Towett *et al. Globalization and Health* (2024) 20:64
https://doi.org/10.1186/s12992-024-01067-3

Globalization and Health

REVIEW Open Access

Discursive framework for a multi-disease digital health passport in Africa: a perspective

Gideon Towett[1,2*], R Sterling Snead[1], Julia Marczika[1] and Isaac Prada[1]

Abstract
Africa's dual burden of rising incidence of infectious diseases and increasing prevalence of non-communicable diseases (NCDs), such as cardiovascular diseases and diabetes, demands innovative approaches to disease surveillance, response, and cross-border health management in response to growing economic integration and global connectivity. In this context, we propose a discursive framework for the development and implementation of a multi-disease digital health passport (MDDHP) in Africa. The MDDHP would serve as a secure platform for storing and sharing individual health data, offering a comprehensive solution to track and respond to infectious diseases, facilitate the management of NCDs, and improve healthcare access across borders. Empowering individuals to proactively manage their health and improve overall outcomes is a key aspect of the MDDHP. In the paper, we examine the key elements necessary to effectively implement MDDHP, focusing on minimizing risks, maintaining efficacy, and driving its adoption while also taking into consideration the unique contexts of the continent. The paper is intended to provide an understanding of the key principles involved and contribute to the discussion on the development and successful implementation of MDDHP in Africa.

Keywords African healthcare, Multi-disease digital health passport, Cross-border health management, Healthcare access, Patient empowerment, Infectious diseases, Noncommunicable diseases

Background

Africa's growing economic integration and global connectivity hold immense promise, but they also bring forth critical public health considerations. This interconnectedness, for example, amplifies the risk of infectious disease transmission across borders. The recent COVID-19 pandemic demonstrated how interconnectedness can fuel outbreaks, affecting not only individual countries but entire regions [1]. It also increases the risk of individuals being exposed to new pathogens and can worsen their existing conditions due to travel-related factors [2]. Moreover, communication barriers and incompatible health record systems present major hurdles to effective cross-border patient management, particularly during medical emergencies, potentially leading to misdiagnoses, medication errors, and even adverse drug reactions [3, 4].

These challenges are amplified in the African context by a strained healthcare system grappling with resource constraints, infectious diseases like malaria and HIV/AIDS, and a rising burden of noncommunicable diseases (NCDs) like cardiovascular diseases, diabetes, and cancer, attributed in part to changing lifestyles and urbanization [5–7]. Notably, NCDs increase vulnerability to severe infections, further straining the system, as observed during pandemics like COVID-19 [8]. This complex landscape necessitates comprehensive and adaptable strategies that address the convergence of

*Correspondence:
Gideon Towett
gideon@selfresearch.org
[1]The Self Research Institute, Broken Arrow, Oklahoma, USA
[2]Department of Biochemistry, Microbiology and Biotechnology, Kenyatta University, Nairobi, Kenya

global connectivity, infectious diseases, NCDs, and limited healthcare access.

Digital health technology (DHT) has emerged as a revolutionary instrument for delivering innovative healthcare, offering new possibilities to overcome conventional obstacles and improve access to quality care [9]. While Africa still faces a persistent digital divide, the past decade has witnessed remarkable progress in expanding internet connectivity and fostering digitization initiatives. Notably, mobile app usage has surged, driven by growing enthusiasm for health-focused apps and widespread smartphone adoption [10]. This, coupled with advancements in mobile technology and patient empowerment, has led to the integration of electronic health records (EHRs) into healthcare. Innovative digital platforms and applications seamlessly transform paper health passports into personalized digital profiles. For instance, during the COVID-19 pandemic, pandemic-focused digital health passports (DHPs) played a pivotal role. They enabled secure sharing of individual vaccination and test records at borders and other entry points via mobile devices, facilitating safe reintegration into social and economic activities [11].

Building on this success, multi-disease digital health passports (MDDHPs) offer a holistic health overview within a single platform. They empower healthcare providers and authorities to swiftly identify individuals at risk of contagious diseases, track outbreaks, and deliver targeted interventions. By eliminating physical records, MDDHPs could simplify access to healthcare services across borders, minimize paperwork errors, and empower individuals with personalized insights into their health risks. This could potentially save time and money, promoting proactive health management [3, 12]. Ultimately, MDDHP has the potential to improve patient outcomes, reduce strain on healthcare systems, and bolster Africa's pandemic preparedness.

However, developing a truly effective and inclusive MDDHP system across diverse African countries is a complex challenge requiring a tailored approach and collaboration from a wide range of stakeholders. Recognizing these intricate requirements, we employ a discursive lens to illuminate the multifaceted nature of MDDHP integration in this unique context. This analysis will involve examining crucial elements like robust data security policies, strong privacy protections, and a supportive technological ecosystem, all vital for successful MDDHP adoption. Our paper takes the first step in exploring the essential prerequisites for MDDHP success, aiming to contribute to the development of a successful implementation strategy for Africa. This, in turn, will equip stakeholders with valuable insights to build a system that significantly improves disease surveillance, cross-border health management, and ultimately, health outcomes across the continent.

An overview of the evolution of health passport systems in Africa

Even before the advent of digital technologies, paper-based health passports, also known as patient-held health records, played a vital role in primary healthcare across parts of Africa. As early as the 1990s, countries such as Zambia and Malawi implemented physical passports containing both curative and preventive medical records, including immunization histories and chronic disease management. Notably, pediatric passports (age < 5) featured growth charts on their cover for easy monitoring, distinguishing them from adult versions. These passes were offered for a nominal fee, generating a sustainable funding mechanism to address healthcare stationery shortages [13, 14].

