Standard Operating Procedures for a Secure Electronic Health Record in Low-Resource Settings

May 2020

USAID
FROM THE AMERICAN PEOPLE

PEPFAR

MEASURE Evaluation

Standard Operating Procedures for a Secure Electronic Health Record in Low-Resource Settings

May 2020

MEASURE Evaluation
University of North Carolina
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. MS-20-194

ISBN 978-1-64232-259-0

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.

We'd like to acknowledge the project management team and the technical support we received from Jason B Smith, Manish Kumar, Herman Tolentino, Steven Yoon, Tadesse Wuhib, Eric-Jan Manders, Daniel Rosen, Mark DeZalia, Nega Gebreyesus, Kristen Wares, Jacob Buehler, Carrie Preston, Nathan Volk, David La'vell Johnson, and Adebowale Ojo.

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 testing this tool and providing valuable feedback and insight. We would also like to thank the implementing partners that allowed us to visit their facilities during the testing of this assessment tool, including the Rakai Health Service Program, The AIDS Support Organization, the Elizabeth Glaser Pediatric AIDS Foundation, the Infectious Disease Institute, management of Alive Medical Services Clinic, and the Makerere University Joint AIDS Program. The testing of the assessment tool 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 team who developed the assessment tool: 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: Panchenko Vladimir/Shutterstock.com

Suggested citation: MEASURE Evaluation. (2020). Standard Operating Procedures for a Secure Electronic Health Record in Low-Resource Settings. Chapel Hill, NC, USA: MEASURE Evaluation, University of North Carolina

CONTENTS

ABBREVIATIONS

ATEHRS	Assessment Tool for Electronic Health Record Security
EHR	electronic health record
IP	implementing partner
IT	information technology
PHI	personal health information
USAID	United States Agency for International Development

OBJECTIVES

These standard operating procedures have the following objectives:

- Provide guidance for implementing security safeguards for an electronic health record (EHR) in a low-resource country using current best practices tailored for low-resource settings.
- Incorporate best practices based on National Institute of Standards and Technology Special Publication 800, International Organization for Standardization 27001, the Office of the National Coordinator Security Risk Assessment Tool, and other international privacy and security standards.
- Understand common threats to security that must be regularly assessed.

INTENDED AUDIENCE

The intended audience for this document is project managers, data and information systems security administrators, digital health/eHealth officers, and other personnel involved in the implementation and maintenance of EHRs. It will also be of interest to monitoring and evaluation specialists, health information systems officers, healthcare providers, data entry officers, and other primary users of EHRs. In addition, it will be of interest to policymakers and information system developers to improve their understanding of safeguards needed to protect electronic health information.

INTRODUCTION

- Safeguarding an EHR to maximize privacy, confidentiality, and security while ensuring that the system data are accessible to users is critical to EHR adoption and acceptance as well as respecting the rights of patients to private and confidential treatment. EHR implementers should take advantage of safeguards built into software and operating systems that enhance privacy and security. In addition, policies and procedures should be in place that promote a culture of information and system security awareness and respect for privacy.
- Best practices around privacy and security for information systems are widely available, but often they do not account for the availability of resources, such as human resource capacity and Internet connectivity. This job aid has been curated to highlight critical privacy and security safeguards based on international best practices while taking into account EHR implementation scenarios commonly practiced in low-resource settings. These generalized implementation scenarios are outlined in Table 1.

Table 1. Security requirements level by implementation scenario

Security requirements level	Implementation Scenario Description
Minimum	Facility-based standalone instance of EHR on a local area network that is rarely or never connected to the Internet. This instance of EHR is used for retrospective data entry.
Intermediate	Facility-based standalone instance of EHR on a local area network that is sometimes connected to the Internet. This instance of 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. EHR is being used for point-of-care service delivery and clinical decision making.

