mHealth Data Security, Privacy, and Confidentiality Guidelines:

Companion Checklist

January 2018

USAID FROM THE AMERICAN PEOPLE

PEPFAR

MEASURE Evaluation

mHealth Data Security, Privacy, and Confidentiality Guidelines:

Companion Checklist

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-17-125B

ISBN: 978-1-64232-002-2

USAID FROM THE AMERICAN PEOPLE PEPFAR MEASURE Evaluation

WHAT IS THE PURPOSE OF THIS CHECKLIST?

The mHealth Data Security, Privacy, and Confidentiality Checklist will help mHealth project managers and health information systems (HIS) officials from ministries of health assess security, privacy and confidentiality concerns of mHealth programs.

This checklist is designed to be used hand in hand with the *mHealth Data Security, Privacy, and Confidentiality Guidelines* (available here: https://www.measureevaluation.org/resources/publications/ms-17-125a). It is organized to follow the same order as the sections in the guidelines.

The checklist has two main goals:

- **Self-assessment:** This checklist is to be used by mHealth managers and ministry of health HIS officials to assess the ability of mHealth programs to ensure the security, privacy, and confidentiality of sensitive health data. Although there is no built-in scoring system, items in the checklist are considered best practices.
- **Plan:** This checklist will help implementers and policy managers identify security, privacy, and confidentiality considerations for mHealth programs. This checklist is not comprehensive, but it lays out critical elements of a robust security system within mHealth programs.

WHAT DOES THE CHECKLIST CONTAIN?

This checklist contains action-oriented steps that organizations and policymakers can take to bolster protections of sensitive data stored in mHealth ecosystems.

The sections of the checklist are as follows:

- **National governance:** This section outlines leadership and policies required to address mHealth data security, privacy, and confidentiality.
- **Organizational governance:** This section contains the considerations related to data security, privacy, and confidentiality that organizations should take into account throughout a project's life cycle.
- **Technology:** This section describes technology-related vulnerabilities that exist within an mHealth ecosystem (app, operating system, device, network, and storage) and offers suggestions on how organizations can minimize risks.
- **User behavior:** This section delves into how organizations can minimize the risk of data breach because of errors or inefficiencies arising from how a person uses a device.

HOW DO I USE THE CHECKLIST?

At what project stage should I use the checklist?

This checklist can be used at various stages throughout the lifetime of your project. It can be used:

- **Before a project begins,** to help organizations, managers, or policymakers create a **plan** to safeguard the security, privacy, and confidentiality of sensitive data.
- **During project implementation,** to assess the current state of data security, privacy, and confidentiality and to determine how to **bolster** protections of sensitive data.

- **After a project ends,** to **evaluate** the extent to which a project or policy protected the data security, privacy, and confidentiality of sensitive data, and how to make improvements for future projects.

How do I respond to the checklist questions?

Most items in the checklist use the same scale: "yes," "no," "in progress," and "not applicable." Check the box that best describes the situation of your mHealth program:

- Check the "**Yes**" box if the action has already been taken.
- Check the "**No**" box if the action has not been taken.
- Check the "**In progress"** box if the action has been started, but not completed.
- Check the "**Not applicable"** box if the action is not applicable to the item you are assessing.

What should I do with the results?

Use the results from the assessment as a starting point for discussion around how to strengthen protections of sensitive data. The checklist is action-oriented and covers best practices related to policies, standard operating procedures, technology, design, and training, as outlined in the guidelines. The checklist should help organizations and governments identify areas of improvement.

Although not every item on the checklist will be applicable to your program or country, generally, the more "yes" answers you have in each category, the stronger your system is to protect sensitive data. Programs can use the checklist periodically to improve security of sensitive data.

More information about each item in the checklist can be found in the guidelines.

