COMScDS252P-013

A. Healthcare Data Privacy

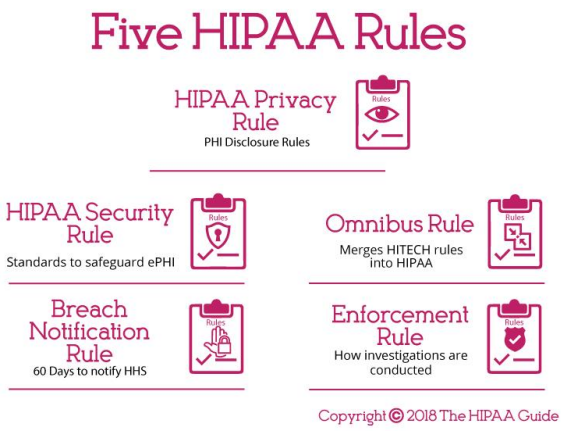
HIPAA

The health Insurance Portability and Acoountability Act of 1996.

This is a United States Federal Law which is to protect sensitive patient health information from unauthorised disclosure.

This covers and governs many entities like Healthcare providers, Hospitals, Private Dispensaries and Laboratories.

There are 5 key components of this rule



https://www.hipaaguide.net/hipaa-for-dummies/

HIPAA is enforced by the Department of Health and Hunan Services for Civil Rights.

People in this context get benefited by the strong policies of the act, so individuals have the right to know who has accessed their information and take necessary actions and counter-actions to protect their rights.

GDPR

The General Data Protection Regulation.

European Unions's strict, comprehensive data privacy law which is impact on European Union and European Economic areas.

This act is effective since 2018 May 25th.

https://thelegalschool.in/blog/gdpr-principles

GDPR aspcts:

Applicability: the law is applied to all small, medium and large level enterprises despite the size of the organization. This policy ensures, the data should be handled with utmost responsibility

Core rights :

1. Individual rights
2. Access to data
3. Right to be forgotten : (Data should be erased when not needed anymore)

4. Data Portability

Compare and Contrast

While HIPAA focuses on protecting personal health information in healthcare sector, GDPR got a broader coverage consists of health information protection, data erasure(right to be forgotten), data minimization and more.

In geographical context, HIPAA works on United States and associated areas. But GDPR covers most of the European Continent and it has shapen the global standards. This mechanism is known as Brussels effect which adapted worldwide.

Challenges:

Overlapping compliance is complex for global organizations; GDPR has stricter consent and deletion rights than HIPAA, which lacks a deletion mandate.

Anonymization Challenges:

Simple de-identification like removing names or telephone numbers is insufficient due to re-identification risks via linking with auxiliary data (eg:- zip code, gender, birth date can re-identify people).

Why Stricter Protection Is Needed for Healthcare Data?

Health data is extremely sensitive, disclosing traits like mental health or genetics that, if compromised, could cause harm, stigma, or discrimination. It has a direct connection to patient care and calls for ethical protections that go beyond basic personal information.

particular instances:

i. Breach of genetic data may result in insurance rejections or discrimination at work on the basis of predispositions (eg:- risk of hereditary diseases).

ii. A data leak exposing mental health records could lead to targeted exploitation (predatory marketing, for example) or social stigma.

B. Algorithmic Bias in Medical AI

Sources of Bias :

- Under-representation in Training Data: Datasets often lack diversity in demographics

