Question 03 – AI Ethics in Health Care Sector

1. Healthcare Data Privacy Challenges

Health care data privacy focuses on protecting data, networks & computers that belongs to healthcare providers and companies. There are several healthcare laws in different counties. One of the most important and strong health care privacy acts is Health Insurance Portability & Accountability Act (HIPAA).

Health care private laws in different countries:

- European Union – General Data Protection Regulation (GDPR)
  Empowers people with considerable control over their health information, focusing on consent and data portability.
- US - Health Insurance Portability & Accountability Act (HIPAA)
  governs the use and disclosure of protected health information by covered entities.
  Aims to protect patients' privacy and supply health information access for quality care and public health.
- China – Personal Information Protection Law (PIPL)
  An enforcement law requiring agreement to process personal data, including medical information
- Canada – Consumer Privacy Protection Act (CPPA)
  Focuses on clear communication on the usage of health data and strong health information technology.
- India – Digital Personal Data Protection Act (DPDP)

GDPR is strong for EU personal data protection but adds extra weight on healthcare data, which requires more regulations, technical measures, and administrative controls. Other countries have additional requirements on top of GDPR (e.g., HIPAA in the US, PIPL in China, India's DPDP Act). These regimes all differ on sanctioned uses, breach notification requirements, cross-border transfer rules, and the manner in which de-identification is determined. So, getting GDPR compliant doesn't necessarily get you compliant with other jurisdictions' legal or practical ones

Special healthcare data challenges that go beyond GDPR:

- Different legal frameworks and extra covered acts: - HIPPA governs the use and disclosure of protected health information by covered entities. Different requirements for consent, lawful basis and cross border transfers are enforced by several counties.

- Re – identification risk - Health data combined with auxiliary datasets can re-identify individuals even after de-identification. Genomic and rare-disease data are nearly impossible to anonymize. De-identified data may still be personal under some laws or ethically not safe to share.

- Cross border transfer complexity – PIPL and DPDP add conditions for transfers but GDPR doesn’t do this. It can block cloud hosting or internal researches. This is a matter because some multi side studies requires permissions.

HIPAA Vs GDPR Comparison

	HIPAA	GDPR
Scope	Applied to covered entities	Applied to all organizations
Protected Data	Protected Health Information (PHI)	Personal data
Laws	No Lawful basis	Required lawful basis

2. Algorithm Bias in Medical AI

Sources of bias in medical data set: -

- Demographic bias –Women, children, older people, or minority ethnic populations underrepresented in training data.
  Example: There are lighter skin tone biases in some imaging datasets (e.g., radiology, dermatology).
- Geographic bias - Data from a single hospital, geographic area, or nation will not always be extrapolatable to global populations.
  Example: U.S. or European hospital training data models will not be effective in African or Asian environments due to differences in disease patterns and geographical difference.
- Socioeconomic bias - Poorly insured patients may have late diagnosis, missing records, or lack of access to care — compromising data quality.
  Example: Insurance-based data may overcount those with stable healthcare access and undercount the uninsured

How bias medical AI perpetuates health disparities: -

- Diagnostic disparities: A less precise AI system for particular demographic groups may widen health disparities (e.g., delayed diagnosis of cancer in minorities).
- Resource allocation bias: Decision-making algorithms allocating which patients need more care and which patients need less care.

- Trust erosion: Populations that are subjected to biased outputs will be disillusioned with medical AI systems, which in turn can lead to increased disengagement with the healthcare system

Real world examples: -

- Skin cancer screening (dermatology AI)
- Pulse oximeters
- Risk prediction algorithm in the United States (2019 study, Obermeyer et al.)

Fairness metrics for healthcare algorithms: -

- Demographic parity: Proportions of predictions must be evenly distributed over groups (e.g., proportional referral rates for men vs. women).
- Equal opportunity: True positive rates (sensitivity) should be similar across groups.
- Equalized odds: Both false positive and false negative rates should be even across groups.
- Calibration within groups: Predicted probabilities should be calibrated to outcomes within each group.

Methods to detect and Reduce Bias AI

- Methods to Detect –
  check the demographic, geographic, socioeconomics representations of the dataset.
  Create bias dashboards to monitor fairness metrics over time
  Measure model accuracy by evaluating subgroups

- Methods to Reduce –
  collect more diverse data
  Careful throughout the validation
  Re – weighted the groups which are underrepresented
  Fairness constrained training

3. Ethical Decision-Making Framework

Medical data science initiatives need to have a systematic ethical approach that guarantees that technological innovation is aligned with the rights of patients and social accountability. An operative framework begins with an ethical checklist that comprises complying with healthcare privacy legalization such as HIPAA in the US and GDPR in Europe Union, robust data governance, and bias testing by demographic segments, and privacy protection. This checklist forms the foundation for ethical project evaluation and accountability.

Step 1 – Data collection and governance

- Is there a lawful basis or secondary use?
- Did you meet legal compliance (HIPAA or GDPR or any other)
- Have you pay you attention to minimizing the data?
- Is there any documentary describe about Who, how and why did they collect data
- Have you investigated that about the geographic, demographic and socioeconomic representation in the dataset

Step 2 – Data processing and modeling

- Are you testing stratified performance across subgroups (to check bias and fairness)?
- Did you apply privacy-preserving approaches like anonymization, differential privacy, federated learning?
- Are there any data sharing agreements with collaborators?
- Are your algorithms explainable and auditable?

Step 3 – Development

- Is there a right to explanation procedure for both clinicians and patients?
- Is there ongoing monitoring, feedback and model training system?
- Have you address harms of false positive or false negative across various groups

Health care data science ethical framework should be:

- Lawful and fair
- Privat and secure
- Transparent and well explainable
- Continuous evaluation and time to time monitoring
- Bias detection and fairness

4. Stakeholder Impact Analysis

Healthcare AI impacts different stakeholders in different manners. For patients, AI promises to provide faster diagnoses, personalized treatment, and preventive care but promises privacy invasion, opacity, and bias. For medical professionals, AI promises efficiency gains and clinical decision support but promises the erosion of professional judgment through algorithm over-reliance or incorrect interpretation. Researchers and data scientists are given high-leverage tools and high-volume data but are burdened with ethical responsibilities to design systems that are fair, transparent, and privacy-preserving.

Besides individual stakeholders, AI has significant global, social, and economic effects. As much as it can reduce costs and improve access, unequal technology availability may aggravate existing disparities, especially between high- and low-resource settings. Global health equity requires inclusive data sets, international collaboration, and responsive models to address heterogeneity. Equally poised is integrating innovation with accountability, where AI improves patient trust, provider competence, and universal healthcare outcomes.