In Lesotho, health passports further included details of drug allergies and medication sensitivities, screening activities (e.g., HIV, malaria), and clinical features of common infectious diseases, such as tuberculosis, on the back page. Additionally, 16 empty pages were allocated for healthcare provider notes, with each set of records securely attached to the next for continuity [15]. Similarly, South Africa's passports featured a list of existing medical conditions and allergies on the first page, followed by subsequent records of blood pressure, blood glucose levels, body mass index, and peak expiratory flow rates [16]. In Mozambique, paper-based records were used specifically for prenatal, postnatal, and child healthcare records, including immunizations and growth monitoring [17]. However, despite their benefits, paper-based passports faced limitations. Manual data entry was prone to human error, confidentiality concerns existed, interpretation was challenging for non-healthcare professionals, and damage or loss due to fire or weather was a risk [13, 14, 18].

The rise of digital technologies has led to the development of EHRs, or DHPs, in Africa. These systems address the limitations of paper-based solutions by providing secure, accessible, and interoperable management of health data. One such example is the priv-ID system in South Africa, developed through a collaboration between a digital identity solutions company (priv-ID) and the Medical Knowledge Institute. These health passports contained medical histories and used a biometric identity check for authentication. Primarily targeted at local healthcare facility users, particularly mothers and children, these passports aimed to provide easy access to accurate records, empower individuals to manage their health, and make informed decisions [19]. Another example is Afya Moja in Kenya, a DHP designed by Safaricom Plc specifically for diabetic patients. Afya Moja

empowers patients to manage their health by enabling access and sharing of medical records, facilitating active participation in treatment plans and health monitoring [20].

The Virus Outbreak Data Network (VODAN) initiative in Africa merits mention within the context of DHPs. Established to address challenges in outbreak preparedness and control, VODAN focuses on improving data collection, analysis, and sharing capabilities across the continent. The FAIR data principles form its foundation, guaranteeing the findability, accessibility, interoperability, and reusability of data [21]. This focus on interoperability lays the groundwork for the development and implementation of MDDHPs in Africa.

The COVID-19 pandemic spurred the rapid development of DHPs in Africa to manage travel and health data during the crisis [22, 23]. The need for standardized documentation led to initiatives like the African Union (AU) and the Africa Centers for Disease Control and Prevention's Trusted Travel platform, promoting mutual recognition of COVID-19 certificates [24]. Similarly, the World Health Organization's (WHO) Digital Documentation of COVID-19 Certificates provides technical specifications for secure digital vaccination certificates for international travel [25]. Though focused on technical aspects, the WHO's document highlights the potential of standardized digital health records (DHRs) not only for travel but also for broader health data management in the future.

In addition to the COVID-19 specific initiatives, the WHO African Regional Office has proposed a comprehensive Digital Health Platform. This facility-wide EHR system focuses on seamless information exchange between healthcare facilities through standardized formats. A robust information infrastructure supports this exchange, integrating components like patient registries, data repositories, and secure identity management. By bridging previously siloed data systems, the platform lays the groundwork for integrating various disease-specific solutions into a more cohesive system. This approach enables efficient data flow, simplifies clinical data collection, and allows customization for individual hospitals [26].

While existing DHPs in Africa have shown promise, their current applications in health management are limited to specific functions and a narrow range of conditions. This presents a significant opportunity for advancement, building upon the foundation laid by existing eHealth platforms to develop robust MDDHPs. MDDHPs could address a wider spectrum of diseases, fostering improvements in disease surveillance, prevention, and management while also incorporating functionalities to address cross-border health needs.

Data points for a multi-disease digital health passport

Ensuring the effectiveness and usefulness of MDDHP relies on the inclusion of relevant and impactful data points. Demographic information, including name, date of birth, ID number, gender, and blood group, forms the essential foundation of DHPs [27]. This information ensures accurate patient identification and facilitates seamless integration with existing healthcare systems, like EHRs, allowing for personalized medical records and tailored interventions based on individual characteristics [28, 29]. Knowing an individual's preferred language can bridge communication gaps in diverse settings, preventing errors and enhancing the patient experience (for example, reducing medication errors due to misunderstandings) [29]. Biometric identifiers, where feasible, can further strengthen security and minimize identity errors [30].

Data on medical history, including details of past and current medical conditions, surgeries, allergies, medications (including prescription periods), and medical devices, empowers healthcare professionals with the information they need to make informed decisions, prevent adverse drug interactions, and provide tailored treatment plans. This information is particularly crucial in emergency situations, enabling swift and appropriate medical interventions. Furthermore, diagnostic data, encompassing laboratory test results, imaging reports (e.g., X-rays, CT scans, MRIs, or ultrasounds), and body mass index, enables informed clinical decision making by providing healthcare professionals with a comprehensive picture of an individual's current health status. Family history information, including details of diseases or health conditions that run in the individual's family, provides insights into potential genetic predispositions, aiding in the early detection and prevention strategies of disease conditions [27, 31].

Vaccination records in MDDHP, secured by public key infrastructure technology, [32] play a crucial role in mitigating the spread of infectious diseases, especially during pandemics, by providing a readily accessible and verifiable record of an individual's immunization status. These could include details about the vaccines received, such as type, manufacturer, vaccination date, location, dose, batch number, expiration date, and the targeted disease [11]. This information allows for verification of vaccination status and identification of potential issues like counterfeit vaccines or outdated doses. Moreover, the availability of such records enables authorities to implement targeted travel policies. For example, entry restrictions on unvaccinated individuals or mandating specific vaccinations for travelers based on their destination. This not only enhances public safety but also contributes to the overall efficiency of disease control measures.

Information such as occupation, addictions, and travel history in a health passport, while not directly impacting disease management, could offer valuable insights into potential health risks, lifestyles, and social networks of individuals [33].

Integrating real-time monitoring and tracking of vital signs into MDDHPs has the potential to revolutionize chronic disease management. Wearable, portable, and ingestible technological advancements have made this method possible [34, 35]. It has a lot of potential for collecting important digital biomarkers linked to different health conditions, which would allow for continuous monitoring and early interventions. By providing healthcare providers with a real-time overview of an individual's physiological status, it could facilitate timely detection of anomalies, personalized treatment plans, and improved clinical outcomes [36]. Furthermore, the inclusion of data on lifestyle factors such as exercise habits, dietary preferences, and stress levels can provide a comprehensive perspective on an individual's overall health and risk of developing chronic conditions [37]. Ultimately, the decision about what to include in a health passport will come down to balancing the needs of patients, doctors, and other stakeholders with the privacy concerns of individuals.