The safeguards that should be implemented will depend on the degree of risk and the potential harm that a given threat or vulnerability poses to the implementing partner (IP) and the individual patients whose data are stored in the EHR. Additional safeguards may be required by a ministry of health, a funding organization, or an IP. For example, in the minimum scenario described above, an EHR used to collect data retrospectively is primarily used for reporting on a small number of patients and would likely need less auditing and backups than a system used for point-of-care in a busy, urban facility. Further, it may be cost prohibitive to maintain certain safeguards at remote, low-volume facilities.

This tool is not comprehensive. It addresses implementation scenarios typically seen in low-resource settings, and your organization may need additional safeguards, depending on the complexity and reach of your information systems. It is designed for systems that primarily fall under the minimum and intermediate scenarios in Table 1 and provides a starting point for the advanced scenario. A paperless or near-paperless system will need more safeguards to ensure availability, because the EHR will be critical to day-to-day operations after paper records are removed. In addition, this job aid does not include country-specific legal requirements that may apply to your EHR.

HOW TO USE THIS DOCUMENT

These standard operating procedures contain a step-by-step guide for implementing a security management process as well as a checklist of best practices for security, as outlined in the Assessment Tool for EHR Security (ATEHRS). Implementing all of the items found in this tool would address each of the controls in the assessment tool. However, individual IPs should prioritize which controls to implement based on relative risk and cost factors. The safeguards are divided into administrative, physical, and technical, as described in the Health Insurance Portability and Accountability Act security information series (U.S. Department of Health and Human Services, n.d.). Administrative safeguards primarily cover policies and procedures that should be in place to oversee and enforce EHR security. Technical safeguards are software features, settings, and automated processes that may be used to enhance security. Physical safeguards refer to protections from environmental hazards, unauthorized access, and theft.

STANDARD OPERATING PROCEDURES DEVELOPMENT

These procedures were adapted from National Institute of Standards and Technology Special Publication 800-53, International Organization for Standardization 2700, and Health Insurance Portability and Accountability Act safeguards, prioritizing those that were most applicable to low-resource settings and taking into account the implementation scenarios described in the ATEHRS developed by MEASURE Evaluation. Links to these guidelines are provided in the Resource section.

IMPLEMENTING A SECURITY MANAGEMENT PROCESS

This section contains guidance for how to set up a security management process. These steps are adapted from the Office of the National Coordinator for Health Information Technology's *Guide to Privacy and Security of Electronic Health Information* (Office of the National Coordinator for Health Information Technology, 2015). They are intended for IPs or service delivery organizations that are responsible for implementing and maintaining and EHR, especially those that are new to incorporating security planning into their regular operations.

The following steps should be taken in setting up your security management process.

1. **Be aware of the security landscape.** Ensure that your organization is aware of local and regional policies related to electronic health information and electronic identity information. In addition, if you are receiving donor funding, you may be subject to privacy and security regulations as a part of the funding.
2. **Designate a security team.** Information security should be seen as an organizational priority. One or more people should be designated as a security focal person, with the responsibilities of overseeing information security included in their job descriptions. This person should be responsible for being aware of and up to date regarding the security landscape described in Step 1. This person should also be aware of security safeguards and security limitations of the EHR software that your organization is using.

   The security focal person should be responsible for leading the initial and ongoing security risk analysis. It may be useful to obtain the support of an information security specialist who can guide you through the initial or ongoing security processes. The information security specialist can help ensure that your risk analysis is not subjective and should help your organization in determining and prioritizing steps to mitigate risks found.

   The security focal person should also be responsible for promoting a culture of privacy and security of electronic health information. This includes overseeing trainings related to EHR security and ensuring that they are conducted regularly.

An information security specialist can help with developing your security management plan, conducting a security assessment, and determining priorities for safeguards based on the security assessment results. The availability of information security specialists can vary greatly from country to country. If you think your organization has the resources and can benefit from contracting with a security specialist, consider these suggestions:

- Check if your local university offers applicable security and privacy training programs and can recommend graduates or faculty of the program.
- Look for someone with information security qualifications. One such qualifying organization is the International Information System Security Certification Consortium (**https://www.isc2.org/**), which offers certifications as Certified Information Systems Security Professional and HealthCare Information Security and Privacy Practitioner. A person with one of these certifications could assist with an assessment.