NATIONAL GOVERNANCE

This section covers best practices related to leadership and governance of mHealth programs. It can be used to assess governance issues typically implemented by policymakers and project managers at the following levels:

- **Policy level:** To identify gaps in policies related to mHealth data privacy and security
- **Organizational level:** As a fact-finding tool for project and HIS officers trying to understand the mHealth policy landscape

National Governance Considerations for mHealth Security, Privacy, and Confidentiality

Checklist question		Yes	No	In progress	Not applicable
Leadership	Does a national eHealth/mHealth strategy exist? **If yes…**				
	Does the eHealth/mHealth strategy specify a national governance or oversight committee?				
	Does the eHealth/mHealth strategy have a section on data privacy and security?				
	Does a technical working group exist for eHealth/mHealth?				
Coverage	Does a national policy document specify data security and privacy items with which individuals and other entities must comply?				
	Does a national policy document state what entails personal or sensitive health information?				
Consent	Does a national policy document or guidelines require clients to give consent before giving their personal health information?				
	Does a national policy document or guideline require clients to give consent before using their personal health information?				
Data security obligations	Are there policies or guidelines regarding the retention of data?				
	Are there policies or guidelines regarding the disposal of data?				
	Does a national policy document or guidelines specify the location, format, or medium in which sensitive data must be stored?				
	Does a national policy document or guidelines require that clients be notified about data breaches?				
Data transfer	Does a national policy or guidelines specify how sensitive data should be managed? **If yes…**				
	Does the policy or guideline specify how data should be collected?				
	Does the policy or guideline specify how data should be stored?				
	Does the policy or guideline specify how data should be transferred from one media or location to another?				
	Does the policy or guideline specify how data should be disposed of?				
Enforcement and sanctions	Does a national policy document or guideline outline how privacy laws will be enforced?				

ORGANIZATIONAL GOVERNANCE

This section is mainly for **organizations** implementing mHealth projects. This checklist is organized to address the phases of project development. Before you begin assessing organizational governance, determine the stage of your project: conceptual stage, implementation stage, or post-implementation stage. Complete the part of the checklist that corresponds to the appropriate project stage.

Which stage is your project in?

Project stage	Yes	No	Instructions
Conceptual stage			If yes, skip to Conceptual Stage questions
Implementation stage			If yes, skip to Implementation Stage questions
Post-implementation stage			If yes, skip to Post-Implementation Stage questions

Conceptual Stage

Complete this checklist if your project is in the planning phase and implementation of activities has not begun.

Checklist question	Yes	No	In progress	Not applicable
Has your mHealth team held meetings with an eHealth/mHealth committee or an eHealth/mHealth technical working group to discuss mHealth data management, including data security?				
Does your mHealth team understand the national and local policies, guidelines, and laws related to management of sensitive information?				
Has your mHealth team conducted a feasibility study to understand the mHealth security landscape and requirements?				
Does your mHealth team have or has it contracted services of trained electronic data security professionals?				
Do you have an mHealth standard operating procedure (SOP) in your project? **If yes…**				
Does the SOP outline how data would be recovered if lost?				
Does the SOP outline how data will be disposed of?				
Does the SOP outline how devices with data will be disposed of?				
Does the SOP outline how organizations will respond to loss of devices?				
Does the SOP outline how organizations will respond to data breaches?				
Does the SOP outline which data security procedures to use?				
Have you incorporated elements of "privacy by design" in your mHealth systems development to make sure that security features reflects user needs and context? **If yes…**				
Have you completed the Design Process checklist?				
Have you developed a memorandum of understanding between all partners that outlines everyone's roles and responsibilities?				
Have you set up a monitoring and evaluation system to track mHealth data security, privacy, and confidentiality?				

Implementation Stage

Complete this checklist if your project has already begun implementation.

Checklist question	Yes	No	In progress	Not applicable
Do you have **meetings** to get feedback from relevant stakeholders (e.g., technical working groups, eHealth governance committee, local stakeholders, other partnering organizations)?				
Do you monitor data breaches?				
Do you document data breaches?				
Do you respond to data breaches?				

Post-Implementation Stage

Complete this checklist if your project has completed implementation.

Checklist question	Yes	No	In progress	Not applicable
Have you disposed of data according to the standard operating procedure?				
Have you disposed of devices according to standard operating procedure?				