Prioritizing data security and privacy in multi-disease digital health passports

While MDDHPs offer promising benefits, they raise valid concerns regarding data security and privacy. This is especially critical given the inherent risks associated with the digital health environment. The widespread sharing of sensitive health data, such as patient records, across healthcare providers and borders increases the potential for harm, with a single data breach impacting a significant number of individuals [38]. The dynamic and evolving digital landscape further amplifies these concerns. Malicious actors or unethical businesses seek to exploit this valuable resource as more personal data, including health information, becomes readily available online. They might use this data for targeted advertising, identity theft, or even insurance fraud [39].

Beyond the immediate associated financial losses, health data breaches can inflict significant social and psychological damage. Sensitive information contained within MDDHPs could be used to stigmatize or stereotype individuals based on their health conditions [40]. For instance, access to an individual's health records by insurance companies or employers could lead to discriminatory practices such as denial of coverage or employment based solely on preexisting health conditions [41]. This concern is magnified in the context of a MDDHP, where individuals might seek to protect multiple confidential health conditions. Furthermore, significant ethical concerns arise from the possibility of data repurposing for unintended uses beyond the initial collection objectives, such as government surveillance or political campaigns [42].

Therefore, ensuring robust data security and privacy is paramount for the successful and ethical implementation of MDDHPs. Addressing these concerns necessitates a multipronged approach that includes reinforcing controls over data access and utilization while also leveraging relevant legislation to navigate these challenges.

Data access controls

Access control stands as a cornerstone for ensuring the confidentiality, integrity, and availability of sensitive patient information within MDDHPs. It involves a three-pronged approach comprising identification, authentication, and authorization [43]. Identification establishes unique user profiles or identities within the system, typically linked to personal identifiers like names, birthdates, national IDs, and contact information [44]. Existing national identification programs, like India's Aadhaar project, could offer valuable lessons for large-scale identity management. While primarily an identification system, Aadhaar's design facilitates integration with various services, including healthcare, by providing a unique ID to over a billion residents [45]. This integration has significant implications for healthcare access and data management, as it allows for streamlined patient identification and service delivery across government and private sectors [46].

Accurate identification ensures that individuals rightfully access their health records and related services [47]. Authentication verifies the claimed identity through various methods, including knowledge-based (passwords and PINs), possession-based (mobile devices), or biometric factors (fingerprints, retina scans, and facial recognition) [48]. Multifactor authentication, requiring multiple forms of verification before gaining access to the system, greatly enhances security [49].

Authorization determines the actions or resources an authenticated user can access. It safeguards data confidentiality by permitting only authorized personnel to modify or retrieve records, upholding patient privacy and data integrity [47]. MDDHPs necessitate a highly granular approach to authorization, allowing tailored access based on roles. This granularity allows healthcare providers, patients, and other stakeholders to access only specific health-related information or services they are authorized to view or modify based on their roles and responsibilities, [50] thereby minimizing unauthorized exposure of sensitive information. MDDHPs should empower individuals with autonomy over their data. This includes the ability to consent to or reject access

requests, ensuring individuals maintain control over their health information [51].

However, while robust data access controls are essential for MDDHP security, their design needs to consider potential consequences for users affected by the digital divide. It is conceivable that limited access to digital devices, internet connectivity, and digital literacy, [52] could hinder the ability to complete or navigate complex security protocols that depend on internet access. A tiered access system could help address some of these challenges. For instance, a system that necessitates basic verification for individuals to access their own health data but demands enhanced verification for actions such as data sharing with third parties could potentially improve accessibility. Additionally, streamlining security processes to require fewer steps and minimal technical knowledge, such as biometric verification that eliminates complex interactions with digital interfaces, could enhance accessibility. Furthermore, leveraging SMS-based registration and verification could be beneficial for individuals with basic mobile phones [38].

Beyond the traditional access control triad (identification, authentication, and authorization), encryption emerges as a crucial layer for safeguarding sensitive data in MDDHPs. Recognized as a cornerstone of modern data security, encryption utilizes cryptographic algorithms to transform sensitive information into an unreadable format, accessible only to authorized individuals possessing the decryption key [53]. This renders healthcare data incomprehensible to unauthorized parties, even if they manage to breach the system, significantly deterring malicious intrusions and preventing unauthorized data exploitation.

Secure data storage forms the bedrock for robust access controls. One approach to achieving secure data storage leverages blockchain technology, which offers a promising avenue due to its decentralized and immutable nature. This ensures data integrity and immutability, making modifications or tampering virtually impossible [22, 54]. This property offers invaluable protection against data breaches and unauthorized alterations, which is particularly relevant in light of recent reports of falsification of vaccination certificates for diseases such as COVID-19 and yellow fever in the region [55, 56]. Furthermore, blockchain empowers individuals with true ownership and control over their health data. Individuals can manage access permissions by granting specific rights to different entities, facilitating granular control, and enhancing patient autonomy [57]. Estonia's national health system, particularly its DHR, could offer valuable insights for integrating digital solutions into healthcare [58]. The Estonian system prioritizes data security and patient privacy through strong encryption and blockchain technology [59]. Furthermore, patients have control over who can access their health data, fostering trust and engagement with the digital health system [60].

Legal frameworks

While some African countries have established robust legal frameworks for inclusive and reliable DHSs, many others lack key legal provisions and regulatory structures [61]. Additionally, enforcement of existing frameworks may be inadequate, they may misalign with international standards, or they may be outdated, having been established before the emergence of advanced DHS technologies [62].

Despite these challenges, there are also promising opportunities for improving the legal landscape for DHSs in Africa. As of September 2023, fifteen AU members had ratified the AU Convention on Cyber Security and Personal Data Protection (Malabo Convention) [63]. Mirroring several standards from the European Union's (EU) General Data Protection Regulation (GDPR), considered the industry benchmark, [64] the Malabo Convention presents a comprehensive pancontinental framework aimed at aligning data protection policies across Africa by promoting and championing digital rights, particularly those related to data protection, privacy, and internet freedom.

