Implementation of the UgandaEMR

Results of a Security Assessment

March 2020

USAID FROM THE AMERICAN PEOPLE

PEPFAR

MEASURE Evaluation

Implementation of the UgandaEMR

Results of a Security Assessment

March 2020

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

This publication was produced with the support of the United States Agency for International Development (USAID) under the terms of MEASURE Evaluation cooperative agreement AID-OAA-L-14-00004. MEASURE Evaluation is implemented by the Carolina Population Center, University of North Carolina at Chapel Hill in partnership with ICF International; John Snow, Inc.; Management Sciences for Health; Palladium; and Tulane University. Views expressed are not necessarily those of USAID or the United States government. TR-20-413
ISBN: 978-1-64232-242-2

USAID FROM THE AMERICAN PEOPLE PEPFAR MEASURE Evaluation

ACKNOWLEDGMENTS

We thank the United States Agency for International Development (USAID) for its support of this work.

The USAID- and United States President's Emergency Plan for AIDS Relief (PEPFAR)-funded MEASURE Evaluation project would like to thank the Monitoring and Evaluation Technical Support Program at the Makerere University School of Public Health for its cooperation and support in conducting this assessment. We would also like to thank the implementing partners that allowed us to visit their facilities during this assessment, including the Rakai Health Service Program, The AIDS Support Organization (TASO), the Elizabeth Glaser Pediatric AIDS Foundation, and the service delivery partners that participated in the assessment.

This assessment would not have been possible without the support of Rachel Kwezi, of USAID in Uganda; Ray Ransom, of the United States Centers for Disease Control and Prevention, Uganda; and technical assistance from the United States Centers for Disease Control and Prevention, PEPFAR, and USAID headquarters.

We acknowledge the assessment team who conducted the assessment and wrote this report: Christina Villella, Olivia Velez, Annah Ngaruro, and Samuel Wambugu, MEASURE Evaluation, ICF. We also thank Cindy Young-Turner and Mylene San Gabriel, of ICF, for editing, graphics, and formatting support, and MEASURE Evaluation's knowledge management team, at the University of North Carolina at Chapel Hill, for editorial, design, and production support.

Cover

Photo: Riccardo Mayer/Shutterstock.com

Suggested citation

MEASURE Evaluation. (2020). Implementation of the UgandaEMR: Results of a Security Assessment. Chapel Hill, NC, USA: MEASURE Evaluation, University of North Carolina.

CONTENTS

Abbreviations iv
Executive Summary v
Introduction 1
Assessment Purpose 2
Assessment Process 3
Assessment Scope 4
Findings 5
Criticality and Sensitivity Assessment 5
Data and Systems Assessment 6
Vulnerability and Testing Scan 12
Recommendations 14
Stakeholder Comments 15
Resources 16
References 17
Appendix 1. Uganda Electronic Medical Record Security Recommendations 18

Tables

Table 1. Assessment facilities 3
Table 2. Criticality and sensitivity assessment findings 5
Table 3. Data and systems assessment findings 6
Table 4. OpenMRS version.2.9 vulnerability scan results 13
Table 5. Comments on specific assessment categories 15

ABBREVIATIONS

API	application programming interface
ART	antiretroviral therapy
CDC	United States Centers for Disease Control and Prevention
EMR	electronic medical record
IDI	Infectious Disease Institute (Makerere School of Public Health)
IP	implementing partner
ISO	International Standards Organization
IT	information technology
LAN	local area network
METS	Monitoring and Evaluation Technical Support Program (Makerere School of Public Health)
NIST	U.S. National Institute of Standards and Technology
PEPFAR	United States President's Emergency Plan for AIDS Relief
RHITES SW	Regional Health Integration to Enhance Services in South West Uganda
USAID	United States Agency for International Development

EXECUTIVE SUMMARY

The United States Agency for International Development (USAID), the United States President's Emergency Plan for AIDS Relief (PEPFAR), and the United States Centers for Disease Control and Prevention (CDC) have all contributed significant funding to the development and implementation of electronic medical records (EMRs) to support the capture of patient medical data. Using USAID's Software Global Goods Valuation Framework, it has been estimated that the total development cost for development of OpenMRS—a widely used open-source EMR system—is roughly $8 million (Center for Innovation and Impact, 2019). The increased demand for patient-level data needed to achieve epidemic control of HIV and for other health monitoring has caused a shift from using EMR software for retrospective data entry to real-time point-of-care systems.

As these systems move from a single computer to interconnected computers at multiple sites, the need for improved security has become more critical. Security guidelines, such as International Standards Organization (ISO) 2700 and National Institute of Standards and Technology (NIST) 800, are burdensome to use as assessment tools in these settings. Instead, implementing partners (IPs) in low-resource settings require tools that can be tailored to their circumstances so they can continuously assess the privacy and security of the health information systems they manage.

PEPFAR asked the USAID- and PEPFAR-funded MEASURE Evaluation project to develop an assessment tool to address this issue. We took high- and moderate-impact priority controls from NIST 800, ISO 2700, and the Health Insurance Portability and Accountability Act and adjusted them to be practical in a low-resource setting. We then used the tool to conduct a security assessment. This was a step-by-step process involving questionnaires, in-person assessment and verification, and automated security testing tools.

USAID chose the UgandaEMR system for us to assess because it uses the most recent reference implementation of OpenMRS—version 2.9—and because it is being widely used at more than 1,000 facilities in Uganda. The Monitoring and Evaluation Technical Support (METS) Program, at the Makerere University School of Public Health, acts as the above-site mechanism to support the development and implementation of UgandaEMR, and numerous IPs; their subgrantees oversee the day-to-day use and maintenance. The assessment team visited six sites representing a range of IPs and donors as part of this assessment.

