

DIGITAL HEALTH AND RIGHTS

BY MAXINE MBUGUA

According to digital health and rights project, digital health and rights refer to the intersection of technology, healthcare, and human rights. It involves using digital tools and technologies, such as mobile apps, electronic health records, and telemedicine, to improve healthcare access, delivery, and outcomes while ensuring that individuals' rights, such as privacy, equity, and autonomy, are respected.



[This Photo](#) by Unknown Author is licensed under [CC BY-SA-NC](#)

According to Ashesh Anand under <https://www.analyticssteps.com> a number of privacy, autonomy, access, and ethical issues are all included in the significant and complex topic of the connection between digital health and rights. Here are some important things to think about when talking about digital rights and health;

- ❖ Privacy
- ❖ Data Ownership and Control
- ❖ Access and Equity
- ❖ Ethical Considerations:

We have the Digital Health and Rights Project (DHRP) that brings together international social scientists, human rights lawyers, health advocates, and networks of people living with HIV to conduct research and advocate for rights-based digital governance globally. (<https://gnpplus.net/project/digital-health-and-rights/>). In order to determine the future of human rights in the digital era, the Future of Human Rights in the Digital era project employs a transnational participatory action research methodology, giving different young people' leadership and voices a central place. Along with the University of Warwick, GNP+ is pleased to be a member of the BOTNAR-funded collaboration. The Digital Health and Rights Project consortium is utilizing a transnational participatory method to study how different grassroots groups in low- and middle-income countries might influence the future of human rights in the digital age. The research aims to understand the perceptions of young

adults in Colombia, Ghana, Kenya, and Vietnam about digital governance, what constitutes meaningful participation in strategy and policy talks, and what kind of training in digital literacy and empowerment they would like to receive to assist policy advocacy. Throughout the entire endeavor, including the global steering committee, young adults and civil society members took part in the study.



[This Photo](#) by Unknown Author is licensed under [CC BY-SA](#)

Digital health and rights is something we should look at in depth firstly let's look at privacy firstly what is privacy according to (The Office of the Australian Information Commissioner) Freedom of expression, association, and thinking, as well as freedom

from discrimination, are all based on the fundamental human right to privacy. Additionally, there are other perspectives on privacy, including: physical privacy such as providing a body sample for medical purpose, surveillance when information isn't recorded or your identity can't be verified and information privacy the treatment of your personal data. (The Office of the Australian Information Commissioner).

under digital health privacy is very crucial and that's why legal frameworks have been established such as the DIGITAL HEALTH ACT NO. 15 OF 2023.

Under Digital Health Act No. 15 of 2023 in Kenya PART V CONFIDENTIALITY, PRIVACY AND SECURITY OF DATA states the confidentiality, privacy and security of all sensitive information personal data held in system will be the responsibility of the cabinet secretary. (2) No third party may receive sensitive personal information stored in the system unless—

(a) the data subject is incapable of providing informed consent for the disclosure and that consent is provided by a person authorized by the data subject in writing;

(b) the disclosure is permitted by the application of written law or the enforcement of a court order; or

(c) a health service is being provided without informed consent as permitted by written law or a court order;

(d) the data subject is receiving emergency care;

(e) failing to treat the data subject or a group of people that includes the data subject would pose a serious risk to public health; or

(f) the data subject has not explicitly, implicitly, or through their actions refused a health service and a delay in providing that service could result in death or irreversible harm to their health.

According to Digital Health: what does it mean for your rights and freedoms it states that;

Every patient has the fundamental right to privacy and nondiscrimination in healthcare delivery and access. Patients are at serious risk if their personal information is misused, disclosed without their informed consent, compromised, or utilized in any other way due to the extensive processing of personal data in the delivery of healthcare services. In order to give health data greater protection, several governments have taken steps to acknowledge its unique status and classify it as "sensitive personal data" or "special category of data." These enhanced safeguards might also apply to information that discloses private health information, like information that can be used to determine, infer, or forecast a medical condition (e.g. a person's past purchases). The inclusion of general lifestyle and wellness information is a topic of growing discussion, though.

The adoption of new technology in the health sector in recent years has only increased privacy and data protection concerns. AI-enabled technologies, for instance, might increase the amount of personal data that is exploited and shared.