In the Malabo Convention, there are six fundamental principles that govern the handling of personal data, including consent, which refers to the requirement that individuals freely give clear and informed permission for their personal data to be collected, processed, or shared; lawfulness and fairness in processing of personal data; which means personal data processing must be lawful, fair, and transparent; purpose or relevance, which means personal data should only be collected and processed for specific, explicit, and legitimate purposes; accuracy, which requires personal data to be accurate and up-to-date; transparency in processing of personal data; and confidentiality and security, which requires personal data to be processed in a secure manner, ensuring appropriate technical and organizational measures to protect against unauthorized or unlawful access, accidental loss, destruction, or damage.

Both legal frameworks establish roles and responsibilities for the various stakeholders involved in digital solutions, as well as mechanisms for enforcing compliance with the framework's provisions. The Malabo Convention is, however, enforced by National Data Protection Authorities (NDPA) in each Member State, as opposed to the GDPR, which is enforced by the European Data Protection Board, an independent EU agency. Certainly, the Malabo Convention is reinforced by individual national data protection regulations. As of December 2021, 33 (61%) African nations had implemented data protection laws at the domestic level, while 6 countries (11%) had

draft bills related to data protection. At least 10 (19%) African countries were yet to enact specific legislation concerning data protection, while there was no data available in 5 (9%) countries [65].

Therefore, addressing legal challenges and leveraging existing opportunities for MDDHPs in Africa requires a multifaceted approach. In the absence of national laws, aligning MDDHPs with internationally recognized privacy principles provides baseline protection while regulations are developed. Strengthening cooperation among NDPAs fosters trust and accountability through consistent enforcement of the Malabo Convention and other data protection frameworks. Developing and implementing national data protection laws where they are lacking creates comprehensive legal frameworks for responsible data governance. Moreover, to ensure the effectiveness and security of MDDHPs in the face of rapid technological advancements, legal frameworks must be continuously updated to address emerging challenges.

Creating an enabling ecosystem for effective multi-disease digital health passports

The success of MDDHPs hinges on creating a user-friendly and reliable system where various components, like user motivation, technical limitations, and local realities, work together seamlessly [66]. Studies in low- and middle-income countries highlight the need to consider both technical and human aspects while considering the unique characteristics of healthcare systems and the external environments in which they operate [67]. Therefore, understanding the dynamic interaction between these technical and human aspects, along with local factors influencing their effectiveness, is crucial for designing and implementing MDDHPs that resonate with diverse African settings. Ultimately, this harmonization is key to unlocking the potential of MDDHPs as valuable tools for disease surveillance, cross-border health management, and improved healthcare accessibility across Africa.

Technical considerations

Driving adoption and ensuring the effectiveness of a MDDHP requires careful attention to various technical factors. These factors are essential to creating a system that is interoperable, user-friendly, secure, and adaptable to the diverse healthcare systems in Africa, which are characterized by varying levels of technological advancement. Where feasible, MDDHP should be designed to seamlessly integrate with the existing technology ecosystem, [68] harmonizing with the systems used by healthcare providers and other stakeholders, such as EHRs, immunization databases, and other health information systems. Integrating data from various sources not only ensures accurate and up-to-date information but also improves efficiency and reduces the burden on healthcare workers, who might otherwise have to manage separate systems [69]. Existing internationally recognized standards, such as Health Level Seven Fast Healthcare Interoperability Resources, could serve as valuable guides in specifying data formatting and exchange between different systems, ensuring a smooth exchange of data [70, 71]. Furthermore, to enhance patient care, minimize errors, and ensure precise and consistent medical decision-making across borders, it is imperative to ensure that health passport information is readily comprehensible to medical professionals. Achieving this necessitates strict adherence to international standards and nomenclatures for classifying medical conditions and medications. By aligning with established global standards in medical terminology and categorization, healthcare practitioners can efficiently interpret and utilize the information contained in the health passport, thus contributing to more effective and error-free patient care [69]. There are many different classification systems for medical conditions and medications. However, the International Classification of Diseases and the Anatomical Therapeutic Chemical Classification Systems are the most widely used and accepted systems [72, 73].

A user-centered approach in designing any DHS is paramount to ensuring its contextual appropriateness and value for all stakeholders, spanning end-users to policymakers [74, 75]. This is particularly crucial in resource-limited settings like Africa, where many digital health innovations often fall short of benefiting those in need due to a convergence of factors including a lack of infrastructure, user skills, and proven effectiveness [76]. Functional simplicity is also important because simple solutions are more scalable and less dependent on external factors [77]. Moreover, the intrinsic attributes of DHTs should address unmet needs while incorporating end-user perspectives from the outset [78]. Running pilot programs in select regions is a great way to test functionality, gather feedback, and refine the system before wider use. This ongoing engagement with end users, from design to testing and integration, ensures MDDHPs align with real-world needs and improve clinical workflows for everyone involved.

Given Africa's growing mobile phone penetration, optimizing the MDDHP for mobile platforms is critical. This necessitates compatibility with a variety of devices and screen sizes to accommodate users across different socioeconomic backgrounds. Additionally, given existing infrastructure limitations, including the variability in internet connectivity across regions, designing solutions to function efficiently in low-bandwidth environments or even offline is critical to enabling users to access and update their health information even without an internet connection [78].

Moreover, considering the linguistic diversity of Africa, ensuring the application is available in multiple languages enhances its acceptance and wider geographical use. The ever-evolving landscape of technology also presents a compelling opportunity for the comprehensive enhancement of MDDHP. For example, embracing emerging technologies, such as artificial intelligence (AI) and machine learning (ML) innovations, could significantly elevate the capabilities of these passports. By leveraging AI and ML, it can be possible to harness their potential for precise predictions, advanced analytics, and data-driven optimizations [79]. This, in turn, fosters sustainable improvements in health outcomes, marking a pivotal step towards more effective and efficient healthcare delivery.

