



INTERNATIONAL JOURNAL OF HUMAN RIGHTS LAW REVIEW

An International Open Access Double Blind Peer Reviewed, Referred Journal

Volume 5 | Issue 4 | 2026

Art. 52

Algorithmic Healthcare and Legal Accountability: Patient Rights, Data Protection, and the Intersection with Digital Forensic Evidence

Sabila Iffath Shujathullah

*LL.M Student, 2nd Year,
Tamil Nadu Dr. Ambedkar Law University,
School of Excellence in Law, Chennai*

Recommended Citation

Sabila Iffath Shujathullah, *Algorithmic Healthcare and Legal Accountability: Patient Rights, Data Protection, and the Intersection with Digital Forensic Evidence*, 5 IJHRLR 750-760 (2026).

Available at www.ijhrlr.in/current-issues/.

This Article is brought to you for free and open access by the International Journal of Human Rights Law Review by an authorized Lex Assisto & Co. administrator.

For more information,
please contact submission.ijhrlr@gmail.com

Algorithmic Healthcare and Legal Accountability: Patient Rights, Data Protection, and the Intersection with Digital Forensic Evidence

ABSTRACT

The rapid integration of artificial intelligence (AI) and algorithmic decision-making into healthcare systems has fundamentally transformed medical practice, raising complex questions of legal accountability and patient protection. This research critically examines the intersection of algorithmic healthcare with medical jurisprudence, focusing on patient rights, informed consent, and data protection within increasingly digitized clinical environments. It explores how AI-driven diagnostic and treatment tools challenge traditional standards of medical negligence, duty of care, and professional liability, particularly when decision-making is partially or wholly delegated to automated systems. From a legal perspective, the paper analyses the adequacy of existing regulatory frameworks in safeguarding patient autonomy and ensuring meaningful informed consent in the context of opaque “black-box” algorithms. It further evaluates data protection concerns arising from the extensive collection, processing, and sharing of sensitive health data, emphasizing the risks of misuse, breaches, and surveillance. In addition, the study investigates the growing role of digital forensic evidence in both civil and criminal proceedings involving medical technologies. It highlights evidentiary challenges relating to the admissibility, reliability, and authenticity of algorithm-generated outputs and electronic health records. The article argues for a robust, adaptive legal framework that integrates principles of transparency, accountability, and technological due diligence. It concludes by proposing reforms to harmonize healthcare innovation with constitutional protections, ensuring that technological advancement does not undermine fundamental patient rights and the integrity of the justice system.

KEYWORDS

Algorithm, Patent, Medical Negligence, Technology, Artificial Intelligence

INTRODUCTION: ALGORITHMIC TRANSFORMATION IN HEALTHCARE

A paradigm change in medical science has occurred with the introduction of artificial intelligence (AI) into healthcare, moving from

physician-centric procedures to data-driven, algorithmically assisted systems. In the past, healthcare professionals' clinical knowledge and experience were the main factors used to make medical decisions. But with the advent of machine learning, predictive analytics, and automated diagnostic tools, healthcare has become a technologically enhanced field where clinical results are informed by large datasets and computational models. Applications of AI are currently found in many other fields, including radiology, genomics, drug development, and personalised medicine, and they show promise for improving the efficiency and accuracy of diagnosis. With real-world health data being essential for training and evaluating AI models, this quick evolution highlights the increasing reliance on data as the fundamental component of contemporary healthcare systems.¹

Even while AI has the potential to be revolutionary, integrating it presents difficult moral and legal issues, especially with regard to patient safety and accountability. Conventional medical jurisprudential frameworks are based on identifiable human actors, and culpability is assigned on the basis of carelessness, duty breach, or departure from accepted norms of care. However, by adding non-human actors to the decision-making process, algorithmic decision-making complicates this structure. Concerns regarding transparency, traceability, and accountability are raised by the fact that AI systems, which are frequently defined by opaque "black-box" features, might create results that are challenging to understand or explain. According to academics, this opacity makes it harder to assign blame when harm happens, endangering the fundamental tenets of liability law.²

