mHealth Data Security, Privacy, and Confidentiality:

Guidelines for Program Implementers and Policymakers

January 2018

USAID FROM THE AMERICAN PEOPLE

PEPFAR

MEASURE Evaluation

mHealth Data Security, Privacy, and Confidentiality:

Guidelines for Program Implementers and Policymakers

Lauren Spigel, MPH
Samuel Wambugu, MPH, PMP
Christina Villella, MPH

January 2018

MEASURE Evaluation
University of North Carolina at Chapel Hill
123 West Franklin Street, Suite 330
Chapel Hill, NC, USA 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. MS-17-125A

ISBN: 978-1-64232-003-9

USAID FROM THE AMERICAN PEOPLE PEPFAR MEASURE Evaluation

ACKNOWLEDGMENTS

These guidelines are the result of many people's hard work. Lauren Spigel, Samuel Wambugu, and Christina Villella—all of MEASURE Evaluation, ICF—led the development of the guidelines from start to finish. We thank Steven Wanyee of IntelliSOFT Kenya and Irene Okwara, who helped coordinate the Kenya workshops; Frances Baaba da-Costa Vroom, of the University of Ghana School of Public Health, and Debbie Mangortey (independent consultant) organized the Ghana workshops. We also thank all of the workshop participants, who reviewed the guidelines and provided invaluable feedback and contributions to strengthen this resource (see Appendix B).

We recognize technical review, guidance, and support from Ana Djapovic Scholl, of the United States Agency for International Development. We appreciate the thorough review of these guidelines by a team of digital health experts: Olivia Velez and Denise Johnson, of ICF; Joy Kamunyori, of MEASURE Evaluation, ICF; and Manish Kumar, of MEASURE Evaluation, University of North Carolina at Chapel Hill.

We are grateful to those who gladly shared their case studies to enrich the guidelines: Cathy Mwangi, Tychus Nyanga, Harris Dindi, and Collins Mudogo, of MHealth Kenya limited, and Reina Marie-Antoinette Mwinbang Der, of FHI360/Ghana.

We recognize the meticulous work of ICF's editor, Cindy Young-Turner, and ICF's creative services team for the design and layout work, and MEASURE Evaluation's Knowledge Management team for the overall review, branding, publication, and dissemination of the guidelines.

CONTENTS

Figures

Tables

ABBREVIATIONS

ePHI	electronic personal health information
HIS	health information system(s)
ICT	information communication technology
LMIC	low- and middle-income country
OS	operating system(s)
PHI	personal health information
SMS	Short Message Service

GLOSSARY

application	Any mHealth tool, regardless of mobile platform
breach	"An impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information" (Office for Civil Rights, U.S. Department of Health and Human Services, 2013)
Cloud computing	A technology in which information technology resources are provided as services via Internet (Kalaiselvi, Kousalya, Varshaa, & Suganya, 2016)
Cloud-based server	A server that is run by a third party that sells space to organizations for data storage (Kalaiselvi, Kousalya, Varshaa, & Suganya, 2016)
Confidentiality	"The obligations of those who receive information to respect the privacy interests of those to whom the data relate" (Cohn, 2006)
Dedicated local server	A server that is reserved for serving the specific needs of a project. It is often owned and stored by the organization or government that owns the mHealth project data.
eHealth	The use of information and communication technologies for health (World Health Organization, 2017)
eHealth strategy	The product of a country's strategic planning process for developing or continuing to build out investments in digitizing its health information systems (World Health Organization & International Telecommunication Union, 2012)
Encryption	A process by which information is converted to a code to protect sensitive data (Arora, Yttri, & Nilson, 2014)
Geofencing	The use of GPS technology to trigger a response if the device leaves a specific geographic region
Geolocation	A process to locate a device, such as mobile phone, through the Internet or mobile network
ISO20000 standards	A service management system standard that specifies requirements for the service provider to plan, establish, implement, operate, monitor, review, maintain, and improve the system
mHealth	Use of mobile wireless technologies for public health (World Health Organization, 2017)
Personally identifiable information	Data relating to an individual who can be identified directly or indirectly by the data or by linking the data to other information reasonably available (United Nations Development Group, 2017)
Phishing	An attempt to gain access to sensitive information by disguising oneself as a trustworthy entity

Principles for Digital Development	Guidelines that can help "practitioners integrate established best practices into technology-enabled programs" (Principles for Digital Development, 2017)
Privacy	"An individual's right to control the acquisition, uses, or disclosures of his or her identifiable health data" (Cohn, 2006). This includes any information the person wants to keep private.
Security	"Physical, technological, or administrative safeguards or tools used to protect identifiable health data from unwarranted access or disclosure" (Gejibo, 2015)
Sensitive data	All personal data relating to religious, philosophical, political, and trade union opinions and activities, as well as to sex life or race, health, social measures, legal proceedings, and penal or administrative sanctions (African Union, 2014)
Server	"A computer in a network that is used to provide services (such as access to files or shared peripherals or the routing of e-mail) to other computers in the network" (Merriam-Webster, 2017)
Virtual private network	"A method of creating secure connections between mobile devices and the back end while using public, often unsecured networks" (Grandison, 2017)

PREFACE

Information technology is spreading fast, and its adoption in the health sector is gaining ground rapidly. Under the banner of eHealth, mHealth, or digital health, mobile technology (such as laptop computers, mobile phones, and tablets) has become an indispensable tool to increase health coverage. As countries strive toward universal health coverage, mobile wireless technologies—mHealth tools—in support of enumeration, registration, and unique identification of patients, along with maintenance of health records, will facilitate improved health system performance. Electronic forms and registry systems will enable routine monitoring of the coverage of essential interventions for individuals in relevant populations.

Because mobile technology is widespread, governments and organizations are harnessing their power to collect, collate, transmit, and present data in a timely fashion, thereby overcoming barriers inherent in paper-based systems. The rapid progression of technology enables the increased sharing of data between electronic systems. This can provide decision makers with valuable data and improve their ability to make critical decisions on health programs.

As healthcare organizations turn to mobile devices to improve efficiency and productivity, many are introducing risks that could all too easily result in a data breach and the exposure of protected health information. Organizations around the world are taking note and providing guidelines on how to safeguard electronic personal health information (ePHI).

Building the infrastructure to safeguard ePHI is an evolving area. High-income countries have not found a lasting solution to this problem, much less the low- and middle-income countries (LMICs). Technology is changing so fast that keeping up with all the issues of security and privacy is daunting. LMICs lack national and comprehensive instruments such as laws and guidelines to protect the data-rich digital health sector. A few high-income countries have established laws and policies for healthcare data privacy and confidentiality from which other countries can learn.

Privacy generally refers to patients having substantial control over the extent, timing, circumstances, and sharing of information about oneself with others (Golstin, et al., 2003). Confidentiality refers to the treatment of identifiable information that has been disclosed to others in relation of trust and with the expectation that it will not be divulged to others except in previously agreed-upon ways. Protecting a person's health information is particularly important for sensitive health issues such as HIV and for stigmatized populations that are at elevated levels of acquiring sexually transmitted diseases, including HIV.

In its October 2017 Cybersecurity Newsletter, the United States Department of Health and Human Services Office for Civil Rights reminded insured entities of the risks associated with mobile devices that are used to create, receive, maintain, or transmit ePHI. Entities covered by the Health Insurance Portability and Accountability Act were reminded of the need to conduct an organization-wide risk assessment and develop a risk management plan to address all mobile device security risks identified during the risk analysis and reduce them to an appropriate and acceptable level. Although many covered entities allow the use of mobile devices, some prohibit the use of those devices to create, receive, maintain, or transmit ePHI. These risks are not specific to the United States; data breach incidents continue to plague healthcare organizations around the world. The potential cost to the healthcare industry could be as much as $5.6 billion annually (Patrick, 2014). Often these devices are also used for personal digital activities, such as calling, texting, playing games, taking photos, web browsing, e-mailing, and accessing social media. Given that mobile devices are not always connected to secure Internet, these

personal activities may inadvertently expose the device to viral attacks and other security risks, leading to data breaches. In addition, due to their portability, mobile devices are susceptible to breakage, loss, and theft. Cyber-attacks are also increasingly common, especially targeting sensitive health data stored on digital health systems (Goldman, 2017; Institute for Critical Infrastructure Technology, 2016).

The media are increasingly reporting instances of breaches in the security of large amounts of electronically stored personal data. Attracted by both the sensitivity and utility of health data, hackers are always devising new ways to gain access. They exploit vulnerabilities in the software, device, or data transmission channels, sometimes with far-reaching ramifications. If health services data are stolen, clients can be exposed to social or economic risks and their trust in those services would diminish. In addition, if data are compromised, health managers may be making decisions based on inaccurate data. Countries and programs must therefore continuously review and tighten their technology tools, rules, and regulations to protect patients' health data.

International law recognizes the individual right to privacy. Privacy is a basic human right. For example, the International Covenant on Civil and Political Rights and the European Convention on Human Rights and Fundamental Freedoms acknowledge the individual right to privacy. Many countries have privacy laws, either as omnibus data protection regulation such as the European laws or general personal data protection laws. These kinds of laws give equal weight to all types of personal data. The U.S. laws are different; they are more specific and are categorized by different sectors, ensuring that protection measures of certain types of data are more stringent (Trustlaw Connect, et al., 2013). In fact, the United States has enacted laws to protect health and medical data through the Health Insurance Portability and Accountability Act. LMICs have expressed interest in establishing data protection regulations, but few have enacted such mechanisms. The countries that have enacted these kinds of protections are Kenya, Mauritius, Morocco, and South Africa (TrustLaw Connect, et al., 2013). Many other countries have ethical codes of practice for medical workers who come into contact with privileged patient information. The World Health Organization's 1994 Declaration on Promotion of Patients' Rights recognizes a patient's right to privacy.

To understand and frame the digital health landscape issues of personal health information privacy and confidentiality, particularly in an mHealth environment, MEASURE Evaluation, with funding from the United States Agency for International Development, conducted a landscape analysis. Its results are reported in *mHealth for Low- and Middle-Income Countries—Challenges and Opportunities in Data Quality, Privacy, and Security* report (Wambugu & Villella, 2016). The landscape analysis was conducted in two countries (Kenya and Tanzania), but the results broadly portray the situation of LMICs, especially in the African region. The main objective of that analysis was to help understand the data security and privacy practices and the preparedness of countries in the sub-Saharan region to tackle emerging data ethics issues. This landscape analysis was supplemented by a review of gray and peer-reviewed literature on this subject. The findings were telling. They show that digital systems are nascent but developing fast, and there is need for strong leadership for national health information systems (HIS) to establish or improve existing governance mechanisms. In addition, standard operating procedures were commonly cited as tools that countries need to guide issues of data security and privacy (Wambugu & Villella, 2016).