UgandaEMR was determined to be a moderate-impact system based on three criteria: confidentiality, integrity, and availability. The assessment found gaps in all the control areas, although there was some variation between facilities. The recommendations to address and mitigate the gaps were identified though prioritization, and their implementation will vary by IP based on available resources and relevant risk.

INTRODUCTION

Uganda has an estimated population of 41.5 million people, with more than 56 percent of those under age 15 (MEASURE Evaluation, n.d.). The Joint United Nations Programme on HIV/AIDS estimates that 1.4 million people are living with HIV/AIDs in Uganda (prevalence 5.6%); 59 percent are women and 6 percent are children under age 14 (Joint United Nations Programme on HIV/AIDS, n.d.). To reach the 90-90-90 HIV treatment targets (90% of people living with HIV/AIDS know their status, 90% are on antiretroviral therapy [ART], and 90% on ART are virally suppressed), providers must access to timely data regarding patient care.

To meet data needs of the 90-90-90 goals, as well as other healthcare priorities, there has been a significant investment in expanding the number of implementations of UgandaEMR. UgandaEMR is a derivative of OpenMRS, an open-source EMR system that has been implemented in many USAID-, CDC-, and PEPFAR-supported countries. UgandaEMR was piloted in Uganda in 2011 at 20 facilities, and it operates now in more than 1,000 health facilities. UgandaEMR contains an ART clinic module and other modules to support other functions and levels of health facilities. Built from OpenMRS, UgandaEMR is supported by the METS Program at the Makerere University School of Public Health and is being expanded to include more point-of-care implementations, lab integration, and biometric screening. Each regional service delivery IP and subgrantee in Uganda is responsible for the day-to-day maintenance of the system at its facilities.

ASSESSMENT PURPOSE

UgandaEMR builds upon the latest long-term support versions of the OpenMRS platform, the latest release of the reference application (2.9.0), and additional modules. USAID, PEPFAR, CDC, and other donors have invested heavily in OpenMRS and other open-source medical record systems to increase the capture of patient-level data needed to achieve HIV epidemic control and address other health challenges. As these systems move from retrospective data entry to real-time point-of-care systems with laboratory and other system integration, it is important to understand the privacy and security status of the systems as well as to provide usable tools that in-country IPs can use to continually assess system security. However, most privacy and security assessment guidelines were developed for use in high-resource settings that have strong financial drivers, such as insurance claims processing, more resources for security assessments, and legal frameworks to support regular security enforcement.

A security assessment identifies potential threats to security and privacy, assesses risk, and provides guidance for implementing improved security practices. To assess the security of the UgandaEMR, the USAID- and PEPFAR-funded MEASURE Evaluation project developed a tool representing international best practices, including Federal Information Security Management Act/NIST guidelines, the Health Insurance Portability and Accountability Act, and ISO 2700. The assessment we conducted in Uganda using this tool had the following goals:

- Establish a baseline security assessment of UgandaEMR implementations.
- Gather feedback on the security assessment tool so it could be modified for use in low-resource settings.

The security assessment is expected to increase awareness of security risks and help stakeholders consider how they may need to increase privacy and security practices as they move from retrospective data entry to point-of-care systems. The refined tool will help IPs by guiding regular security assessments needed to maintain patient privacy and security and adjust for the additional risks posed by increasing system interconnectedness.

ASSESSMENT PROCESS

An information systems security expert led the development of the security assessment tool. Two health informatics specialists from MEASURE Evaluation conducted the assessment using the following tools and steps:

- First, we conducted preliminary requirements gathering to determine the scope of the assessment and ensure that it would cover the appropriate data, systems, and functions. This was limited to UgandaEMR because integration with other systems is still uncommon.
- Then we made a sensitivity and criticality determination of the system and data, to assess the impact of data compromise based on three criteria: confidentiality, integrity (including authentication, nonrepudiation, and accountability), and availability.
- We conducted a confidentiality assessment using a privacy impact assessment questionnaire to determine the sensitivity and criticality of the data collected, stored, and transmitted by the system.
- We used a security control questionnaire to assess the presence and implementation of management, operational, and technical controls.
- Finally, we conducted a system vulnerability testing scan on a typical UgandaEMR installation using the most current iteration of the software.

Both the in-person assessments and the vulnerability scan were conducted in January 2020. The in-person assessments were conducted at six facilities (Table 1), representing a range of IPs, health facility levels, and donor support. Although there was some variation in security practices at each facility, the findings and recommendations in this report are a synthesis of the results from the in-person assessments, system examinations, and vulnerability scan.

Table 1. Regional IP facilities visited during EMR assessment

Regional IP	Facilities Visited	Funding source
Infectious Disease Institute (Makerere School of Public Health) (IDI)	3	CDC
Rakai Health Sciences Program	1	CDC
Regional Health Integration to Enhance Services in South West Uganda (RHITES SW)	2	USAID

ASSESSMENT SCOPE

The assessment was limited to the UgandaEMR implementation and usage. The integration with the lab information system that is currently being rolled out was not taking place at any of the facilities included in the assessment. In addition, only one facility reported exporting data to a custom external system through an application programming interface (API), and, as such, it was excluded as nontypical of current implementations. Although stand-alone implementations of UgandaEMR (a single computer with its own instance of UgandaEMR for a facility) are more common, this assessment only considered facilities in which UgandaEMR was implemented on a secure server and accessed via a local area network (LAN).