Additionally, the boundaries of informed consent and patient autonomy are being redefined by the transition from human-centric to hybrid decision-making systems in which physicians rely on algorithmic advice. The effectiveness of traditional permission frameworks may be questioned since patients may not completely understand the function or role of AI tools employed in their diagnosis or treatment. Significant worries about data ownership, privacy, and potential misuse are also brought up by the growing reliance on extensive health data. The hazards of data breaches, unauthorized sharing, and monitoring are increased by AI systems' intrinsic need for broad access to private health

¹ The development and functioning of AI in healthcare is heavily dependent on large-scale data collection and regulatory compliance requirements

² The opacity and autonomous functioning of AI systems complicate traditional notions of liability and accountability

information.³

CONCEPTUAL FRAMEWORK: AI, ALGORITHMS, AND MEDICAL DECISION-MAKING

The use of computing systems that can mimic human intelligence functions like learning, reasoning, and problem-solving through data-driven algorithms is known as artificial intelligence (AI) in healthcare. AI is fundamentally based on machine learning models that find patterns in large datasets and produce predictions or judgments without the need for explicit programming. Algorithmic decision-making in medicine refers to the use of structured computing processes, from straightforward rule-based systems to intricate neural networks, to support or automate clinical decisions, such as prognosis, diagnosis, and therapy planning. Healthcare has historically employed medical algorithms, which are generally understood to be computational formulas or decision trees. However, contemporary AI systems greatly broaden their application by facilitating autonomous and adaptive decision-making based on real-time data inputs.

The use of AI in healthcare falls into a number of functional categories. In radiology and pathology, diagnostic AI tools especially those that use deep learning are commonly employed to analyze medical pictures with high precision, frequently spotting patterns that human clinicians might miss. Another crucial area is predictive analytics, in which machine learning algorithms evaluate patient data to predict the course of an illness, the possibility of complications, or the chance of being readmitted to the hospital. AI-powered clinical decision support systems also help doctors by producing recommendations based on evidence and customized to each patient's profile. The technological advancement of healthcare is further demonstrated by robotic and AI-assisted surgical devices, which allow for greater patient outcomes, minimally invasive treatments, and increased precision.

The "black-box" aspect of many sophisticated AI systems is a distinguishing feature. Black-box algorithms are those that have opaque internal decision-making processes, which means that even developers and consumers cannot access the underlying rationale, even when inputs and outputs are visible. In deep learning models, where intricate neural networks process several layers of data to generate results that are challenging to understand, this lack of transparency is more noticeable. Such opacity poses serious difficulties in the healthcare industry since patients and clinicians may not be able to comprehend the reasoning behind important medical decisions. According to academics, this

³ Data privacy and ethical concerns are central to AI deployment in healthcare, particularly due to the use of sensitive patient information

inexplicability might compromise patient autonomy, make informed consent more difficult, and make it difficult to hold people accountable when mistakes are made.

LEGAL FOUNDATIONS OF MEDICAL LIABILITY IN THE AGE OF AI

The well-established concepts of negligence, duty of care, and standard of care have historically served as the foundation for the legal framework controlling medical responsibility. A healthcare provider is held accountable under traditional tort law when a patient is harmed as a result of a duty violation, measured against what a "reasonable medical practitioner" would have done in the same situation. This standard, which serves as the cornerstone of medical negligence jurisprudence, calls for evidence that the practitioner's actions actually caused harm and fell short of recognized professional standards. Because of this, medical responsibility has generally been human-centric, with courts concentrating on the professional judgment, actions, and omissions of physicians. Hospitals and other healthcare facilities are also subject to liability under the theories of institutional responsibility and vicarious liability.

However, these conventional legal underpinnings are seriously disrupted by the incorporation of Artificial Intelligence (AI) into clinical decision-making. AI systems are becoming more and more involved in risk assessments, diagnosis, and treatment suggestions, bringing non-human actors into the decision-making process. It is unclear whether the human practitioner, the organization, or the technology itself should bear liability when clinical judgment is delegated to algorithmic algorithms. Notably, current legal theories still place a high priority on human accountability; doctors are typically required to use their own discretion and cannot rely exclusively on AI outputs as a defense. If a doctor relies on AI outputs that differ from the acknowledged standard of care, they may still be held liable even if the system makes wrong recommendations.

