Digital data ethics in low- and middle-income countries:

The road ahead

July 2019

USAID
FROM THE AMERICAN PEOPLE

MEASURE Evaluation

Digital data ethics in low- and middle-income countries:
The road ahead

Samuel Wambugu, MPH
James C. Thomas, MPH, PhD
Denise Johnson, MA, ME
Christina Villella, MPH

July 2019

MEASURE Evaluation
University of North Carolina at Chapel Hill
123 West Franklin Street, Suite 330
Chapel Hill, North Carolina 27516
Phone: +1 919-445-9350
measure@unc.edu
www.measureevaluation.org

This publication was produced with the support of the United States Agency for International Development (USAID) under the terms of MEASURE Evaluation cooperative agreement AID-OAA-L-14-00004. MEASURE Evaluation is implemented by the Carolina Population Center, University of North Carolina at Chapel Hill in partnership with ICF International; John Snow, Inc.; Management Sciences for Health; Palladium; and Tulane University. Views expressed are not necessarily those of USAID or the United States government. TR-17-149

ISBN: 978-1-9433-6469-5

USAID
FROM THE AMERICAN PEOPLE

MEASURE
Evaluation

ACKNOWLEDGMENTS

We wish to thank the MEASURE Evaluation offices in Nairobi, Kenya and Dar es Salaam, Tanzania for helping to coordinate the field work. We are grateful to the study participants in Kenya and Tanzania for their insights. We thank the following MEASURE Evaluation staff for providing technical reviews of this report: Manish Kumar, MPH, MS, senior technical specialist for health systems strengthening; Joy Kamunyori, MCS, PMP, health informatics advisor; and Annah Ngaruro, MS, PMP, CISSP, senior technical specialist. The authors thank Cindy Young-Turner, a member of ICF's Creative Services staff, and MEASURE Evaluation's Knowledge Management unit at UNC, for reviewing and editing the report.

CONTENTS

ABBREVIATIONS

HIPAA	Health Insurance Portability and Accountability Act of 1996
HIS	health information system(s)
LMIC	low- and middle-income country
MOH	Ministry of Health
PHI	personal health information
PII	personally identifiable information
SOP	standard operating procedure
USAID	United States Agency for International Development
WHO	World Health Organization

EXECUTIVE SUMMARY

Background

Digital health contributes to strong health information systems, facilitating improved access to healthcare and quality of care, and decreased health system costs. Health data are at risk of tampering by malicious actors or inadvertent access if stored on porous and poorly maintained information systems. The thoughtful application of information technology in the health sector requires the careful integration of legal, technological, medical, and societal perspectives to safeguard the privacy of individuals and populations.

Methods

With support from the United States Agency for International Development (USAID), MEASURE Evaluation conducted an assessment of health data security, privacy, and confidentiality practices through a literature review and key informant interviews with stakeholders in the health sector in Kenya and Tanzania.

Results

Stakeholders in the two countries expressed a keen interest in the need to address the issues of data security, privacy, and confidentiality. All agreed that digital health data ethics, including security and privacy, are important but are uncharted territory in these countries. The study revealed several issues: inadequate capacity to effectively implement secure information systems; weak or non-existent legal frameworks for data protection; and lack of a dedicated unit in ministries of health, with appropriately skilled staff, to oversee data ethics. Participants in Kenya and Tanzania called for the establishment of an institutional framework for data governance that would oversee digital health data ethics issues.

Conclusions

Maintaining client confidentiality in the digital era is difficult, especially in the health sector where data are among the most sought-after by hackers. Study participants in Kenya and Tanzania stated that they need tools and expertise to help assess the preparedness of existing systems and their conformity with the changing digital health landscape; and awareness raising among health policy planners and decision makers on the need for guidance on digital data ethics. Discussions on these topics and lessons from digital health projects provide important evidence for developing or updating national digital health frameworks. This article highlights the importance of bringing data ethics to the forefront of efforts to integrate digital health in health service delivery management in low- and middle-income countries.

Key words: Digital health, data ethics, data security, data privacy, eHealth

INTRODUCTION

Health information systems (HIS) worldwide are shifting from the use of paper to electronic technologies. Although there are many advantages to digital systems, they bring new risks and require protective steps. Even in high-income countries, companies with large stores of personal data are racing to keep up with advances in nefarious techniques to penetrate data systems and misuse data. The governments of low- and middle-income countries (LMICs) are implementing electronic HIS, but are behind in building data security protections.