3. **Document security process, results, and actions**. It is critical that policies and procedures regarding information security are documented and maintained (see the List of Policies, Procedures, and Other Security Documents section). These documents outline plans for maintaining security and also document responses to security assessments and incidents. Having clearly outlined processes will make security assessments more efficient, promote a culture of information security within your organization, and ensure that you have documentation about measures taken to ensure information security in the case of an audit or incident.
4. **Conduct a security assessment.** A security assessment will help identify threats and vulnerabilities to your EHR. The ATEHRS was developed to support organizations to conduct a security assessment that aligns with international best practices. The security focal person should oversee this process, with the support of an information security specialist, if possible. The security assessment should identify the following:
    4.1. *How electronic personal health information (PHI) is created, used, and transmitted from your EHR*. This should include reports generated in both paper and electronic format. The risk may vary depending on how the EHR is implemented and accessed. See implementation scenarios in the ATEHRS.
    4.2. *Threats and vulnerabilities to the EHR*. These are things that can compromise confidentiality, integrity, and availability of the EHR. They can be human, such as losing a staff person, losing a lost-to-follow-up list, or theft of equipment containing PHI, or they can be environmental, such as a loss of power.
    4.3. *Information risks and their associated levels*. This looks at the susceptibility of your EHR to threats and vulnerabilities given the current safeguards in place. For example, the minimum scenario described in Table 1 is likely at low risk for denial of service and other Internet-based human threats, even without all the appropriate safeguards. On the other hand, you may find that users are transferring reports via encrypted USB drives that are also used for personal reasons and leave your facility without monitoring. The risk here would be high because

there is no monitoring or tracking of the data being stored on those devices and no safeguards in place.

5. **Implement an action plan.** In Step 4, you conducted a security assessment to identify and assess risks to electronic PHI and your EHR. You should use this assessment to prioritize and mitigate risks by instituting the necessary administrative, technical, and physical safeguards. If you are using an external assessor, he or she should assist you in this process. The Safeguards Checklist section represents the core set of administrative, technical, and physical safeguards that should be in place, and addresses organizational protocols, policies, and procedures. Your organization may need additional or fewer safeguards, depending on how your EHR is implemented. You may also need to involve other stakeholders in the development and implementation of these safeguards, depending on how your EHR and service delivery activities are funded and overseen.

   Policies and procedures should be in place for all safeguards, and staff should be aware of these. It may be necessary to conduct a refresher training to raise awareness among staff. International best practices suggest that new staff or contractors should be trained when hired and that all staff should receive yearly training as well as training when there are changes to policies and procedures, systems, location, or infrastructure. See the Resources section for training guidance.

   Make sure that you are up to date on local legislation regarding a patient's right to access data and your organization's responsibility to maintain confidentiality and privacy of a patient's PHI. Ensure that the required consent is obtained from patients for exchanging PHI and that mechanisms are in place for notifying patients of major system changes that impact how their data are used, stored, and processed.

6. **Conduct continuous security planning and monitoring.** Maintaining security is a continuous process. Your security policies and procedures should outline how and when security audits should be conducted. Auditing should take into account the overall system risk. For example, a standalone retrospective EHR in a low-volume facility will require less frequent auditing than a high-volume point-of-care system.

   The security focal person should ensure that both the EHR and hardware being used have appropriate monitoring and auditing functions in place and are configured to meet the needs outlined in your security plan. That plan should outline the following:

   - What to audit (server logs, system logs, etc.) and how audits will occur
   - Non-routine audit triggers for potential incidences of compromised PHI
   - Guidance for conducting random audits
   - A schedule for routine audits (for geographically dispersed sites, it may be easier to include routine audits as part of regular maintenance)

   In addition to regular auditing, reassessing security risks should be done on a regular basis to ensure that there has not been a lapse to adhering to best practices and that newly implemented safeguards have been effective, or whenever there is a major system change.