The dynamic nature of the "standard of care" exacerbates the difficulties presented by AI delegation. Adherence to AI-assisted decision-making may itself become a recognized aspect of medical practice as AI tools become more commonly used. This dynamic creates a paradox: while physicians may be held liable for deviating from traditional norms, they may also be held negligent in the future if they fail to use cutting-edge AI tools that improve accuracy. Furthermore, the opaque operation of AI systems, especially black-box models, makes it challenging to determine fault and causation, which complicates evidential evaluation and

litigation.

PATIENT RIGHTS AND INFORMED CONSENT IN ALGORITHMIC HEALTHCARE

The fundamental tenets of patient rights, especially the right to autonomy and self-determination, are drastically altered by the incorporation of artificial intelligence (AI) into healthcare systems. A fundamental component of medical ethics and legal theory, autonomy guarantees that patients are free to make decisions about their care based on sufficient knowledge and without being forced to do so. AI has the ability to both strengthen and weaken this right in the context of algorithmic healthcare. While AI-driven solutions can empower patients by offering tailored treatment alternatives and data-driven insights, an over-reliance on automated decision-making may marginalize patient engagement and diminish meaningful human connection in clinical settings.

The effectiveness of informed consent in AI-mediated healthcare is a crucial issue brought about by this change. Informed consent often calls for the patient's understanding, voluntary permission to treatment, and the revelation of pertinent facts. But AI adds levels of technological complexity that are difficult to explain in traditional consent frameworks. The legitimacy of consent gained under such circumstances is seriously questioned because studies show that patients are frequently unaware that AI techniques are being employed in their diagnosis or treatment. Furthermore, information on algorithmic operation, potential biases, error rates, and the degree of human oversight are all included in the disclosure requirements for AI-based healthcare, which go beyond the conventional risks and benefits. Healthcare providers face additional challenges due to the novelty and sophistication of AI technologies.

Furthermore, the dynamic and ever-evolving nature of AI systems makes current consent models inadequate. It is challenging to offer comprehensive and correct information at a single moment since AI algorithms, in contrast to static medical procedures, are constantly learning and adapting based on fresh data inputs. Because of this, more adaptable and continuous consent procedures that include continuing disclosure and patient involvement are required. Redesigned consent procedures that make use of visual aids, individualized communication, and simpler language may improve patient comprehension and confidence in AI-driven healthcare, according to academics. However, obtaining properly informed permission is still severely hampered by the intrinsic complexity of AI systems.

Transparency and explainability, which are crucial for maintaining

patient autonomy and legal accountability, are closely related to these concerns. Many AI systems, especially deep learning-based ones, function as "black boxes," generating results without offering a clear explanation for their conclusions. The patient's capacity to make educated decisions is compromised by this lack of explainability, which also erodes confidence in medical decision-making procedures. Because explainability promotes comprehension, encourages independent decision-making, and strengthens the validity of clinical results, it is widely seen as a normative criterion in healthcare AI.

DATA PROTECTION AND PRIVACY IN DIGITAL HEALTH ECOSYSTEMS

The digital transformation of healthcare has led to the large-scale generation, collection, and processing of health data, which is widely recognized as one of the most sensitive categories of personal information. Health data encompasses a broad spectrum of information, including medical histories, diagnostic reports, genetic data, biometric identifiers, prescriptions, and even real-time data from wearable devices and telemedicine platforms. Such data is inherently intimate, revealing not only an individual's physical and mental health status but also aspects of their identity and lifestyle. Consequently, its misuse or unauthorized disclosure can result in severe consequences, including discrimination, stigmatization, and economic harm. The sensitivity of health data necessitates heightened legal protection and strict governance standards, particularly in AI-driven healthcare systems that rely heavily on continuous data flows.