The landscape analysis report recommended developing data security, privacy, and confidentiality guidelines that HIS managers and policymakers can use to guide their digital health work. That's why we developed this document: *mHealth Data Security, Privacy, and Confidentiality: Guidelines for Implementers and Policymakers*, and its companion checklist, which is available here: https://www.measureevaluation.org/resources/publications/ms-17-125b.

In developing these guidelines over the course of a year, we reviewed the landscape analysis report; searched and analyzed additional gray and peer-reviewed literature; spoke with subject matter experts; and, in line with the Principles for Digital Development, engaged with country advisory teams in Kenya and Ghana. Ghana was included, because we intended to leverage other MEASURE Evaluation work in the country and assess that country's interest in having the guidelines.

mHealth technology comprises many layers that can affect data security, privacy, and confidentiality throughout the data life cycle. These layers include national and organizational policy; technology used in data collection, management, storage, and use; as well as user behavior. Each layer requires careful analysis to identify and protect potential vulnerabilities. The sensitivity of health data requires that the developers of mobile apps for health should build systems that have a secure back-end database; keep minimal or no personal health information data on the device; and ensure that the hardware, software, and communication channels between the device and other systems are secure.

These guidelines are meant to help mHealth program managers and ministry of health officials systematically address mHealth data privacy and security issues. For each of the layers of technology, these guidelines explore common vulnerabilities and propose ways to proactively address them to reduce possibilities of data breaches.

The guidelines also address overarching topics, such as national data leadership and governance, user behavior, and training. Other topics are technology-specific, such as mobile devices (hardware), operating systems, applications, networks, and data storage. To demonstrate how elements described in these guidelines have been applied in programs, two case studies are included. In addition, an accompanying checklist provides users with a structured mechanism to assess the strengths and gaps of each of the mHealth components.

These guidelines and the corresponding checklist are meant to be implemented at the national, subnational, or program level, and they are public goods that countries and organizations can use to strengthen the security, privacy, and confidentiality of their respective mHealth programs and national HIS. Like most other tools in the digital health space, these guidelines are living documents. They will undergo regular updates based on new lessons and to keep them attuned to the ever-evolving health and technology ecosystem.

INTRODUCTION

What is the purpose of these guidelines?

These guidelines are intended to strengthen national HIS, by providing a tool to guide decisions on security, privacy, and confidentiality of personal health information (PHI) collected and managed using mobile devices.

Who is the audience for these guidelines?

These guidelines are intended for nongovernmental mHealth program managers as well as ministry of health policymakers and HIS officers who use mHealth programs. Each group will use the guidelines differently, depending on their level of operation in the health system, priorities, and needs. This list of intended audiences is not comprehensive. As the use of mHealth increases, the audience for these guidelines could expand. It is also important to note that the guidelines are not "one size fits all." They are intended to be adapted to meet the specific needs of programs and countries.

Table 1. Intended audiences for the guidelines

Nongovernmental Organizations
mHealth program managers: mHealth program managers are responsible for overseeing the design, development, deployment, and implementation of a wide range of mHealth programs. These guidelines specifically focus on security, privacy, and confidentiality aspects of data management, so mHealth program managers will find them useful for thinking through how to safeguard data that are collected on mobile devices and stored in the mHealth ecosystem.
Ministry of Health
HIS officers: HIS officers are responsible for supporting the health information management system of the country. This includes managing staff, building staff capacity, and developing HIS guidelines and quality improvement protocols. HIS managers will find these guidelines useful for building capacity of staff whose responsibilities include overseeing data security, privacy, and confidentiality; maintaining the security, privacy, and confidentiality of patient data; and integrating guidelines in national HIS frameworks. **Policymakers:** Although the position will vary from country to country, HIS officials, health information leads, or information communication technology managers of ministries of health are responsible for overseeing digital health assets and programs, as well as outlining national strategy related to digital health. These ministry officials will find these guidelines useful for building the capacity of their department to oversee the security, privacy, and confidentiality of mHealth programs in the country. They can also use these guidelines to direct mHealth implementers on how to increase the security, privacy, and confidentiality of their mHealth programs.

These guidelines are limited in scope, because their goal is not to transform a ministry official or an mHealth program manager into an expert on digital data security. The guidelines, instead, can serve as a building block that will allow stakeholders to be informed managers of a team responsible for developing and implementing responsible data practices, especially data security and privacy.

What are security, privacy, and confidentiality?

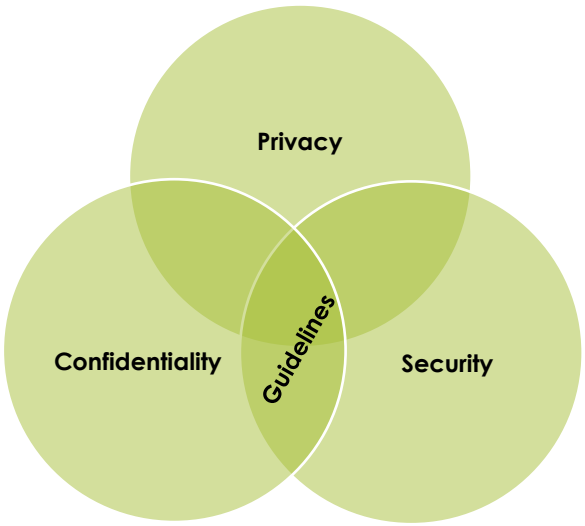
Security, privacy, and confidentiality are interrelated, but there are distinctions between the terms, as follows:

- **Security** refers to the technology infrastructure that protects sensitive information.
- **Privacy** refers to the client's right to control what "individually identifiable health information" is collected, used, and shared (HealthIT.gov, 2016).
- **Confidentiality** refers to the obligation to keep sensitive information private. It is a mechanism for protecting privacy.

What information is contained in these guidelines?

These guidelines are built on the premise that securing technology, improving the skills of technology users, and establishing a supportive environment can improve protection of sensitive client data from malicious or inadvertent access. They focus on the intersection between security, privacy, and confidentiality for mHealth programs. Figure 1 provides a visual representation of the scope of these guidelines.

Figure 1. Overlaps between mHealth data security, privacy, and confidentiality



In addition, these guidelines focus **on mHealth programs that collect personal health data,** which are also referred to as "sensitive data." Consequently, mHealth programs that focus on behavior change communication and eLearning are beyond the scope of these guidelines, unless they collect sensitive data from their users.

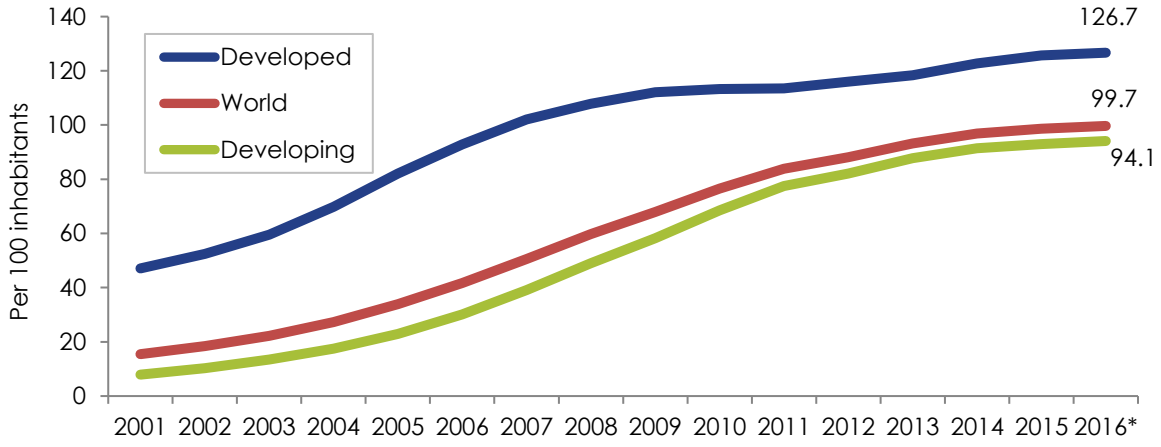
The primary assumption of these guidelines is that, by strengthening technological, administrative, and physical safeguards surrounding mobile devices, sensitive personal health data are also more likely to be kept both private and confidential. The authors acknowledge that provider behavior outside the mobile technology ecosystem also contributes to client data privacy, security, and confidentiality, but this is beyond the scope of these guidelines. The authors developed Figure 2 as a visual model of the guidelines' content.

Figure 2. Visual model for mHealth data security, privacy, and confidentiality guidelines

What does the growth of mobile technology mean for health services?

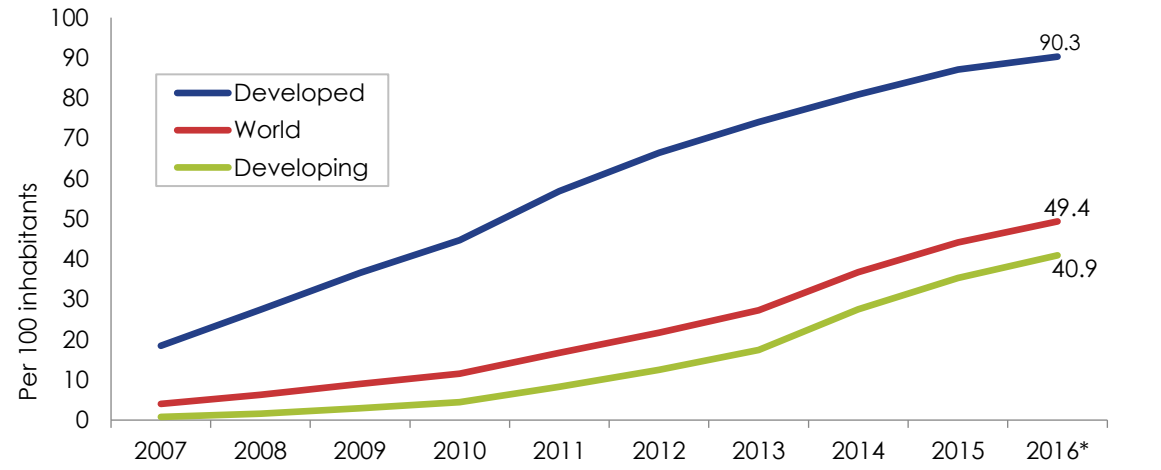
Mobile phone penetration worldwide is on the rise. As of 2016, low- and middle-income countries had 94 cellular subscriptions per every 100 inhabitants (International Telecommunications Union, 2016). In addition, active mobile broadband subscriptions are increasing at a rapid rate, growing nearly fivefold over the past five years (8.3 per 100 inhabitants in 2011 to 40.9 per 100 inhabitants in 2016) (International Telecommunications Union, 2016). Figures 3 and 4 illustrate the rapid growth of mobile cellular subscriptions and mobile broadband subscriptions.

