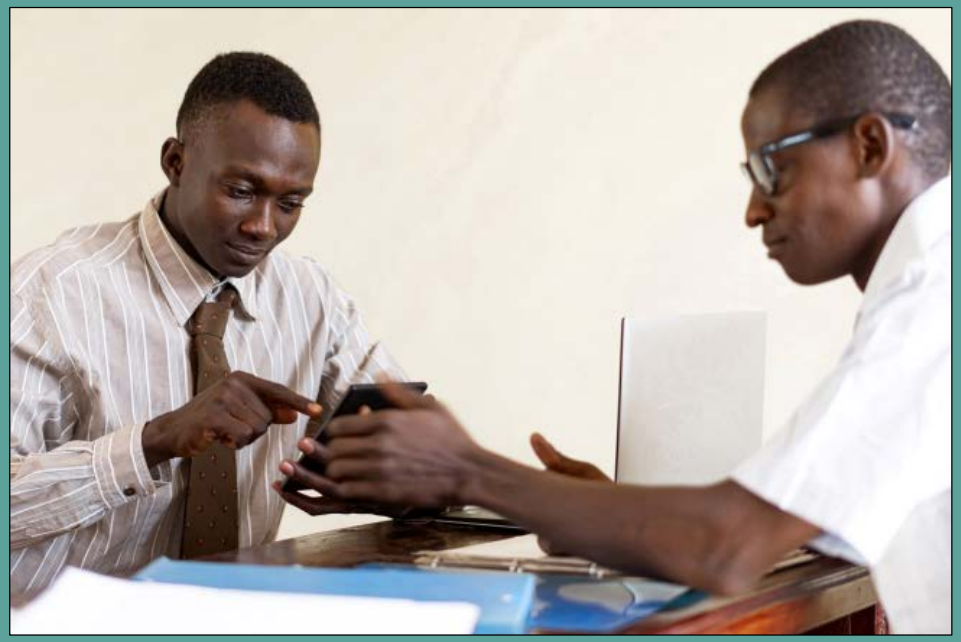
Tool for the Assessment of Electronic Health Record Security in Low-Resource Settings



Annah Ngaruro, CISSP PMP
Olivia Velez, PhD MS MPH RN
Christina Villella, MPH TOGAF
Sam Wambugu, MPH PMP
MEASURE Evaluation

USAID FROM THE AMERICAN PEOPLE
PEPFAR
MEASURE Evaluation

Meeting agenda

- Overview of security assessment tools
- Standard operating procedures for implementing electronic health record (EHR) security
- Q&A

Why electronic health records?

- Increased demand for patient-level monitoring
- Double burden of disease requires complex clinical decision making
- Total cost of development for OpenMRS ~$8M USD