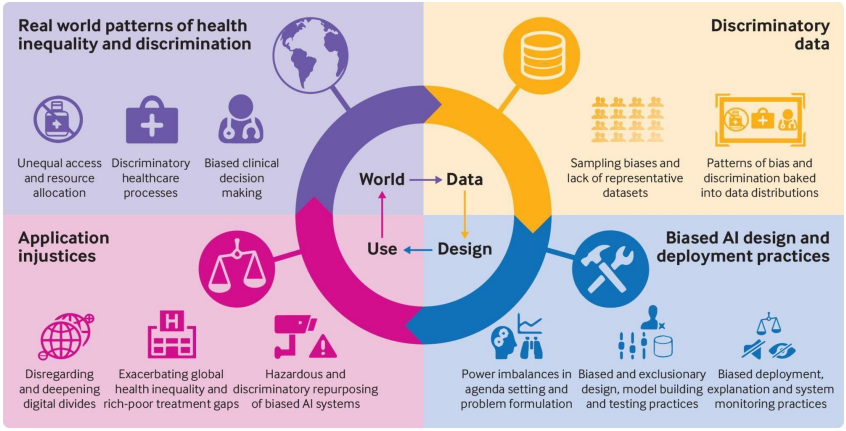
  eg:- over-represent white males, leading to poor performance for underrepresented groups like women or ethnic minorities like tribes.

- Geographic/Socioeconomic Collection Bias:

  Data from urban, high-income and high-population areas (eg:- mostly US/China/Europe datasets) ignores rural or low-resource populations, causing global inequities.

- Historical Treatment Biases:

  AI learns from past data reflecting systemic inequalities (eg:- unequal care access for minorities), perpetuating disparities in predictions.



https://ubisglobal.com/blog/addressing-bias-in-ai-advancing-gender-race-and-age-equality/

Real-World Impact :

By prioritizing healthier white patients for care management and using healthcare costs as a stand-in for illness severity, Optum's risk prediction algorithm—which is utilized by US insurers—underestimated the needs of Black patients. This worsened racial disparities by lowering Black patients' access from 17.7% to 46.5% after correction.

https://magazine.publichealth.jhu.edu/2023/rooting-out-ais-biases

Mitigation Strategies :

Examples of technical approaches include the utilization of datasets that are both representative and diverse, the implementation of algorithms that are aware of fairness (such as re-weighting and oversampling underrepresented groups), and the execution of bias audits utilizing metrics such as equalized odds.
Process approaches include involving stakeholders in the process of continuous monitoring, carrying out external validation and re-calibration, and involving multidisciplinary teams (including clinicians and ethicists) in the process of development.

C. Ethical Decision Framework

i. Is the data reprsentative and free from bias?

Check for under-representation to avoid perpetuating disparities.

ii. Does the model respect privacy and consent?

Get informed consent before using data and make sure that laws like GDPR and HIPAA are followed.

iii. Is the AI interpretable and explainable?

To foster trust and facilitate oversight, provide mechanisms for comprehending decisions

iv. Has the model's safety and equity been verified?

To reduce harm and guaranteed equitable results, test across a variety of populations

v. Who is accountable for errors or biases?

Describe the chains of liability that include users, providers, and developers.

vi. Does it conform to moral precepts like justice and beneficence?

Determine whether it supports patients' well-being in an inclusive manner.

D. Stakeholder Impact Analysis

1. Patients :
Benefits: better results (eg:- AI predictive tools), quicker diagnoses, and personalized care.
Risks: diminished autonomy if AI replaces human input, privacy violations, and biased algorithms that exacerbate disparities.
Protection: Demand informed consnt, opt-out choices, and openness in the application of AI.

2. Medical Professionals:
Impact: AI increases efficiency (eg:- image analysis), but it also shifts the focus to oversight and may increase liability for mistakes.
Liability: It's unclear when AI fails, but providers are responsible for final decisions.
Training: Requires instruction in ethical use, bias detection, and AI literacy.

3. Researchers and Developers:
Responsibilities: addressing biases in design and ensuring fairness, transparency, and validation.
Role: Follow ethical guidelines and work with clinicians to prevent harm (eg:- through diverse data).

Policy Recommendation Balancing These three Interests

Mandate interdisciplinary oversight boards (including patients, providers, developers) for AI approval, requiring bias audits, transparency reports, and equitable access to balance innovation with safety and equity.