Figure 3. Mobile cellular subscriptions per 100 inhabitants in low- and middle-income countries, 2001–2016



The developed/developing country classifications are based on the UN M49, see:
http://www.itu.int/en/ITU-D/Statistics/Pages/definitions/regions.aspx.html
Note: * Estimate
Source: ITU World Telecommunication/ICT Indicators database

Figure 4. Active mobile broadband subscriptions per 100 inhabitants, 2007–2016



The developed/developing country classifications are based on the UN M49, see:
http://www.itu.int/en/ITU-D/Statistics/Pages/definitions/regions.aspx.html
Note: * Estimate
Source: ITU World Telecommunication/ICT Indicators database

The use of mobile devices in healthcare can make it easier to access care, improve care delivery, empower patients through targeted messaging, and collect real-time data to optimize resources and decision making (World Bank, 2016). Over the past decade, public health practitioners have been taking advantage of the growing mobile penetration rate, by incorporating mobile technology in health programs. Practitioners use mobile health, or mHealth, to increase access to health services and information in some of the hardest-to-reach places on earth, and mobile interventions span the entire health system (Labrique, et al., 2013).

As a result, health programs are exploring ways to harness mobile technology to increase health coverage, improve the quality of care, and reduce healthcare costs. Labrique and colleagues identified 12 common

mHealth and information communication technology (ICT) applications, which range from behavior change communication and diagnostics to electronic health records, data collection, and vital events tracking (Labrique, et al., 2013). Box 1 outlines the 12 common mHealth and ICT applications. These guidelines are most relevant to the mHealth and ICT applications that appear in bold.

Box 1. 12 common mHealth and ICT applications

- Client education and behavior change
- Sensors and point-of-care diagnostics
- **Registries and vital events tracking**
- **Data collection and reporting**
- **Electronic health records**
- **Electronic decision support**
- Provider-to-provider
- Provider work planning and scheduling
- Provider training and education
- Human resource management
- Supply chain management
- Financial transactions and incentives

As mHealth programs become ubiquitous, policymakers and program implementers are beginning to take a closer look at data security, privacy, and confidentiality concerns related to mHealth programs. Data need to be credible and consistent, and they should be collected and stored securely in a trusted electronic health record with managed access for patients, caregivers, and healthcare professionals (Kumar & Wambugu, 2015). As data collected by mobile devices contain protected health information or personally identifiable information, there are considerable concerns around data confidentiality (Sacks, J., et al. 2015). Personal and sensitive health information stored on mobile devices and servers can affect the landscape of data security policies and procedures.

These guidelines are a practical tool for policymakers and program implementers, to ensure that mHealth programs protect sensitive health information. There are several layers of security that an mHealth program should focus on to improve data security. Because the security of mHealth data relies on the security of each layer, these guidelines cover the layers of mobile device security: that is, the application, the operating software, the device, the network, and the servers (TrustLaw Connect, et al., 2013). These guidelines go beyond the technology and address security issues related to user behavior and national policies.

How do the Principles for Digital Development apply to data security, privacy, and confidentiality?

These guidelines were developed in line with the Principles for Digital Development (Principles for Digital Development, 2017), which outline best practices for digital health programming. The Principles for Digital Development are written by and for international development professionals and are freely available for use. Broadly, these guidelines operationalize three of the eight Principles for Digital Development that ensure responsible data practices throughout the data life cycle, from collection to disposal. These Principles are:

- **Design with the user:** Engage users during the design process to build systems that protect sensitive information, keeping in mind user priorities, needs and contexts. See the Designing for and with the User section of these guidelines for more information.

- **Understand the existing ecosystem:** To ensure protection of sensitive information, implementers should make sure that their mHealth programs abide by national and organizational policies related to data security, privacy, and confidentiality. One way to do this is by engaging with technical working groups and national eHealth committees. See the National and Organizational-Level Leadership and Governance section of these guidelines for more information.
- **Ensure data privacy and security:** Data privacy, security, and confidentiality considerations should be incorporated in all aspects of your mHealth program. See Table 5, Recommendations to ensure data security throughout the project life cycle, for more information.

How were these guidelines developed?

These guidelines were developed as a follow-up to one of the recommendations of the most recent report in MEASURE Evaluation's mHealth data security series, *mHealth for Health Information Systems in Low- and Middle-Income Countries: Challenges and Opportunities in Data Quality, Privacy, and Security* (Wambugu & Villella, 2016). One of the main recommendations in this report was the need for a follow-up guideline for policymakers, decision makers, and mHealth program implementers to strengthen the security, privacy, and confidentiality of mHealth programs. This report and its recommendations resulted from information gleaned both from key informant interviews in Kenya and Tanzania and from a literature review of data security and privacy practices and risks in using mHealth in HIS strengthening in LMICs. In Kenya and Tanzania, informants working with mHealth programs identified varying levels of capacity and preparedness to protect data collected via mHealth programs. The literature review revealed the unique data security and privacy risks that come with using mobile devices to collect, transmit, and store sensitive data. The report identified a lack of guidelines or best practices for protecting mHealth data in strengthening HIS. More information about the results of the report, the report can be found at this link: https://www.measureevaluation.org/resources/publications/tr-16-140.

Although more stakeholders in the development sector have identified the need to have responsible data practices and have created subsequent resources to guide implementation of these practices, such as Oxfam's *Responsible Data Training Pack* (Hastie & Bolton, 2017) and the Responsible Data Forum's *The Hand-Book of the Modern Development Specialist: Being a Complete Illustrated Guide to Responsible Data Usage, Manners & General Deportment* (2016), we found that some resources were more focused on a project lifecycle and not on routine HIS. We also did not find resources specific to the unique challenges in protecting data that is collected using mobile devices. This gap in practical guidance and interest from countries for more information on this topic led to the development of these guidelines.

Additionally, this work builds on MEASURE Evaluation's previous work on digital health's privacy and security. See Appendix A for a list of related MEASURE Evaluation resources.

The development of the mHealth Data Security, Privacy and Confidentiality Guidelines followed these steps:

- Meetings with digital health stakeholders to assess interest and need in guidelines related to mHealth data security, privacy, and confidentiality
- Literature review
- Two half-day workshops with 50 Kenyan and Ghanaian digital health stakeholders to provide feedback on the draft guidelines
- Draft guidelines review by a panel of technical experts in digital health, HIS, and mHealth data security, privacy, and confidentiality

Additional information regarding the development of the guidelines is available in Appendix C.

A resident enumerator in Niamey, Niger, prepares for the first round of data collection for PMA2020, a mobile technology-based survey project that supports routine, rapid-turnaround, high-quality data on family planning and other health indicators.
Photo: © 2015 PMA2020/Shani Turke, courtesy of Photoshare

ORGANIZATION OF THE GUIDELINES

These guidelines are organized in three broad sections, which are outlined as follows:

- **National and Organizational-Level Leadership and Governance:** How leadership, policy and governance at the national and organizational levels can strengthen protections around sensitive information
- **Technology:** How to safeguard sensitive data from vulnerabilities intrinsic to mobile systems throughout the data lifespan, including the mHealth application, the operating system, the device, the mobile network, and data storage services
- **User Behavior:** What users of mHealth applications and tools need to know to ensure the security, privacy, and confidentiality of sensitive data stored on mHealth devices

Each section provides an overview of best practices and considerations for protecting sensitive data in the mHealth context.

NATIONAL AND ORGANIZATIONAL-LEVEL LEADERSHIP AND GOVERNANCE

Although technology has a variety of tools that can be applied to safeguard sensitive data, strong leadership and organizational and national governance are necessary to ensure the protection of sensitive data that are collected, stored, and transmitted through mobile devices in mHealth programs. This section describes key components of national- and organizational-level governance that, if implemented, could strengthen mHealth data security, privacy, and confidentiality.

National-Level Leadership and Governance of mHealth Programs

The integration of mobile technologies in national and local health systems has security and privacy implications at the policy level. This section outlines common components of national eHealth strategies, as well as core elements of privacy laws to consider while developing policies to oversee mHealth programs.

Questions Answered in This Section

- What components are usually included in a national eHealth strategy?
- What core elements of health data privacy laws do mHealth project managers need to know?

To oversee and coordinate the influx of digital technology in their HIS, many ministries of health are developing their own eHealth strategies, which outline their visions, strategic objectives, and implementation and oversight plans for incorporating digital technologies in their health systems. mHealth is recognized by the Global Observatory of eHealth as a key component of eHealth to support universal health coverage (World Health Organization, 2015). In its National eHealth Strategy Toolkit, the World Health Organization and the International Telecommunication Union identify mHealth as an example of eHealth that would be addressed in an eHealth strategy (2012). Therefore, an eHealth strategy in a country can have important governance implications for mHealth programs in the country. Countries have different priorities, but there are similarities across their eHealth strategies. We reviewed eHealth strategies from Ghana, Kenya, Malawi, Tanzania, Uganda, and Zambia, and outlined the common components of their eHealth strategies (see Table 2). Countries can use this as a tool to include or improve data security sections of their eHealth strategies. Some countries choose also to develop an mHealth strategy, outlining their plans for the use of mHealth in the health sector, as a defined subset of eHealth activities in the country. For example, South Africa's mHealth Strategy for 2015–2019 was embedded in its eHealth Strategy and linked to the eHealth Strategy objectives (National Department of Health, Republic of South Africa, 2015).

Table 2. Common components of eHealth strategies

Year published	Uganda 2013	Ghana 2009	Malawi 2014	Kenya 2011	Tanzania 2013	Zambia 2014
Standardizes health data through HMIS or eHMIS	●	●	●	●	●	●
Builds mHealth capacity and focus on eLearning	●	●	●	●	●	●
Develops eHealth/mHealth Governance Committee	●	●	●	●	●	●
Focuses on national awareness campaigns	●	●	●	●	●	●
Uses a phased approach to implement eHealth strategy	●	●	●	●	●	●
Includes a monitoring and evaluation plan	●	●	●	●	●	●
Considers privacy and security issues	●	●	●	●	●	○
Bridges equity gap through ICT	●	●	●	●	○	●
Outlines how eHealth will be funded	●	●	●	○	○	○
Moves towards a paperless reporting system	●	●	○	○	○	○
Mentions designing for the user	●	○	○	○	○	○

Key	
Yes	●
No	○

HMIS=health management information system

For more information on how to develop a national eHealth strategy, the World Health Organization and United Nations Global Pulse offer additional resources, as shown in Table 3.

