

AI ETHICS IN HEALTHCARE

Coursework_COMScDS252P-010 – Amalka Chandrasiri

A. HEALTHCARE DATA PRIVACY

Healthcare data contains highly personal information, including an individual's identity, medical history, genetic details, insurance records, and diagnostic results. Due to the sensitive nature of this data, it must be protected using strong security measures. However, protection is not limited to technical controls alone; it also involves ethical responsibility in how the data is collected, shared, and used. Misuse of healthcare data can lead to social stigma, discrimination, exploitation, and psychological harm. Because of this sensitivity, healthcare providers have a moral and professional obligation to handle data responsibly and maintain patient trust.

HIPAA - Health Insurance Portability and Accountability

This act was established in the United States to define national standards for protecting Personal Health Information (PHI). It regulates how personal health data can be used and disclosed. The act also emphasizes security requirements such as encryption, access control, and audit mechanisms to protect data. These requirements create an ethical foundation that ensures patient data remains confidential, accurate, and accessible only to authorized individuals.

GDPR - General Data Protection Regulation

The General Data Protection Regulation (GDPR) classifies health data as a special category that requires stronger protection than general business data. It emphasizes obtaining explicit consent before processing personal information and grants individuals' rights such as access, rectification, and deletion. GDPR also introduces the "right to be forgotten," allowing individuals to request the removal of their data when it is no longer necessary. While medical records may be retained for clinical history and research that benefits society, individuals still have the right to request deletion if they believe their data is being used unethically or unlawfully.

Even when personal data is deleted or anonymized, simple de-identification is often not sufficient in healthcare contexts. Healthcare data, like many other data types, can potentially be re-identified through links with external datasets, the use of AI-based inference techniques, and the presence of high-dimensional data patterns. As a result, privacy risks may still exist even after direct identifiers such as names or identification numbers are removed. This highlights the need for stronger anonymization techniques and continuous ethical oversight when handling healthcare data.

B. ALGORITHMIC BIAS IN MEDICAL AI

Algorithmic bias is a major concern in medical AI used for research, diagnosis, and clinical decision-making. Since AI models learn from data, any bias in the training data can lead to inaccurate or unfair outcomes. Bias can occur at multiple stages. At the data level, training datasets may not adequately represent all demographic groups, causing models to reproduce existing inequalities. Bias can also emerge at the design level, where selected features or proxy variables unintentionally encode social disparities.

A well-known study published in *Science* showed that a U.S. hospital risk prediction model underestimated the health needs of Black patients because it used healthcare spending as a proxy for illness severity (Obermeyer et al., 2019). Historical underinvestment led to systematically lower risk scores and reduced access to care.

Even when AI models appear accurate and neutral, improper interpretation by health care providers can still cause harm. Therefore, AI models should be used as supportive decision-making tools under the supervision of clinical expertise, rather than as replacements for professional judgment.

C. ETHICAL DECISION FRAMEWORK FOR HEALTHCARE DATA SCIENTISTS

Ethical Checklist for Healthcare Data Scientists

When applying data science in healthcare, the risks are much higher because errors can directly affect human lives. It is essential to ensure training data represents real patient populations, protect patient privacy over model performance, and keep clinicians involved in all high-impact decisions. Models should be continuously monitored after deployment, their limitations clearly communicated, and their potential harm carefully evaluated before use.

Right to Explanation

The Right to Explanation means patients and health care providers should understand why an AI system produced a particular medical recommendation. Decisions should never be justified solely by “the system said so,” ensuring transparency and accountability, especially under regulations such as General Data Protection Regulation (GDPR).

Importance of Model Interpretability

Model interpretability is critical in healthcare because clinicians must understand why a prediction was made. This builds trust, improves patient safety, and helps doctors take appropriate and informed treatment actions.

D. STAKEHOLDER IMPACT ANALYSIS

Patients:

AI can improve diagnosis speed and enable personalized treatment, but it also raises concerns about privacy, data misuse, and decisions made by systems that patients cannot question. Clear consent, transparency, and opt-out options are essential to protect patient trust.

Healthcare Providers:

AI supports clinicians by reducing errors and assisting decision-making, but it also introduces uncertainty around responsibility and liability. Proper training is needed so clinicians understand AI outputs and use them as support rather than replacement.

Researchers and Developers:

Developers have a responsibility to ensure fairness, transparency, and safety. Models must be tested for bias and failure cases before deployment.

Policy Recommendation:

A transparent *Clinical AI Passport* can help balance trust, accountability, and safety across all stakeholders. This passport would act as a standardized record describing how an AI system was trained, its intended medical use, known limitations, and confidence levels. Making this information accessible to clinicians and patients improves transparency, supports informed decision-making, and encourages responsible deployment of AI in healthcare.