DATA PRIVACY, ARTIFICIAL INTELLIGENCE AND HEALTH RIGHTS: LEGAL FRAMEWORKS AND GAPS

Harshita Bairwa, Delhi Metropolitan Education, Noida

ABSTRACT

The convergence of data privacy, artificial intelligence (AI), and health rights creates a complicated set of legal and ethical issues, especially as AI becomes more deeply embedded in healthcare. As AI-powered systems are used for diagnostics, individualized treatments, and health monitoring, they require extensive collection and analysis of personal medical data. This growing dependence on sensitive health information heightens concerns about data security, privacy protection, and the risks of misuse or unauthorized access. Protecting people's privacy and health information is the goal of legal frameworks like the Health Insurance Portability and Accountability Act (HIPAA) in the US and the General Data Protection Regulation (GDPR) in the EU. These frameworks, however, frequently fail to address the particular difficulties presented by AI, especially with regard to responsibility, consent, and transparency.

One of the key gaps in current legal frameworks is the lack of clear guidelines on how AI systems, which rely on vast datasets for training and operation, can be compliant with data privacy laws while maintaining effectiveness. Moreover, technology is advancing so quickly that lawmakers often struggle to keep pace, resulting in uncertainties and gaps in how laws address AI-based healthcare tools .Questions of data ownership, consent for use, and the right to be forgotten are particularly pressing in the context of health data, where information is both highly personal and potentially life-saving.

To address these gaps, stronger legal frameworks are needed—ones that balance privacy safeguards with AI-driven innovation, protecting health rights while still enabling progress in medical technology. These frameworks must ensure informed consent, safeguard against biases in AI algorithms, and hold entities accountable for breaches or misuse of health data, thereby protecting individuals' rights to privacy and access to equitable healthcare.

INTRODUCTION

What is AI?

Artificial Intelligence (AI) is a technology that enables machines to mimic human cognitive abilities, such as learning, reasoning, solving problems, making decisions, and understanding language.. AI-powered systems can analyze data, recognize patterns, make recommendations, and operate autonomously.[1]

Evolution of AI in Healthcare

AI in healthcare began in the 1950s–1970s with rule-based expert systems like MYCIN and DENDRAL. These systems laid the foundation for AI's role in clinical decision-making. In the 1980s–1990s, machine learning and neural networks allowed for more advanced pattern recognition. The 2000s saw the rise of electronic health records (EHRs) and big data, enabling AI to analyze massive datasets. In the 2010s, deep learning and computational power accelerated AI applications in imaging, genomics, and predictive analytics.

Artificial Intelligence (AI) is transforming multiple sectors—including healthcare, finance, transportation, education, and research. In academia, AI-powered tutoring systems enhance learning outcomes, while in research, AI makes it possible to identify patterns in massive information, which advances areas like drug discovery and genomics..

In healthcare, AI is revolutionizing clinical practice by enabling rapid analysis of vast medical data, assisting in early disease detection, and supporting personalized treatment planning. Its applications range from medical imaging and predictive analytics to administrative optimization. AI helps healthcare systems become more efficient, reduce costs, and improve patient outcomes.

As AI continues to advance, it becomes essential to encourage its ethical growth and provide healthcare professionals with the skills and resources needed for its proper use. In the long run, AI is paving the way for healthcare that is more precise, accessible, and focused on patient

[1] Shuroug A. Alowais., "Revolutionizing Healthcare: The Role of Artificial Intelligence in Clinical Practice" *BMC Medical Education* (22 September 2023). https://bmcmededuc.biomedcentral.com/articles/10.1186/s12909-023-04698-z

needs.[2]

IMPORTANCE OF DATA PRIVACY AND HEALTH RIGHTS

Data privacy in healthcare includes safeguarding sensitive patient information such as medical histories, diagnoses, treatments, insurance details, and personal identifiersUpholding the integrity of healthcare systems and preserving patient trust depend on protecting this privacy. Protecting digital data has grown more difficult as Electronic Health Records (EHRs) have become widely used. Due to insufficient access controls and the use of third-party apps that might not have strong security safeguards, many healthcare systems are still vulnerable.[3]