Human factors

The success of MDDHPs relies heavily on earning the trust and acceptance of all stakeholders involved. This includes healthcare providers, the public, and other actors responsible for adopting and utilizing these health passports. Building trust and addressing diverse attitudes towards digital technologies across these groups is crucial to driving widespread adoption. Consequently, investing in training and capacity building for healthcare workers is critical for effective MDDHP implementation, [80] including facilitating the registration and verification process for MDDHPs. Educational initiatives such as self-paced online courses, webinars, and resource manuals are vital in helping providers understand how to leverage these platforms. Equipping them with the necessary skills and knowledge ensures seamless integration of MDDHPs into daily routines, accurate data entry, and ultimately, optimized patient care based on accessible health information [81, 82].

Building public trust and fostering awareness about MDDHPs is equally important. Comprehensive public awareness campaigns, strategically disseminated through relevant channels like social media, healthcare publications, and collaborations with trusted organizations, can educate the public about the benefits and potential risks associated with these passports. Open communication regarding information access, usage, and privacy safeguards empowers individuals to actively participate in their healthcare data management and make informed decisions about their participation in the platform [38]. Transparency is key: users must be clearly informed about how their information is used and shared, what options exist in case of privacy violations, and the ability to opt-out or leave the platform entirely.

Policy frameworks: cornerstones for a successful multi-disease digital health passport in Africa

Robust policy frameworks serve as the foundation for successful MDDHP implementation across Africa's diverse healthcare landscape. Policies directly influence the availability, use, and incentives surrounding these DHTs, ultimately impacting their effectiveness [66]. The AU has demonstrated its commitment to digital health advancement through key documents like the Digital Transformation Strategy for Africa (2020–2030), the AU Data Policy Framework 2022, and the Agenda 2063, [83] which provide a roadmap for Africa to embrace digital health solutions. However, translating this potential into reality requires translating these broad AU policies into concrete national strategies and action plans.

Consequently, national policies should prioritize strategic areas directly impacting digital health success. One crucial area is bridging the digital divide with a particular emphasis on special groups, [84] and marginalized groups such as immigrants and refugees who have been forced to flee their homes due to civil conflicts and economic hardships, [85] a crisis particularly prevalent in parts of the African continent. Expanding internet connectivity and mobile networks, making them affordable and accessible even in remote areas, is essential. Additionally, providing access to appropriate devices and ensuring reliable electricity supply are crucial steps towards enabling broad utilization of digital health solutions like MDDHPs [86].

Building trust and encouraging adoption hinges on robust data privacy and security policies. Consequently, these policies should address data storage, access, quality assurance, and monitoring standards, ensuring the safety, security, and effectiveness of MDDHPs while streamlining regulatory clearance processes for these solutions [87]. Furthermore, clinical governance policies are necessary to ensure MDDHPs are used appropriately and in line with established medical practices [88]. Additionally, fostering innovation is crucial for ensuring continual improvement and effectiveness. Policies should incentivize developers to create tailored solutions that address local needs, making them accessible and affordable [89].

Significant investments in robust research dedicated to DHTs play a pivotal role in equipping policymakers with valuable insights and empirical evidence [90]. This data-driven approach empowers policymakers to make informed decisions that are not only well-founded but also responsive to the evolving healthcare landscape. Regular assessments and updates to policy frameworks are essential for adapting to emerging technologies and applying lessons learned from implementation [91]. This iterative approach fosters trust, encourages wider adoption, and ultimately enhances the overall effectiveness of MDDHPs in the African context.

Conclusion

The paper proposes a discursive framework for implementing MDDHPs in Africa. By harnessing digital tools, we can potentially revolutionize cross-border disease control, enhance healthcare access, and empower individuals to manage their health effectively. The framework emphasizes the importance of considering diverse data points within MDDHPs, aiming to enhance clinical decision-making, disease management, and public health interventions. However, alongside these benefits, robust data security measures and supportive regulatory frameworks are crucial to building confidence and encouraging widespread adoption. Addressing technical challenges, human factors, and supportive policies is essential for creating an ecosystem conducive to MDDHP success. Stakeholders, including policymakers, developers, healthcare professionals, and communities, can use this framework as a starting point to maximize the impact of MDDHPs on health outcomes across Africa. While further research and adaptation are necessary for specific contexts, this framework serves as a valuable roadmap to unlock the full potential of MDDHPs in Africa.

Abbreviations

AI	Artificial intelligence
DHP	Digital health passport
DHR	Digital health record
DHT	Digital health technology
EHR	Electronic health record
EU	European Union
GDPR	General Data Protection Regulation
MDDHP	Multi-disease digital health passport
ML	Machine learning
NCD	Noncommunicable disease
NDPA	National Data Protection Authority
VODAN	Virus Outbreak Data Network

Acknowledgements

Not applicable.

Author contributions

RSS conceived the study. GT conducted the initial literature search, gathered and organized relevant articles, and drafted the manuscript sections. JM and IP then collaborated on editing and revising the entire manuscript, providing critical feedback on the structure and flow.

Funding

The authors received no financial support for this article's research, authorship, and/or publication.

Data availability

No datasets were generated or analysed during the current study.

Declarations

Ethics approval and consent to participate

Not applicable.

Consent for publication

Not applicable.

Competing interests

R Sterling Snead is the CEO of The Self Research Institute, working with health informatics and a health passport app. All other authors declare no competing interest.