Table 3. eHealth strategy resources

National eHealth Strategy Toolkit
The World Health Organization developed a **toolkit** that Ministries of Health can use to help them create their own national-level eHealth strategies
Privacy and Data Protection Principles
United Nations Global Pulse outlined key **principles** of data privacy and protection that organizations and decision makers can use as a guide for creating their own principles.

A key component of many eHealth strategies is the development of an eHealth and mHealth governance committee, tasked with developing policies and overseeing their implementation. Having strong leadership is crucial for ensuring that mHealth programs abide by data security, privacy, and confidentiality guidelines. eHealth strategies should also articulate issues such as who is accountable for breaches of privacy and under what circumstances; whether technology companies take responsibilities for weak hardware, software, and communication technologies; whether national and subnational health authorities in a country are responsible for not putting in place failsafe mechanisms on information systems when data security is breached; and the recourse for health system clients when their privacy is breached.

In addition, health data privacy regulation is critical in providing a legal framework on which eHealth operates. According to the mHealth Alliance and TrustLaw Connect's report addressing privacy law in mHealth, national policies on data security, privacy, and confidentiality should include the components described in Table 4.

Table 4. Core elements of security, privacy, and confidentiality laws for mHealth

Component	Content
Coverage	What persons or entities are obligated to comply with national laws / policies?
	What personal information is covered?
	What is the scope of the coverage?
Information/notification requirements	What are the consent requirements?
Data security obligations	What policies are needed regarding the retention or disposal of data?
	What are the technical and organization security requirements (including cloud storage)?
	What are the breach notification obligations?
Data transfer (including cross-border requirements)	What are the policies related to how sensitive data are transferred from device to server?
Enforcement and sanctions	How will privacy laws be enforced?

Adapted from TrustLaw Connect, et al., 2013

Organizational-Level Leadership and Governance of mHealth Programs

Governments are responsible for creating national-level policies to oversee the growing mHealth sector, and implementing organizations have an obligation to follow national policies and best practices to protect sensitive health information that are collected and managed within an mHealth system. This section outlines key activities and recommendations that can enhance the security of mHealth programs through leadership and governance within implementing organizations.

Questions Answered in This Section

- What should my organization do before, during, and after implementing an mHealth project to make sure that we protect sensitive data?
- What resources will help my organization prepare for data security needs of an mHealth project?
- How do organizational policies align with national data protection laws and policies?

Organizations implementing mHealth programs should consider the recommendations listed in Table 5 to ensure data security, privacy, and confidentiality.

Table 5. Recommendations to ensure data security throughout the project life cycle

Project stage	Recommendation
Conceptual stage	Form a technical working group or engage with an existing eHealth and mHealth governance committee and other local stakeholders. This group would have the authority to oversee, review, and advise on data security. Data breaches would be reported to this group.
	Check national and local policies, guidelines, and laws related to management of sensitive information. For data that passed through Internet service providers, understand the data that they retain, how long they keep them, and how they are used.
	Conduct a feasibility study to understand the mHealth security landscape, requirements, and strengths and weaknesses of your mHealth program. For example, use the mHealth Assessment and Planning for Scale **Toolkit** and the Centers for Disease Control and Prevention's Checklist for Assessment of Data Security and Confidentiality Protections to guide your feasibility study (see Table 6).
	Consider hiring or contracting the services of trained security professionals.
	Write or adapt a standard operating procedure outlining how data would be recovered if lost, how devices with data will be disposed of, how organizations will respond to theft or loss of device or data, how organizations will respond to data breaches, how organizations will respond to protocol violations, and what security provisions to use.
	During the design phase of your mHealth program, incorporate elements of "security by design" to ensure that security features reflect user needs and context. See the User Behavior section for more information.
	Develop memorandums of understanding between collaborating partners, outlining their roles and responsibilities.
	Set up a rigorous monitoring and evaluation system to monitor data breaches and ensure quick response.
Implementation Stage	Implement a mechanism for monitoring and evaluation for continuous improvements.
	Establish ongoing collaboration with the technical working group, the eHealth governance committee, local stakeholders, and other partnering organizations.
	Monitor, document, and respond to data breaches or privacy challenges.
	Provide ongoing trainings and refresher trainings for users. For more information, see the Training and Technology Literacy section.
	Provide feedback to the overseeing body or committee.
Post-Implementation Stage	Conduct an evaluation with a focus on responsible data practices, including data security and privacy measures for the project.
	Share lessons learned with all involved parties.
	Dispose of data and devices according to the country's established standard operating procedures.

Table 6. Resources for conducting a feasibility assessment

mHealth Assessment and Planning for Scale Toolkit
The World Health Organization, the UN Foundation, and Johns Hopkins Global mHealth Initiative developed the mHealth Assessment and Planning for Scale **Toolkit** to help mHealth programs track key components they need to scale (WHO, UN Foundation,JHU GmI, 2015). Several domains include indicators that can be used to implement and monitor protocols that protect mHealth data security, privacy, and confidentiality.
Checklist for Assessment of Data Security and Confidentiality Protections
The Centers for Disease Control and Prevention developed **guidelines and an accompanying checklist** to assess the data security and confidentiality protections for programs related to HIV, viral hepatitis, sexually transmitted diseases, and tuberculosis (Centers for Disease Control and Prevention, 2011). The checklist provides programs with guidelines on how to: • Identify key individuals and designate a leadership team. • Review current policies and gather resources. • Identify weaknesses and barriers. • Assess physical security and define the secure area. • Assess electronic security, protections, and methods of data transfer and storage. • Assess training needs

TECHNOLOGY

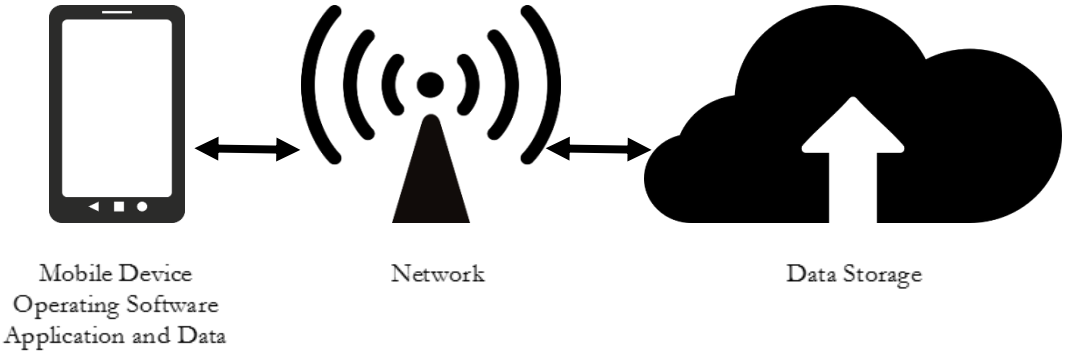
A 56-year-old auxiliary nurse midwife in Badagaon block, Jhansi district, Uttar Pradesh, India, learns how to register a beneficiary using her tablet-based mSakhi application, a mobile phone-based job aid developed by IntraHealth International under the Manthan Project. Photo: © 2015 Girdhari Bora for IntraHealth International, Courtesy of Photoshare

Having a detailed security protocol that addresses the most common reasons for data loss will prevent most data security, privacy, and confidentiality breaches (Arora, Yttri, & Nilson, 2014). This section contains suggestions for increasing the security of mHealth data, but implementers and policymakers should find a balance between the level of security and the functionality of the mHealth program (Arora, Yttri, & Nilson, 2014).

Mobile technology operates within a mobile ecosystem, so mHealth implementers and policymakers should consider the many layers of security configurations available within an mHealth ecosystem. This section outlines the levels of a mobile ecosystem that affect mHealth data security and measures that program implementers can take to ensure the security of personal health information stored in this system.

Figure 5 illustrates the interaction between the components of an mHealth ecosystem. The mobile device transmits data to remote data storage through the mobile network. This interaction may take mere seconds or minutes (or longer, depending on the strength of the network), but it can leave sensitive data vulnerable to data breaches. Decisions made by mHealth managers regarding which device, operating system, app, mobile network, and storage system to use in their programming could have implications for data security, privacy, and confidentiality. This section will explore these decision points and potential vulnerabilities.

Figure 5. Mobile technology ecosystem



Each component in the ecosystem is interconnected, and the security of the overall mHealth system relies on the security of each individual part.

mHealth Application and Data

A mobile software application, or app, is a program designed to perform a specific function or set of tasks or activities on a mobile device. For the purposes of these guidelines, the term "application" is platform agnostic; the authors use the term "application" to describe any mHealth tool, whether it is a smartphone app, interactive voice response, or Short Message Service (SMS). Having said that, the authors recognize that not all recommendations apply to SMS or interactive voice response-based programs. The sensitivity of health data requires that the developers of mobile apps for health should build systems that have a secure back-end database; keep minimal or no PHI data on the device; and ensure that the hardware, software, and communication channels between the device and other systems are secure.

Many mHealth apps record, transmit, and store PHI, and thus the design and configuration of mHealth apps play a significant role in determining the overall security of the data. This section outlines methods of securing data throughout the life cycle of data in relation to the mHealth app.

Questions Answered in This Section
• What steps can I take throughout the data management life cycle to increase the security, privacy, and confidentiality of data stored within my mHealth application? • When are sensitive health data most vulnerable?

A mobile app store is a repository of mobile applications. Examples include Google Play and Apple's App Store. This repository provides a selection of approved applications that can be downloaded and installed on the device, because most app stores offer safeguards to protect users from installing apps that could steal sensitive information (Clark, 2009; Perakovic, Husnjak, & Remenar, 2012). From the developer perspective, data security can be strengthened within an app, particularly related to how

sensitive data are stored, accessed, and transferred (Majchrzycka & Poniszewska-Maranda, 2016; Arora, Yttri, & Nilson, 2014).

Developers can take steps to mitigate certain vulnerabilities at each stage in the data life cycle, although it is important to note that increased security usually correlates with increased cost. It is up to the program staff to determine the appropriate balance of data security and cost for their respective mHealth projects. Table 7 outlines steps to mitigate security risks.

