

Summary Document:

Ethics, Legal, and Regulatory Aspects of AI in Healthcare

WMA Educational Webinar - Medical Technologies Workgroup – 27 February 2025

Introduction

This document provides a summary of key points discussed in the second installment of the WMA Educational Webinars on Artificial Intelligence in Medicine. The session focused on ethical, legal, and regulatory aspects of AI in healthcare, exploring patient rights, accountability, and risk mitigation strategies.

Key Topics Discussed

1. Ethical Considerations in AI-Powered Healthcare

- **Autonomy & the Doctor-Patient Relationship**
 - AI can either empower patients by enhancing autonomy or reduce it if decisions are overly dependent on AI-generated recommendations.
 - Different global perspectives influence ethical views (e.g., Western consumerism vs. paternalistic models in China).
- **Informed Consent Challenges**
 - Traditional informed consent involves doctor-patient discussions.
 - AI's "black-box" nature makes it difficult for physicians to explain how AI arrived at a decision, raising concerns about whether true informed consent is possible.
 - Some legal frameworks (e.g., EU regulations) mandate disclosure when AI is used in patient care, while others (e.g., US law) do not explicitly require it.
 - The level of AI intervention significantly impacts informed consent.
 - It's essential to consider whether patients should be informed about AI use in their care, balancing transparency with the risk of overwhelming them with information.

- The "explainability" of AI is crucial when AI significantly influences healthcare decisions.
- **Loss of Human Touch in Medicine**
 - AI-driven healthcare may reduce direct physician-patient interaction, leading to concerns about dehumanization.
 - There is potential for over-reliance on AI, which can introduce confirmation bias.

2. Legal and Regulatory Challenges for AI in Healthcare

- **Liability & Accountability**
 - Three primary perspectives on liability:
 - **Physician Liability** – Doctors are traditionally held accountable if AI-driven decisions harm patients.
 - **Institutional Liability** – Hospitals may be responsible if they implement AI tools in ways that contribute to harm.
 - **Developer Liability** – AI manufacturers and software developers could be held accountable, though legal precedents are still evolving.
 - In the future, AI could potentially influence the standard of care, shifting liability from doctors to institutions or developers.
- **Regulating AI Across Its Lifecycle**
 - Three key stages where regulation is needed:
 - **Research & Development:** Ensuring ethical AI design, data bias mitigation, and proper validation.
 - **Market Approval:** Regulatory approvals vary across countries (e.g., FDA in the US, MDR in the EU, SFDA in Saudi Arabia).
 - **Post-Market Oversight:** Mechanisms to hold AI accountable after deployment (e.g., WHO global governance frameworks).
- **Public Sector vs. Private Sector Regulation**
 - Different countries adopt different approaches:
 - Free-market-driven approach with minimal AI regulation to encourage innovation.
 - Strong regulatory frameworks prioritizing patient protection.
 - AI governance is largely centralized, with government oversight playing a key role.
- **Documentation:** Hospitals may need subcommittees to set internal documentation standards for AI use.
- **Best practices:** Until clear guidelines emerge, physicians must exercise clinical judgment and understand the standard of care, as relying solely on AI may not be a legal defense.

Privacy and Rights in AI-Assisted Healthcare

- **Data privacy laws:** Legal frameworks, such as GDPR, impact AI development and deployment, but they also have gaps, such as exceptions for research and public benefit.
- **Data security:** Blockchain technology may offer a path to securing health data, with systems allowing patients to approve data access requests.
- **Patient data ownership:** Patients should maintain ownership over their data, raising questions about data removal from AI systems and models. Balancing the desire to create comprehensive AI systems with the need for patient autonomy and control is a real tension.
- **Intellectual property:** AI developers may protect their algorithms as trade secrets, complicating transparency and regulation.
- **Global variability:** There is tremendous variation in what developers do to ensure data is unbiased and patients have recourse if harm is caused.

3. Risk Mitigation Strategies for AI in Clinical Practice

- **Best Practices for Physicians Using AI Tools**
 - Physicians should document AI-assisted decision-making in patient records.
 - Human-in-the-loop (HITL) models should ensure physician oversight in AI-generated recommendations.
 - AI tools should augment, not replace clinical judgment.
- **Patient Data Protection & Security**
 - AI relies heavily on patient data, raising privacy concerns.
 - **Key data risks:**
 - **Bias in Training Data** – AI can perpetuate biases if trained on unrepresentative datasets.
 - **Data Privacy** – Regulations in different regions attempt to protect patient rights, but gaps remain.
 - **Security Threats** – Blockchain technology is being explored for securing patient data.
 - **Should patients have the right to remove their data from AI models?**
 - While AI requires large datasets, patients should maintain ownership and be informed about how their data is used.
- **Human Oversight & AI Transparency**
 - AI should not function as an independent actor in patient care. Instead:
 - **Explainability:** AI systems must provide reasoning for decisions where possible.
 - **Regulatory Alignment:** Healthcare institutions should align AI usage with existing medical guidelines.