LIST OF POLICIES, PROCEDURES, AND OTHER SECURITY DOCUMENTS

This section provides a list of recommended policies that should be prepared and maintained as part of security planning. This list can also be helpful to ensure that an IP has all relevant documents in preparation for a security audit or assessment. The following documents should be included in the policies:

- Security plan
- Contingency plan
- Training materials and policy
- Any agreements with external organizations, such information technology (IT) service company, information security specialist, EHR software developers, or above-site mechanisms
- Security risk assessment reports
- EHR and server audit logs
- Risk management plan
- Incidence response plans
- Existing incident reports
- Maintenance plans
- Access control policies

SAFEGUARDS CHECKLIST

Administrative Safeguards

☐ **A1. Develop, document, and implement policies and procedures for analyzing, assessing, and managing risks to PHI**
Considerations: The policy and procedures should include an inventory of all electronic devices accessing the system, including computers, flash drives, and backup drives. The policies and procedures should also outline handling policies for all files that are exported from the EHR, whether paper or digital, that contain PHI. It should outline a process for who has access to those files, how they are securely transferred, and when they are destroyed.
Threats addressed: Unauthorized access or inappropriate use of PHI
☐ **A2. Implement a process for periodically reviewing policies and procedures for analyzing, assessing, and managing risks to PHI**
Considerations: The policies and procedures outlined in A1 should be periodically reviewed and assessed to ensure that they address changes in technology, vulnerabilities, and threats. They should also be reviewed in response to planned system use changes, such as the addition of biometric identification or changing from retrospective data entry to point-of-care service delivery. Processes, policies, and procedures should be documented and should include a "reviewed" and "approved" date. Changes in policies and procedures should be disseminated to facility staff as needed.
Threats addressed: The review will ensure that unauthorized access or inappropriate use of PHI is not compromised by system changes or evolutions of threats.

☐ **A3. Develop, document, and implement policies and procedures for incident response**

Considerations: In the event of an incident or a suspected incident, such as theft of a computer, loss of data, or compromised PHI, there should be a clear procedure for reporting the incident and procedures for assessing the magnitude of harm caused by the incident and risk of future incidents. The procedure should include development of a remediation plan to prevent a reoccurrence.

Threats addressed: Unauthorized access, use, disclosure, disruption, modification, loss, or destruction of EHR data

☐ **A3. Formalize and document a process for risk and security assessment**

Considerations: The policies and procedures outlined in A1 and A2 should include regular security assessments (such as use of the ATEHRS) that ensure that administrative, technical, and physical safeguards are in place to address existing or evolving threats and vulnerabilities. Identified risks should be associated with a control or method planned or in place to address the risk. For example, if a facility is currently backing up data on an unencrypted device, other means of backup should be explored that would not result in the threat of compromised PHI.

The plan for the assessment should include dissemination procedures that include all stakeholders responsible for risk mitigation, including donors, software developers, implementing partners, subgrantees, and above-site mechanisms. A plan of action for implementing safeguards with responsible parties and milestones should result from the security assessment.

Consider what existing practices can help facilitate and streamline security assessments, such as including security assessments or audit processes as part of regular computer maintenance or data quality assessment activities.

Threats addressed: Unauthorized access, use, disclosure, disruption, modification, loss, or destruction of EHR data and PHI

☐ **A4. Formalize and document an overarching security plan**

Considerations: A security plan addresses the confidentiality, integrity, and availability of your system. It includes the previously described risk and security assessment plan, incident response plan, and plans for continuity, emergency access, disaster recovery, and vendor management. In addition, the security plan should include all documented procedures and policies for administrative, physical, and technical safeguards. It should also document the methods in place or planned to mitigate the threats and vulnerabilities to the EHR and PHI that are identified as a result of conducting a continuous risk analysis.