Table 7. Steps to mitigate security risks throughout the data life cycle

Data management stage	Best practice
Data capture and storage	Limit the amount of data that are collected and stored on the device, including the internal memory or removable storage such as SD card and SIM card (Arora, Yttri, & Nilson, 2014).
	Encrypt sensitive data using Advanced Encryption Standard algorithm (Majchrzycka & Poniszewska-Maranda, 2016; Arora, Yttri, & Nilson, 2014).
	Back up or archive data to prevent data loss.
	Be aware of the data management policies of each platform you use (i.e., telecom provider, mobile application).
Access to data	Decide which users should have access to which data. Restrict access to sensitive data using passwords or two-factor authentication (Arora, Yttri, & Nilson, 2014).
	Use geolocation to track the location of the device when it requests access to sensitive information to flag potential misuse of sensitive data. Google Maps API is one way to implement this (Majchrzycka & Poniszewska-Maranda, 2016).
	Use an application device identifier, which should be a randomly generated 32-bit string, to identify requests for sensitive information (Majchrzycka & Poniszewska-Maranda, 2016).
	Train users to log out after every session, or program the session to time out after a certain length of time (Majchrzycka & Poniszewska-Maranda, 2016).
	Ensure that mHealth apps do not request permissions that they do not require, such as access to SMS, camera, contacts, etc.
Data transfer	Use end-to-end data encryption when transferring sensitive data to hide the content of the message (Arora, Yttri, & Nilson, 2014; Majchrzycka & Poniszewska-Maranda, 2016).
	Use a digital signature to ensure that the message received is the same as the message that was sent (Majchrzycka & Poniszewska-Maranda, 2016).
	Ensure that security keys contain at least 128-bits to offer sufficient security (Arora, Yttri, & Nilson, 2014; Majchrzycka & Poniszewska-Maranda, 2016).
	If your mHealth program uses a web application, consider using secure transfers such as HTTPS.
Data disposal	Outline how to dispose of sensitive data in a standard operating procedure to ensure that there is no risk of exposure.
	Best practices for disposal of digital data include "clearing (using software or hardware products to overwrite media with non-sensitive data), purging (degaussing or exposing media to a strong magnetic field in order to disrupt the recorded

Data management stage	Best practice
	magnetic domains), or destroying the media (disintegration, pulverization, melting, incinerating or shredding)" (Office for Civil Rights, 2015).

Operating System

A mobile operating system (OS) is specifically designed to run on mobile devices, such as mobile phones, smartphones, personal digital assistants, tablet computers and other handheld devices. Some mobile device OS are Apple iOS, Google Android, Research in Motion's BlackBerry OS, Nokia's Symbian, and Microsoft's Windows Phone OS. Some, such as Microsoft's Windows 8, function as both a traditional desktop OS and a mobile OS.

Given the context of each project, the authors recognize that mHealth practitioners might not have the luxury to choose an operating system, because most users may already have a certain type of phone. If they can choose, however, this section should be used to help mHealth practitioners choose an operating system that is best suited for their program.

Questions Answered in this Section
• What security considerations should I be aware of when choosing a mobile operating system? • How do I balance functionality and security of different operating systems?

Whichever operating system program managers choose, they should make sure that users keep their device's operating system updated for the best protection. Hackers search for vulnerabilities in systems, so keeping current with computer updates is important, because these generally patch known vulnerabilities.

Choosing an operating system for your mHealth program is a balance between functionality and security. Both Android and iOS are relatively secure. Although Android provides more functionality for mHealth programs than iOS, it also gives more autonomy to the user, which can create vulnerabilities if the user is not properly trained. Table 8 outlines questions to consider when choosing operating systems.

Table 8. Considerations related to the security of operating systems

Security questions to consider when choosing an operating system	Rationale
Is the OS open source, or is it a closed environment?	Open source allows for more contributions from the developer community, but it can leave some vulnerabilities, making it prone to security threats.
Are there existing policies that protect users from downloading apps prone to insecurity?	Some OS and OS app stores protect users from downloading insecure apps, such as iOS and Android.
Does the OS require user permission to install and update apps?	Asking for user permission is an additional layer of protection.
Does the OS support restricted profiles?	Preventing users from accessing non-work-related websites and apps can limit data breaches.

Device

Security and privacy of data begin with the mobile device. Many mHealth managers need to decide whether users will operate the mHealth application on their personal device or whether the project will

procure devices for the users. Each decision has pros and cons. One factor to consider is that using a personal device can increase the vulnerability of sensitive data, such as by getting viruses, leaving the phone around for others to find, or getting hacked. Users will also use their devices for personal reasons, and the project will not have control over how devices are used. A recent report, *Mobile Technology in Support of Frontline Health Workers,* outlined several pros and cons after surveying 70 mHealth experts (Agarwal, et al., 2016).

Whether health workers use their own device for health service provision or data management activities, or are provided with a device by the mHealth program, proper training can prevent many common data breaches. This section outlines common security risks for mobile devices and possible solutions to counter those risks.

Questions Answered in This Section
• What are common security risks to mobile devices? • How do I care for my device so that it will serve the program longer?

Common breaches occur when mobile devices are lost or left unsecured, when password rules are not enforced, and when mHealth users transfer or access sensitive information over an unsecured public network (Arora, Yttri, & Nilson, 2014). People who are responsible for mHealth devices should also be trained to resist phishing attempts, where people inadvertently give away sensitive information to hackers (Perakovic, Husnjak, & Remenar, 2012). Table 9 outlines common security risks and their corresponding solutions.

Table 9. Common security risks for mobile devices and possible solutions

Risk	Best practice
Unauthorized users gain access	Lock device in a secure location when not in use.
	Enable remote wiping of data or device-locking protocols, also called geofencing.
Hacked passwords	Use as many types of characters as possible (uppercase, lowercase, punctuation, etc.) If the device has provision for biometric security such as fingerprints, explore the feasibility of its use.
	Use at least 8–12 characters for a password.
	Change passwords regularly.
	Use a password management program; do not write the password down.
	Avoid easy-to-guess passwords, like "password," "123456," or a user's name.
Phishing attempts	Train users to recognize and report phishing attempts.
Viruses	Avoid adding removable storage to mHealth devices.
	Train users to recognize possible sources of viruses.
	Keep the application and operating system up to date.
	Ensure that devices undergo regular maintenance.
Physical security	Whenever possible, use a case to protect the mobile device from damage, moisture, dust, and dirt.
	Keep mobile devices within optimal temperature range, according to the manufacturer.
	Make sure that the mobile phone has access to a charging station. If this is not possible, users should continuously save data so that they are not lost if the power runs out.

Network

A network is a connection of mobile devices, servers, and computers through communication media. A network is used to transmit information from one device to another. Networks can be accessed in many ways, each with its own level of security. This section outlines the risks and benefits of transmitting sensitive health information through each type of network, including public and private wireless networks, virtual private networks, mobile broadband networks, and Bluetooth.

Questions Answered in This Section
• What loopholes do hackers exploit to compromise data? • Which networks are the most secure for transmitting sensitive data? • What can you do to keep your device safe in a network?

Implementers of mHealth programs need to provide a secure network for data transfer as well as train users to recognize vulnerable networks to ensure the security, privacy, and confidentiality of sensitive data. As Arora and colleagues observe, because wireless connections are "more susceptible to monitoring and interception than broadband (internet) networks…security protocols [are] the only barriers protecting data against a breach" (Arora, Yttri, & Nilson, 2014). Thus providing a secure connection, using encryption, training users in data security, and following a security protocol will help prevent data breaches. In addition, it is critically important to put in place an intrusion detection system, that is, a network appliance that uses a set of heuristics to match known attack signatures against incoming network traffic and raises alerts when suspicious traffic is seen.

When planning your mHealth program, you have options—each with its own risks and benefits—for providing a secure network for data transfer. Table 10 outlines how to make the different types of wireless networks more secure for your mHealth program.

Table 10. Networks and mHealth data security

Network	Considerations
Public wireless Internet	Sensitive data should **never** be transferred over public wireless Internet because data will be vulnerable to hacking by unauthorized users.
	All users of mHealth programs must be trained on how to recognize vulnerable networks. These include slightly misspelled Wi-Fi network names or suspicious network names such as Free PUBLIC WI-FI. Be especially careful not to connect to personal hotspots or to ad hoc networks that you do not know and trust.
	Programs should install and update firewall software regularly on their mobile devices to further safeguard data.
Virtual Private Network (VPN)	If you must use public Wi-Fi, VPNs are the most secure option, because they use authentication and encryption to provide "'virtual private' tunnels for your data through the public internet" (Goldsborough, 2013). A disadvantage of VPNs is that data transfer may be slow, which might burden users, and VPNs are comparatively expensive (Arora, Yttri, & Nilson, 2014).
Private wireless Internet	Private wireless networks are relatively secure but must be secured with a password (Goldsborough, 2013).
	Wi-Fi Protected Access 2 networks are the most secure, but they must be enabled on the device (Goldsborough, 2013; Arora, Yttri, & Nilson, 2014).

Network	Considerations
Mobile broadband network (3G/4G/LTE)	3G, 4G, and higher networks are generally secure, using encryption and authentication.
	The network is not always reliable, and transmission can be slow.
Bluetooth	Organizations should change default settings of Bluetooth devices to reflect security policies (Padgette, et al., 2017).
	Bluetooth security features include authentication, confidentiality (preventing eavesdropping), and authorization (Padgette, et al., 2017).
	Bluetooth BR/EDR/HS mode 1 is not secure; mode 4 is the most secure (Padgette, et al., 2017).
	Bluetooth LE uses Advanced Encryption Standard-Counter. Bluetooth LE Security Mode 1 Level 3 is the most secure option (Padgette, et al., 2017).
	Bluetooth is susceptible to "denial of service attacks, eavesdropping, MITM attacks, message modification, and resource misappropriation" (Padgette, et al., 2017).

Data Storage

Once data are collected, mHealth programs need to decide where data should be stored. Different programs will have different storage needs, and some might choose to have either on-device or server backups to avoid data loss. mHealth programs often store sensitive health information, so this section can be used to outline security risks and benefits of data storage options, including on-device storage, dedicated local severs, and cloud-based servers.

Questions Answered in This Section
• What are our options for storing mHealth data? • What are the risks and benefits of storing data on the device? • What are the risks and benefits of storing data on a cloud or dedicated server?

Storing sensitive data on a server, rather than on a device, can increase the security of the data, because it minimizes the risk of human error (e.g., accidentally deleting data, compromising data through personal Internet usage) (Majchrzycka & Poniszewska-Maranda, 2016). In resource-strained environments where security is a concern, the emphasis should be on cloud-based services served through HTML5 apps (Celi, et al., 2017), and Table 11 outlines the risks and benefits of storing data on the device, local dedicated servers, and cloud-based servers. The case study on pages 23–24 outlines how one mHealth program has taken steps to protect patient data in several of the components of the mobile technology ecosystem.