Received: 29 March 2024 / Accepted: 5 August 2024
Published online: 20 August 2024

References

1. Iken O, Abakporo U, Ayobami O, Attoye T. COVID-19: travel health and the implications for sub -Saharan Africa. Travel Med Infect Dis. 2020;35:101645.
2. Leung DT, LaRocque RC, Ryan ET. Travel medicine. Ann Intern Med. 2018;168(1):ITC1–16.
3. Sørensen HT. Patients with chronic diseases who travel: need for global access to timely health care data. Clin Epidemiol. 2022;14:513–9.
4. Odekunle FF, Odekunle RO, Shankar S. Why sub-saharan Africa lags in electronic health record adoption and possible strategies to increase its adoption in this region. Int J Health Sci (Qassim). 2017;11(4):59–64.
5. Inzaule SC, Ondoa P, Loembe MM, Tebeje YK, Ouma AEO, Nkengasong JN. COVID-19 and indirect health implications in Africa: impact, mitigation measures, and lessons learned for improved disease control. PLoS Med. 2021;18(6):e1003666.
6. Oleribe OO, Momoh J, Uzochukwu BS, Mbofana F, Adebiyi A, Barbera T, et al. Identifying key challenges facing healthcare systems in Africa and potential solutions. Int J Gen Med. 2019;12:395–403.
7. Mudie K, Jin MM, Tan KL, Addo J, Dos-Santos-Silva I, Quint J, et al. Non-communicable diseases in sub-saharan Africa: a scoping review of large cohort studies. J Glob Health. 2019;9(2):020409.
8. Sertbas Y, Solak EE, Dagci S, Kizilay V, Yazici Z, Elarslan S, et al. Clinical outcomes of COVID-19 in patients with chronic diseases. North Clin Istanb. 2023;10(4):401–10.
9. Olu O, Muneene D, Bataringaya JE, Nahimana MR, Ba H, Turgeon Y, et al. How can digital health technologies contribute to sustainable attainment of universal health coverage in Africa? A perspective. Front Public Health. 2019;7:341.
10. Rinke de Wit TF, Janssens W, Antwi M, Milimo E, Mutegi N, Marwa H, et al. Digital health systems strengthening in Africa for rapid response to COVID-19. Front Health Serv. 2022;2:987828.
11. Wang B, Ping Y. A comparative analysis of COVID-19 vaccination certificates in 12 countries/regions around the world: rationalizing health policies for international travel and domestic social activities during the pandemic. Health Policy. 2022;126(8):755–62.
12. Tuan Soh TY, Nik Mohd Rosdy NMM, Mohd Yusof MYP, Azhar Hilmy SH, Md Sabri BA. Adoption of a digital patient health passport as part of a primary healthcare service delivery: systematic review. J Pers Med. 2022;12(11):1814.
13. van der Hoek W, Ngoma M, Soeters R. The home-based health passport: a tool for primary health care. Trop Doct. 1994;24(1):21–3.
14. Neville R, Neville J. What can health care professionals in the United Kingdom learn from Malawi? Hum Resour Health. 2009;7:26.
15. Henbest RJ, Germond T, Fehrsen GS. I keep my health book with me': a national survey of 20 years' experience of patient-retained medical records Lesotho. SA Family Pract. 1995;16(2):80–94.
16. Norden AL, Marincowitz GJ, Fehrsen GS. Patients' thoughts on patient-retained medical records. SA Family Pract. 2004;46(7):30–3.
17. Lumbandali N, Mocumbi A. Retention of patient-held medical records for chronic diseases in Mozambique. Pan Afr Med J. 2021;39:1.
18. Wagner AL. The use and significance of vaccination cards. Hum Vaccin Immunother. 2019;15(12):2844–6.
19. Lane L. Healthy start for South African health passport. Biom Technol Today. 2009;2009:2–3.
20. Safaricom Plc. Safaricom partners with Nakuru County to pilot mobile health records system. https://www.safaricom.co.ke/media-center-landing/press-releases/safaricom-partners-with-nakuru-to-pilot-mobile-health-records-system (2021). Accessed 20 Feb 2024.
21. Inau ET, Sack J, Waltemath D, Zeleke AA. Initiatives, concepts, and implementation practices of FAIR (findable, accessible, interoperable, and reusable) data principles in health data stewardship practice: protocol for a scoping review. JMIR Res Protoc. 2021;10(2):e22505.