Technological protection alone is not sufficient—regulatory compliance is also essential. Laws such as India's **Digital Personal Data Protection Act (DPDP Act)**, the U.S. **HIPAA**, and Europe's **GDPR** set clear requirements for data handling, encryption, consent, and breach notification. However, human error remains a common cause of privacy violations, often due to improper use of personal devices or unintentional data sharing. Healthcare organizations must therefore adopt comprehensive data governance strategies, including strong encryption, regular staff training, strict access controls, and data backups.[4]

Healthcare data encompasses a wide range of sensitive categories: 'Personally Identifiable Information' (PII), 'Protected Health Information '(PHI), financial records, and medical research data. Each type carries distinct risks if exposed. For instance, PHI can be exploited for identity theft or insurance fraud, while breaches in research data can affect the credibility of medical studies and compromise patient anonymity.

Ethically, privacy is linked to respect for patient autonomy, dignity, and the principle of nonmaleficence—"do no harm." Ensuring privacy reduces risks like discrimination or stigma, encouraging patients to be more open with their healthcare providers, which in turn leads to better care outcomes. Moreover, protecting privacy promotes social trust and supports participation in medical research.

[2] Xsolis, https://www.xsolis.com/blog/the-evolution-of-ai-in-healthcare/ last visited at April 20, 2025
[3]Andrii Krylov, "Data Privacy in Healthcare: Importance & Problems" (2023). https://kodjin.com/blog/the-value-of-data-privacy-in-healthcare/
[4] National Library of Medicine, available at https://www.ncbi.nlm.nih.gov/books/NBK9579, last visited on April 20, 2025

In today's digital era—especially with the growth of IoT devices and continuous health monitoring—protecting data privacy has become a technical necessity and an ethical duty, vital for safeguarding accuracy, security, and public trust in healthcare services.[5]

UNDERSTANDING THE KEY CONCEPTS

1) ARTIFICIAL INTELLIGENCE IN HEALTHCARE

AI in healthcare uses tools like machine learning, natural language processing (NLP), deep learning, and expert rule-based systems to support and improve medical care for both clinicians and patients. These technologies help deliver quicker, more precise diagnoses, streamline access to medical records, and enable timely, customized treatment. Large volumes of clinical data are processed by machine learning to find patterns that help with precision medicine, diagnosis, and disease prediction. By extracting valuable insights from unstructured data, natural language processing (NLP) enables computers to comprehend and evaluate human language, simplifying clinical paperwork and facilitating more accurate diagnoses. Even though they are fundamental, traditional rule-based expert systems have limitations as their complexity increases. AI also supports diagnosis and treatment planning, but challenges remain in integrating these systems into clinical workflows and electronic health records (EHRs). Beyond clinical applications, AI is revolutionizing healthcare administration by automating routine tasks like scheduling, claims processing, and data entry, thereby reducing errors and enhancing efficiency. This allows medical professionals to focus more on patient care, ultimately improving outcomes and lowering operational costs. AI is expected to play a crucial role in both clinical and administrative healthcare operations as it develops.[6]

1. Disease Diagnosis

- AI supports **early and accurate disease diagnosis** using machine learning and analysis of electronic health records (EHRs).
- Used in predicting conditions like **Alzheimer's** and **dementia**, assisting in **emergency**

[5] Why data protection in healthcare is important? Available at https://vipre.com/blog/why-data-protection-in-healthcare-is-important, last visited on April 20, 2025
[6] AI in Healthcare, available at https://www.foreseemed.com/artificial-intelligence-in-healthcare ,last visited on April 19, 2025

departments, and offering **real-time decision support**.

- A 2023 study showed higher satisfaction with ChatGPT-generated medical advice compared to that of physicians, though with some criticism over methodology.

2. Electronic Health Records (EHRs)

- AI helps interpret EHRs using **natural language processing (NLP)** to consolidate terminology and remove redundancies.
- Algorithms can predict disease risk from individual records using **rule-based systems** and **predictive modeling**, increasing efficiency as data volume grows.

3. Drug Interactions

- NLP and machine learning detect **drug-drug interactions** from literature and adverse event reports.
- Datasets like **FAERS** and **VigiBase** are used to train deep learning systems.

4. Telemedicine

- AI enables **remote patient monitoring** through wearables and sensors.
- Chatbots are being explored for **mental health care**, though they raise ethical and privacy concerns.
- Especially beneficial for **elder care**, but with ongoing debates around privacy.