Security

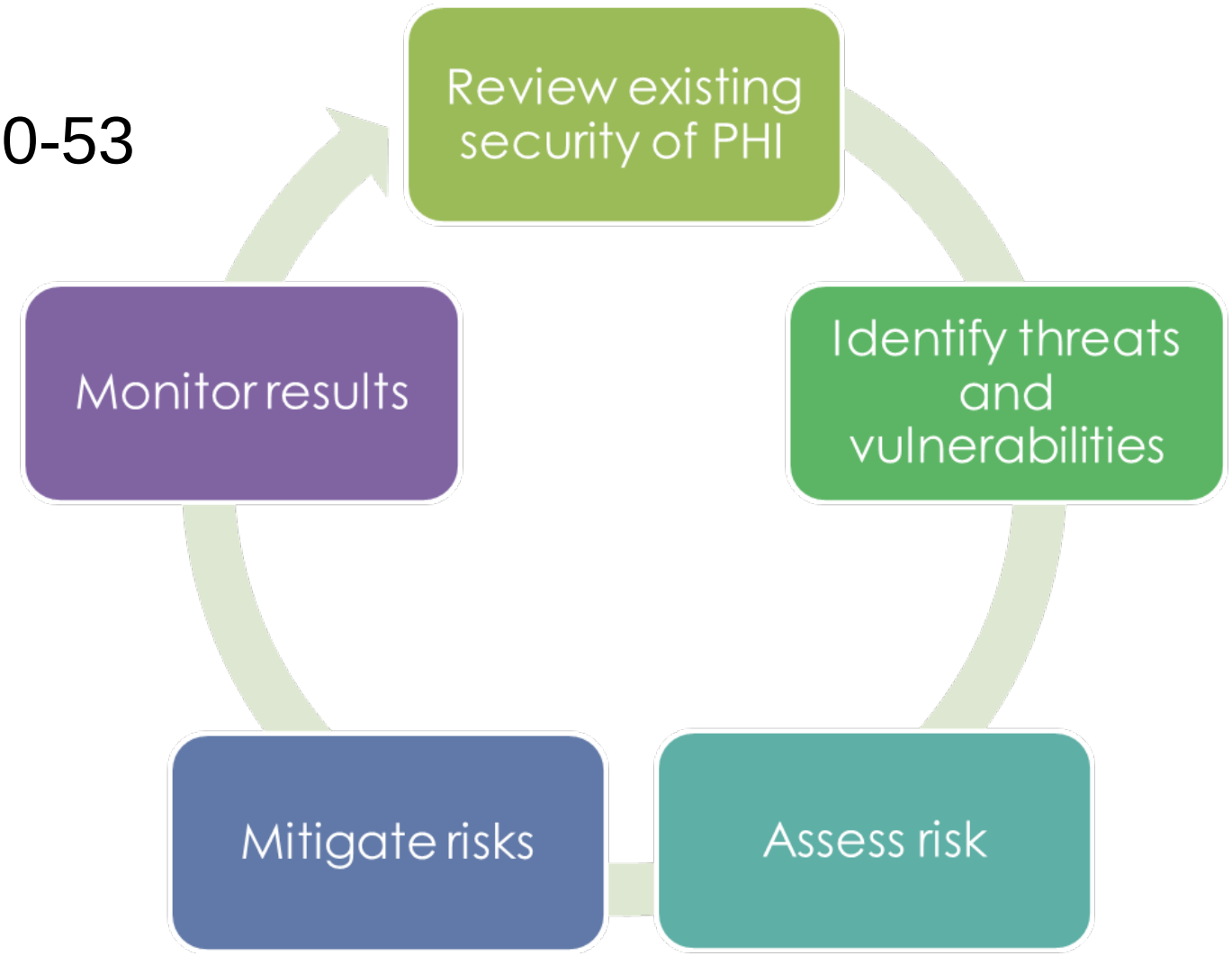
- Security is often an afterthought in digital health implementations
- Actualization of patient's rights is also an afterthought
- Lack of in-country capacity for information security
- Threats, vulnerabilities, and legal ramifications are in flux

International and regional policies

- African Union Convention of Cyber Security and Personal Data Protection (2014)
- Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Information Series
- General Data Protection Regulation (GDPR)
- National government regulations