Table 11. Risks and benefits of storage on devices, local dedicated servers, and cloud-based servers

Data storage	Benefits	Risks
On-device storage	Users can still access the data if the network goes down.	Unauthorized access to the device
	Users can collect data in areas with limited or no access to the network.	Data loss and changes
	Storage is convenient and easy to use.	Physically vulnerable (i.e., device could be damaged, lost, or stolen)
	Users can more easily monitor their own data at a local level.	Human error (i.e., not saving, deleting data)
Local dedicated server	Users can more easily enforce and monitor data security practices.	Need onsite technical team to set up and maintain server
	In some countries, this option is preferred. This preference is common in countries with strict data ownership regulations.	Physically vulnerable (i.e., server could be compromised)
	Server resources are not shared with other projects or clients.	Expensive to maintain
Cloud-based server	Option is more cost-effective and scalable than local dedicated servers (Kalaiselvi, et al., 2016).	Unauthorized access and use of data if terms and conditions are not clearly stated and understood
	Renting space on a server buys more affordable security and maintenance than a local dedicated server.	Political implications for sharing data across borders, particularly if countries have different regulatory frameworks
	Cloud servers follow internationally recognized quality standards, so users can ensure that the data are secure. Look for Information Technology Infrastructure Library or International Organization for Standardization (ISO20000)-certified cloud providers.	Difficult to access data in cases of limited or no network access

A health worker uses the mVacciNation mobile app to record vaccination data in Nampula, Mozambique.
Photo: © 2017 Arturo Sanabria, courtesy of Photoshare

CASE STUDY: COMMUNITY-BASED HYPERTENSION IMPROVEMENT PROJECT IN GHANA

Fast Facts	
Who	FHI360 and Ghana Health Service
What	Community-based Hypertension Improvement Project, which collects patient health data for diagnostics and treatment support
Where	Lower Manya Krobo municipality, Ghana
Primary users	109 health providers, including nurses, medical doctors, physician assistants, pharmacists, pharmacy assistants, and licensed chemical sellers
Device	Samsung Tab 4
Platform	CommCare

This case study examines how the Community-based Hypertension Improvement Project handled some of the security considerations in the development of its mHealth application to help protect patient data confidentiality and privacy.

Application Layer

Because the health workers use the information on the device for ongoing diagnostics and treatment, a copy of patient information is stored on the device and another copy is transmitted to a cloud server. The application is protected by a unique username and password. The system generates a password for each authorized user that allows users to access the application during their work. This mechanism is useful because if a user is unable to log into the app, the system administrator can help the user access the app because he or she can trace the password from a log.

Data Access within the Application

The program is organized in groups, so that providers who are in close geographic proximity work in the same group. To further protect patient information in the application, access is restricted to those in the group of providers with whom the cardiovascular nurse works.

Device

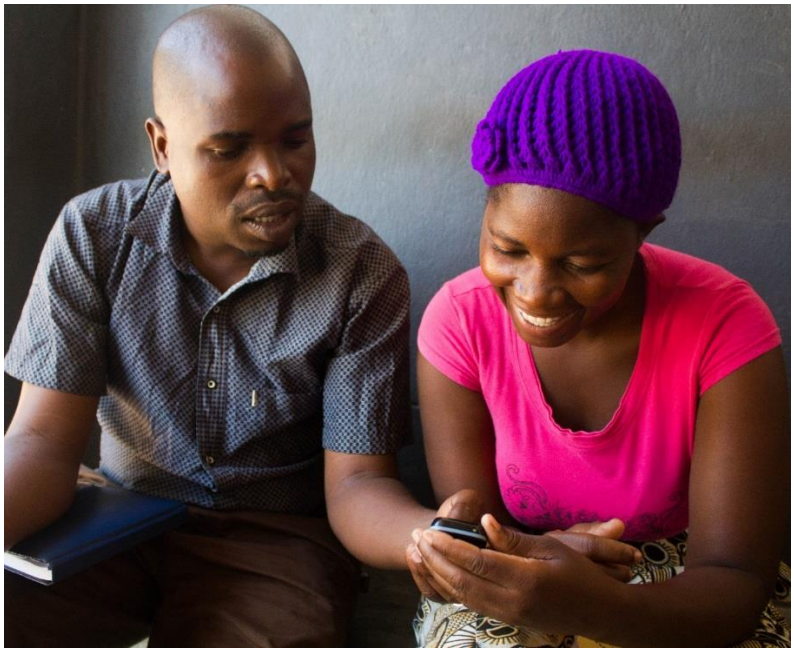
The project has a routine maintenance plan for the devices. The devices are inspected monthly to ensure that they function as they should. Any unauthorized apps are removed, and damaged devices are either repaired or replaced as soon as possible. One lesson the project learned about managing the devices is to set policies about which applications could be installed on the device, because the system administrator spends time during the monthly inspections deleting third-party applications.

Data Storage

The patient information is transmitted from the device to a cloud server, using GSM mobile services. Access to data on the server is restricted to people cleared to access them. As an added security feature, the server automatically records all transactions that occur in the database. The database administrator monitors this log to see whether an unauthorized person accesses the data. By reviewing this log, the administrator can identify any unauthorized access or attempted access.

Case study author: Reina Marie-Antoinette Mwinbang Der, M&E/mHealth Officer II, FHI360

USER BEHAVIOR



A trainer in Ntcheu, Malawi, uses a mobile phone as part of a VillageReach two-way SMS project that allows community health workers to register pregnant women in their villages, log their estimated delivery dates, encourage them to continue attending antenatal care, and discuss where they will deliver.
Photo: © 2015 Jodi-Ann Burey/VillageReach, courtesy of Photoshare

User behavior is inextricably linked to the security, privacy, and confidentiality of an mHealth program. Although the technology provides certain levels of security, people who operate and control the mobile devices are the first line of defense against breaches of security, privacy, and confidentiality. The Principles for Digital Development encourage implementers to train data users to minimize security risks (Principles for Digital Development, 2017). This section explores user-behavior aspects of data security and where they overlap with privacy and confidentiality.

Training and Technology Literacy

Health workers often maintain the mobile devices, input and transmit health data, and sometimes use the mobile device for personal Internet activities. Therefore they must be trained to improve their technology literacy and to minimize privacy and security risks (Arora, Yttri, & Nilson, 2014). This section outlines the components of effective trainings to increase technology literacy regarding security.

Questions Answered in This Section
• What content should a training cover? • What is the optimal length of a training for an mHealth program?

According to a recent systematic review of the literature, training health workers to use mobile phones can be an effective way to increase data quality (Agarwal, et al., 2015). A training of trainers model could be a useful training model for scaling up an mHealth program (Agarwal, et al., 2015). Table 12 describes key components of an effective training aimed at increasing the technology literacy of users of mHealth programs.

Table 12. Components of an effective training to increase technological literacy

Training component	Best practice
Training length	Continuous training over a minimum of a six-month period with built-in refresher trainings
	Varied training length, depending on health workers' level of technology literacy (Agarwal, et al., 2015)
Training content	User literacy/how to use a mobile phone (Agarwal, et al., 2015)
	Understanding the importance of data security, privacy, and confidentiality
	How to use the mHealth application and avoid deleting the app (Agarwal, et al., 2015; Wambugu & Villella, 2016)
	Roles and responsibilities of users related to data security, privacy, and confidentiality; How to address technical difficulties and data breaches (Agarwal, et al., 2015)
	How to make passwords secure (Arora, Yttri, & Nilson, 2014; Goldsborough, 2017)
	Standard operating procedure for maintaining data security, covering data management throughout the data life cycle, including how to dispose of data at the end of the project
	Common human errors that could affect data security, privacy, and confidentiality (For more information on training topics related to human error, see Table 9 in the Technology section.)
	How to transmit data to the server to reduce amount of data stored on the device (Arora, Yttri, & Nilson, 2014; Wambugu & Villella, 2016)

Designing for and with the User

Designing for, and with the specific users of your mHealth program will help ensure that the app is easy to use, which will minimize human errors. User-centered design puts the perspective of the end user at the center of the design process. This section outlines questions that should be answered during the design process to maximize the security of data from an mHealth program.

Questions Answered in This Section
• What questions should we ask the developers during the design stage? • How can we incorporate "privacy by design" in the mHealth application? • Where can we learn more about human-centered design?

Making sure that users are engaged throughout the design process is the best way to "make the user interface intuitive and easy to understand" (Agarwal, et al., 2015). The "privacy by design" approach is the idea that measures to protect the security, privacy, and confidentiality of sensitive data can and should be incorporated in the design of the app (Information Commissioner's Office, 2017). The Principles for Digital Development lists "design with the user" as the first principle, and the website provides a number of useful resources for implementers (Principles for Digital Development, 2017). Table 13 lists resources for user-centered design.

Table 13. User-centered design resources

Field Guide for Human-Centered Design
IDEO's **Field Guide for Human Centered Design** explains the design process and provides examples of participatory activities that can be used to understand the user's perspective.
Principles for Digital Development
The Principles for Digital Development website also provides a **list of toolkits** to help implementers design with the user.

Putting the user at the center of the design process makes the app easier to use, and increasing health workers' understanding of the app can also improve data security, privacy, and confidentiality (Agarwal, et al., 2015). Table 14 outlines questions that are related to data security, privacy, and confidentiality that should be addressed during the design process. The case study on pages 29–30 outlines how one mHealth program addressed planning for security in its design and implementation and user training.

Table 14. Data security, privacy, and confidentiality questions to ask during the design process

Category	Questions to consider	Security implication
Audience	What is the technology literacy level of the users?	Are users aware of how to avoid threats to privacy, security, and confidentiality? Will users accidentally delete or share sensitive data? What training needs to be provided? What additional safety features should be added to the app?
	What language are users most comfortable speaking, reading, and writing?	Is the mHealth app in a language that is understood by the users (e.g., to avoid mistakes that would jeopardize sensitive data)?
Technology landscape	How much network connectivity will be available?	Will sensitive data be stored on the device? How much and for how long? What data storage or backup system will the program use?
	What type of connectivity will be available for users to transmit data (e.g., 2G, 3G, 4G, wireless Internet)?	How will users transmit sensitive data?
	What other systems will the application need to integrate with?	How can the system be designed to maintain security, privacy, and confidentiality of sensitive data when it is integrated with another system?
Functionality of mHealth app	How will sensitive data be managed in the app and mHealth system?	Are there instructions and reminders to help health workers save and transmit data? Will health workers have the ability to review and edit data to ensure data quality?
	Will users use the device for personal Internet browsing as well as the mHealth activity?	What safety features need to be added to the device or app (e.g., restricted websites, passwords, antivirus software)? What training needs to be provided regarding safe Internet browsing? What data do social media apps on the device collect?
	Do users share their device with anyone else?	What safety features need to be added to the app (e.g., passwords, multi-factor authentication, multiple user profiles with restrictions)?
	How long will data be stored on the device?	How will data be backed up in case of loss, theft, or damage to the device? What safety features need to be added to protect sensitive data on the device?