5. Workload Management

- AI automates **administrative tasks**, **coordinates care**, and helps prioritize patient needs—freeing healthcare workers to focus on direct care.

6. Clinical Applications

- **Cardiology**: AI predicts heart attacks (up to 90% accuracy), interprets echocardiograms, and supports early event detection via wearables.

- **Dermatology**: AI matches or exceeds dermatologist performance in image-based skin cancer diagnosis, but concerns exist about testing on diverse skin types.
- **Gastroenterology**: AI enhances **endoscopic detection** and predicts **colitis flare-ups** with ~80% accuracy.
- **Obstetrics/Gynecology**: AI aids in fetal monitoring and imaging diagnostics.
- **Infectious Diseases**: Used for outbreak tracking (e.g., COVID-19), detecting malaria, antimicrobial resistance, and more.
- **Musculoskeletal**: Algorithms identify knee pain causes missed by doctors, especially in underserved populations.
- **Neurology**: AI helps diagnose and predict Alzheimer's progression using MRI and deep learning models.
- **Oncology**: Applied in cancer diagnostics (e.g., breast, prostate) and treatment personalization using genetic/molecular data.
- **Ophthalmology**: AI is used for **diabetic retinopathy detection** and blindness prevention.
- **Pathology**: AI assists in cancer detection, slide analysis, and mutation prediction—enhancing efficiency and cost-effectiveness.
- **Primary Care**: AI supports decision-making and treatment planning, though few systems have been clinically validated.
- **Psychiatry**: AI is used for **predictive modeling**, chatbots, and screening, though concerns remain about bias and oversight.
- **Radiology**: Deep learning supports **image interpretation**, **noise reduction**, and **dose optimization**, particularly useful in mammography and CT/MRI scans.
- **Pharmacy**: AI aids in **drug discovery, delivery systems,** and **treatment personalization**.

7. Industry and Innovation

- AI in healthcare is driven by **big tech** and **startup ecosystems**:
    - **IBM Watson**, **Microsoft Hanover**, **Google DeepMind**, and **Tencent** focus on diagnostics and treatment predictions.
    - **Neuralink** develops brain implants for neuroprosthetics.
    - AI-powered robots (e.g., "Xiao Man", "Pepper") support patient interaction and diagnostics.
    - Chatbots like those by **Haptik** and **Infermedica** provided COVID-19 assessments.
- **AI in pharmacy** enables optimization of drug development and clinical trials.[7]

HEATH DATA PRIVACY

1) PERSONAL HEALTH INFORMATION

Personal Health Information (PHI) refers to any sensitive data related to an individual's health, including physical and mental health conditions, medical history, treatments, and personal identifiers. PHI also encompasses personal details such as names, contact information, genetic data, biometric identifiers (like fingerprints and facial images), and demographic information. This data is protected by laws like the **Health Insurance Portability and Accountability Act (HIPAA)** in the U.S., which mandates strict privacy regulations to prevent unauthorized access and disclosure.[8][9]

PHI can exist in electronic, written, or verbal forms and is typically managed by healthcare providers, insurance companies, and other healthcare-related entities. Unauthorized disclosure of PHI can have serious consequences, such as discrimination or harm. However, there are

[7] Artificial Intelligence in Healthcare available at https://en.wikipedia.org/wiki/Artificial_intelligence_in_healthcare, last visted on April 18,2025
[8] Personal Health Information, available at https://www.sciencedirect.com/topics/computer-science/personal-health-information, last visited on April 18,2025
[9] Protected Health Information , available at https://www.ncbi.nlm.nih.gov/books/NBK553131/, last visited at April 20, 2025

certain exceptions where PHI can be shared without patient consent, such as for public health purposes, legal proceedings, scientific research, or when there is a threat to someone's safety or health.

2) IMPORTANCE OF CONFIDENTIALITY AND INFORMED CONSENT

Confidentiality in healthcare is a crucial ethical and legal obligation that ensures a patient's personal information remains private and protected, even after death. It underpins the trust between healthcare providers and patients, promotes honest communication, preserves dignity, supports autonomous decision-making, and prevents misuse of sensitive data. While minors under 16 are generally entitled to confidentiality, their ability to consent depends on their maturity, based on the **Gillick competence** principle, which allows treatment without parental consent if the child fully understands the implications. If a child is not Gillick competent, the General Medical Council (GMC) allows disclosure to parents if it's in the child's best interest.