Existing security guidelines

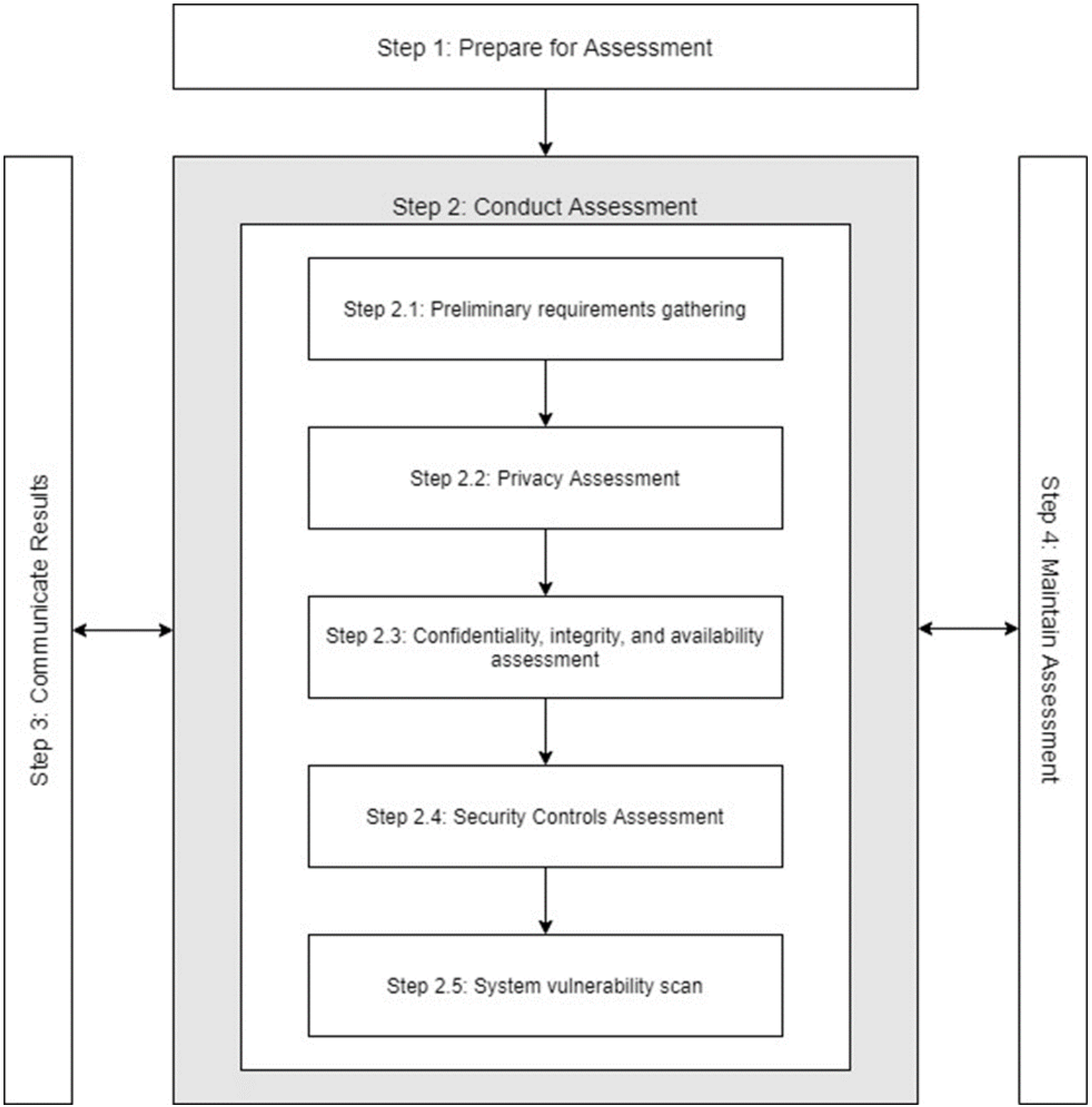
- ISO 2700
- NIST SP 800-53
- HIPAA



Development of assessment tool

- Limited to high- and medium-priority controls
- Customized language to be specific to EHRs