CASE STUDY: mLAB IN KENYA

Fast Facts	
Who	mHealth Kenya, in partnership with the Kenya Ministry of Health
What	Mobile laboratory (mLab), which transmits laboratory results through a mobile application from laboratories to health facilities
Where	Kenya, in more than 300 health facilities (in more than 20 counties)
Primary users	Caregiver (clinician) at the Comprehensive Care Clinic and lab technician at the lab
Device	Cell phone and tablet (Android-supported phone or tablet (version 5.0 and above)
Platform	SMS-based Android app and web-based app

Mobile laboratory (mLab), a CDC-funded project implemented by mHealth Kenya, in partnership with the Kenya Ministry of Health, aims to reduce the time taken from the dispatch of results from laboratories to the receipt of those results at the health facilities. The project is being implemented in more than 300 health facilities. The goal of the program is to link people living with HIV to care in a reasonable time, thus contributing to the third 90 of the Joint United Nations Programme on HIV/AIDS 09-90-90 targets.

The mLab application has a web and an SMS-based mobile application. Data from Early Infant Diagnosis and Viral Load lab results are sent from the lab through a web platform to the mobile app in the form of an SMS. This SMS is sent to a facility-owned phone, where providers can check the results. Providers can also opt to receive messages in their own devices when the results are ready, but the results themselves are sent only to the facility-owned phone. mHealth Kenya took security, privacy, and confidentiality of lab results into account during both the planning and implementation stages in the following ways.

Planning for Security

During the design phase, mHealth Kenya was engaged in several mapping activities to identify risks and vulnerabilities in the system. They mapped all the potential system users and their use cases. They then matched the different users with their roles and identified their access levels (see below). They also mapped all the access points to the system (e.g., APIs and forms) and ensured that they were protected against unauthorized access by third-party applications. This mapping included a system analysis and a risk assessment of the existing systems and asked questions such as:

- Does the facility have a secure place to put the device?
- What is the sensitivity of the data?
- What is the bandwidth availability?

Implementation

Application Security

As mentioned earlier, only the one facility-owned phone receives the SMS with the lab results. This SMS is encrypted and cannot even be read until it is ingested in the application. Providers must use a login and password to access the application and view the test results. SMS are sent to other users' phones, letting them know that results are ready to be viewed. But to view the results, they must go to the facility-owned phone and log in to the application.

Data Access Levels

The mLab program has set up levels of users, and each level has the ability to see only certain information. The levels are as follows:

- **Health facilities:**
  - Able to see individual patient data and test results
- **Service delivery partners:**
  - Not able to see lab results
  - Able to add facilities, remove users, and view dashboards of results that have been sent to facilities
- **National level:**
  - Able to view dashboards with high-level information such as how many facilities are receiving results

Data Transmission

Sensitive data sent using the mLab web application from the client to the server and vice versa are shielded, to avoid privacy leaks using Secure Sockets Layer. The SMS messages containing the test results that are sent to the facility tablet or phone are also encrypted, and can be read only when they are ingested in the mLab mobile application.

User Training

mHealth Kenya trains service delivery partners implementing mLab in the health facilities, so that the partners can then train their facility staff. This is a day-long training, as is the training for facility users. The training is done through a practical demonstration of the use of the platform. The program uses random supportive supervision at the facilities to ensure that users are comfortable with the application. The program also sends notifications to users about emerging security trends, as they arise.

Training topics are the following:

- How to add facilities and counties
- How to add facility administrators and notifiable persons for the facilities
- How to use training tools
- Password management
- Emerging security trends

Case study authors and team:

Dr. Cathy Mwangi, CEO and Principal Investigator, mHealth Kenya Limited
Tychus Nyanga, Technical Director, mHealth Kenya Limited
Harris Dindi, Lead Software Developer, mHealth Kenya Limited
Collins Mudogo, Monitoring and Evaluation Officer, mHealth Kenya Limited

CHECKLIST

These guidelines have a companion checklist that organizations can use to plan and assess the ability of their mHealth system to safeguard sensitive data. This may be used as-is or adapted at different stages of program planning and implementation, and to put in action the practices the guidelines recommend. Indeed, the guidelines should be a living document that changes to fit the ever-evolving digital environment. The checklist can be found here:
https://www.measureevaluation.org/resources/publications/ms-17-125b

REFERENCES

African Union. (2014). *African Union Convention on Cyber Security and Personal Data Protection.* Malabo: African Union. Retrieved from https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf

Agarwal, S., Perry, H., Long, L., & Labrique, A. (2015). Evidence on feasibility and effective use of mHealth strategies by frontline health workers in developing countries: Systematic review. *Tropical Medicine and International Health, 20*(8), 1003–1014. Retrieved from: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4692099/

Agarwal, S., Rosenblum, L., Goldschmidt, T., Carras, M., Goel, N., & Labrique, A. (2016). *Mobile technology in support of frontline health workers: A comprehensive overview of the landscape, knowledge gaps and future directions.* Baltimore, MD: Johns Hopkins University Global mHealth Initiative. Retrieved from: http://www.chwcentral.org/sites/default/files/Mobile%20Technology%20in%20Support%20of%20Frontline%20Health%20Workers.pdf

Apple. (2017, March 28). Keeping iPhone, iPad, and iPod touch within acceptable operating temperatures. Retrieved from https://support.apple.com/en-us/HT201678

Arora, S., Yttri, J., & Nilson, W. (2014). Privacy and security in mobile health (mHealth) research. *Alcohol Research: Current Reviews, 36*(1), 143–150. Retrieved from https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4432854/

Celi, L.A.G., Fraser, H., Nikore, V., Osorio, J., & Paik, K. (Eds.). (2017). *Global health informatics principles of eHealth and mHealth to improve quality of care.* Cambridge, MA, USA, London, UK: The MIT Press.

Centers for Disease Control and Prevention. (2011). *Data security and confidentiality guidelines for HIV, viral hepatitis, sexually transmitted disease, and tuberculosis programs: Standards to facilitate sharing and use of Surveillance data for public health action.* Atlanta, GA, USA: United States Department for Health and Human Services, Centers for Disease Control and Prevention. Retrieved from https://www.cdc.gov/nchhstp/programintegration/docs/pcsidatasecurityguidelines.pdf

Clark, C. (2009, May 19). Mobile application security: Challenges and opportunities. San Francisco, CA, USA: iSEC Partners, Inc.

Cohn, S. (2006). *Privacy and confidentiality in the nationwide health information network.* Washington, DC, USA: National Committee on Vital and Health Statistics. Retrieved from https://www.ncvhs.hhs.gov/recommendations-reports-presentations/june-22-2006-letter-to-the-secretary-recommendations-regarding-privacy-and-confidentiality-in-the-nationwide-health-information-network/

Council of Europe. (1950). European Convention on Human Rights and Fundamental Freedoms, amended by Protocols No. 11 and 14, Article 8. Retrieved from http://conventions.coe.int/treaty/en/treaties/html/005.htm

Gejibo, S.H. (2015). *Towards a secure framework for mHealth: A case study in mobile data collection systems.* Bergen, Norway: University of Bergen. Retrieved from: https://bora.uib.no/handle/1956/10652

Goldman, J. (2017). Healthcare industry suffers the most cyber attacks. Retrieved from: https://www.esecurityplanet.com/network-security/healthcare-industry-hit-most-frequently-by-cyber-attacks.html

Goldsborough, R. (2013). VPNs: When sniffing your data is rude. *Teacher Librarian, 40*(5), 64. Retrieved from http://connection.ebscohost.com/c/articles/88257509/vpns-when-sniffing-your-data-rude

Goldsborough, R. (2017). Don't take a pass on passwords. *Teacher Librarian*, 61. Retrieved from: https://www.highbeam.com/doc/1G1-485167952.html

Golstin, L., Hodge, J.G., Valentine, N.B., & Nygren-Krug, H. (2003). The domains of health responsiveness: A human rights analysis. Geneva, Switzerland: World Health Organization. Can't access this link Retrieved from http://www.who.int/helathinfor/paper53.pdf

Grandison, T. (2017). Data Security for Mobile Health Care. In L. Celi, H. Fraser, V. Nikore, J. Osorio, & K. Paik, *Global Health Informatics: Principles of eHealth and mHealth to Improve Quality of Care* (p. 168). Cambridge, MA, USA; London, England: The MIT Press.

Hastie, R. & Bolton, S. (2017). Responsible data management training pack. Retrieved from https://policy-practice.oxfam.org.uk/publications/responsible-data-management-training-pack-620235

HealthIT.gov. (2016, May 2). Your health information privacy. Retrieved from https://www.healthit.gov/patients-families/your-health-information-privacy

HIPAA Journal. Tips for reducing mobile device security risks. (2017). *HIPAA Journal.* Retrieved from https://www.hipaajournal.com/mobile-device-security-risks/

Information Commissioner's Office. (2017). *The guide to data protection.* Wilmslow, Cheshire, UK: Information Commissioner's Office. Retrieved from https://ico.org.uk/for-organisations/guide-to-data-protection/

Institute for Critical Infrastructure Technology. (2016). Hacking Healthcare IT in 201: Lessons the healthcare industry can learn from the OPM breach. Retrieved from http://icitech.org/wp-content/uploads/2016/01/ICIT-Brief-Hacking-Healthcare-IT-in-2016.pdf

International Telecommunications Union. (2016). Statistics. Retrieved from http://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2016/ITU_Key_2005-2016_ICT_data.xls

Kalaiselvi, R., Kousalya, K., Varshaa, R., & Suganya, M. (2016). Enhanced secure sharing of personal health records in cloud computing. *Gazi University Journal of Science*, 583-591. Retrieved from: http://dergipark.gov.tr/download/article-file/225514

Kumar, M., & Wambugu, S. (2015). A primer on the security, privacy, and confidentiality of electronic health records. Chapel Hill, NC, USA: MEASURE Evaluation, University of North Carolina. Retrieved from https://www.measureevaluation.org/resources/publications/sr-15-128-en

Labrique, A., Vasudevan, L., Kochi, E., Fabricant, R., & Mehl, G. (2013). mHealth innovations as health system strengthening tools: 12 common applications and a visual framework. *Global Health Science and Practice*, 160-171. Retrieved from http://ghspjournal.org/content/1/2/160.full.pdf+html

Majchrzycka, A., & Poniszewska-Maranda, A. (2016). Secure development model for mobile applications. *Technical Sciences, 64*(3), 495-503. Retrieved from https://www.degruyter.com/view/j/bpasts.2016.64.issue-3/bpasts-2016-0055/bpasts-2016-0055.xml

MEASURE Evaluation. (2017). *Improving data quality in mobile community-based health information systems—Guidelines for design and implementation*. Chapel Hill, NC, USA: MEASURE Evaluation, University of North Carolina. Retrieved from https://www.measureevaluation.org/resources/publications/tr-17-182