FINDINGS

Criticality and Sensitivity Assessment

The goal of performing a criticality and sensitivity assessment is identifying and quantifying the risks to the information and system assets and the level of impact should data be compromised. This information can be used to determine how to prioritize activities for mitigating those risks. Preserving the confidentiality and integrity of data while maintaining the availability of data is critical to balancing security and operational needs. Table 2 provides the definitions of each criterion and the associated impact level based on the findings from the assessment.

Table 2. Criticality and sensitivity assessment findings

Criteria	Criticality and sensitivity assessment and determination	Overall 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	**Finding: Moderate to high.** This determination was made because UgandaEMR stores sensitive patient information, including personally identifiable information, medical conditions, and treatment regimens. **Impact:** The loss and cost accrued to the stakeholders' interest if the system's confidentiality is compromised would be **serious** disruption, potential **significant** financial loss, and **substantial** reputational loss, requiring legal action for correction.	**Overall finding:** The current, typical implementation of UgandaEMR should be considered **moderate,** based on the assessment of the confidentiality, integrity, and availability criteria and because this system collects, stores, and transmits sensitive personal and health information. **Overall impact:** Systems that collect, store, and transmit sensitive personal information are typically assessed at a medium impact level at a minimum. The loss and cost accrued to the stakeholders' interest if the system's confidentiality is compromised would be **serious** disruption, **significant** financial loss, and **substantia**l reputational loss, requiring legal action for correction. It should be noted that the Uganda Data Protection and Privacy Act, 2019, which took effect in March 2019, outlines offenses such as "unlawful obtaining or disclosing of personal data" and associated penalties such as "a fine not exceeding two hundred and forty currency points or imprisonment for ten years or both" for persons and corporations that contravene these regulations.
Integrity: Includes authentication, nonrepudiation, and accountability, and refers to the system's ability to be accurate and complete and provide protection from unauthorized modification	**Finding: Low.** This determination was made because most sites were doing retrospective data entry into Uganda EMR, and the data were generally not used for clinical decision making. **Impact:** The loss and cost accrued to the stakeholders' interest if the system's integrity is compromised would be **minor** disruption, **minor** financial loss, and **minor** reputational loss, requiring administrative action for correction.	
Availability: Refers to a system's ability to be accessible and usable on demand by an authorized entity	**Finding: Low.** This determination was made because most sites were capturing data on paper in addition to UgandaEMR; therefore, the information can be restored. There was a mechanism for capturing data in case the network or server is down. **Impact:** The loss and cost accrued to the stakeholders' interest if the system's integrity is compromised would be **minor** disruption, **minor** financial loss, and **minor** reputational loss, requiring administrative action for correction.	

Data and Systems Assessment

The goal of performing a data and systems assessment is to assess the presence and implementation of the following:

- **Management controls** that focus on the management of the information technology (IT) security system and the management of risk for a system (Swanson, 2001). These controls are typically addressed by all organizational stakeholders.
- **Operational controls** that address security methods, focusing on mechanisms primarily implemented and executed by people (Swanson, 2001). These controls are put in place to improve the security of a system.
- **Technical controls** that focus on security controls that the system executes (Swanson, 2001). These controls can provide automated protection against unauthorized access or misuse, facilitate detection of security violations, and support security requirements for applications and data.

Table 3 defines the assessment categories and shows the findings and gaps for each assessment category. It should be noted that the gaps reflect best practices for high-resource settings and may not all be practical or feasible for the current level of maturity of the UgandaEMR implementation. Furthermore, addressing some of these gaps may be cost-prohibitive when balancing the mitigation of risk against the human and other resources needed to effectively implement them.

Table 3. Data and systems assessment findings

Assessment category	Findings	Gaps
Access control: Controls for managing accounts, access to the system and its information, separation of duties, least privilege, login attempts, network and remote access, external system access, and information sharing	All facilities stated that consent was obtained for collecting data for medical records, although none specified the use of an EMR system. Policies and procedures for a patient's right to access personal information contained in UgandaEMR were unclear. Sites install the system using the installation package provided by METS. Most sites did not change the default admin password so their IT teams or METS could access the system if needed. Users obtain user accounts through a local system administrator/data manager. Most system users were data entry officers, and some sites also had clinicians using the system. There was no documented guidance on how roles were assigned, and practices varied widely across sites. Some users had all roles available; many had system developer of full privileges, which means that they can change	• Mechanisms that implement a patient's right to access personal information as outlined in the Uganda Data Protection and Privacy Act, 2019 (Republic of Uganda, 2019) • Role-based privileges have not been defined based on security criteria mapped to functional roles, meaning that all system users have access to sensitive patient data, regardless of why they need to access the system and the functions they need to perform. Best practices assert that even in cases in which the EMR is used for retrospective data entry, role-based privileges should still be in place to support separation of duties. • Detailed documentation for managing role-based privileges and user accounts to ensure least privilege and separation of duties that would guide overall