However, confidentiality is not absolute. It may be legally breached in specific situations such as when there is a serious threat to others, during public health crises, or when legally mandated (e.g., gunshot wounds, sexually transmitted diseases). The **Egdell case** highlighted that doctors may override confidentiality to protect third parties from serious harm. Technological advances demand additional safeguards for electronic records, such as password protection, encryption, audits, secure deletion, and remote wipe capabilities for mobile devices.[10]

Although there are no comprehensive data protection rules in India, confidentiality is governed by the **Indian Medical Council** (Professional Conduct, Etiquette and Ethics) **Regulations, 2002**.. The proposed **Digital Information Security in Healthcare Act (DISHA), 2018** aims to address this by giving patients full ownership of their digital health records. Still, privacy can be overridden in the public interest, as demonstrated in several landmark cases:

1. **Mr. X v. Hospital Z** – The Supreme Court held that the right to be informed about a life-threatening disease (HIV) outweighed the patient's right to privacy, especially when the disclosure served the public good.

[10] Personal Health Information, available at https://www.sciencedirect.com/topics/computer-science/personal-health-information, last visited on April 18,2025

2. **Mr. Surupsingh Hrya Naik v. State of Maharashtra (2007)** – The Bombay High Court ruled that the **Right to Information Act, 2005** can override the Medical Council's Code of Ethics when public interest is involved, particularly if the medical institution is state-run.

3. **Radiological & Imaging Association v. Union of India (2011)** – The Bombay High Court upheld the legality of monitoring mechanisms (like the Silent Observer) under the **Pre-Conception and Pre-Natal Diagnostic Techniques (PCPNDT) Act**, ruling that privacy rights could be restricted for compelling public interest, such as addressing the declining sex ratio.

Breaches of confidentiality—whether accidental, intentional, or systemic—can erode the provider-patient relationship, lead to poor health outcomes, and result in legal or professional penalties for healthcare providers. To minimize harm, breaches must be reported and addressed promptly.

In the end, protecting privacy and confidentiality in healthcare must be balanced with broader societal interests. Advancing legislation—such as completing the DISHA framework—and fostering cooperation between public and private stakeholders are crucial for creating a strong legal and ethical system that upholds patient rights while permitting limited, well-justified exceptions for the public benefit.

HEALTH RIGHTS

1) RIGHT TO PRIVACY

The right to privacy is a fundamental right that allows individuals to control how, when, and to what extent their personal information, including health data, is shared. In healthcare, patient privacy ensures that protected health information (PHI) is only disclosed to those involved in medical care or, with proper approval, for research purposes—often requiring anonymity and institutional review board (IRB) clearance. Broadly, privacy is a complex concept, shaped today by the interplay between technology and legal frameworks. With the rise of digital surveillance, smart devices, artificial intelligence (AI), Big Data, and biometrics, personal data is increasingly collected, analyzed, and commodified, raising ethical and legal concerns. This has led to greater focus on user consent, transparency, and control over personal data. Laws

like the EU's GDPR aim to safeguard data rights across borders. In India, the right to privacy, not explicitly stated in the Constitution, is inferred from Article 21, which guarantees life and personal liberty. The Supreme Court has recognized privacy as implicit within this right but allows exceptions in cases of public interest, especially in sensitive issues like matrimonial disputes, child custody, or when health conditions (e.g., HIV) may impact others. In such cases, medical examinations or DNA tests may be permitted without consent, as long as they serve a greater public or legal interest.[11][12]

2) RIGHT TO HEALTH

The **right to health** is a fundamental human right recognized internationally. It was first outlined in the **1946 Constitution of the World Health Organization (WHO)** and legally reinforced in **Article 12 of the International Covenant on Economic, Social and Cultural Rights (1966)**. It guarantees every individual the right to the **highest attainable standard of physical and mental health** and encompasses both **healthcare services** and the **underlying social determinants** of health—like clean water, nutritious food, housing, education, and a healthy environment.[13]

The right to health is structured around **four core elements**:

1. **Availability** – Sufficient quantity of health services and facilities must exist.

2. **Accessibility** – Healthcare services should be available to all individuals without discrimination, ensuring equal physical, financial, and informational access..