- Ethical Oversight: AI should be reviewed by hospital ethics committees before clinical deployment.

Closing Thoughts & Next Steps

- AI in healthcare presents unprecedented opportunities and challenges.
- Legal and ethical frameworks are still evolving, with no single global standard yet.
- Clinicians must remain engaged in discussions about AI governance to ensure safe, ethical, and effective AI integration.

Next Webinar in the Series

 March 27, 2025 – *"Current and Future Applications of AI in Medicine"*

Speaker Introduction: TBD

Topics will include:

- Breakthrough AI applications in diagnostics and treatment
- AI's role in precision medicine and drug discovery
- Challenges in AI adoption across healthcare settings

Feedback & Further Reading

 Feedback Form: Please share your thoughts via the [link](#).

 Recommended Reading:

- *Research Handbook on Health, AI, and the Law* – Available online (Open Access).
- *Informed Consent & AI in Healthcare* – Article by Prof. Glenn Cohen.

For further inquiries, contact WMA at wma@wma.net.

FAQs:

Ethical, Legal, and Regulatory Aspects of AI in Healthcare

1. What are the primary ethical considerations when using AI in medicine?

Core ethical principles like autonomy, beneficence, non-maleficence, and justice are crucial. AI's impact on the doctor-patient relationship is a key concern. Does AI increase patient autonomy by giving them more control over their data and care, or does it lead to a more paternalistic dynamic where doctors overly rely on AI-driven insights? There is also a risk of ceding too much authority to AI developers who set the standards for AI device usage if regulations are inadequate. The potential loss of the human touch is also a major consideration and must be addressed to maintain patients' trust and the therapeutic alliance with their doctors.

2. How does AI impact informed consent in healthcare?

The traditional informed consent process involves a doctor explaining treatment options and the reasoning behind their recommendations to a patient. When AI is involved, especially in decision-making, the explainability of the AI's reasoning becomes crucial. If the AI's decision-making process is too complex to understand (even for its developers), how can a doctor adequately explain the basis of the recommendation to a patient, fulfilling the requirements for informed consent? The level of AI involvement in the medical decision greatly impacts informed consent. Transparency about the AI's role and limitations is essential.

3. Should patients be informed about the use of AI in their clinical care, and to what extent?

There are varying opinions. Some argue that informing patients about every instance of AI use (e.g., in radiology for dose reduction) would be overwhelming and ineffective. Others believe transparency is necessary, especially when AI significantly influences treatment recommendations.

4. Who is liable if a patient is harmed by AI in healthcare?

Liability is a complex issue with several potential actors: the doctor, the healthcare institution (hospital/clinic), the AI developer, and even (controversially) the patient. Currently, existing tort law dictates that doctors are responsible if their actions fall below the standard of care, regardless of whether AI was used. Hospitals may also be liable under vicarious liability if doctors are hospital employees. The liability of AI developers is less clear, but is something that is beginning to garner more attention. It is likely to increase in prominence in coming years. The implementer, who connects the system, validates the data, and turns things on, also carries some shared liability.

5. What steps can healthcare professionals take to mitigate liability risks associated with AI?

As of right now, clinicians must take responsibility for medical decisions even when relying on AI, but in the future this may not always be the case. AI setting the standards of care could shift liability elsewhere. Clinical judgment is paramount. Careful documentation of AI's role in decision-making is crucial. Hospitals should form subcommittees to establish internal principles, guidelines, and standards for AI implementation and documentation.

6. What aspects of AI in healthcare should be regulated, and why?

Regulation is needed across AI's entire life cycle, from research and development to deployment and post-market surveillance.

Areas for regulation include:

- **Research and Development:** Ensuring developers adhere to best practices, such as engaging with patient groups and using appropriate data sources to mitigate against biases.
- **Market Approval:** Establishing clear requirements for regulators to assess AI devices, not just regarding risk, but also issues like medical liability and informed consent.
- **Clinical Practice:** Creating mechanisms to ensure patients can exercise their medical law rights (informed consent, liability) when AI is used in their care.

7. What are the potential risks of AI to the physician-patient relationship?

AI could potentially dehumanize healthcare by leading to over-reliance on technology and a loss of human touch. Doctors may become overly reliant on AI, exhibiting confirmation bias and potentially overlooking crucial information. There is concern AI may lead doctors to become "lazy" and simply rely on AI decisions without question. It is critical to consciously guard against that.

8. How can patient data be secured and ethically used in AI systems?

Data bias, privacy concerns, and security vulnerabilities must be addressed.

- **Data Bias:** Careful data selection in the research phase is critical to avoid building AI systems that are ineffective or discriminatory.
- **Data Privacy:** Existing data protection laws (e.g., GDPR) provide a framework, but local authorities should supplement these with healthcare-specific guidelines.
- **Data Security:** Technologies like blockchain can enhance data security by giving patients greater control over who accesses their data. The issue of intellectual property rights surrounding algorithms can complicate data privacy regulations.