TECHNOLOGY

This section outlines best practices for maintaining the security, privacy, and confidentiality of mHealth data from collection to disposal. **Program implementers** and **policymakers** can use this section of the checklist to assess technology in mHealth as it relates to

- The data management life cycle
- Operating systems
- Mobile devices
- Mobile networks
- mHealth data storage options

mHealth Application and Data: Mitigating Security Risks Throughout the Data Life Cycle

Complete this section if your program collects, stores, or transfers sensitive data.

	Checklist question	Yes	No	In progress	Not applicable
Data capture and storage	Do you keep only the necessary amount of data on the device by:				
	Only collecting data that are needed to meet the objectives of the project?				
	Only keeping data necessary for service delivery on the device?				
	Do you encrypt sensitive data using the Advanced Encryption Standard algorithm?				
	Do you restrict access to sensitive data using passwords? **If yes…**				
	On devices?				
	On removable storage (e.g., SD card, SIM card)?				
	Do you restrict access to sensitive data using two-factor authentication?				
	Do you back up or archive data to another location or medium to prevent data loss?				
	Are you aware of the data management policies of each platform you use (e.g., telecom provider, mobile apps)?				
Access to data	Do you use geolocation features to track the location of the devices?				
	Are users required to log out of their device after every session?				
	Does the session time out after a predetermined length of time?				
	Does your mHealth app request permissions only to access programs and resources that it requires (e.g., access to camera, SMS, contacts)?				
	Does your mHealth app encrypt sensitive data prior to data transfer?				
	Does your mHealth app use a digital signature to ensure that the message received is the same as the message that was sent?				
	Does your mHealth app use security keys (e.g., password, PIN, or biometric solutions such as finger scanning) to encrypt data?				
	If your mHealth program uses a web application, do you use secure transfers such as HTTPS?				

	Checklist question	Yes	No	In progress	Not applicable
Data disposal	Is a procedure for data disposal outlined in your standard operating procedure (SOP)? **If yes…**				
	Does the SOP outline a clearing protocol to overwrite media with nonsensitive data?				
	Does the SOP outline a device purging protocol to use a strong magnetic field to disrupt the recorded magnetic domains?				
	Does the SOP outline a device destruction protocol that involves any of these procedures: disintegration, pulverization, melting, incineration or shredding of sensitive data?				

Considerations Related to the Security of Operating Systems

Complete this section to help you decide which operating system to use.

Checklist question	Yes	No	In progress	Not applicable
Have you considered the pros and cons of an open source operating system?				
Are there existing policies within the OS or app store that protect users from downloading apps prone to insecurity?				
Does the operating system require user permission to install and update apps?				
Does the operating system support restricted profiles?				

Common Security Risks for Mobile Devices

Complete this section of the assessment to evaluate how well your program is positioned to mitigate common vulnerabilities related to mobile devices.

	Checklist question	Yes	No	In progress	Not applicable
Protecting data from unauthorized access	Do you device users lock their devices in a secure place when not in use?				
	Have you enabled remote wiping of data or device-locking protocols?				
Passwords	Does your device require passwords that use different types of characters (e.g., uppercase, lowercase, special characters, alphanumeric)?				
	Does your system require passwords to be at least 8–12 characters in length?				
	Does the program have a mechanism in place to ensure that passwords are changed regularly?				
	Do you have a password management program to guide the use of passwords in mHealth systems?				
	Do you have in place a system to prohibit users against using easy-to-guess passwords (e.g., “password,” “123456,” their name)?				
Viruses	Do you have in place a mechanism to prohibit users from adding removable storage to mHealth devices?				
	Do you have a mechanism in place to keep application and operating system up to date?				

	Checklist question	Yes	No	In progress	Not applicable
	Do your devices undergo regular physical and system maintenance?				
Physical security	Do users protect the devices (e.g., using a case) from physical damage, moisture, dust, and dirt?				
	Do you have a mechanism in place to ensure that users keep mobile devices in a temperature range recommended by the manufacturer?				
	Do you provide users with battery-charging options depending on where the device is used?				
	Do you have a mechanism in place to ensure that users save data regularly to avoid data loss?				