3. **Acceptability** – Healthcare services should align with cultural values and adhere to established medical ethics.

4. **Quality** – Health care must be scientifically and medically sound.[14]

[11] Medical Information Privacy,available at https://www.radiologyinfo.org/en/info/article-patient-privacy, last visited on April16, 2025
[12] Dr. Vivek Kumar Gupta, "The Right to Privacy in India: A Comparative Study with Global Implications" *International Journal of Law, Justice and Jurisprudence* (2024). https://www.lawjournal.info/article/114/4-1-41-748.pdf
[13] Agnes Binagwaho and Kedest Mathewos 2, "The Right to Health" *Health and Human Right Journal* (2023). https://pmc.ncbi.nlm.nih.gov/articles/PMC9973503/
[14] Human Rights, available at https://www.who.int/news-room/fact-sheets/detail/human-rights-and-health, last visited on April 14,2025

This right includes **freedoms** (such as bodily autonomy and freedom from non-consensual treatment) and **entitlements** (like access to essential health services and conditions that support health).

Countries that ratify international treaties have obligations to:

- **Respect** the right by avoiding policies that restrict access.
- **Protect** by regulating private actors to prevent rights violations.
- **Fulfil** by implementing laws, policies, and resources to support health services and systems.

A **Human Rights-Based Approach (HRBA)** to health requires embedding principles like **non-discrimination, participation, accountability**, and **equality** into health systems. It promotes **equity** by prioritizing the needs of marginalized and vulnerable groups, using an **intersectional approach** to address overlapping forms of exclusion (e.g., based on gender, race, disability, or poverty).

The concept of **accompaniment**, promoted by Paul Farmer and Heidi Behforouz, emphasizes walking alongside patients—supporting not only their medical needs but also addressing barriers such as poverty, transportation, and food insecurity. This approach recognizes that **healthcare alone is insufficient** unless structural and social barriers are also addressed.

International treaties, including those on the rights of women, children, migrants, and persons with disabilities, reinforce this right. **WHO** supports countries by offering policy guidance, building capacity, advocating for equitable access, and encouraging **Universal Health Coverage (UHC)** grounded in **primary healthcare**, to ensure no one is left behind in the pursuit of health and well-being.

EXISTING LEGAL FRAMEWORKS

India's data protection landscape underwent significant changes with the passing of the **Digital Personal Data Protection Act, 2023 (DPDP Act)**, which aims to address data privacy concerns in the country. Prior to this, India's data protection framework was governed by the **Information Technology Act, 2000**, with its accompanying Privacy Rules of 2011. The DPDP

Act, however, represents a major shift toward stronger and more comprehensive protection for digital personal data. The Act outlines principles such as lawful data processing, transparency, minimal data collection, and strict safeguards against breaches. It gives individuals rights to access, correct, erase, and withdraw consent for their data, and mandates the formation of the **Data Protection Board of India** to oversee enforcement. Although the Act has addressed digital data, it does not cover non-digital or non-personal data, and its rules are still being refined with public consultation.[15]

Globally, data protection regulations have been developing in response to the expanding digital footprint. A leading example is the **European Union's General Data Protection Regulation (GDPR)**, which took effect in 2018. The GDPR provides a strong legal structure for safeguarding personal data, granting individuals rights to know how their data is used, and to access, correct, delete, or limit its processing. It also highlights the importance of data portability and requires organizations engaged in large-scale data handling to appoint Data Protection Officers (DPOs) to ensure compliance. Because of its extra-territorial reach, the GDPR applies to any entity around the world that processes the personal data of EU residents.[16]

In the **United States**, **HIPAA (Health Insurance Portability and Accountability Act)** plays a critical role in safeguarding healthcare data. Enacted in 1996, HIPAA's **Privacy Rule** governs the use and disclosure of protected health information (PHI) by healthcare providers, insurers, and other entities. It grants individuals rights over their health data while balancing privacy with the need for quality healthcare. HIPAA's **Security Rule** focuses on electronic PHI, ensuring its confidentiality, integrity, and security, with penalties for violations. HIPAA's comprehensive framework underpins trust in the U.S. healthcare system, particularly with rising cyber threats.[17]

The **EU Artificial Intelligence (AI) Act**, adopted in 2024, marks the first comprehensive regulatory framework for AI, applying a **risk-based approach** to categorize AI systems. High-risk AI systems, such as those in healthcare, must meet strict requirements and undergo