The security plan should include purpose, scope, roles, responsibilities, management commitment, expected coordination among internal and external stakeholders, and legal compliance requirements, including, where applicable, national eHealth and information and communication technology strategies. The policy should include procedures for the implementation of the security plan and safeguards. Staff and key stakeholders should be aware of security plan policy and procedures. The plan should be reviewed and updated annually, as well as in response to major system modifications or incidents.

Policies and procedures should describe the methods in place to limit access to PHI in the EHR.

The security plan should include a process for periodically monitoring the physical environment, operations, and computers to assess the effectiveness of security safeguards.

The security plan and other plans described in this document should be formally written and available to staff and retained following your organization or legal policies.

Threats addressed: Unauthorized access, use, disclosure, disruption, modification, loss, or destruction of EHR data and PHI

☐ **A5. Formalize documented human resources policies aligned with country laws that address the consequences of system misuse**

Considerations: The security point of contact (see A8) should be aware of any country's national eHealth framework as well as specific country laws related to PHI and should work with the human resources department to ensure that policies are aligned with organizational and legal guidelines. This may require consulting with legal representation, especially because laws regarding electronic PHI and other health data evolve. Consider whether donor funding influences policy (e.g., donor encourages specific privacy and security protocols to be followed).

It is important to apply appropriate sanctions against staff who fail to comply with the security policies and procedures so that staff are aware of the severity of consequences of violation policies and laws.

Threats addressed: EHR and PHI misuse, abuse, and any harmful activities by staff

☐ **A6. Conduct security awareness training**

Considerations: Staff should receive training on security awareness before gaining access to the EHR as well as at least an annual refresher training. Training should include review of human resources policies and procedures related to securing PHI and review of legal frameworks related to PHI and health data. Staff should be aware of both HR sanctions in response to PHI violations as well as the impact to the organization and its patients.

Training should include information about how viruses and malware can get into computers, and information about phishing and how to prevent it. It should also advise staff not to store their login information in their web browser if the EHR is accessed through that method. Staff should be reminded to protect their username and password and not to share them.

Training should include information about how to protect the integrity and availability of data through proper backup procedures. The training should also include how to securely handle all media (digital and non-digital) that contains PHI. In addition, staff should be trained in how new information systems that that impact PHI are deployed or how existing systems are upgraded.

Records should be kept of training dates and participants. Training should be periodically reviewed in response to changes to the EHR, how it is used, in response to incidents, or in response to changes in threats and vulnerabilities. If warranted by the size and complexity of your organization, the training should be role-based (e.g., different training for providers compared to data entry clerks).

Security awareness should be reinforced through periodic reminders that encourage staff to remain vigilant about security.

Threats addressed: Unauthorized access, use, disclosure, disruption, modification, loss, or destruction of EHR data and PHI. Loss of IP reputation, medical identity theft, and legal action from either patients or government. Loss of donor funding.

☐ **A7. Develop policies and procedures for reviewing EHR activity**

Considerations: A security focal person should be identified who is responsible for analyzing EHR and computer activity, incident reports, audit reviews, exception reports, and audit logs. An audit and accountability policy should be included in the security plan. It is important to include a timeline for regular review in the plan. Reviewing of logs could be included in the system maintenance procedures for remote facilities with limited Internet access. For a networked server, it is important to monitor for attacks and unauthorized connections through the use of server monitoring devices and software.

Login monitoring of both the EHR and the computers used to access the EHR should be included in policies and procedures.

Threats addressed: Security violations and unauthorized use

☐ **A8. Designate a security focal person/point of contact**

Considerations: At least one person in the organization should be designated as an information security focal person. This person's job responsibilities should include development and implementation of a security plan and policies. Staff should be aware of who this person is to report an incident or address security concerns. Depending on the number of facilities, this person may also be responsible for leading other activities described under the Administrative Safeguards section, or more than one person may be required in this role.

This person should have the necessary training and qualifications to oversee these activities and management commitment to provide resources to implement them. Ideally, there should be a separation of duties, and this person should not also hold the role of data entry clerk or healthcare provider.