A wide range of information systems fall under the umbrella of digital health: health management information systems for aggregated health data; electronic medical records for facility-based patient-level data; mobile apps for use by community health workers in front-line healthcare; logistics management information systems for ensuring the delivery of essential medicines; and laboratory information systems for tracking samples and test results.

Government agencies and nongovernmental organizations are often unaware of the significant potential for harm when adopting new technologies for data management. For example, during the Ebola epidemic in West Africa in 2014, many humanitarian organizations actively encouraged governments and other organizations to share data in ways that were illegal, without user consent or the invocation of governmental emergency powers [1]. The concern extends more broadly to the proliferation of digital applications for international development, especially mobile or mHealth applications [2]. In this context, the need for countries to have their own policy frameworks, institutional structures, and a workforce that is technologically aware is paramount.

LMICs are just now beginning to address the issues and establish the necessary guidelines and frameworks for data security and privacy. A review of data policies and practices in 77 LMICs that are scaling up HIV and AIDS services found that few countries had developed appropriate guidelines [3]. In addition, many ethics review boards in LMICs have been found to be ill-equipped to respond to the increasing number and complexity of studies involving human subjects [4].

The United States Agency for International Development (USAID) supports LMICs in the development of their HIS through the MEASURE Evaluation project. The project reviewed the literature and engaged with HIS stakeholders in Kenya and Tanzania to identify:

1. Current standards in LMICs for managing digital health data, especially as they pertain to data security, privacy, and confidentiality in public health settings.
2. The practices, policies, strategies, and legal and regulatory mechanisms to support ethical practices for managing digital health data in Kenya and Tanzania.

METHODS

We addressed our objectives by: (1) reviewing peer-reviewed and gray literature; (2) interviewing HIS experts in Kenya and Tanzania; and (3) obtaining input from health informatics and ethics experts at MEASURE Evaluation who, in addition to providing their input, directed the researchers to additional gray literature relevant to the study.

Key themes identified through the initial literature review:

- Legal frameworks
- Sensitivity of data
- Local context
- Information systems security

Key themes identified through the country consultations:

- Institutional structures
- Tools and standard operating procedures

Key themes identified through expert review:

- Ethical norms
- Big data and emerging ethical concerns

Literature review

The initial targeted literature review, conducted in 2016, consisted of a search of several electronic databases for articles published from 2010 to 2016. The databases searched were Academic Search Complete database, SocINDEX with Full Text database, Social Sciences Full Text database, H.W. Wilson databases, MEDLINE with Full Text database, CINHAHL Complete database, Web of Science database, Google Scholar, and ResearchGate. We searched the databases using combinations of the following key words: confidentiality, community health worker, data privacy, data security, data use, developing countries, ethics, electronic medical records, health, HIV, low- and middle-income countries, medical records, mHealth, and privacy. The results of this initial search formed the basis of questions for the key informant interviews and focus group discussions for the country consultations in Kenya and Tanzania.

In-country interviews and discussions

We conducted the interviews in Kenya and Tanzania because both countries were in the process of enacting legal frameworks for data protection: the Data Protection Act in Kenya, and the Statistics Act in Tanzania. Both countries use a mix of paper and electronic data management systems with associated guiding documents that are in different stages of development, including policies and strategic guidelines. Both countries had recently launched their five-year strategic frameworks for eHealth. Moreover, MEASURE Evaluation has an office in each country, which facilitated logistical and administrative support for the field work.

In Kenya, we asked MEASURE Evaluation's office in Nairobi for the names of key contacts who held decision-making positions in the government's HIS, and who could provide insight on digital data broadly, and on data security and privacy specifically. We sent a similar request to the Kenya Health Informatics Association secretariat. These queries resulted in a list of 16 potential key informants. They comprised the top leadership of the country's health management information systems, including the heads of eHealth and Health Information Systems in the Ministry of Health (MOH); representatives from Nairobi and Kenyatta Universities; a representative from the Kenya Medical Research Institute (KEMRI); the Standards Officer

from the Kenya Bureau of Standard's Informatics section; a representative from the AfyaInfo and MEASURE Evaluation–PIMA projects (HIS strengthening projects supported by USAID); and a representative from the Kenya Health Informatics Association. All 16 key informants agreed to share their insights on Kenya's HIS. We interviewed them individually via email and then as a group in person.

