Raising the “Trust Bar” in Digital Health Data

Christina Villella, MPH
MEASURE Evaluation
ICF

September 2017
MERL TECH 2017
To this...
Where’s all the data gone?
Objectives

• Digital health data ethics

• Landscape assessment

• Example of our work: mHealth data security, privacy, and confidentiality guidelines
Objective: To strengthen host-country systems to generate high-quality health information that is used for decision making at local, national, and global levels.

Result 1: Strengthened collection, analysis, and use of routine health data.

Result 2: Improved country-level capacity to manage health information systems, resources, and staff.

Result 3: Methods, tools, and approaches improved and applied to address health information challenges and gaps.

Result 4: Increased capacity for rigorous evaluations.
Digital data considerations

- Data security on the devices where it is collected, transmitted, stored, and managed
- Privacy and confidentiality of data held on digital devices
- Data loss
- Data volume
- Interoperability
- Capacity to use the digital health information systems
  - Data analysis
  - Use the principles for digital development
  - Interoperability
  - Maintain systems and protect against threats
  - Ability to use them in places of no signal coverage
Digital health data ethics

- Information Systems Security
- Public Health Ethics
- Clinical/Research Ethics

Venn diagram illustrating the intersection of digital health data ethics with information systems security and public health ethics.
Landscape assessment

• Identify key themes for digital health data ethics in low- and middle-income countries

• Describe the state of the field around those key themes

• Propose a set of practical steps countries can take to bring ethical considerations into the practice of managing health data
Findings

- Legal frameworks
- Institutional structures
- Information systems security
- Know your context & user
- Tools and standard operating procedures
Moving forward

• mHealth data security, confidentiality, and privacy guidelines
• Build health informatics capacity
• Work with countries to strengthen HIS governance structures
mHealth data security, privacy, and confidentiality guidelines

- Joint development with Kenyan and Ghanaian stakeholders
- Considerations for:
  - Organizational and national policies
  - Technology layers
  - User behavior
- Interest to integrate into national policies
Why do data ethics matter for data quality?

- Device loss
- Incomplete transmission
- Client mistrust
- Unauthorized data access
- Inability of health worker to check or clean data

Risks

Incomplete data

Inaccurate data

Lack of confidence

Erosion of data integrity
This presentation 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.

www.measureevaluation.org