Assessment category	Findings	Gaps
	anything in the system, including their own roles and privileges. METS confirmed that most users have system developer privileges so they do not experience delays in accessing the necessary functionality due to limited IT support resources. Some sites had a shared administrator account, and at other sites each administrator had his or her own account. Most sites deactivated user accounts when staff leave the facility. The system gives users an error message if they enter the wrong username and password. The system does not lock out after three failed login attempts (industry standard). The system does lock after a certain number of minutes (number of minutes was unclear to users) of inactivity. When a session is terminated, it locks on the last page used, meaning that patient information could still be exposed. Some sites' operating systems terminated after a designated period of time. There is no documentation on session termination for the system or the computer's operating system. The system was installed on a local server and accessed through a LAN at all sites and wireless networks at some sites. Procedures for accessing the LAN varied across sites. Wireless networks were password protected. At the sites visited, UgandaEMR does not share information with external systems. Sites had an undocumented process for handling requests for information that generally involved getting senior-level approval (District Health Office, facility in-charge, or IP manager) for sharing data.	procedures for issuing and managing user credentials • Documentation for secure LAN and wireless implementation • Session termination lockout screen to terminate user sessions after a determined amount of system inactivity • Policies on access control and lockout of the operating system • Documented policies for handling information sharing requests and documented criteria for approving and denying requests • A system use message to users detailing and reminding users of appropriate system use
Audit and accountability: Controls for documenting and monitoring system events and ensuring that events can be tracked by users	The system does not track events, such as user logins and failed login attempts. The system does track system errors in a log file that includes time stamps. There is no regular review of system log files. They are reviewed when troubleshooting errors. All users had their own account, and most users did not share a username	• System ability to track system events such as user logins and unsuccessful login attempts • Procedures for regularly monitoring system audit files to determine whether any security breaches or suspicious activity has occurred and needs further investigation. Regulations on

Assessment category	Findings	Gaps
	and password, with the exception of some sites that had shared administrator accounts. All sites indicated that they had quality control practices implemented for records. The frequency varied by site and patient load as well as the availability of documented procedures.	notification of data security breaches outlined in the Uganda Data Protection and Privacy Act, 2019 cannot be implemented.
Awareness and training: Controls specifying how to provide users with awareness of and training on security procedures, roles, and responsibilities	Security awareness training for users was generally incorporated into general user training. Topics covered were mainly having one account per user, keeping passwords private, protecting the data room, and performing regular backups of the data in the system. Refresher trainings were not done consistently at all sites, but when they were done it was usually on a quarterly or annual basis, depending on the IP. Users relied on the METS-developed user manual for security procedures, which contains limited security procedures.	• Role-based security training • Additional security awareness training topics, such as locking computers when not in use, handling reports printed from the system with personally identifiable information, etc. • Documented security training requirements by role
Configuration management: Controls for documenting the baseline configurations of the system and processes for making changes to the configurations	All sites had one version of UgandaEMR installed on a server that was accessed remotely through a LAN or wireless access. Sites used minimum computer requirements provided by METS, which specify the operating system, memory, and processor minimum capacity needed. Because UgandaEMR was hosted on one computer, there was not an inventory of machines with the system installed. The METS user manual also specifies the recommended minimum software requirements. The UgandaEMR configuration was based on the version of the installer that was downloaded from METS, which includes MySQL and Tomcat. Sites were not making their own edits to the configurations unless supervised by METS, but they do have the ability to make their own changes to system. There are no formal processes in place to review changes made to the system for security implications. Most sites did not have restrictions on what additional software could be	• Processes for verifying that security controls are still in place or not impacted by system changes • Guidance on limitations for functions, ports, protocols, and additional software on the computers where UgandaEMR is hosted or remotely accessed • Documentation on configuration settings necessary for security and protocols for making changes to these settings • Inventory of servers and computers/laptops accessing UgandaEMR

Assessment category	Findings	Gaps
	installed on the server hosting UgandaEMR. One site blocked the USB ports on the computers that accessed UgandaEMR.	
Contingency planning: Controls for ensuring information system backup and contingency plans for disruptions in network services	Most sites had daily backups of the system to the server. Most sites also had alternate site storage, where the backup would be placed on an external hard drive and stored in a separate location from the server. At some facilities, the alternate storage device was stored in the same location as the server. If there was disruption to the LAN service, users lost access to the system until the LAN service was restored. In this case, system availability was more critical at facilities doing point-of-care rather than retrospective data entry.	• Documented backup procedures that ensure that the alternate storage site is not the same location as the primary system backup
Identification and authentication: Controls for identifying and authenticating users and devices that access the system	UgandaEMR uses passwords as the user authentication method. There are no restrictions on reuse of passwords or how long they can be used. Some sites encourage users to change their password on a regular basis. At some sites, Windows required users to change their password at a certain interval. UgandaEMR does not verify that login attempts come from verified devices. At all sites, users could only access the system if they were on the LAN. Passwords are salted and one-way encrypted.	• No password encryption to obscure plain text passwords • Additional password management procedures or policies • Documented policies on how to grant access to users from outside the organization • IP-based user access restrictions to the system
Incident response: Controls for how to handle and monitor for security incidents and how to train staff on incident response	Most sites did not have specific procedures for reporting security incidents and reported that they had not previously had security incidents. Only one site reported having had computers stolen. In general, users said that they would report an incident to the in-charge at the facility or their IP management.	• Documented procedures on how to handle and monitor for security incidents that include definitions of what is a security incident • Training on how to handle security incidents
Maintenance: Controls used to monitor the installation of, and updates to, hardware and software to ensure that the system functions as expected and that data backup procedures are being performed	All sites had a backup process in place, but the robustness of the process varied widely. Maintenance personnel was generally limited to IP IT staff or a third-party IT company and METS. Policies were in place not to use unapproved IT providers, although in general policies were "understood" and not documented. Maintenance schedules were monthly to quarterly.	• Guidelines for best practices for backup procedures, such as dedicated, encrypted external drives • Documentation of system maintenance policies and procedures