In Tanzania, the MEASURE Evaluation office in Arusha suggested several people who held decision-making positions for the country's HIS and who could provide insights about the system. We contacted these people by email, asking to speak with them about the HIS. Those who responded were asked about other individuals who could provide insights. We contacted and interviewed a total of seven people, including the MOH's Director of eHealth, and representatives from projects working with the MOH to strengthen the health management information systems. The latter group included representatives of projects run by nongovernmental organizations, such as MEASURE Evaluation, PATH, Palladium, and D-Tree International. We attempted to establish an advisory group similar to the one formed in Kenya, but it was not possible due to distance and conflicting schedules. Therefore, these respondents were interviewed individually by email and in person, but not as a group.

Identification of themes

We identified themes through an iterative process. Starting with the articles identified in the literature review, we identified several most commonly mentioned topics. Those topics informed the semi-structured interviews we conducted with the respondents. The respondents then shared their perspectives on those topics in our email communications and in face-to-face interviews. We took handwritten notes on the topics covered during the face-to-face interviews and transcribed the notes to a word processing program. Two of the authors (SW and DJ) examined the email communications and transcribed interview notes visually to identify additional themes mentioned by the respondents. We then referred to the grey literature and websites for any information to further flesh out important details of the themes emerging from the respondents.

RESULTS

We identified 27 potentially relevant abstracts. We eliminated ten after reading the full articles because they did not discuss data security, privacy, and confidentiality in public health. We identified themes in the remaining 17 articles by reading the full articles and recording key terms and concepts that were repeatedly mentioned. The themes emerging from the literature review were legal frameworks and ethical norms; data sensitivity; new technologies; systems security; and tools and standard operating procedures (SOPs). Institutional structures was an additional theme that emerged from the interviews with respondents. The following sections are organized by these six themes.

Legal frameworks and ethical norms

Although 70 percent of 113 countries surveyed by the World Health Organization (WHO) had legislation related to basic privacy rights, only 30 percent of those countries had legislation on the privacy of electronic health records [5]. Even fewer countries had legal frameworks for electronic health records that addressed more than privacy. A lack of policies and legal frameworks on such topics as data ownership, confidentiality, and security has been identified as a major challenge to scaling up eHealth in LMICs [6]. Apart from official government policies, many international and humanitarian organizations have begun to develop data privacy and security principles that address some of the ethical issues in response to the rapidly growing amount and use of data globally. For example, the United Nations Global Pulse Initiative has developed policies pertaining to data minimization (using the least amount of data needed); data retention (storing data for a project for only the necessary time period); and data sensitivity (using stronger policies when conducting research on vulnerable populations) [7].

Respondents in Kenya and Tanzania shared a keen awareness of the need to address the issues of data security, privacy, and confidentiality in the era of digital health. The discussions revealed that ethics for digital health data are important, but an uncharted territory. The two countries are in the process of enacting legal frameworks for data protection: the Data Protection Act in Kenya and the Statistics Act in Tanzania. Prior to the adoption of these legislative frameworks, both countries laid some groundwork for information system security and patient confidentiality through existing MOH standards and guidelines.

Institutional structures

Apart from laws, regulations, and policies, institutional structures are often described in terms of leadership and governance. For example, the WHO-International Telecommunication Union eHealth Strategy Toolkit lists leadership and governance as key components of the eHealth enabling environment [8]. The Toolkit describes leadership and governance as "components required to direct and coordinate national, state, regional and local eHealth activities towards the delivery of a national eHealth environment." Leadership and governance include program management, stakeholder engagement, management and operations, monitoring and evaluation, and policy oversight. In Nigeria, an assessment of the eHealth enabling environment found that the Federal Ministry of Health and Federal Ministry of Communication Technology are responsible for the governance of digital health. Between the Federal Ministry of Health and the Federal Ministry of Communication Technology, more than 15 stakeholder departments and agencies have a role in leading digital health [9].

Respondents noted that the lack of institutional structures in the MOHs in Kenya and Tanzania charged with overseeing data ethics was a major limiting factor in the application of data ethics in digital health. Participants felt the need for a dedicated unit to support ethical considerations in the application of digital health, and personnel with appropriate skills, responsibility, and authority. They also called for the establishment of an institutional framework for data governance, noting that a clearly defined approach would help in systematically building the structure for data ethics in digital health.

