policy, *supra* note 9.

 [ISSN 2581-5369]

governance.[40] Regional cooperation initiatives should be established to provide mutual assistance for healthcare data protection, ensuring that human rights violations are prevented and addressed through collaborative approaches. Developing countries should receive technical assistance and capacity building support to implement effective data protection measures that meet international human rights standards, ensuring that global disparities in protection do not create unequal enjoyment of fundamental rights.[41]

VII. CONCLUSION

Data privacy in digital and autonomous healthcare systems represents a fundamental human right that is essential for protecting human dignity, autonomy, and well-being, requiring recognition that healthcare data protection is not merely a technical or regulatory issue but a cornerstone of human rights protection in the digital age.[42] The analysis demonstrates that the right to privacy, enshrined in international human rights instruments such as the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights, provides the foundation for protecting individuals from arbitrary interference with their most sensitive personal information.[43] The protection of healthcare data privacy is therefore essential not only for individual well-being but also for maintaining the integrity of healthcare systems and public trust in medical institutions, which are necessary for fulfilling state obligations to protect and promote the right to health.[44] The integration of artificial intelligence and advanced technologies in healthcare has introduced new dimensions of human rights challenges. The successful implementation of privacy-preserving AI technologies, including federated learning, differential privacy, and secure multi-party computation, offers promising pathways for protecting human rights while enabling beneficial uses of healthcare data for medical advancement and patient care.[45] Future research and policy development in healthcare data privacy must focus on strengthening human rights protection while addressing the evolving challenges of protecting patient information in an increasingly connected and AI-enabled healthcare environment[46]. Research is needed to better understand the long-term psychological and social impacts of healthcare data breaches on individuals and communities. Policy development should focus on creating more flexible and adaptive regulatory frameworks that respond to rapidly evolving technological threats while

[40] Europe, *supra* note 25.
[41] Human Rights and Digital Health Technologies, *supra* note 7.
[42] Article 12 of The Universal Declaration of Human Rights, *supra* note 2.
[43] Article 17, *supra* note 6.
[44] WHO Personal Data Protection Policy, *supra* note 9.
[45] Human Rights and Digital Health Technologies, *supra* note 7.
[46] Europe, *supra* note 25.

 [ISSN 2581-5369]

maintaining strong human rights protections, including specific provisions for AI governance and algorithmic accountability in healthcare settings[47]. The future of digital and autonomous healthcare data system privacy will depend on our collective ability to recognize privacy as a fundamental human right that must be protected through comprehensive legal frameworks, advanced technological solutions, and strong international cooperation that prioritizes human dignity and equality while enabling beneficial uses of health data for improving global health outcomes.[48] From the hospital beds of developed nations to the rural clinics of emerging economies, the human right to healthcare privacy must be universal, unwavering, and unconditional. In our interconnected world, a violation of privacy anywhere becomes a threat to human dignity everywhere. The technology that promises to revolutionize healthcare must be harnessed not just for efficiency or innovation, but as an instrument of human rights protection that honors the sacred trust between healthcare providers and patients.

*****

[47] WHO Personal Data Protection Policy, *supra* note 9.
[48] Article 12 of The Universal Declaration of Human Rights, *supra* note 2.

 [ISSN 2581-5369]