Overview of assessment process

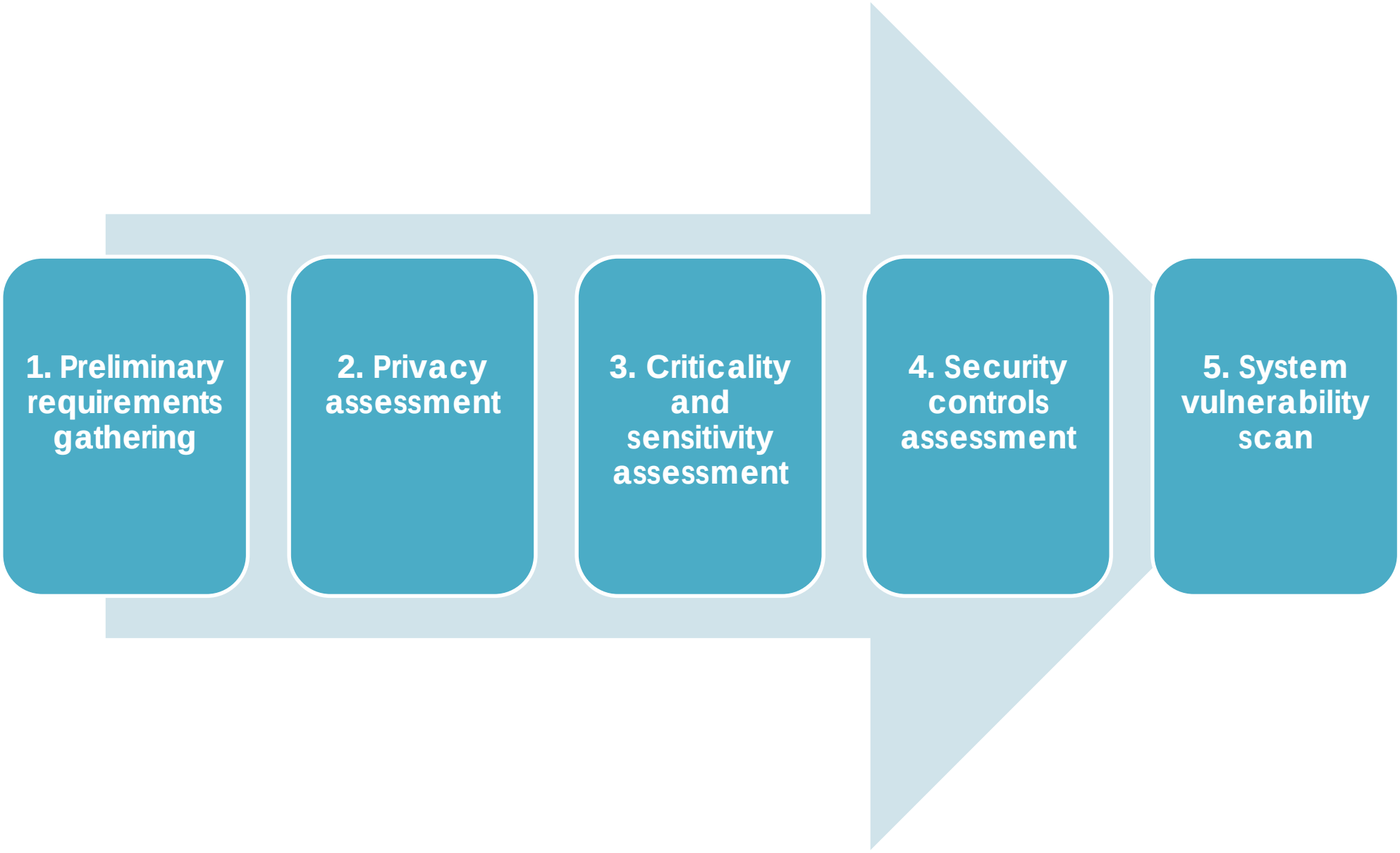


Preparing for the assessment

Identify:

- Purpose of the assessment
- Scope of the assessment
- Assumptions and constraints of the assessment
- Sources of information to be used and inputs of the assessment

Conducting the assessment



1. Preliminary requirements gathering

- Using the information from Step 1, determine the scope of the assessment, ensuring that it covers the appropriate data, systems, and functions of the EHR being assessed
- Share with external assessors
- Organizations and assessors should explicitly agree on the boundaries of the assessment

Implementation scenarios

Security requirement level	Implementation scenario description
Minimum	Facility-based standalone instance of an EHR (on a LAN) that is rarely or never connected to the Internet. This instance of an EHR is used for retrospective data entry.
Intermediate	Facility-based standalone instance of an EHR on a LAN that is sometimes connected to the Internet. This instance of an EHR is used for point-of-care service delivery and clinical decision making. Few data are captured on paper.
Advanced	Facility-based standalone instance of an EHR or a networked instance of an EHR in which multiple facilities are accessing a shared database. The EHR is exchanging data with other information systems. The EHR is being used for point-of-care service delivery and clinical decision making.