Data sensitivity

Globally, many countries have established data protection frameworks that classify personally identifiable information (PII) (an individual's name, birthdate, and address) as important for protection, and that classify personal health information (PHI), in particular, as highly sensitive. The importance of protecting PHI has often been noted in the case of HIV infections [10]. The United Nations Guidelines on HIV Surveillance state that populations targeted for HIV surveillance are already among the most vulnerable and should be given special protection and consideration because of the increased risk of harm due to stigma, economic loss, or legal liability [11]. In this context, the guidelines provide basic digital data security procedures, such as ensuring that data are password-protected and encrypted, and that all PII is stripped from forms before data entry.

Country participants reported that the importance of data security, privacy, and confidentiality are generally recognized, but that procedures for ensuring them need to be better understood and upheld. Respondents noted that the financial sector has taken the lead in the protection of PII and can provide valuable lessons. They also stated that the lack of attention to these issues by the health sector began with paper-based systems and continues with digital systems. The digital health environment presents a higher risk for harm, especially because it provides a platform for the wide sharing of data that, if compromised, can affect large numbers of people. Moreover, hackers have used ransomware in developed countries to freeze access to medical records, demanding a payment before access is restored. Financial losses affecting healthcare providers or care seekers and compromised medical records can erode patients' and providers' trust in using electronic health systems [12]. As digital health becomes a common tool for business in LMICs, hackers could infiltrate and frustrate health systems and care givers.

New technologies

Access to mobile phone technology has rapidly expanded in developing countries [13]. Decreasing costs, increasing coverage, and ease of use by people with low literacy skills open up new possibilities for this technology by the health system [14]. The availability and ease of use of mobile phones give on-the-ground health workers an unprecedented ability to rapidly collect and transmit detailed data. Rebecca Braun and her colleagues noted that "when equipped with mobile devices, CHWs [community health workers] became capable collectors of complete, high-quality, and timely data from the field" [15]. Placing a powerful multimedia tool in the hands of untrained workers has implications. For example, patients interviewed by community health workers using mobile phones have expressed concerns that the interviewers might use the phone camera to film or photograph them [16].

Systems security

Over the past decade, high-income countries have passed legislation on the protection of individual health data through technological, procedural, and policy requirements. An important element of these protections has been the mapping of government legislation and regulation to practical security guidelines. These laws, including the Health Insurance Portability and Accountability Act of 1996 (HIPAA) in the United States and the National eHealth Security and Access Framework in Australia, have established national standards for the security and privacy of patient health data [17, 18]. In their review of policies about electronic health record systems in low-, middle-, and high-income countries, Rezaeibagha, Win, and Susilo [19] classified the security and privacy policies and regulations they reviewed in seven categories:

- Access control
- Authorization
- Delegation
- Governing and regulations
- Disclosure
- Sharing and integrating
- Medical regulations

The respondents in Kenya and Tanzania spoke about the shortage of the expertise needed to implement information system security. They emphasized the inconsistent application of existing technical standards in digital information systems, attributing it to the lack of expertise of software developers and insufficient national guidelines to support the application of security best practices in the health sector. The participants underscored the strong focus on general interoperability of information systems and other aspects of information system design without a specific focus on information system security. They also mentioned that the MOH and stakeholders were interested in benefitting from the efficiencies delivered by digital health but have not examined the threats that come with it. Respondents emphasized the lack of expertise in cyber security, which is needed to implement the necessary system security controls and to conduct information system security audits. This is understandable because information system security constitutes a specific information technology skillset, which is in short supply globally. The independent, nonprofit, global association, ISACA, predicts that there will be a global shortage of two million cyber security professionals by 2019 [20].

Tools and SOPs

Some promising tools and SOPs for digital health have been developed in recent years, drawing on several disciplines. During a discussion of the Principles for Digital Development (https://digitalprinciples.org), participants highlighted the ability of a "risk, harms, and benefits" framework to bring together information from technological, programmatic, and legal or regulatory perspectives. This can help decision makers understand and balance the potential benefits of a given information technology initiative against the risks and potential for harm [7]. A 2018 post on the Information Communication Technologies for Development website highlighted the use of threat modeling to gain a comprehensive overview of the threats to a digital

health effort. After digital health practitioners gain a comprehensive understanding of the threats to digital health data, decision makers can then determine how to mitigate those threats [21].