Assessment category	Findings	Gaps
Media protection: Data confidentiality controls are used to protect data privacy and unauthorized access. Data integrity controls are used to protect data from accidental or malicious alteration or destruction and to provide assurance to the user that the information meets expectations regarding quality and integrity. Information media access controls are procedures for storing, handling, and destroying media.	Media access was not restricted at any site. There was some password protection for USB drives used for backups, but only one site reported using encrypted drives. No digital security measures were taken to restrict media access. Media transport access varied widely, with some IPs highly restricting access and others allowing staff to take home USBs with patient data. There were no documented policies and procedures.	• Restrictions of ports on drives or limited access to approved media • Password-protection and encryption for external media • Media used for backups should be used exclusively for that purpose as well as password protected and encrypted. Media used for backups should be stored in a secure location when not in use. • Documented policies regarding use of external media • Data retention policies and procedures in accordance with retention of records of personal data regulations in the Uganda Data Protection and Privacy Act 2019, including defining and enforcing a data retention period
Physical and environmental protection: These measures are taken to protect servers, systems, buildings, and related supporting infrastructures against threats associated with their physical environment.	All sites had servers in restricted areas with access control policies following those required by Uganda Ministry of Health for paper records because they were often in a shared space. Uninterruptible power supply was observed in all sites. Few sites had mechanisms for environmental protection, such as fire suppression or temperature control.	• Many server rooms lacked environmental controls.
Personnel security: Many important issues in computer security involve human users, designers, implementers, and managers. A broad range of security issues relates to how these individuals interact with computers and the access and authority they need to do their jobs. Security awareness, training, and education enhance security by improving awareness of the need to protect system resources.	No sites assigned risk designations to personnel and relied on human resources for screening individuals. All described processes for removing access for reassigned or terminated staff and for third-party access, but no documentation was available.	• Risk designations where warranted by clinic volume

Assessment category	Findings	Gaps
Training also develops skills and knowledge so computer users can perform their jobs more securely and build in-depth knowledge.		
Planning: These controls look at the policy and procedures in place to manage and maintain security. They include the preparation, approach, assumptions, and information security architecture.	Security is done ad hoc in response to specific incidents. No security planning policies and procedures were documented.	• Document security policies and procedures and align with best practices where possible. Consider a response plan to specific security threats and formulate appropriate procedures and points of contact. • No processes to cross-reference the Uganda Data Protection and Privacy Act, 2019 to verify implementation in UgandaEMR
Risk assessment: Measures used to assess, review, document, and disseminate risk assessment results	No risk assessment practices were described or documented.	• No documented or instituted risk assessment practices
Security assessment and authorization: Controls used for security assessment, role-based authorization, management commitment, coordination among organizational entities, and compliance, including continuous monitoring and penetration testing.	No clear policies around security assessments or role management. Security monitoring is done ad hoc (e.g., physical security was improved in response to theft of a server) and not continuously. No penetration testing or vulnerability scanning conducted.	• Policies and procedures needed for overall security, including role management, continuous monitoring, and testing for penetration and vulnerability
Systems communications and protection: Controls for application partitioning, security function isolation, denial of service protection, cryptography, and other related communication protections	Workstations did not lock after a period of inactivity. UgandaEMR does not terminate network connections. No cryptography implemented. Only passwords are encrypted. No other encryption available. OpenMRS does not sign information coming out of the system to protect integrity. Front- and back-end functions of OpenMRS are partitioned, but there is no isolation of security functions and no security framework was consistently used in development.	• Ensure that all users have unique names and passwords to both computers (i.e., Windows) and UgandaEMR, including the admin role. • Despite separation of front- and back-end functions, security was not built into the system from the ground up. This means that new features and enhancements do not adhere security controls by default.

Assessment category	Findings	Gaps
System and information integrity: Controls related to flaw remediation, malicious code protection, spam protection, error handling, and other threats to data integrity	All tables have audit fields. Data are generally voided, not deleted, although administrators may delete data. Virus protection and anti-malware installed on computers with regular maintenance schedules at all sites. OpenMRS has a mechanism for reporting security flaws, but there is no method for pushing out updated code in response.	• Auditing mechanism cannot track user performing action because multiple users have access to the admin account. • Tracking of maintenance procedures is inconsistent. • Flaw remediation response is limited. • There are no procedures available for patients to correct erroneous information in the system. The Uganda Data Protection and Privacy Act, 2019 explicitly requires a data controller (administrators of UgandaEMR) on request from a data subject to "correct or delete personal data about the data subject held by or under the control of the data controller that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully."
Systems and services acquisition: Controls for development processes, configuration management, and developer security architecture	As a derivative of OpenMRS, UgandaEMR relies on an open-source community of practice for development and is limited to those available and with interested to provide support and expertise.	• Developers with security expertise in the OpenMRS community

Vulnerability and Testing 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 (Souppaya & Scarfone, 2008). It is not meant to take the place of implementing security controls and maintaining system security, but instead to help organizations confirm that their systems are properly secured and identify any organizational security requirements that are not met as well as other security weaknesses that should be addressed.

Vulnerability scans were conducted on OpenMRS v.2.9 using the Arachni V1.5.1 vulnerability scanner tool. A copy of OpenMRS v.2.9 was downloaded from the OpenMRS website and installed on an Amazon WebServices virtual machine, running Amazon Linux AMI and CentOS, Quad Intel Xeon CPU @ 2.30 GHz, with 16GB RAM, and scanned using the Arachni tool. Note that this configuration **does not** mirror any of the partner implementations available in the facilities visited by the assessment team. Therefore, these findings should be considered a minimum set of findings scans.

Arachni is a feature-full, modular, high-performance Ruby framework aimed toward helping security testers and administrators evaluate the security of modern web applications. It is free, with its source code public and available for review at https://www.arachni-scanner.com/#. It is multiplatform, supporting all major operating systems (MS Windows, Mac OS X, and Linux) and distributed through portable packages that allow for instant deployment.

