Privacy and Security Implications of Health Applications in Sub-Saharan Africa
By Chinasa T. Okolo PhD '23

Mobile health (mHealth) is formally defined as "the provision of health services and information via mobile technologies" [1] and has been used to help diagnose infectious diseases, record patient information, and manage medication adherence. The use of mHealth is burgeoning in Sub-Saharan Africa and throughout the rest of the global south due to the prevalence of mobile devices in households and the low implementation cost associated with establishing digital frameworks for medical care. However, the current rush to innovate within this space combined with the range of established governmental policies in regards to mHealth applications in these countries could compromise the security of patients' personal health information. Current policy regulations regarding the use of electronic services and mobile applications for healthcare vary within countries across Sub-Saharan Africa, from established governmental policies in countries such as South Africa and Rwanda to strategic frameworks with no tangible policy implementation in countries like Nigeria, Lesotho, and South Sudan [2]. Without prioritizing these considerations, mHealth solutions meant to address the problems of infectious disease diagnosis, patient care management, and healthcare information accessibility in under-resourced regions could put these already vulnerable populations at further risk of harm.

Only 3% of all healthcare workers in the world are in Africa, even though Africans make up 17% of the global population [3, 4, 5]. The shortage of medical professionals and lack of access to basic healthcare faced by many people across the African continent contributes heavily to this disparity. The ubiquity of mobile phones and strong mobile network coverage across the African continent has led to a surge of mobile innovations, mostly in the areas of finance and e-commerce. Healthcare has seen a strong shift in mobile innovations as well. Insurers in countries such as Kenya allow patients to pay using mobile money services, and various companies throughout the continent have new applications for the remote diagnosis and treatment of common medical ailments [6, 7]. While the opportunity is ripe for mHealth initiatives to thrive in Sub-Saharan Africa, existing issues are exacerbated even further by the lack of security practices integrated by the researchers and developers of mHealth applications.Along with infrastructure hampering how securely mHealth applications can be deployed across low-resource regions, informed consent, privacy, and data security are other issues affecting mHealth. Beverly Townsend, a South African lawyer who specializes in digital health in Africa, addresses these concerns in her thesis, covering the legal and ethical challenges that mobile health poses in South Africa.

In her work, she finds that privacy and confidentiality of patient health information are covered by policies and legislation in conventional patient-doctor interactions, but is unclear when it comes to mediums such as telehealth and electronic health [8]. When researching mHealth interventions designed and implemented within Sub-Saharan Africa, privacy measures and potential security implications associated with their use are discussed non-comprehensively or not even at all. With these omissions, it is unknown how these methods are affecting their target populations and if the healthcare policies of the countries where the applications are being deployed are followed. As mHealth developments scale across the continent, strong security and privacy practices are critical in ensuring the safety of patent data. With many healthcare systems in the United States and across the world experiencing data breaches and theft of personal health information, these malicious attacks could target countries within Africa next [9]. To combat this, it will be important for stakeholders such as the World Health Organization, the African Medical and Research Foundation, the Global Alliance for Africa, academic research institutions, and academic researchers to collaborate with nationwide healthcare systems to create standards for the implementation of mHealth applications.

Sub-Saharan Africa will benefit most from the opportunities provided by mHealth if robust regulations are established in countries' national health systems. The current lack of robust policies in this domain have proven challenging when designing solutions for scale, weakening the environment for mHealth innovation in countries throughout the continent [10, 11]. Despite lacking policies, it is essential for researchers to begin developing mHealth applications with the best privacy and ethical decisions in mind. Small decisions such as authenticating sign-ins, verifying who has access to patient health information, or requiring data to be securely transferred through validated servers can make progress in addressing these issues. Just because there are no regulations to enforce the methods of mHealth researchers and app developers, the design process and subsequent implementation should not compromise the health and privacy of vulnerable patients. Governments should also be proactive in forming partnerships with researchers across various fields (medicine, sociology, computer science, human-computer interaction, etc.) who are working to improve healthcare in low-resource regions. This breadth of collaboration will not only ensure that these new policies surrounding mHealth are well-developed but that they also tackle issues associated with privacy, transparency, and ethics in this domain. Generally speaking, improving how ethical considerations are incorporated into the design and deployment of mHealth systems in low-resource regions will increase their effectiveness and protect the populations they intend to serve.

Chinasa Okolo is a Computer Science PhD student in the College of Engineering at Cornell University. She can be contacted at chinasa@cs.cornell.edu.

References

1. Hagan, D., & Uggowitzer, S. (2015). Information and communication technologies for women's and children's health: a planning workbook for multi-stakeholder action. Geneva: The Partnership for Maternal, Newborn & Child Health (PMNCH); 2014.
2. The World Health Organization (WHO). (2016). "Directory of eHealth policies." Global Observatory for eHealth. https://www.who.int/goe/policies/countries/en
3. Global Burden of Disease Collaborative Network (2018). Global Burden of Disease Study 2017 (GBD 2017) Burden by Risk 1990-2017. Institute for Health Metrics and Evaluation (IHME).
4. Population of Africa (2020). Worldometer. https://www.worldometers.info/world-population/africa-population/
5. World Health Organization. (2006). The world health report 2006: working together for health. World Health Organization. https://www.who.int/whr/2006/overview/en/
6. Crul, S. (2014). The mHealth Opportunity in Sub-Sahara Africa: The Path Towards Practical Application. The Netherlands: Deloitte.
7. Krah, E. F., & de Kruijf, J. G. (2016). Exploring the ambivalent evidence base of mobile health (mHealth): A systematic literature review on the use of mobile phones for the improvement of community health in Africa. Digital health, 2, 2055207616679264.
8. Townsend, B. A. (2013). E-health, social media and the law in South Africa can ethical concerns in e-health practice be addressed through regulation? (Doctoral dissertation, University of Cape Town).
9. Patil, H. K., & Seshadri, R. (2014, June). Big data security and privacy issues in healthcare. In 2014 IEEE international congress on big data (pp. 762-765). IEEE.
10. Holst, C., Sukums, F., Radovanovic, D., Ngowi, B., Noll, J., & Winkler, A. S. (2020). Sub-Saharan Africa—the new breeding ground for global digital health. The Lancet Digital Health, 2(4), e160-e162.
11. Labrique, A. B., Wadhwani, C., Williams, K. A., Lamptey, P., Hesp, C., Luk, R., & Aerts, A. (2018). Best practices in scaling digital health in low and middle income countries. Globalization and health, 14(1), 103.