2. Privacy assessment

- Evaluates whether the system collects personal information or personally identifiable information (PII) and determines whether the privacy of that PII is adequately protected
- Understand whether all PII is necessary
- Important to interview different users of the system

3. Criticality and sensitivity assessment

Confidentiality	Refers to the system's ability to provide assurance that data and information are not made available or disclosed to unauthorized individuals, entities, or processes.
Integrity	Includes authentication, nonrepudiation, and accountability, and refers to the system's ability to be accurate and complete while providing protection from unauthorized modification.
Availability	Refers to a system's ability to be accessible and usable on demand by an authorized entity.

4. Security controls

Appendix C. Table C2. Security controls and assessment guidance and questions

Control type: Access control				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
Account management	**Minimum**	Does the organization: manage information system accounts, including the following: *identifying account types (i.e., individual, group, system, application, guest/anonymous, and temporary); * establishing conditions for group membership; * identifying authorized users of the information system and	Information system account types include, for example, individual, shared, group, system, guest/anonymous, emergency, developer/manufacturer/vendor, temporary, and service. Some of the account management requirements listed above can be implemented by organizational information systems. The identification of authorized users of the information system and the specification of access privileges reflects the requirements in other security controls in	1.1. Once the EHR was been successfully installed, explain how you first logged into the system. 1.2. Did you use a default admin password to first login? Explain the steps you follow to assign access to users in the system. 1.3. Does anyone authorize each user's access before it is activated/granted? 1.4. When individuals who have

- 17 families/types
- Managerial, technical, and operational
- Need to interview multiple people

Interviewing

- Be reassuring and don't ask leading questions
- Remind interviewees that this is not an audit
- Process can be long and tiring for both interviewers and interviewees
- Interview a variety of system users and IT personnel

Access control

The requirements for using—and prohibitions against the use of—various system resources vary considerably from one system to another.

Sample questions:

Did you use a default admin password to first login? Explain the steps you follow to assign access to users in the system.

Explain the steps taken to deactivate a user no longer working with the organization.

Awareness and training

Making system users aware of their security responsibilities and teaching correct practices.

Sample questions:

What instructions are given to system users about system security?

Has the organization performed security awareness training for system users?

Does each user have a username and password?

Audit and accountability

Adequacy of system controls and ensuring compliance with established policies and operational procedures

Sample questions:

When is the audit file reviewed? Is there a process to regularly review it or is it reviewed when there is an issue?

Describe the process established for audit review, analysis, and reporting.

Certification, accreditation, and security assessments

Testing or evaluation of the management, operational, and technical security controls on a system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome.

Sample questions:

Has a previous security assessment been conducted?

Describe how changes are reviewed to ensure that security functionality is not impacted. Provide documents.

Configuration management

Activities focused on establishing and maintaining the integrity of information technology products and systems through the control of processes for initializing, changing, and monitoring the configurations of those products and systems throughout the software development life cycle

Sample questions:

Does the organization specify certain settings in the system that are used to control security?

Has the organization or facility made any changes to the baseline configuration of the EHR installed? How are those changes managed?

Contingency planning

Planning for events with the potential to disrupt system operations.

Sample questions:

If the EHR is being used for point-of-care service delivery, what happens if the system goes down (either the EHR or the network connection to access the EHR)? How do you continue providing care and documentation?

Identification and authentication

Controls related to verifying the identity of a user, process, or device, typically as a prerequisite for granting access to resources in a system.