Results of vulnerabilities present in OpenMRS version2.9 and identified by the Arachni Scanner are described and ranked based on their threat level severity and potential impact to the system if exploited. The scan results are summarized in Table 4 and categorized by:

- **Type of vulnerabilities present and identified:** The number of unique vulnerabilities identified across the OpenMRS version 2.9 system
- **Number of occurrences:** The locations where each unique vulnerability is present and needs to be addressed. For example, the presence of a form with an unencrypted password (i.e., password stored as clear text) was found in two OpenMRS version 2.9system components, including the main user login screen.

Table 4. OpenMRS version.2.9 vulnerability scan results

Threat level and description	Type of vulnerabilities present and identified	Summary of type of vulnerability	Number of occurrences
High: These vulnerabilities are the most dangerous and put the scan target (i.e., the OpenMRS v2.9.0 system) at the maximum risk for system hacking and data theft.	3	Cross-Site Scripting (XSS) in script context	1
		Cross-Site Request Forgery	2
		Cross-Site Scripting (XSS)	2
Moderate: These vulnerabilities are caused by server misconfiguration and site coding flaws, which can result in server disruption and intrusion and put the scan target at a moderate security risk.	1	Unencrypted password form	2
Low: These vulnerabilities result from a lack of encryption of data traffic or directory path disclosure. Their impact on the scan target if exploited presents a low risk.	2	Common administration interface	1
		Missing 'X-Frame-Options' header	1
Informational: These vulnerabilities result from some best practices not being implemented. Their impact on the scan target if exploited presents a minimal risk.	3	Interesting response	19
		HTML object	1
		Allowed HTTP methods	1

The Arachni scan results reports provide in-depth technical details of other vulnerabilities present and identified. Recommended remediation steps are also included for each vulnerability. Due to the lengthy nature of these reports, they are linked here: https://www.measureevaluation.org/resources/files/openmrs_report3.html.zip/at_download/file.

RECOMMENDATIONS

Based on the comprehensive assessment conducted, MEASURE Evaluation recommends improving security practices by adopting a multilayered security approach to ensure the embedding of a strong security management culture that will continuously implement, manage, and mitigate data and system security risks during the life and operation of the system. To enhance the security of UgandaEMR, all relevant stakeholders need to be engaged, including OpenMRS, METS, regional IPs, service delivery partners, donors, the Ministry of Health, and the National Information Technology Authority—Uganda. Such an approach would involve the following:

- Implement IT governance structures to provide overall management and oversight, including ensuring compliance with the Uganda Data Protection and Privacy Act, 2019 in the system.
- Develop and operationalize robust security policies, plans, and procedures, borrowing from best industry practices such as ISO and NIST.
- Implement management, operational, and technical security controls at all levels.
- Formalize security planning and institute continuous risk management and mitigation to ensure responsiveness to expanded system use and interconnectedness as well as existing and emerging security threats.
- Donors should support the expansion of security assessments beyond the facilities included in this report and facilitate the uptake of the security assessment tool and implementation of enhanced security, as outlined in the recommendations, through local capacity building and investment in resources to support security activities.

Financial resources and security capacity building are needed to move these recommendations forward. Because security is a continuous process, in-country expertise and capacity are critical to maintaining security over the long term as well as meeting the needs of increasingly interconnected systems. The assessment team observed that although there was an understanding of and interest in having improved security, especially for sites that were moving from retrospective data entry to point-of-care, IT support was limited, and both METS and the IPs expressed justifiable concerns that implementing some security measures without supportive resources could decrease system availability and therefore have a negative impact on adoption. For example, facilities without UgandaEMR system administrators would be dependent on the availability of remote support or waiting for in-person technical support.

Appendix 1 provides specific recommendations for implementation. The assessment team recommends that these stakeholders come up with an agreed-upon action plan that specifies which stakeholders are responsible for following up on and implementing the recommendations in this report. Decisions will need to be made regarding the level of implementation for certain security controls and their respective policies and procedures.

STAKEHOLDER COMMENTS

The comments are synthesized from a post-assessment interview with stakeholders and also from feedback received on an initial draft of this report.

The assessment looked only at implementations in which there was a local instance of the server connected to the Internet in a secure data room. The instance is accessed via a LAN from workstations or laptops within the LAN. This does not represent the majority of implementations, because most are single computers stored in secure data rooms. In these instances, implementing many of the security safeguards would provide little benefit to outweigh the cost of implementing and maintaining them.

Table 5. Comments on specific assessment categories

Assessment category	Stakeholder comments
Access control	• In current implementations used for retrospective data entry, role-based access control are not necessary.
Authenticator management	• Database passwords are hashed with a salt.
Identification and authentication	• Verifying devices is outside the scope/ability of UgandaEMR. It needs to be done at operating system or network levels.
Physical and environmental protection	• The system is accessed by authorized staff in data rooms where paper records are stored and in clinician offices. Access to these rooms is limited only to those authorized. Rooms are locked and secured when not in use.
Systems communications and protection	• Termination of network connections would need to be set on the web server; it cannot be done from UgandaEMR. • The security value of signing information exported from the system is dubious. It does not fit in the existing ministry workflow, and without a central identity authority for signing certificates, there is no sense of an authoritative source for the exported information. • Existing archival/compression formats provide checksums to guard against data corruption in transport/storage; intentional integrity attacks are a separate matter.
System and information integrity	• UgandaEMR is updated with OpenMRS modules as they become available and released as per scheduled releases.
Vulnerability Scanning	• Vulnerability scanning is not relevant to non-Internet facing installations.