22. Ait Bennacer S, Aaroud A, Sabiri K, Rguibi MA, Cherradi B. Design and implementation of a new blockchain-based digital health passport: a Moroccan case study. Inf Med Unlocked. 2022;35:101125.
23. van Vuuren CJJ, van Vuuren JMJ. Perspectives of healthcare workers in South Africa on COVID-19 vaccination passports. Health SA. 2022;27:1823.
24. Africa CDC. Trusted Travel. https://africacdc.org/trusted-travel/ (2020). Accessed 17 Dec 2023.
25. WHO. Digital documentation of COVID-19 certificates: vaccination status: technical specifications and implementation guidance. https://www.who.int/publications-detail-redirect/WHO-2019-nCoV-Digital_certificates-vaccination-2021.1 (2021). Accessed 17 Jun 2024.
26. Ibeneme S, Karamagi H, Muneene D, Goswami K, Chisaka N, Okeibunor J. Strengthening health systems using innovative digital health technologies in Africa. Front Digit Health. 2022;4:854339.
27. Li YC, Detmer DE, Shabbir SA, Nguyen PA, Jian WS, Mihalas GI, et al. A global travelers' electronic health record template standard for personal health records. J Am Med Inf Assoc. 2012;19(1):134–6.
28. Jones DA, Shipman JP, Plaut DA, Selden CR. Characteristics of personal health records: findings of the Medical Library Association/National Library of Medicine Joint Electronic Personal Health Record Task Force. J Med Libr Assoc. 2010;98(3):243–9.
29. Chan J. Exploring digital health care: eHealth, mHealth, and librarian opportunities. J Med Libr Assoc. 2021;109(3):376–81.
30. Zuniga AEF, Win KT, Susilo W. Biometrics for electronic health records. J Med Syst. 2010;34(5):975–3.
31. Nittari G, Pirillo I, Amenta F, Ricci G. The right to medical assistance for seafarers. Ethical and practical consequences of the introduction of telemedicine to improve healthcare on board ships. Mar Policy. 2019;106:103525.
32. Cascini F, Causio FA, Failla G, Melnyk A, Puleo V, Regazzi L, et al. Emerging issues from a global overview of digital COVID-19 certificate initiatives. Front Public Health. 2021;9:744356.
33. Koenig HG. Religion, spirituality, and health: the research and clinical implications. ISRN Psychiatry. 2012;2012:278730.
34. Mukherjee S, Suleman S, Pilloton R, Narang J, Rani K. State of the art in smart portable, wearable, ingestible and implantable devices for health status monitoring and disease management. Sens (Basel). 2022;22(11):4228.
35. Richey AG, Kovacs I, Browne S. Use of an ingestible, sensor-based digital adherence system to strengthen the therapeutic relationship in serious mental illness. JMIR Ment Health. 2022;9(12):e39047.
36. Motahari-Nezhad H, Al-Abdulkarim H, Fgaier M, Abid MM, Péntek M, Gulácsi L, Zrubka Z. Digital biomarker–based interventions: systematic review of systematic reviews. J Med Internet Res. 2022;24(12):e41042.
37. Houlden RL, Yen HH, Mirrahimi A. The lifestyle history: a neglected but essential component of the medical history. Am J Lifestyle Med. 2017;12(5):404–11.
38. Tiffin N, George A, LeFevre AE. How to use relevant data for maximal benefit with minimal risk: digital health data governance to protect vulnerable populations in low-income and middle-income countries. BMJ Glob Health. 2019;4(2):e001395.
39. Filkins BL, Kim JY, Roberts B, Armstrong W, Miller MA, Hultner ML, et al. Privacy and security in the era of digital health: what should translational researchers know and do about it? Am J Transl Res. 2016;8(3):1560–80.
40. Rothstein MA. Is deidentification sufficient to protect health privacy in research? Am J Bioeth. 2010;10(9):3–11.
41. Grande D, Luna Marti X, Feuerstein-Simon R, Merchant RM, Asch DA, Lew-son A, et al. Health policy and privacy challenges associated with digital technology. JAMA Netw Open. 2020;3(7):e208285.
42. Nageshwaran G, Harris RC, Guerche-Seblain CE. Review of the role of big data and digital technologies in controlling COVID-19 in Asia: public health interest vs. privacy. Digit Health. 2021;7:20552076211002953.
43. Glagola MJ. Access control for electronic patient records. Radiol Manage. 1998;20(5):44–50.
44. George M, Chacko AM. Health passport: a blockchain-based PHR-integrated self-sovereign identity system. Front Blockchain. 2023;6:1075083.
45. Pathak C, Pawah S, Sikri A, Rao I. Unique denture identification system for all Indian nationals. Contemp Clin Dent. 2018;9(1):185–8.
46. Nadhamuni S, John O, Kulkarni M, Nanda E, Venkatraman S, Varma D, et al. Driving digital transformation of comprehensive primary health services at scale in India: an enterprise architecture framework. BMJ Glob Health. 2021;6(5):e005242.
47. Røstad L, Nytrø O. Towards dynamic access control for healthcare information systems. Stud Health Technol Inf. 2008;136:703–8.
48. Jayabalan M, O'Daniel T. A study on authentication factors in electronic health records. JATI. 2019;3(1).
49. Suleski T, Ahmed M, Yang W, Wang E. A review of multi-factor authentication in the internet of Healthcare things. Digit Health. 2023;9:20552076231177144.
50. Fernández-Alemán JL, Señor IC, Lozoya PÁ, Toval A. Security and privacy in electronic health records: a systematic literature review. J Biomed Inf. 2013;46(3):541–62.
51. Carrión Señor I, Fernández Alemán JL, Toval A. Gestión Del control de acceso en historiales clínicos electrónicos: revisión sistemática de la literatura [Access control management in electronic health records: a systematic literature review]. Gac Sanit. 2012;26(5):463–8.
52. Sui W, Facca D. (2020). Digital health in a broadband land: the role of digital health literacy within rural environments. Health Science Inquiry. 2020;11(1):140–3.
53. Rashid MM, Choi P, Lee SH, Kwon KR. Block-HPCT: blockchain enabled digital health passports and contact tracing of infectious diseases like COVID-19. Sens (Basel). 2022;22(11):4256.
54. Odoom J, Huang X, Danso SA. COVID-19 and future pandemics: a blockchain-based privacy-aware secure borderless travel solution from electronic health records. Softw Pract Exp. 2022;52(10):2263–87.
55. Mbunge E, Dzinamarira T, Fashoto SG, Batani J. Emerging technologies and COVID-19 digital vaccination certificates and passports. Public Health Pract (Oxf). 2021;2:100136.
56. Abdalla RO, Yousif SA, Tagelsir A, Akola M, Almaleeh A, Elhadi YA, Sabahelzain MM. The global health challenge of counterfeit vaccination certificates: the case of yellow fever vaccination among travelers departing from Khartoum International Airport in Sudan. Public Health Chall. 2022;1(4):e45.
57. Chenthara S, Ahmed K, Wang H, Whittaker F, Chen Z. Healthchain: a novel framework on privacy preservation of electronic health records using blockchain technology. PLoS ONE. 2020;15(12):e0243043.
58. Oja M, Tamm S, Mooses K, Pajusalu M, Talvik HA, Ott A, et al. Transforming Estonian health data to the Observational Medical Outcomes Partnership (OMOP) common data model: lessons learned. JAMIA Open. 2023;6(4):ooad100.
59. Hiwale M, Walambe R, Potdar V, Kotecha K. A systematic review of privacy-preserving methods deployed with blockchain and federated learning for the telemedicine. Healthc Analytics. 2023;3:100192.
60. Priisalu J, Ottis R. Personal control of privacy and data: Estonian experience. Health Technol. 2017;7(4):441–51.
61. Galvin HK, DeMuro PR. Developments in privacy and data ownership in mobile health technologies, 2016–2019. Yearb Med Inf. 2020;29(1):32–43.
62. Iyamu I, Gómez-Ramírez O, Xu AX, Chang HJ, Watt S, Mckee G, et al. Challenges in the development of digital public health interventions and mapped solutions: findings from a scoping review. Digit Health. 2022;8:20552076221102255.
63. African Union. African Union Convention on Cyber Security and Personal Data Protection. https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection (2014). Accessed 11 Dec 2023.
64. Sun N, Esom K, Dhaliwal M, Amon JJ. Human rights and digital health technologies. Health Hum Rights. 2020;22(2):21–32.
65. UNCTAD. Data protection and privacy legislation worldwide. https://unctad.org/page/data-protection-and-privacy-legislation-worldwide (2021). Accessed 13 Dec 2023.
66. Cripps M, Scarbrough H. Making digital health solutions sustainable in healthcare systems: a practitioner perspective. Front Digit Health. 2022;4:727421.
67. LeFevre A, Chamberlain S, Singh NS, Scott K, Menon P, Barron P, et al. Avoiding the road to nowhere: policy insights on scaling up and sustaining digital health. Glob Policy. 2021;12(6):110–4.
68. Principles for Digital Development. The Principles for Digital Development: a compass for those working to promote sustainable and inclusive development in today's complex digital landscape. https://digitalprinciples.org/ (2014). Accessed 13 Dec 2023.
69. Martín AQ, Lantada AD. An open source medical passport based on an android mobile application and near-field communication. SoftwareX. 2020;11:100492.
70. AlQudah AA, Al-Emran M, Shaalan K. Medical data integration using HL7 standards for patient's early identification. PLoS ONE. 2021;16(12):e0262067.
71. Ayaz M, Pasha MF, Alzahrani MY, Budiarto R, Stiawan D. The fast health interoperability resources (FHIR) standard: systematic literature review of implementations, applications, challenges and opportunities [published