Sample questions:

What administrative procedures for lost, compromised, or damaged authenticators have been implemented?

Incident response

Standard operating procedures to mitigate threat events.

Sample questions:

Is there an incident response plan that details the above? Provide details and documents.

Describe how the organization tests its incident response procedures.

Maintenance

Procedures for the maintenance of organizational systems.

Sample questions:

Describe how the organization manages the system and laptop maintenance process, including how it is scheduled, performed, and documented, and whether it is performed remotely or local, etc.

Media protection

Defense of digital and nondigital media.

Sample questions:

Does any of the EHR data stored on media include both digital and nondigital media?

Are there any restrictions on what type of media can be used to store data from the EHR?

Physical and environmental protection

Measures taken to protect systems, buildings, and related supporting infrastructure.

Sample questions:

Describe how personnel and visitors are granted physical access to enter the area with the computers on which the EHR is installed.

Are there mechanisms to maintain temperature and humidity levels in the facility?

Planning

System security plans are developed to provide an overview of the security requirements of the system and security controls.

Sample questions:

Are there documented security plans, information security architecture, expected user behavior policies, and procedures? Please provide details and documents.

Personnel security

Personnel security seeks to minimize the risk that staff pose to organizational assets through the malicious use or exploitation of their legitimate access to organizational resources.

Sample questions:

Describe how screening of individuals before granting access to the information system is done.

Describe what happens to an individual's access to the EHR when reassigned or terminated.

Risk assessment

Planning and procedures to regularly assess and mitigate risk.

Sample questions:

Describe how risk assessment of the information system and the information it processes, stores, or transmits is done, including the likelihood and magnitude of harm from unauthorized access, use, disclosure, disruption, modification, or destruction. Please provide details and documents.

System and services acquisition

Planning and management of security through the software development life cycle.

Sample questions:

For the system being acquired, describe the review of development processes, standards, tools, and tool options and configurations to determine whether those selected and employed can satisfy security requirements.

System and communications protection

Physical and logical system and communications protection controls.

Sample questions:

Describe how the EHR protects the integrity of transmitted information by means such as encryption or protected distribution systems.

System and information integrity

Guarding against improper information modification or destruction; includes ensuring information nonrepudiation and authenticity.

Sample questions:

Describe how the EHR implements security safeguards to protect its memory from unauthorized code execution.

5. Vulnerability scan

Vulnerability testing is a type of technical testing used to identify, validate, and assess technical vulnerabilities and assist organizations in understanding and improving the security posture of their systems and networks.