Networks and mHealth Data Security

Complete this section if your program transfers or will transfer sensitive data through a mobile or wireless network.

Checklist question	Yes	No	In progress	Not applicable
Do you use data transmission protocols that address the use of a public wireless network? **If yes…**				
Do you install and update firewall software regularly on mobile devices?				
Do you prohibit the transmission of sensitive data over a public wireless network?				
Do you use data transmission protocols that address the use of a private wireless network? **If yes…**				
Do you secure your private wireless network with a password?				
Do you use a WPA2 network for your private wireless network?				
Do you use data transmission protocols that address the use of a mobile broadband network?				
Do you use VPN to transmit data over insecure networks?				
Do you use data transmission protocols that address the use of Bluetooth to transmit data? **If yes…**				
Have you changed the default Bluetooth settings of your devices to limit the possibility of virtual access to the device?				

Risks and Benefits of Data Storage on the Device, Local Dedicated Servers, and Cloud-Based Servers

Complete this section to help you decide where to store sensitive data.

Checklist question	Yes	No	In progress	Not applicable
Have you assessed the risks and benefits of using on-device storage? **If yes...**				
Have you completed the Common Security Risks checklist?				
Have you assessed the risks and benefits of using a local dedicated server? **If yes...**				
Do you have or have you contracted staff or a technical team to maintain the server?				
Has a technical team inspected the server for data quality?				
Have you assessed the risks and benefits of using a cloud-based server? **If yes...**				
Have you considered any potential political implications of using a cloud-based server?				

USER BEHAVIOR

This section focuses on skills required by mHealth program users to ensure the security, privacy, and confidentiality of sensitive data in their program. It covers:

- Training: Best practices related to mHealth training for security, privacy, and confidentiality
- Addressing security during the design process: Questions to consider related to security, privacy, and confidentiality during the design phase of a program

Training mHealth Users to Protect Sensitive Data

Complete this section to assess the training of the mHealth program team on how to use the mHealth technology. It will help you assess how well you are preparing users to protect sensitive data throughout the data management life cycle.

Checklist question	Yes	No	In progress	Not applicable
Do you assess users' level of technology literacy prior to training to develop appropriate content?				
Do you train and retrain your mHealth staff over a minimum of a six-month period after they start using mHealth technology?				
Does your training program address the importance of data security, privacy, and confidentiality?				
Does your training program teach users how to use the mHealth application?				
Does your training program teach users how to avoid deleting the mHealth app?				
Does your training program teach users how to make passwords secure?				
Does your training program teach users about their roles and responsibilities related to maintaining the security, privacy, and confidentiality of sensitive data?				
Does your training program teach users how to implement the standard operating procedure related to data security, privacy, and confidentiality?				
Does your training program teach users how to avoid common user errors that could affect data security, privacy, and confidentiality?				
Does your training program teach users how to securely transmit data to the server to reduce amount of data stored on the device?				
Does your training program teach users how to recognize phishing attempts?				
Does your training program teach users how to report phishing attempts?				
Does your training program teach users how to recognize possible sources of viruses?				
Does your training program teach users how to recognize vulnerable networks?				

Questions to Ask During the Design Process

Complete this section when you are designing a new mHealth program or tool. This section highlights important questions to ask during the design process because the answers will have both security and design implications.

Checklist question	Yes	No	In progress	Not applicable
Have you considered the technology literacy level of the users?				
Have you considered the language spoken by users?				
Have you considered a language that users can read and understand?				
Have you considered using a language in which users can write?				
Have you considered the strength and spread of network connectivity to be used in this program?				
Have you assessed the type of connectivity available for users to transmit data (e.g., 2G, 3G, 4G, LTE wireless)?				
Have you considered other systems with which the application will need to integrate (e.g., DHIS 2)?				
Have you considered how sensitive data will be managed in the application and in the larger mHealth system? **If yes...**				
Have you completed the Data Management Life Cycle checklist?				
Have you considered whether users will use the device for personal Internet browsing?				
Have you considered whether users will share their device with anyone else?				
Have you considered how long sensitive data will be stored on the device?				

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-17-125B