RESOURCES

Green, S., Chandrasekharan, S., Schwegmann, C., Cohen, J., Sullivan, C., & Raftree, L. (2019). *Considerations for using data responsibly at USAID*. Washington, DC: United States Agency for International Development. Retrieved from https://www.usaid.gov/sites/default/files/documents/15396/USAID-UsingDataResponsibly.pdf

National Institute of Standards and Technology (NIST). (2017). *SP 800-53 Rev. 5: Security and privacy controls for information systems and organizations*. Gaithersburg, MD: NIST. Retrieved from https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/draft

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

MEASURE Evaluation. (n.d.). Uganda. Retrieved from https://www.measureevaluation.org/countries/uganda

Joint United Nations Programme on HIV/AIDS. (n.d.). Uganda. Retrieved from https://www.unaids.org/en/regionscountries/countries/uganda

Republic of Uganda. (2019). *The data protection and privacy act, 2019*. Kampala, Uganda: Republic of Uganda. Retrieved from https://ict.go.ug/wp-content/uploads/2019/03/Data-Protection-and-Privacy-Act-2019.pdf

Souppaya, M., & Scarfone, K. (2008). *Technical guide to information security testing and assessment: Recommendations of the National Institute of Standards and Technology*. NIST Special Publication 800-115. Gaithersburg, MD, USA: National Institute of Standards and Technology. Retrieved from https://www.nist.gov/publications/technical-guide-information-security-testing-and-assessment

Swanson, M. (2001). *Security self-assessment guide for information technology systems*. NIST Special Publication 800-26. Gaithersburg, MD, USA: National Institute of Standards and Technology. Retrieved from https://www.nist.gov/publications/security-self-assessment-guide-information-technology-systems

APPENDIX 1. UGANDA ELECTRONIC MEDICAL RECORD SECURITY RECOMMENDATIONS

Assessment category	Recommendations
Management controls	• **Information technology (IT) governance structure:** The Uganda electronic medical record (UgandaEMR) stakeholders should implement an IT governance structure that communicates a strong commitment to data and system security and provides for and drives the development and implementation of robust processes and procedures that support the necessary legal, regulatory, and best practice requirements. IT governance is a subset discipline of corporate governance, focused on IT and its performance and risk management. A governance structure includes, at a minimum, roles such as the following: – **Management and Oversight Committee,** which would be responsible for ensuring that policies, procedures, and plans are developed, implemented, and continually improved. This role would also ensure that appropriate funding is provided for the security of the system and that all security improvements undertaken are compliant with the Uganda Data Protection and Privacy Act, 2019, which took effect in March 2019. – **Data and System Owner,** determined by the Management and Oversight Committee to reflect the setup in Uganda and define the responsibilities of various stakeholders, such as U.S. Government agencies, the Ministry of Health, the Monitoring and Evaluation Technical Support (METS) Program at the Makerere University School of Public Health, implementing partners (IPs) and their front-line clinical care subgrantees and the developer of OpenMRS. This would allow everyone involved to understand their due care and due diligence responsibilities for the data and system, including the ultimate responsibility for data and system protection. – **Data and System Custodian,** mandated by the Data and System Owner to be responsible on a daily basis for continuous monitoring of security risks, implementation of security controls, development of risk mitigation plans, and real-time monitoring of the system and data for security vulnerabilities and potential breaches. – **Data and System Auditor,** responsible for conducting periodic independent system and data reviews and assessments, including automated security scans and testing. • **Security plan:** Develop a security plan in line with the risk management policy, Uganda Data Protection and Privacy Act, 2019 requirements, and regulatory and best practice requirements. A system security plan provides a summary of the security requirements for the information system and describes the security controls in place or planned for meeting those requirements. The plan may also reference other key security-related documents for the information system as appropriate, such as a risk assessment, plan of action and milestones, accreditation decision letter, privacy impact assessment, contingency plan, configuration management plan, security configuration checklists, and system interconnection agreements. • **Role-based privileges:** Define role-based privileges based on the least privileges paradigm so that user roles reflect "least privilege" for each user. Too many users have "system developer" or "full privilege" access, which is

Assessment category	Recommendations
	a risk to the system because this allows users to make any change to the system. Resources should be allocated toward exploring exactly what privileges are needed for each role in clinics and build out the roles for users. Careful consideration should be taken when defining a roles management process so that it reflects actual system use (retrospective data entry or point-of-care) and allows IPs to manage users without over-encumbering limited IT staff. • **Risk designations:** Develop risk designations for personnel to guide the authorization that individuals need in the information system. As use of the EMR expands into point-of-care, this will be important for helping clarify roles in the system. At this time, however, it is more critical to clarify roles as indicated under access control. • **Security policies and procedures:** Document and maintain security policies and procedures and include all gap areas as noted in Table 3. Policies and procedures should consider the relative risk at a given site (e.g., a high-volume clinic with point-of-care access and Internet connectivity will need greater security planning than a site with a single computer doing retrospective data entry).
Operational controls	• **Secure local area network (LAN) and wireless network implementation:** All facilities had LAN access to UgandaEMR hosted on a central server, and some had access to the LAN through a wireless network. There needs to be documented guidance on best practices in low-resource settings for securing both the LAN and wireless networks that can access UgandaEMR. Policies and procedures should specify how and when access is granted to UgandaEMR systems, laptops, wireless access points, etc., and should be limited to only those individuals who require access. • **Data sharing procedures:** There should be documented procedures for how to handle external requests for information, including criteria for approving and denying requests, that can be referred to by all staff. Currently staff know the processes, but they are not documented. • **Appropriate use message:** Add a notification message for operating systems and UgandaEMR login screens stating the terms of use to provide legal reference in a case of a system compromise. • **Employment change policies and procedures:** Include procedures for terminating the employment of individuals or for staff who change their roles (full-time, part-time, temporary, contractors, etc.). • **Security training:** Conduct regular (at least annually) security training specific to UgandaEMR and computer use and customize training to roles, where applicable, in response to improved role management as recommended under access control. Training procedures should be documented, and information should be available to staff. • **Security testing:** Build and document processes to perform security testing after any and all system updates and changes. • **System inventory:** METS should have a mechanism for tracking IPs that may be using systems that are outdated and in need of upgrades to address critical security issues. IPs should maintain an inventory of computers and servers with configuration information so they can easily track computers that need updates.