[15] Data Protection and Data Privacy Laws in India, available at https://blog.ipleaders.in/data-protection-laws-in-india-2/, last visited on April12,2025
[16] What is GDPR , The EUs new data protection Law, available at https://gdpr.eu/what-is-gdpr/, last visited at April16,2025
[17] Health Insurance Portability and Accountability Act 1996 (HIPAA), available at https://www.cdc.gov/phlp/php/resources/health-insurance-portability-and-accountability-act-of-1996-hipaa.html#:~:text=The%20Health%20Insurance%20Portability%20and,from%20disclosure%20without%20patient's%20consent., last visited on April 17,2025

rigorous assessments. AI applications that manipulate behavior or involve biometric surveillance are largely banned. The law promotes AI innovation through regulatory sandboxes and transparency obligations for generative AI tools like ChatGPT, which must label AI-generated content and avoid producing illegal material.[18]

At the **global level**, frameworks like the **OECD AI Principles** and **NIST AI Risk Management Framework** guide countries in developing policies for responsible AI use. The **OECD Framework for the Classification of AI Systems** encourages risk assessments across dimensions like economic impact, data inputs, and human impact. NIST and ISO frameworks provide detailed guidance on AI governance, focusing on audit mechanisms, lifecycle risk management, and governance structures.[19]

Together, these international frameworks—GDPR, HIPAA, the EU AI Act, and the OECD/NIST/ISO standards—represent a unified effort to protect individual rights and ensure ethical data processing and AI use across the globe. While tailored to specific regions and sectors, these laws share a common goal: to safeguard privacy, promote transparency, and support the ethical deployment of technologies. In India, the DPDP Act is a step toward aligning with these global standards, addressing data protection challenges in the digital age, and enabling innovation while ensuring security and privacy.

LEGAL CHALLENGES AND GAPS

The use of AI in healthcare brings several challenges, especially concerning data security, privacy, regulation, and ethics. Because AI depends on large volumes of highly sensitive health data, medical institutions become attractive targets for cyberattacks. Strong cybersecurity practices—such as encryption, tiered access controls, and routine security assessments—are vital to protect patient information. Adhering to legal standards like India's Digital Personal Data Protection Act (DPDP Act) and global frameworks such as HIPAA and GDPR is also

[18] "EU AI Act: First Regulation on Artificial Intelligence" *The Use of Artificial Intelligence in the EU is Regulated by the AI Act, the World's First Comprehensive AI Law. Find Out How It Protects You* (2023). https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence

[19] Bex Evans, "Managing the Risks Associated with AI Development Can Be Challenging but Following the OECD's Set of Standards Can Give You the Framework to Help Guide Your Efforts" *Approaching the OECD Framework for the Classification of AI Systems* (2023). https://www.onetrust.com/blog/approaching-the-oecd-framework-for-the-classification-of-ai-systems/

crucial. In addition, implementing well-defined ethical guidelines for data use ensures that AI technologies are deployed safely and responsibly within healthcare systems.[20]

In India, there is significant regulatory and legal uncertainty regarding AI use in healthcare due to the absence of AI-specific laws. This gap makes it difficult for healthcare providers, developers, and institutions to understand compliance requirements, which can lead to inconsistent implementation and potential harm. Countries like the U.S. and members of the EU have established regulatory frameworks like the **FDA** and **European Medical Device Regulation (MDR)**, which categorize AI tools as medical devices based on their purpose and risk level, providing structured approval processes and accountability. India could benefit from creating a dedicated regulatory body for AI in healthcare to establish clear guidelines and ensure patient safety.

AI's use in healthcare raises important ethical concerns, especially around informed consent, fairness, and transparency. Many AI systems function as "black boxes," making it difficult for both clinicians and patients to understand their decision-making processes, undermining trust. Clear communication about how AI works, along with regular bias audits, inclusive datasets, and transparent algorithmic development, can help address these concerns. Landmark cases like **Sorrell v. IMS Health, Inc.** (U.S.) and **Griswold v. Connecticut** (1965) have emphasized the need for transparency in healthcare decisions and the patient's right to control how their health data is used, laying a foundation for ethical AI deployment in healthcare.