(<https://privacyinternational.org>)

Digital technology integration in healthcare has enormous potential to empower individuals and enhance health results, but it also greatly increases worries about security, privacy, and the defense of fundamental rights. According to the Office of the Australian Information Commissioner, privacy is fundamental to freedom and dignity, supporting rights including the right to free speech and the right to be free from discrimination. The management of sensitive personal data, the possibility of surveillance, and the possible misuse or unauthorized disclosure of information are all examples of how privacy in the context of digital health transcends geographical boundaries. (*Digital Health: what does it mean for your rights and freedoms*. (n.d.).

Privacy International. <https://privacyinternational.org/long-read/4671/digital-health-what-does-it-mean-your-rightsand-freedoms>)



[This Photo](#) by Unknown Author is licensed under [CC BY-ND](#)

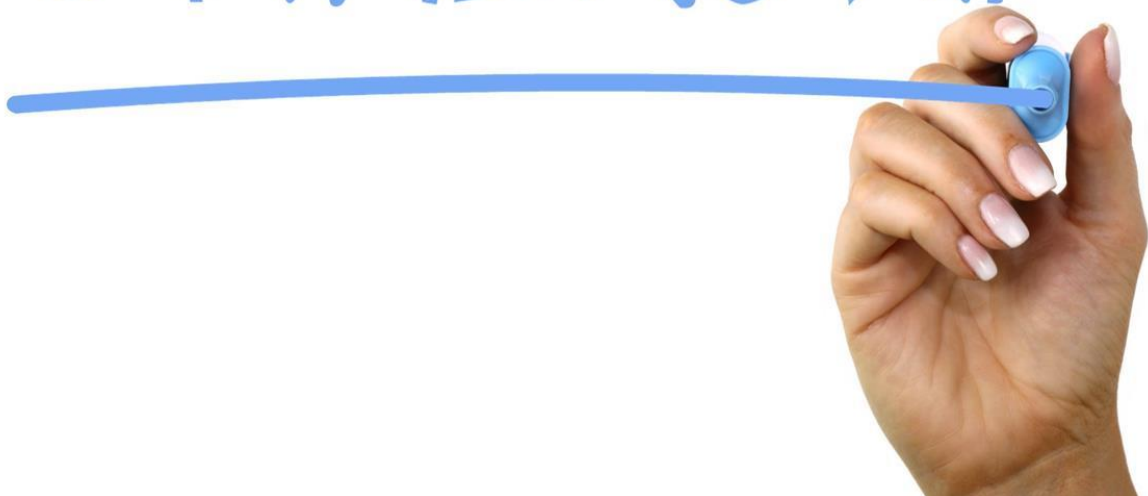
Data Ownership and Control

In digital health, data ownership and control are crucial concerns, particularly with the growing use of AI-driven technologies and electronic health records. These ideas establish who can access health data, who has rights over it, and how it can be shared or used. Let's firstly look at the;

According to (*Own your health data*. (n.d.). <https://www.goinvo.com/vision/own-your-health-data/>) Patients' Rights: It is becoming more widely acknowledged that patients have important rights regarding their medical records. Certain systems allow patients to co-own or even entirely own the health data that is generated about them, particularly data that they create themselves e.g., through health apps or wearable devices. Unless otherwise mandated by law, this includes the freedom to own, distribute, sell, or destroy their data as well as to provide or revoke authorization for

its use. (*Own your health data.* (n.d.). <https://www.goinvo.com/vision/own-your-health-data/>)

OWNERSHIP



[This Photo](#) by Unknown Author is licensed under [CC BY-SA](#)

As Per HIPAA's Privacy Rule, Who Owns Patient Data? Providers as Custodians: Traditionally, healthcare providers have handled patient data as custodians rather than owners. Although they do not have complete ownership, they are in charge of safeguarding, overseeing, and making appropriate use of this data. Their responsibility is to guarantee data security and adherence to moral and legal requirements. (Robin, E. (2024, February 14). As Per HIPAA's Privacy Rule, Who Owns Patient Data? - Newsoftwares.net Blog. *Newsoftwares.net Blog*.