Assessment category	Recommendations
	• **Incident response processes:** Documented process should be in place for incident response that address purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance. • **Staff protocols for incidents:** Remote sites should know not to bring servers to a local repair shop in case of an incident such as malware or a computer crash. Protocols should be outlined for theft, loss of data, power outages, server failures, and other common threats. • **Maintenance procedures:** Maintenance and backup procedures should be documented and implemented in a way that aligns with best practices (see backup procedures). Maintenance should be done regularly, including scanning systems for viruses and malware and operating systems and web browser updates for security patches. • **Media protection:** Procedures for storing, handling, and destroying both digital and nondigital media should be well defined and documented. Digital media includes diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes paper and microfilm (this includes paper reports printed from UgandaEMR). This is critical for both digital and nondigital media that contain personally identifiable information, such as a lost-to-follow-up report. • **Environmental protection:** Sites that house a server connected by a LAN should have temperature and humidity control devices to ensure the integrity of the equipment. • **Categorization of information and the information system:** Risk assessments should be conducted on a regular basis, particularly after major system changes or legal changes, and they should include security categories that describe the potential adverse impacts to organizational operations, organizational assets, and individuals if organizational information and information systems are comprised through a loss of confidentiality, integrity, or availability. Policies and procedures regarding risk assessments should be documented. • **Vulnerability scanning:** Sites with Internet connectivity should regularly conduct vulnerability scanning that checks for patch levels; functions, ports, protocols, and services that should not be accessible to users or devices; and improperly configured or incorrectly operating information flow control mechanisms. • **Ongoing security assessment:** As indicated in the management controls section, security policies should be in place that include regular security assessments, clearly defined roles for users by position that include role-based authorization with least privilege, support from management, and monitoring for compliance. Mechanisms for continuous monitoring should be in place as well as penetration testing for sites where the server or computers with access to the server are regularly connected to the Internet. • **Administrative/system-wide access:** Admin access to the server should be limited and auditable. Many of the sites that the assessment team visited were still using the default admin password from the METS-provided installation package, and multiple users had admin privileges in the system. Determining a course of action that will allow METS and IP administrators to oversee the system and provide technical support while limiting admin access is critical.

Assessment category	Recommendations
Technical controls	• **Access restrictions:** Restrictions documenting and implementing access to functions, ports, and protocols should reflect the minimum access needed to work. Installation of other software on servers and laptops should be limited and only done by designated personnel. Ports on drives should be restricted if not needed for business purposes. • **Locking of the operating system:** The operating system should lock after three failed login attempts or after a period of inactivity so that there is not inadvertent access to the system or its configurations that could pose risks to the data integrity and privacy. • **Audit logs:** Audit log should include system events, errors, logins, unsuccessful login events, password changes, and administrative privilege usage. • **Monitoring audit logs:** There should be designated staff and procedures in place for regular monitoring of audit files related to system volume. • **Configuration settings:** UgandaEMR and computer configuration settings to enhance security should be documented and standardized (such as system lockout time, operating system lockout time, limitations on installation of third-party software, inability to save passwords in browser). This should include protocols for making setting changes. • **Backup procedures:** Procedures should be documented and implemented in a manner that meets best practices for low-resource settings, such as ensuring that backup media is used only for UgandaEMR, that the backup device is password protected and encrypted, and that there are at least three backups, with one backup kept at an offsite location. If the volume of data entered in the system warrants, backups should be done daily. • **User account controls:** Both the operating system and UgandaEMR should require unique logins for all users, including the admin account. The default admin account should be changed from the default password at a minimum. Policies for password management should be outlined (e.g., how often should passwords be changed, what types of characters must be included in a password, whether passwords can be reused). There should be an agreement between METS and IPs on third-party admin access. • **IP restrictions:** For LAN-based systems, IP restrictions on server access should be implemented to prevent unauthorized devices from connecting to the server. • **Encryption:** Computers that store user data, including laptops from which reports generated from UgandaEMR, should use encryption for all data at rest. • **Isolation of security functions:** Security functions in OpenMRS/UgandaEMR should be isolated so they can be easily updated as new security requirements emerge. • **Improved security functionality:** Investment is needed to support increased security functionality in OpenMRS.

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

This publication was produced with the support of the United States Agency for International Development (USAID) under the terms of MEASURE Evaluation cooperative agreement AID-OAA-L-14-00004. MEASURE Evaluation is implemented by the Carolina Population Center, University of North Carolina at Chapel Hill in partnership with ICF International; John Snow, Inc.; Management Sciences for Health; Palladium; and Tulane University. Views expressed are not necessarily those of USAID or the United States government. TR-20-413
ISBN: 978-1-64232-242-2