The Kenya participants mentioned that data quality SOPs and audits are routine and are institutionalized in the MOH's data management processes. They suggested that data quality audits could therefore serve as a vehicle for incorporating ethical controls and could be used until key normative frameworks and institutional structures are established.

DISCUSSION

Digitized information is powerful. It can combine many sources and provides an expansive perspective on an individual. The wide adoption of digital health and the growing enthusiasm for sharing data without due regard for responsible data practices can bring harm to people. Fear of exposure of one's PII can be a deterrent to accessing services at facilities that use technology to capture and manage data. The implementation of ethical principles allows a country to harness the power of electronic data for the good of the population and to minimize the harm. As countries embrace digital opportunities, a strong culture of data ethics is paramount.

Technology is evolving so fast that regulatory mechanisms are always playing catching up. In sub-Saharan Africa, the use of digital systems to collect and manage sensitive PHI is nascent but growing rapidly. Enthusiasm for the use of digital HIS is high, catalyzed, in part, by the need for better data to guide health programs and policies. Many of the digital information systems were developed to satisfy a narrow need, such as improving cost efficiency or accounting for funds donated by multilateral or bilateral agencies. The Balkanized set of specific systems lack a unified philosophy and practices for data security. Our respondents reported that discussions around digital data ethics have not been integrated in the national HIS or digital health data management. As we found in the literature review, laws and other regulatory instruments on how to manage digital and sensitive health data in LMICs are either non-existent or are in the formative stages [5, 6].

Study participants in Kenya and Tanzania were emphatic in expressing their need for tools and expertise to help them (1) assess their existing systems' preparedness or conformity with the changing digital health landscape; (2) raise awareness among the country's health policy planners and decision makers on the need for digital data ethics; and (3) influence responsible data practices.

The field of digital health in LMICs is in short supply of people with the skills to match the fast growth and increasing complexity of digital information systems. For this reason, LMICs should tap the expertise in high-income countries. For example, LMICs are seeking support in establishing SOPs to guide them through these uncharted waters. However, standards are insufficient on their own. They need to be enforced by governance mechanisms with the involvement of the right stakeholders and authority. Efforts to institutionalize digital health data ethics should be broad-based. They should bring together the necessary domain expertise in legal and ethical norms, information systems security, data management, healthcare delivery, and community contexts. A context-specific and rigorous maturity model can provide LMICs with a tool for measuring their capabilities for implementing digital health activities ethically and identifying pathways for improvement. Maturity models are a common approach in the information technology domain to assess the "as is" situation and generate action toward a future "to be" state [22]. Constructing and testing a model for digital health data ethics could provide countries with a common framework for prioritizing action.

The cultural, economic, and political contexts of data systems can impede the ethical use of data. For example, in a hierarchical organizational culture, data analysts may avoid sharing results that do not agree with their supervisor's preconceived agenda [23]. In our study, we found that the countries' perspectives on data ethics were founded in decades of paper-based systems and had not yet adapted to the new digital

technologies. To be effective, the content (e.g., prescribed procedures) and contexts (e.g., organizational expectations) should reinforce each other. Yet, contexts are typically slow to change, and one cannot wait for contextual change to produce the needed content if they are not aligned. Rather, the establishment of policies and procedures that protect the security of PHI may raise topics for which people were previously unaware. And once aware, they may come to expect the systems in which they participate to follow the procedures. Therefore, in some instances, the establishment of policies and procedures can lead to a cascade of system components that bring about a supportive context.

Our respondents in Kenya and Tanzania expressed an interest in pursuing such a path. MEASURE Evaluation is a cooperative agreement with USAID, which allows for the project to suggest to USAID Missions activities that the project could implement. Following the present study and the expression of interest by stakeholders in Kenya, we suggested to the USAID/Kenya Mission an activity in which we would work with stakeholders to strengthen data security in the country HIS. However, the Mission did not regard the suggested activity as a high priority and thus did not agree to it.