6. Communicating results

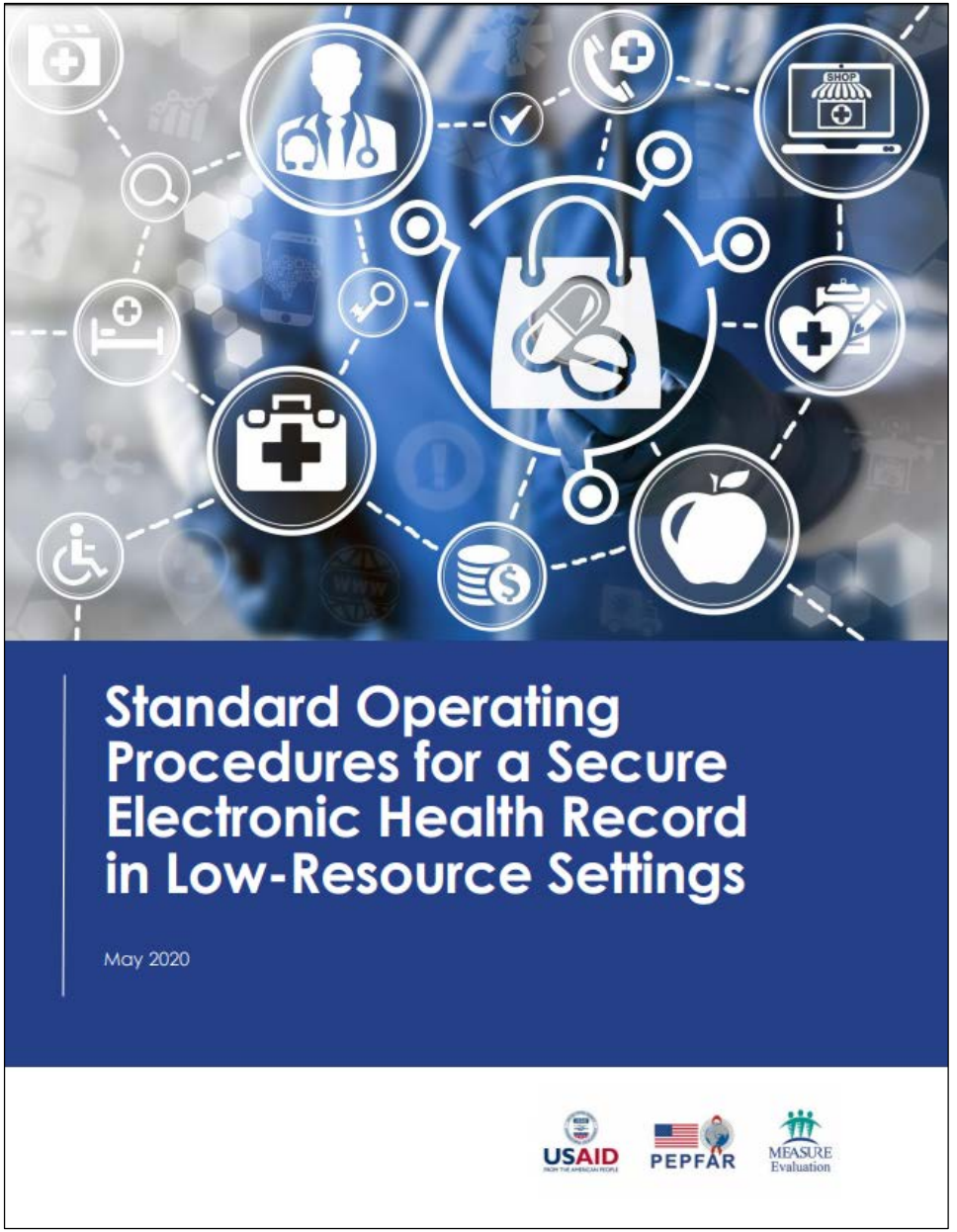
- Summarize findings and gaps by family
- Should be presented in a way that helps implementing partners to prioritize safeguards to implement

7. Maintain the assessment

- Risk assessment and security safeguarding should be a continuous process
- Action planning should be done at this stage based on the results and the changing technology landscape

Standard operating procedures

- Review of implementation scenario
- Developing a security plan
- Safeguards checklist
- Security resources