correction appears in JMIR Med inform. 2021;9(8):e32869]. JMIR Med Inf. 2021;9(7):e21929.
72. Wang X, Wang Y, Xu Z, Xiong Y, Wei DQ. ATC-NLSP: prediction of the classes of anatomical therapeutic chemicals using a network-based label space partition method. Front Pharmacol. 2019;10:971.
73. Fung KW, Xu J, Bodenreider O. The new International classification of diseases 11th edition: a comparative analysis with ICD-10 and ICD-10-CM. J Am Med Inf Assoc. 2020;27(5):738–46.
74. Haroun Y, Sambaiga R, Sarkar N, Kapologwe NA, Kengia J, Liana J, et al. A human centred approach to digital technologies in health care delivery among mothers, children and adolescents. BMC Health Serv Res. 2022;22(1):1393.
75. Mason C, Lazenby S, Stuhldreher R, Kimball M, Bartlein R. Lessons learned from implementing digital health tools to address COVID-19 in LMICs. Front Public Health. 2022;10:859941.
76. Duffy A, Christie GJ, Moreno S. The challenges toward real-world implementation of digital health design approaches: narrative review. JMIR Hum Factors. 2022;9(3):e35693.
77. Kaboré SS, Ngangue P, Soubeiga D, Barro A, Pilabré AH, Bationo N, et al. Barriers and facilitators for the sustainability of digital health interventions in low and middle-income countries: a systematic review. Front Digit Health. 2022;4:1014375.
78. Labrique AB, Wadhwani C, Williams KA, Lamptey P, Hesp C, Luk R, et al. Best practices in scaling digital health in low and middle income countries. Glob Health. 2018;14:1–8.
79. Kumar K, Kumar P, Deb D, Unguresan ML, Muresan V. Artificial intelligence and machine learning based intervention in medical infrastructure: a review and future trends. Healthc (Basel). 2023;11(2):207.
80. Al Knawy B, McKillop MM, Abduljawad J, Tarkoma S, Adil M, Schaper L, et al. Successfully implementing digital health to ensure future global health security during pandemics: a consensus statement. JAMA Netw Open. 2022;5(2):e220214.
81. Bucci S, Schwannauer M, Berry N. The digital revolution and its impact on mental health care. Psychol Psychother. 2019;92(2):277–97.
82. Bakibinga P, Kamande E, Kisia L, Omuya M, Matanda DJ, Kyobutungi C. Challenges and prospects for implementation of community health volunteers' digital health solutions in Kenya: a qualitative study. BMC Health Serv Res. 2020;20(1):888.
83. Swart G. The state of the (African) Union. JoAUS. 2014;3(1):5–22.
84. Holst C, Sukums F, Radovanovic D, Ngowi B, Noll J, Winkler AS. Sub-saharan Africa-the new breeding ground for global digital health. Lancet Digit Health. 2020;2(4):e160–2.
85. van de Vijver S, Tensen P, Asiki G, Requena-Méndez A, Heidenrijk M, Stronks K, et al. Digital health for all: how digital health could reduce inequality and increase universal health coverage. Digit Health. 2023;9:20552076231185434.
86. Hui CY, Abdulla A, Ahmed Z, Goel H, Habib GMM, Hock TT, et al. Mapping national information and communication technology (ICT) infrastructure to the requirements of potential digital health interventions in low- and middle-income countries. J Glob Health. 2022;12:04094.
87. Mengiste SA, Antypas K, Johannessen MR, Klein J, Kazemi G. eHealth policy framework in low and lower middle-income countries; a PRISMA systematic review and analysis. BMC Health Serv Res. 2023;23(1):328.
88. Ekeland AG, Linstad LH. Elaborating Models of eHealth Governance: qualitative systematic review [published correction appears in J Med Internet Res. 2020;22(11):e25853]. J Med Internet Res. 2020;22(10):e17214.
89. Ngongoni CN, Wasswa W, Makubalo L, Moeti M, Chibi M. Towards a healthcare innovation scaling framework-the voice of the innovator. Int J Environ Res Public Health. 2022;19(23):15515.
90. Guo C, Ashrafian H, Ghafur S, Fontana G, Gardner C, Prime M. Challenges for the evaluation of digital health solutions-a call for innovative evidence generation approaches. NPJ Digit Med. 2020;3:110.
91. van Gemert-Pijnen JL. Implementation of health technology: directions for research and practice. Front Digit Health. 2022;4:1030194.

Publisher's Note