



LEGAL AND ETHICAL ISSUES

When addressing ethical challenges in the realm of digital health, it is imperative to consider the various factors that play a role. Among these, one of the most significant is the three stages of digital health usage, namely before, during, and after the utilization of digital health technology.

Prior to engaging with digital health tools, it is essential to have access to accurate and reliable information, feel empowered, and provide informed consent.

During the utilization of digital health, fairness in aspects such as data storage, access, sharing, and ownership is critical, along with the preservation of dignity and autonomy.

Technical components, including safeguarding data through secure storage and firewalls, hold significant importance.

General governance aspects, such as accountability and transparency, should also be carefully considered (Brall, Schröder-Bäck and Maeckelberghe, 2019)



BEFORE UTILIZATION OF DIGITAL HEALTH

01

ACCESS

To successfully implement digital health projects, it's vital that everyone has equal access. Bias and discrimination have no place in this field..(Brall, Schröder-Bäck and Maeckelberghe, 2019)

02

TRUTHFUL INFORMATION, EMPOWERMENT AND INFORMED CONSENT

- It's important to know the good and bad things about digital health methods before deciding to use them. You should also know that your health information might be collected. Make sure to stay informed so you can decide if you want to use these methods.
- Users should be motivate and liftup(both technically and informationally) to use digital health technology..(Brall et al., 2019).

03

INFORMED CONSENT

Patients considering surgery must be fully informed of the risks, benefits, and alternatives. It's crucial they understand the potential consequences before making a decision. (Shah et al., 2020)

DURING UTILIZATION OF THE SERVICES



Fairness in storage

There is no unauthorised access by hacking or other fraud.



SHARING OF OWNERSHIP

Data ownership is crucial for fair data usage. Data custodians must safeguard data and ensure ethical use for everyone involved



Dignity and autonomy

Respect people's autonomy to control and share their personal information. It's necessary for freedom and equality.(Jain, 2023)



Data privacy

Richard Rognehaugh defines privacy as "the right of an individual to keep information about themselves from being disclosed to others; the claim of individuals to be left alone, free of surveillance or interference from other individuals, organisations, or the government.. (Naik et al., 2022)

- kinematic fingerprint (Spiegel, 2018).

GUIDELINES



- The European Commission's independent high-level expert committee produced ethics recommendations in April 2019.
- (i) human agency and supervision,
- (ii) technical robustness and safety,
- (iii) privacy and data governance,
- (iv) openness,
- (v) diversity, non-discrimination, and justice,
- (vi) social and environmental well-being, and
- (vii) accountability are all important considerations..[\(European Commission, 2018\)](#)
- WHO -Digital Health Atlas. (WHO, n.d.)



Security policies

Security is the state of not being jeopardised by any type of risk, whether physical, psychological, financial, emotional. (Weiss and Biermann, 2021)

These are tools, rules, regulations, processes, concepts, and managerial strategies. Many security hazards may be mitigated by using encryption, error-checking procedures, preventative systems, and identifying instructional tools.(Mthunzi et al., 2020)

General governance

The OECD For example, the Organisation for Economic Cooperation and Development has issued a set of principles for health data governance..(Vayena et al., n.d.)

ETHICAL

Regulation
Privacy
Mitigation of Bias
Transparency
Relevance



LEGAL

Governance
Confidentiality
Liability
Accuracy
Decision Making

(Naik et al., 2022)

REFERENCE

Brall, C., Schröder-Bäck, P. and Maeckelberghe, E. (2019b) "Ethical aspects of digital health from a justice point of view," *European Journal of Public Health*, 29(Supplement_3), pp. 18–22. Available at: <https://doi.org/10.1093/eurpub/ckz167>.

Shah, P., Thornton, I., Turrin, D. and Hipskind, J.E. (2020). Informed Consent. [online] PubMed. Available at: <https://www.ncbi.nlm.nih.gov/books/NBK430827/#:~:text=Informed%20consent%20is%20the%20process>.

Jain, D. (2023). Regulation of Digital Healthcare in India: Ethical and Legal Challenges. *Healthcare*, 11(6), p.911. doi:<https://doi.org/10.3390/healthcare11060911>

WHO. (n.d.). WHO | WHO Guideline: recommendations on digital interventions for health system strengthening. [online] Available at: <https://www.who.int/reproductivehealth/publications/digital-interventions-health-system-strengthening/en/>.

European Commission (2018). Ethics Guidelines for Trustworthy AI. [online] FUTURIUM - European Commission. Available at: <https://ec.europa.eu/futurium/en/ai-alliance-consultation.1.html>.

Weiss, M. and Biermann, F. (2021). Cyberspace and the protection of critical national infrastructure. *Journal of Economic Policy Reform*, pp.1–18. doi:<https://doi.org/10.1080/17487870.2021.1905530>

Mthunzi, S.N., Benkhelifa, E., Bosakowski, T., Guegan, C.G. and Barhamgi, M. (2020). Cloud computing security taxonomy: From an atomistic to a holistic view. *Future Generation Computer Systems*, 107, pp.620–644. doi:<https://doi.org/10.1016/j.future.2019.11.013>.

Vayena, E., Haeusermann, T., Adjekum, A. and Blasimme, A. (n.d.). *ETH Library Digital health: meeting the ethical and policy challenges*. [online] Available at: https://www.research-collection.ethz.ch/bitstream/handle/20.500.11850/239873/Vayena_239873.pdf?sequence=2&isAllowed=y.



**THANK
YOU**