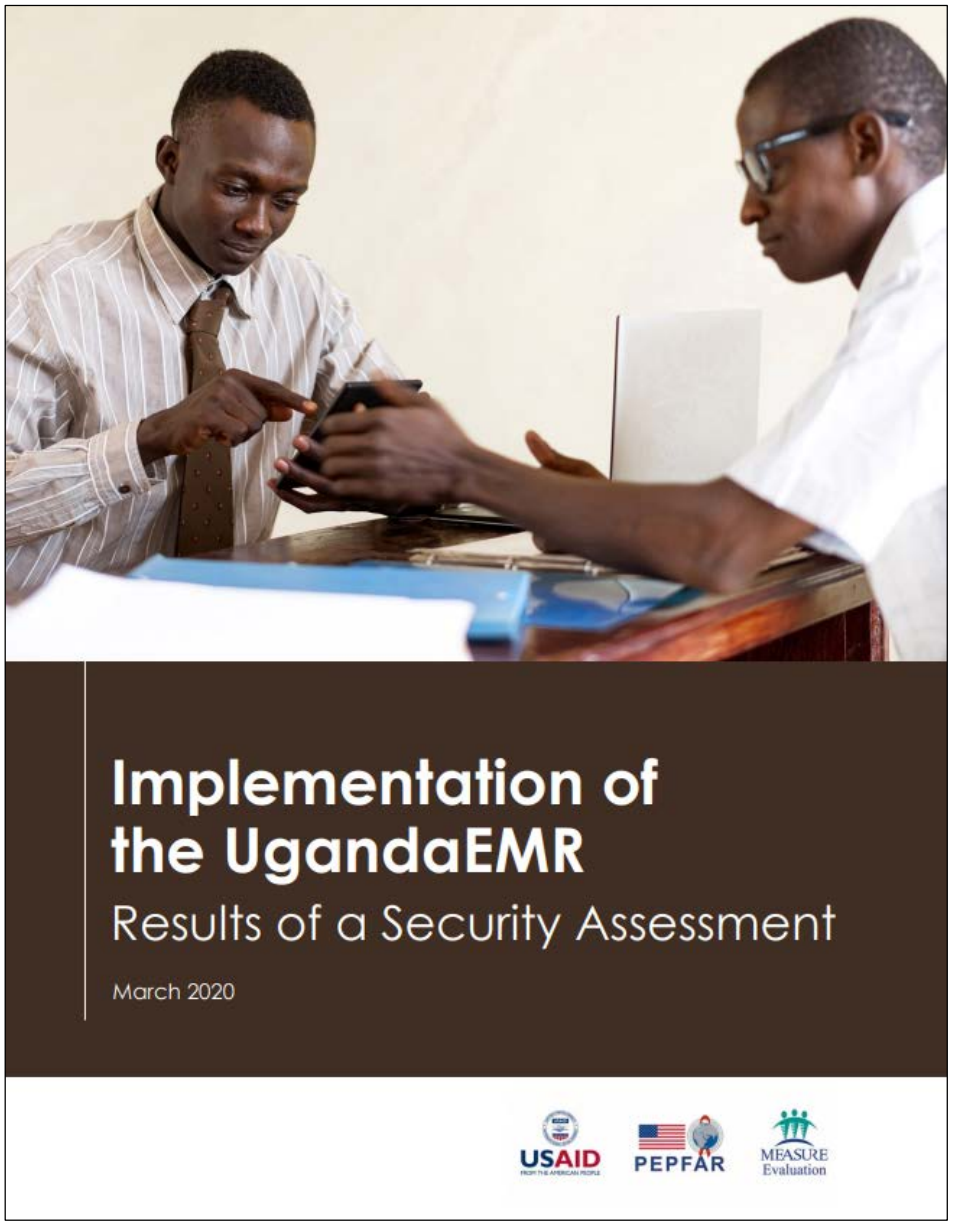


Security management process

1. Be aware of the security landscape
2. Designate a security team
3. Document security processes, results, and actions
4. Conduct a security assessment
5. Implement an action plan
6. Conduct continuous security planning and monitoring

Lessons learned

- Security assessment and controls need to take into account the risk level of a particular installation
- Tools developed by NIST and ISO were designed to be used internally by organizations and don't take into account the layers in the NGO space, be sensitive



Feedback/ Q&A

SOP:

https://www.measureevaluation.org/resources/publications/ms-20-194

Assessment Tools:

https://www.measureevaluation.org/resources/publications/ms-20-195

UgandaEMR Report available:

www.measureevaluation.org/resources/publications/tr-20-413/

Contact:

Olivia.Velez@icf.com

References

Center for Innovation and Impact. (2019). **Software global goods valuation framework: User's guide.** Washington, DC, USA: United States Agency for International Development.

Retrieved from: https://www.usaid.gov/sites/default/files/documents/1864/Software_Global_Goods_Valuation_Framework_VFinal.pdf

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; 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