<https://www.newsoftwares.net/blog/as-per-hipaas-privacy-rule-who-owns-patient-data/>)

According to Data ownership in the AI-Powered Integrative health care landscape. *JMIR Medical Informatics*, new approaches that advocate shared ownership between patients, clinicians, academics, and AI developers include the Collaborative Healthcare Data Ownership (CHDO) framework. These solutions tackle the intricacies of data use in AI-powered healthcare by emphasizing clear access rights, open governance, and cooperative stewardship. (Liu, S., & Guo, L. R. (2024). Data ownership in the AI-Powered Integrative health care landscape. *JMIR Medical Informatics*, 12, e57754. <https://doi.org/10.2196/57754>)

According to *Guide to Healthcare Data Governance Frameworks for Law and Regulation* Consent and manage: Patients are entitled to know what data is collected, to manage who has access to it, and to provide or revoke consent for its use under laws like the EU's GDPR and Kenya's Data Protection Act (DPA) 2019. Specific, informed, freely given, and readily rescindable consent is required. (Krishnan, K. (n.d.). *2025 Guide to Healthcare Data Governance | Concentric AI*. Concentric AI. <https://concentric.ai/data-governance-in-healthcare-a-technical-overview/>)

As Per HIPAA's Privacy Rule, Who Owns Patient Data? Data Governance: Frameworks for effective data governance are crucial. They establish rules for data management, specify roles and duties, and guarantee adherence to national data protection legislation, GDPR (EU), and HIPAA (USA). These frameworks seek to create transparent accountability, guarantee quality and security, and manage data as an asset. (Robin, E. (2024b, February 14). As Per HIPAA's Privacy Rule, Who Owns Patient Data? - Newsoftwares.net Blog. *Newsoftwares.net Blog*. <https://www.newsoftwares.net/blog/as-per-hipaas-privacy-rule-who-owns-patient-data/>)

According Data ownership in the AI-Powered Integrative health care landscape AI and Information Exchange: Because algorithm-generated insights may include several stakeholders, the use of AI in healthcare challenges data ownership. Blockchain and data trust models are being investigated to offer transparent governance and distributed access management and International Variability that is International data sharing is complicated by the fact that different nations have different legal definitions and rights pertaining to data ownership.(Liu, S., & Guo, L. R. (2024b). Data ownership in the AI-Powered Integrative health care landscape. *JMIR Medical Informatics*, 12, e57754. <https://doi.org/10.2196/57754>)

Ethical Considerations

The responsible creation and use of digital health technologies depends on ethical issues first and foremost. Digital health changes healthcare delivery and therefore raises difficult ethical questions including privacy, data security, algorithmic bias, informed consent, and fair access.

Patients should have significant control over their personal health data and be empowered to make educated decisions regarding digital health solutions. Users' informed consent has to be obvious, voluntary, and complete understanding of how their data will be used and any possible advantages or hazards.

Digital health should be equitable, guaranteeing fair access to technologies and avoiding discrimination or prejudice particularly in AI-driven tools. Unfair results can be caused by algorithmic bias and data homogeneity, therefore stressing the importance of inclusive design and continuous monitoring.

Solutions have to be of use to patients and should seek to avoid harm. This includes rigorous clinical validation of AI tools, safeguarding against misuse of data, and ensuring digital health does not undermine Standards for moral digital health are established by regulatory and legislative initiatives, such as the EU's Ethics Guidelines for Trustworthy AI, which highlight the importance of public trust, inclusivity, and oversight.

Overall, the field of digital health presents significant opportunities for improving healthcare outcomes and empowering individuals to take charge of their health.

However, it is essential to ensure that these advancements are accompanied by robust protections for individuals' rights, privacy, and autonomy. Balancing technological advancements with ethical considerations and regulatory frameworks is key to achieving a responsible and inclusive digital health ecosystem.



REFERENCES

Analytics Steps - A leading source of Technical & Financial content. (n.d.).

<https://www.analyticssteps.com/>

DIGITAL HEALTH ACT NO. 15 OF 2023.

Digital Health: what does it mean for your rights and freedoms. (n.d.). Privacy

International. <https://privacyinternational.org/long-read/4671/digital-health-what-does-it-mean-your-rightsand-freedoms>

Krishnan, K. (n.d.). *2025 Guide to Healthcare Data Governance | Concentric AI.*

Concentric AI. <https://concentric.ai/data-governance-in-healthcare-a-technical-overview/>

Liu, S., & Guo, L. R. (2024). Data ownership in the AI-Powered Integrative health care landscape. *JMIR Medical Informatics*, 12, e57754.

<https://doi.org/10.2196/57754>

Own your health data. (n.d.). <https://www.goinvo.com/vision/own-your-health-data/>

Robin, E. (2024b, February 14). As Per HIPAA's Privacy Rule, Who Owns Patient Data? - Newsoftwares.net Blog. *Newsoftwares.net Blog.*

<https://www.newsoftwares.net/blog/as-per-hipaas-privacy-rule-who-owns-patient-data/>

<https://gnpplus.net/project/digital-health-and-rights/>

The Office of the Australian Information Commissioner)