The hazards related to data processing have increased concurrently with the growth of digital health ecosystems. The high value of medical information in illegal markets makes healthcare institutions more susceptible to hackers and data breaches. Unauthorized access, ransomware attacks, and data leaks have increased in frequency, exposing patient records and jeopardizing confidentiality. Algorithmic healthcare creates issues with data usage and profiling in addition to security problems. Predictive profiling of patients based on medical problems, genetic predispositions, or behavioral factors can result from AI systems' frequent aggregation and analysis of massive information to find patterns. If such profiling is not adequately regulated, it could lead to biased hiring, insurance, and healthcare service practices.

With the passage of the Digital Personal Data Protection Act, 2023 (DPDP Act), the nation's first comprehensive data privacy law, India has achieved considerable legal progress in tackling data protection. The Act creates a framework that governs the gathering, processing, storing, and

transfer of digital personal data, including health-related information. It also places requirements on organizations that handle this data to guarantee legal processing and security measures. Additionally, it strengthens informational autonomy by granting people rights including the ability to access, amend, and remove personal data.

ALGORITHMIC BIAS, FAIRNESS, AND ETHICAL CONCERNS

One of the biggest obstacles to the application of artificial intelligence (AI) in healthcare is algorithmic bias, which has a direct impact on justice, equity, and fairness in medical decision-making. Algorithmic bias, in its broadest sense, is the term used to describe systematic and repeated faults in computing systems that result in unfair outcomes, frequently favoring some groups over others because of problems in data, design, or execution. In the healthcare industry, this kind of bias usually comes from training datasets that show past injustices, such as differences in socioeconomic status, access to care, and demographic representation. Therefore, systemic inequality may be reinforced by AI systems educated on such data that reproduce or even magnify current injustices.

Selection bias, measurement bias, and representation bias are just a few examples of how bias in datasets can appear and affect how reliable algorithmic results are. For example, AI systems may generate less accurate diagnoses or treatment suggestions for minority populations that are underrepresented in datasets. Research has shown that healthcare algorithms have occasionally showed racial prejudice by giving patients priority based on past healthcare spending rather than real medical necessity, which disadvantages underprivileged communities. This demonstrates the inherent danger of incorporating social injustices into technology systems that appear to be impartial.

Such bias has consequences that go beyond technical errors to include serious dangers of discrimination in the provision of healthcare. Algorithmic systems may unintentionally discriminate against patients on the basis of their race, gender, age, or socioeconomic position, which could result in differences in clinical results or unequal treatment access. In addition to undermining the moral precepts of fairness and non-maleficence, these discriminatory impacts present significant constitutional issues, especially in countries like India where equality and dignity are fundamental rights. Furthermore, these biases may be hidden by AI systems' apparent objectivity, making biased results less obvious and more challenging to refute.

The question of accountability becomes crucial from an ethical perspective. Algorithmic solutions distribute accountability across developers, data scientists, and healthcare clinicians, in contrast to

traditional medical decision-making, where human actors are explicitly responsible. This diffusion makes ethical accountability more difficult and begs the question of who is to blame for unfair or detrimental results. In addition to proactive steps like bias audits, varied data collecting, and regulatory supervision, ethical frameworks are increasingly emphasizing the necessity of fairness, transparency, and explainability in AI systems. In the end, maintaining equity in algorithmic healthcare necessitates a multidisciplinary strategy that incorporates ethical precepts, legal protections, and technological advancements to stop disparity from continuing.

Digital Forensic Evidence in Healthcare Disputes

The use of digital forensic evidence in medical disputes, both civil and criminal, has greatly increased due to the growing digitization of healthcare systems. Digital prescriptions, medical imaging data, AI-generated diagnostic outputs, and electronic health records (EHRs) are now essential parts of the evidence used in court. Courts can recreate clinical events and evaluate the behavior of healthcare practitioners thanks to these digital records, which offer a thorough and time-stamped account of patient care. This evidence environment is further complicated by the integration of AI, since algorithm-generated outputs like treatment recommendations or predicted diagnoses may impact clinical judgments and come under judicial scrutiny.