Informed consent in AI-driven healthcare is particularly complex due to the opacity of many AI systems. Patients must be provided with clear and comprehensible explanations about how AI influences their medical decisions, how their data is being used, and how AI systems function. Transparent data usage policies, disclosures, and educational tools are necessary to ensure that patients can make informed decisions, fostering trust in AI-assisted healthcare.[21][22]

Liability and accountability in AI-driven healthcare remain complicated because traditional legal frameworks do not fully address the complexities of autonomous systems. In the U.S.,

[20] Kristen Luong, "Challenges of AI Integration in Healthcare" (2024) https://www.ominext.com/en/blog/challenges-of-ai-integration-in-healthcare

[21] Dmitry Enikeev, "Legal and Ethical Consideration in Artificial Intelligence in Healthcare: Who Takes Responsibility?" 9 (2022). https://www.frontiersin.org/journals/surgery/articles/10.3389/fsurg.2022.862322/full

[22] Sorrell v. IMS Health, available at https://supreme.justia.com/cases/federal/us/564/552/, last visited on April 15,2025

clinicians can still be held liable for harm even when AI tools are involved in decision-making. Cases like **Jones v. the American Medical Association** (2020) highlight the principle that healthcare providers must exercise professional judgment and not blindly rely on AI recommendations. Europe is exploring risk-based liability models to fairly distribute accountability, and India must develop a balanced legal framework to clarify responsibilities and ensure fair compensation.[23]

The rise of AI and IoT in healthcare has significantly increased the vulnerability of healthcare systems to cyberattacks. Cases like **Dr. Jagdish Tiwari v. Union of India (2021)**, related to data breaches, emphasize the responsibility of healthcare institutions to ensure robust cybersecurity measures to protect patient data. The landmark **K.S. Puttaswamy v. Union of India (2017)** decision, which upheld the right to privacy, also set a precedent for how health data should be protected in India.[24]

Currently, India lacks a dedicated regulatory framework for AI in healthcare, which leads to uncertainty around patient safety and accountability. Drawing from international models like the **FDA** in the U.S. and **GDPR** in Europe, India can create a regulatory structure that ensures patient protection, promotes transparency, and allows for safe AI integration in healthcare. This will provide clear standards for developers, institutions, and patients, fostering the responsible use of AI in India's healthcare system.[25]

CONCLUSION

The rapid integration of Artificial Intelligence in healthcare has created significant opportunities for improved diagnosis, personalized treatment, and efficient healthcare delivery. However, the growing dependence on vast amounts of sensitive health data raises serious legal, ethical, and regulatory concerns. Existing laws such as the GDPR, HIPAA, and India's DPDP Act provide important protections, but they do not fully address the unique challenges posed by AI—particularly issues related to algorithmic transparency, informed consent, liability, and

[23] Jones v. the American Medical Association, available at https://www.courtlistener.com/opinion/9381042/jones-v-association-of-american-medical-colleges/, last visited at April 15,2025

[24] State of UP and Anr v. Jagdish Saran Agarwal& Ors, available at https://blog.ipleaders.in/state-of-up-anr-v-jagdish-saran-agrawal-ors-case-analysis/, last visited at April 15, 2025

[25] Kavitha Palaniappan 1 and , Elaine Yan Ting Lin, "Gaps in the Global Regulatory Frameworks for the Use of Artificial Intelligence (AI) in the Healthcare Services Sector and Key Recommendations" 9 (2024) . https://pmc.ncbi.nlm.nih.gov/articles/PMC11394803/

data ownership. The absence of clear, AI-specific regulations in India further contributes to uncertainty for healthcare providers, developers, and patients, increasing the risk of misuse and unequal access to AI-driven services.

To move forward responsibly, it is crucial to develop comprehensive legal and ethical frameworks that balance innovation with patient rights. This includes establishing dedicated regulatory bodies, enforcing strict cybersecurity requirements, ensuring transparent and bias-free AI systems, and strengthening mechanisms for informed consent. International models such as the EU AI Act and FDA guidelines offer valuable examples that India can adapt to its healthcare ecosystem. Ultimately, safeguarding health data, ensuring equitable access, and maintaining accountability will be essential for building public trust. A coherent, forward-looking regulatory approach will enable India to harness AI's transformative potential while protecting the fundamental rights and dignity of individuals.