MEASURE Evaluation-SIFSA. (2015a). *Good practices in issuing mobile devices to healthcare workers*. Pretoria, South Africa: MEASURE Evaluation, University of North Carolina. Retrieved from https://www.measureevaluation.org/resources/publications/fs-15-148

MEASURE Evaluation-SIFSA. (2015b). *Interoperability considerations in the design, development, and implementation of mHealth projects*. Chapel Hill, NC, USA: MEASURE Evaluation, University of North Carolina. Retrieved from https://www.measureevaluation.org/resources/publications/fs-15-152-en

Mehl, G., & Labrique, A. (2014). Prioritizing integrated mHealth strategies for universal health coverage. Science, *345*(6202), 1284–1287. Retrieved from http://science.sciencemag.org/content/345/6202/1284

Merriam-Webster. (2017, May 11). Server. Retrieved from https://www.merriam-webster.com/dictionary/server

Morsy, M.A., Grundy, J., & Müller, I. (2010). An analysis of the cloud computing security problem. In *Proceedings of the APSEC 2010 Cloud Workshop*. Sydney, Australia: Asia Pacific Software Engineering Conference 2010 Cloud Workshop. Retrieved from https://arxiv.org/ftp/arxiv/papers/1609/1609.01107.pdf

National Department of Health, Republic of South Africa. (2015). mHealth Strategy 2015–2019. Retrieved from http://static-a.net/cdn/ehna/i/mHealth%20Strategy%20South%20Africa%202015-2019.pdf

Office for Civil Rights, U.S. Department of Health and Human Services. (2015, November 6). What do the HIPAA Privacy and Security Rules require of covered entities when they dispose of protected health information? Retrieved from https://www.hhs.gov/hipaa/for-professionals/faq/575/what-does-hipaa-require-of-covered-entities-when-they-dispose-information/index.html

Office for Civil Rights, U.S. Department of Health and Human Services. (2013, July 26). Breach Notification Rule. Retrieved from https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html

Padgette, J., Bahr, J., Batra, M., Holtmann, M., Smithbey, R., Chen, L., & Scarfone, K. (2017). *Guide to bluetooth security*. Gaithersburg, MD: National Institute of Standards and Technology. Retrieved from http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-121r2.pdf

Patrick, A (2014). *The complete guide to healthcare privacy and information security governance, Massachusetts, United States*. Retrieved from https://www.hcpro.com/

Perakovic, D., Husnjak, S., & Remenar, V. (2012). Research of security threats in the use of modern terminal devices. In *Proceedings of the 23rd International DAAAM Symposium* (pp. 0545–0548). Vienna, Austria: Danube Adria Association for Automation & Manufacturing. Retrieved from https://bib.irb.hr/datoteka/600737.DAAAM_2012_Perakovic_Husnjak_Remenar.pdf

Principles for Digital Development. (2017, May 22). About. Retrieved from http://digitalprinciples.org/about/

Responsible Data Forum. (2016). *The hand-book of the modern development specialist: Being a complete illustrated guide to responsible data usage, manners & general deportment*. Retrieved from https://responsibledata.io/resources/handbook/assets/pdf/responsible-data-handbook.pdf

Sacks, J., et al. (2015). Introduction of mobile health tools to support Ebola surveillance and contract tracing in Guinea. *Global Health: Science and Practice, 3*(4), 646-659. Retrieved from https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4682588/

TrustLaw Connect, et al. (2013). *Patient privacy in a mobile world: A framworkwork to address privacy law issues in mobile health*. London, UK: Thomson Reuters Foundation. Retrieved from http://www.mhealthknowledge.org/sites/default/files/10_trustlaw_connect_report.pdf

United Nations Development Group (UNDG). (2017). *Data privacy, ethics and protection guidance note on big data for achievement of the 2030 agenda*. Geneva, Switzerland: UNDG. Retrieved from https://undg.org/wp-content/uploads/2017/11/UNDG_BigData_final_web.pdf

Wambugu, S., & Villella, C. (2016). *mHealth for health systems in low- and middle-income countries: Challenges and opportunities in data quality, privacy, and security*. Chapel Hill, NC, USA: MEASURE Evaluation, University of North Carolina. Retrieved from https://www.measureevaluation.org/resources/publications/tr-16-140

World Bank. (2016). *World development report 2016: Digital dividends*. Washington, DC, USA: World Bank. Retrieved from http://www.worldbank.org/en/publication/wdr2016

World Health Organization. (2015). Global Observatory for eHealth: Third Global Survey on eHealth-2015. Retrieved from: http://www.who.int/goe/survey/2015survey/en/

World Health Organization. (2017). eHealth at WHO. Retrieved from http://www.who.int/ehealth/about/en/

World Health Organization and International Telecommunication Union. (2012). *National eHealth Strategy Toolkit: Overview*. Geneva: World Health Organization and International Telecommunication Union. Retrieved from http://www.who.int/ehealth/publications/overview.pdf

World Health Organization, United Nations Foundation, Johns Hopkins University Global mHealth Initiative. (2015). *The MAPS Toolkit: mHealth Assessment and Planning for Scale*. Geneva, Switzerland: World Health Organization. Retrieved from http://who.int/reproductivehealth/topics/mhealth/maps-toolkit/en/

APPENDIX A. RELATED MEASURE EVALUATION RESOURCES

Resource	Description
Data Ethics: Harnessing the Power of Digital Health Information Systems (Wambugu, Thomas, Johnson, and Villella, 2017)	This report is based on an assessment in Kenya and Tanzania on the status and challenges of use of digital health systems.
mHealth for Low-and Middle-Income Countries, Challenges, Opportunities in Data Quality, Privacy and Security (Wambugu & Villella, 2016)	This report details emerging best practices and challenges related to how mobile technology is affecting health data quality, privacy, and security.
A Primer on the Privacy, Security, and Confidentiality of Electronic Health Records (Kumar & Wambugu, 2015)	This report describes the importance of cyber security in an increasingly connected health system, particularly in relation to PHI stored in electronic health records. The report discusses the key concepts of security, privacy, and confidentiality; provides information on global standards; and discusses key organizational processes to ensure security, privacy, and confidentiality of PHI. This report provides a firm grounding in the basics of security, privacy, and confidentiality.
Information briefs (MEASURE Evaluation-SIFSA, 2015a; MEASURE Evaluation–SIFSA, 2015b)	These information brief provide an overview of the legal and technological considerations for protecting personal information, including sensitive health data, in the South African context.
Improving Data Quality in Mobile Community-Based Health Information Systems—Guidelines for Design and Implementation (MEASURE Evaluation, 2017)	These guidelines provide information on how to strengthen data quality in mobile community-based HIS.

APPENDIX B. COUNTRY PARTICIPANTS

Guidelines development and review meeting participants

Kenya	
Victor Ouma Achieng	UNICEF
Christine Gichuhi	IntelliSOFT Consulting Limited
Tony Kariri	Partners for Health and Development in Africa
Amos Laboso	I-TECH Kenya
Nancy Macharia	Jomo Kenyatta University of Agriculture and Technology
Shem Mbandu	South Eastern Kenya University
Caroline Mbindyo	Living Goods
Stephen Mburu	University of Nairobi
Samuel Mbuthia	Medic Mobile
Brian Mecha	Muva Technologies
Prachi Mehta	CDC Kenya
Naomi Muinga	KEMRI-Wellcome Trust Research Programme
Edwin M Mulwa	KEMRI Research Care and Training Program and Family AIDS Care and Education Services Program
Alice Ndwiga	Afya Links
Martin Njoroge	KEMRI-Wellcome Trust Research Programme
Hon. Michael Onyango	Kisumu County
Martin Osumba	RTI International
George O. Otieno	Kenyatta University
Otieno Davies Ray	Global Programs for Research and Training
Philomena Waruhari	Moi University—Institute of Biomedical Informatics
Kennedy Sitali	mHealth Kenya

Ghana	
Marcus K. G. Adomey	University of Ghana Computing Systems
Kofi Adu-Koranteng	University of Professional Studies Accra
Harvey Akafu	Ghana Health Service
William Azietsi-Bokor	PharmAccess
Stephen Bewong	National Health Insurance Authority
Adams Bashiru	Palladium
Selasie Brown	University of Professional Studies Accra/White Orange
Reina Marie-Antoinette Der	FHI360
Chase Freeman	Management Systems International
Nii Lante Heward-Mills	VOTO Mobile
Marian Honu	FHI360
David Hutchful	Hutchlabs Atelier
Ernest Mensah	Data Protection Commission
Anthony Ofosu	Ghana Health Service
Nana Kwabena Owusu	Leti Arts
Sarah Sackey	Christian Health Association of Ghana

Ghana	
Frank Twumasi	Not specified
Alex Israel Yao Attachey	PharmAccess
Emmanuel Yartey	FHI360

APPENDIX C. HOW THE GUIDELINES WERE DEVELOPED

In developing these guidelines, the authors reviewed the findings and recommendations from the *mHealth for Health Information Systems in Low- and Middle-Income Countries: Challenges and Opportunities in Data Quality, Privacy and Security* report, and searched for additional literature to update the information in that report. Guided by the results from this literature review, MEASURE Evaluation developed an interview guide, which was used to obtain feedback and insights from a total of 40 mHealth stakeholders in Kenya and Ghana during two half-day workshops.

Kenya and Ghana were selected for several reasons. First, both countries were in the process of enacting legal frameworks for data protection: the Data Protection Act, in Kenya, and the Personal Data Protection Act, in Ghana. Both countries have a good mix of paper and electronic data management systems with associated guiding documents, including policies and frameworks. Both countries have recently launched their five-year strategic frameworks for eHealth and digital health. MEASURE Evaluation also had other related ongoing work in these countries, which made it easier to leverage the resources needed.

In Kenya, MEASURE Evaluation hosted a half-day workshop with a technically-diverse group of 21 participants representing mHealth implementers from the private sector, nongovernmental organizations, government, and donor organizations. Participants were divided in groups to review each section of these guidelines to provide feedback on what should be added, removed, or changed in each section. Follow-up conversations were conducted with some workshop participants to better understand their feedback.

This process was repeated in Ghana two weeks later, where 19 stakeholders, representing the government, nongovernmental organizations, academia, and the private sector participated in the workshop. Changes were made to the document based on suggestions that came from workshop participants. See Appendix B for country contributions.

Finally, the document was sent to six digital health experts involved with MEASURE Evaluation, who were asked to review the guidelines and provide feedback. Five of the six reviewers accepted. They provided their reviews on the content, structure of the document, and applicability to low- and middle-income countries. The authors discussed and incorporated the feedback in these guidelines as appropriate.

MEASURE Evaluation
University of North Carolina at Chapel Hill
123 West Franklin Street, Suite 330
Chapel Hill, NC, USA 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. MS-17-125A