In medical negligence lawsuits, electronic health records in particular are used as main evidence to show the standard of care, treatment history, and causality. Their correctness, comprehensiveness, and capacity to offer contemporaneous evidence of medical contacts are what give them their evidentiary significance. However, there are drawbacks to these records' digital format, such as the possibility of system faults, manipulation, or unauthorized modification. Evidentiary analysis is made more difficult by AI-generated outputs, whose dependability may be questioned because of the opaque operation of underlying algorithms. In order to comprehend such results, courts may need expert testimony, especially in cases involving complex machine learning models that are not explainable.

Digital evidence's admission in civil and criminal procedures depends on its relevance, legitimacy, and dependability. The necessity of certification and verification of electronic records is emphasized by legal frameworks, including clauses similar to Section 65B of the Indian Evidence Act. AI-generated evidence poses extra difficulties because proving the integrity of training data, model design, and operating settings may be necessary to show the dependability of algorithmic

processes. This procedure may be hampered by "black-box" systems' lack of openness, which raises questions about the evidence's probative value.

Regulatory Frameworks and Governance Challenges

The regulatory landscape governing AI in healthcare is currently characterized by a combination of general healthcare laws, data protection statutes, and emerging AI-specific guidelines, yet it remains fragmented and evolving. Existing legal frameworks such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States and the General Data Protection Regulation (GDPR) in the European Union primarily focus on the protection of personal and health data rather than the regulation of AI systems themselves. These frameworks impose obligations relating to data security, consent, and privacy, thereby indirectly shaping the deployment of AI in healthcare. Similarly, in India, the Digital Personal Data Protection Act, 2023, along with sectoral initiatives such as the National Digital Health Mission, provides a foundational structure for regulating health data. However, these laws are largely data-centric and do not comprehensively address the unique challenges posed by algorithmic decision-making.

A significant gap in current regulatory regimes lies in the absence of AI-specific provisions that address issues such as algorithmic transparency, accountability, and risk classification. AI systems in healthcare are often treated either as software or as medical devices, leading to ambiguity in their regulatory classification and oversight. Furthermore, the rapid evolution of AI technologies creates a "pacing problem," wherein legal frameworks struggle to keep up with technological advancements, resulting in regulatory lag. This lag is particularly problematic in high-stakes domains like healthcare, where errors in AI systems can have life-threatening consequences. Additionally, challenges such as algorithmic bias, lack of explainability, and difficulties in attributing liability further expose the inadequacy of existing legal structures.

Another critical governance challenge is the fragmented and sector-specific nature of regulation, which fails to account for the interdisciplinary nature of AI in healthcare. Effective regulation requires the integration of legal, medical, technological, and ethical perspectives. International bodies such as the World Health Organization have emphasized the need for comprehensive governance frameworks that ensure data quality, transparency, and human oversight in AI systems. Moreover, comparative regulatory models, such as the European Union's AI Act, adopt a risk-based approach that categorizes AI applications based on their potential harm and imposes corresponding obligations, offering a potential blueprint for future regulation.

CONCLUSION

The integration of Artificial Intelligence (AI) into healthcare represents a transformative shift that holds immense potential to enhance diagnostic accuracy, optimize treatment outcomes, and improve overall healthcare efficiency. However, as this research demonstrates, such technological advancement simultaneously introduces complex legal, ethical, and regulatory challenges that cannot be adequately addressed by traditional frameworks alone. Issues relating to medical liability, patient autonomy, data protection, and evidentiary reliability highlight the inadequacy of existing legal doctrines in addressing the realities of algorithmic decision-making.

A central concern lies in the diffusion of accountability across multiple stakeholders, including healthcare professionals, institutions, and AI developers, making it increasingly difficult to attribute liability in cases of harm. Contemporary scholarship emphasizes that responsibility in AI-driven healthcare is inherently shared and evolving, requiring coordinated legal and institutional responses. Moreover, concerns surrounding algorithmic bias, lack of transparency, and data privacy risks further underscore the need for robust safeguards to ensure that technological systems do not perpetuate inequality or compromise patient rights.

At the same time, AI should not be viewed as a replacement for human judgment but rather as a complementary tool that enhances clinical decision-making. Effective governance must therefore strike a balance between innovation and regulation, ensuring that AI systems remain subject to human oversight, ethical standards, and legal scrutiny.