LIMITATIONS

This study of the perspectives of HIS stakeholders on the status and needs of health data security in Kenya and Tanzania is informative because it draws from those in the best position to know the situation on the topic in their respective countries. The utility of these findings is limited, however, because awareness of digital security concerns is evolving rapidly, and LMICs in particular do not have the resources to keep up with the developments. Thus, in some instances, our stakeholders may not have even been aware of data security concerns or steps to protect data security that are becoming standard in developed countries. These issues, then, may be missing from our analysis.

CONCLUSIONS

We conclude from this study that HIS in Kenya and Tanzania are not adequately prepared to address known data security issues, and that the stakeholders most informed about the HIS data security are aware of many security concerns but lack the mandate and the resources to address them. In the absence of up-to-date data security policies and processes, ethical breaches may be inevitable. Data breaches can have the effect of lowering public and professional trust in the system. When a system is distrusted, those for whom the system is intended—be they patients, providers, or policy makers—may avoid contributing data to it or avoid investing their time to maintain it. Thus begins a vicious cycle of disuse and distrust.

We assert that data security is essential to data quality, HIS utility, and the long-term sustainability of an HIS. We have identified a glimpse of the improvements needed in Kenya and Tanzania, and the interest of stakeholders in making those improvements. Future research might address the institutional barriers to the allocation of resources to HIS data security, as well as elements within societies that facilitate and accelerate adoption of protections for patients' health data.

Ethical Approval

Institutional review board approval was not necessary because no private or personal data were collected.

Authors' contributions

Samuel Wambugu led the study and the writing of the manuscript. James C. Thomas, as a subject expert, provided guidance during all stages of the study and reviewed the manuscript. Denise Johnson and Christina Villella conducted the literature review, analyzed fieldwork notes, and wrote the seminal report on which this manuscript is based.

REFERENCES

1. McDonald SM. Ebola: A big data disaster: privacy, property, and the law of disaster experimentation. Bengaluru and Delhi, India: The Centre for Internet and Society; 2016. http://cis-india.org/papers/ebola-a-big-data-disaster.

2. Woodard J. The dangers of legal ignorance in digital development. 2016. http://www.ictworks.org/2016/06/17/the-dangers-of-legal-ignorance-in-digital-development/. Accessed 6 June, 2018.

3. Beck EJ, Mandalia S, Harling G, Santas XM, Mosure D, Delay PR. Protecting HIV information in countries scaling up HIV services: a baseline study. J Int AIDS Soc. 2011;14:6. https://www.ncbi.nlm.nih.gov/pubmed/21294916.

4. IJsselmuiden C, Marais D, Wassenaar D, Mokgatla-Moipolai B. Mapping African ethical review committee activity onto capacity needs: the MARC initiative and HRWeb's interactive database of RECs in Africa. Dev World Bioeth. 2012;12(2):74–86. https://www.ncbi.nlm.nih.gov/pubmed/22512919.

5. World Health Organization. Legal frameworks for eHealth: based on the findings of the second global survey on eHealth. Geneva, Switzerland: World Health Organization; 2012. http://apps.who.int/iris/handle/10665/44807.

6. Delponte L, Grigolini M, Moroni A, Vignetti S, Claps M, Giguashvili N. ICT in the developing world. Brussels, Belgium: Science and Technology Options Assessment, Scientific Foresight Unit; 2015. http://www.europarl.europa.eu/RegData/etudes/STUD/2015/563482/EPRS_STU(2015)563482_EN.pdf.

7. United Nations Global Pulse. Privacy and data protection principles. 2018. http://www.unglobalpulse.org/privacy-and-data-protection. Accessed 6 June, 2108.

8. World Health Organization (WHO) and International Telecommunication Union (ITU). National eHealth strategy toolkit. Geneva, Switzerland: WHO and ITU; 2012. http://apps.who.int/iris/bitstream/10665/75211/1/9789241548465_eng.pdf?ua=1.

9. United Nations Foundation. Assessing the enabling environment for ICTs for health in Nigeria: A review of policies. New York, NY: United Nations Foundation; 2014. http://www.unfoundation.org/assets/pdf/nigeria-policy-report.pdf.

10. Cannovo N, Paternoster M, Burlin I, Colangelo M, Graziano V. Ethical and psychosocial aspects of HIV/AIDS. In Barrios E., editor. HIV-infection—impact, awareness and social implications of living with HIV/AIDS. Rijeka, Croatia: InTech; 2011. http://www.intechopen.com/books/hiv-infection-impact-awareness-and-social-implications-of-living-with-hiv-aids/ethical-and-psychosocial-aspects-of-hiv-aids.

11. World Health Organization. Guidelines on surveillance among populations most at risk for HIV. Geneva, Switzerland: WHO; 2011. http://www.unaids.org/sites/default/files/en/media/unaids/contentassets/documents/epidemiology/2011/20110518_Surveillance_among_most_at_risk.pdf. Accessed 6 June, 2108.

12. Cohen IG, Hoffman S, Adashi EY. Your money or your patient's life? Ransomware and electronic health records. Ann Intern Med. 2017;167:587–588. http://annals.org/aim/fullarticle/2654048/your-money-your-patient-s-life-ransomware-electronic-health-records.

13. Aranda-Jan CB, Mohutsiwa-Dibe N, Loukanova S. Systematic review on what works, what does not work and why of implementation of mobile health (mHealth) projects in Africa. BMC Public Health. 2014;14:188. http://bmcpublichealth.biomedcentral.com/articles/10.1186/1471-2458-14-188.

14. Leon N, Schneider H, Daviaud E. Applying a framework for assessing the health system challenges to scaling up mHealth in South Africa. BMC Medical Informatics and Decision Making. 2012;12:123. http://bmcmedinformdecismak.biomedcentral.com/articles/10.1186/1472-6947-12-123.

15. Braun R, Catalani C, Wimbush J, Israelski D. Community health workers and mobile technology: a systematic review of the literature. PloS One. 2013;8(6):e65772. http://journals.plos.org/plosone/article?id=10.1371/journal.pone.0065772.

16. van Heerden A, Norris S, Tollman S, Richter L, Rotheram-Borus MJ. Collecting maternal health information from HIV-positive pregnant women using mobile phone-assisted face-to-face interviews in Southern Africa. J Med Internet Res. 2013;15(6):e116. https://www.ncbi.nlm.nih.gov/pubmed/23748182.

17. HIPAA News. Protecting the privacy of personal health information. http://hipaanews.org/. Accessed 6 June, 2108.

18. Australian Digital Health Agency. Australian national eHealth security and access framework, v 4.0. Sydney, Australia: Australian Digital Health Agency; 2014. https://www.digitalhealth.gov.au/implementation-resources/ehealth-foundations/national-ehealth-security-and-access-framework.

19. Rezaeibagha F, Win KT, Susilo W. A systematic literature review on security and privacy of electronic health record systems: technical perspectives. Health Information Management Journal. 2015; 44(3):23–38. http://journals.sagepub.com/doi/abs/10.1177/183335831504400304.

20. Kauflin J. The fast-growing job with a huge skills gap: cyber security. Forbes. March 16, 2017. https://www.forbes.com/sites/jeffkauflin/2017/03/16/the-fast-growing-job-with-a-huge-skills-gap-cyber-security/#224b208e5163.

21. ICTWorks. What's your ICT4D cyber threat model? November 18, 2015. http://www.ictworks.org/2015/11/18/whats-your-ict4d-threat-model/.

22. Fettke P, Zwicker J, Loos P. Business process maturity in public administrations. In: vom Brocke J, Rosemann M., editors. Handbook on business process management 2. Berlin, Germany: Springer; 2010. p. 485–516.

23. Thomas JC. Contextual factors affecting receptivity to an information culture. Glob Public Health. 2017;12(12):1568-1578. https://www.ncbi.nlm.nih.gov/pubmed/27841079.

MEASURE Evaluation
University of North Carolina at Chapel Hill
123 West Franklin Street, Suite 330
Chapel Hill, North Carolina 27516
Phone: +1 919-445-9350
measure@unc.edu
www.measureevaluation.org

This publication was produced with the support of the United States Agency for International Development (USAID) under the terms of MEASURE Evaluation cooperative agreement AID-OAA-L-14-00004. MEASURE Evaluation is implemented by the Carolina Population Center, University of North Carolina at Chapel Hill in partnership with ICF International; John Snow, Inc.; Management Sciences for Health; Palladium; and Tulane University. Views expressed are not necessarily those of USAID or the United States government. TR-17-149

ISBN: 978-1-9433-6469-5

USAID
FROM THE AMERICAN PEOPLE

MEASURE
Evaluation