Threats addressed: Ineffectively implemented safeguards that lead to unauthorized access and compromise confidentiality, integrity, and availability of the EHR

☐ **A9. Determine access authorization**

Considerations: A clear process should be in place for determining who will be granted access to the EHR and what permissions they will have in the system based on their role. Permissions should be assigned based on the concept of least privilege, assigning only permissions needed for that role. The process should also include a procedure for changing or removing access in the case of a change in role or termination.

The policy should also include procedures for obtaining approvals and authorizing access to non-staff members, such as researchers or other IPs. The approval process should include a method for determining least-privilege permissions that the user would need.

For both internal and external access, there should be a screening process in place to verify that users are trustworthy, such as pre-employment screening.

Threats addressed: Safeguarding user account management against security violations

☐ **A10. Implement role management and separation of duties**

Considerations: Develop procedures that specify authorized users of the EHR, roles, and privileges for each account and how those are assigned. This should specify things such as who can access the system wirelessly and remotely, and who has access to view or modify PHI. This should also address who can change user roles and privileges in the system.

Most users should not be able to change their own roles and privileges. Roles should be created so that users have access to only the functions needed to do their job. System administrative functions should only be assigned to those who have that organizational role. Separation of duties helps catch errors and prevent misuse by establishing clear roles for each user; ensuring that more than one person is responsible for an activity; separating system management, programming, configuration management, quality assurance and testing, and network security roles; and separating access control administration for audit administration (Joint Task Force Transformation Initiative, 2013). Establishing such separation of duties may be challenging for organizations with limited staff and remote locations.

Threats addressed: Safeguarding user account management against security violations. Unauthorized or inappropriate access to PHI.

☐ **A11. Develop maintenance policies and procedures**

Considerations: Policies and procedures should be developed to ensure that software patches are implemented as needed and antivirus and antimalware software is kept up to date. Where possible, the server or computer that contains the EHR instance should be restricted to that software. Only designated staff should be permitted to install software on the computer containing the EHR instance. Furthermore, the policies should describe who is allowed to performance maintenance on the hardware that houses the EHR instance and how the maintenance staff will access these computers.

Threats addressed: Unauthorized or inappropriate access to PHI.

☐ A12. Develop contingency planning policies and procedures
Considerations: A contingency plan should include policies and procedures for the restoration of the EHR and its data in the case of a system breakdown or disaster, including a backup methodology for collecting and maintaining data while the system is inaccessible and how those data will be transferred back to the system when it is running again. Security and IT personnel should be aware if the EHR is needed for decision making about a patient's treatment during an emergency. There should be a plan to prioritize restoration of the system in the case of an emergency or incident. This plan should be regularly tested, reviewed, and updated.
Threats addressed: Accurate information is not available when needed, adversely impacting providers' ability to diagnose and treat their patients
☐ A13. Develop backup planning and procedures
Considerations: A data backup plan is a collection of procedures to create and maintain a retrievable copy of the data and should be included as a part of the contingency plan. Ideally, there should be three backups maintained for each server instance of the EHR: one locally on the server, one on an external device where the server is housed, and one at an offsite facility. External backups should be kept on a password-protected and encrypted drive that is only used for the backup of the EHR. External devices should be locked in a secure location when not in use, and access to and movement of that device should be limited to designated personnel. Clear procedures for system restoration and inputting of data collected while the system was offline should be outlined in the policy.
Threats addressed: Availability of the EHR

Technical Safeguards

☐ T1. Implement security settings for all devices
Considerations: Implement access controls for all computers and devices that can access the EHR or contain data from the EHR, ensuring that all security features available are being used (e.g., passwords for workstations that access the EHR). This should include uniquely identifying all users and encrypting PHI transmission and storage. Avoid using shared passwords for computer access and implement domain services and authentication methods where possible.
Threats addressed: Unauthorized access to devices containing PHI
☐ T2. Ensure unique identification
Considerations: Have policies and procedures in place for the assignment of a unique identifier for each authorized user of the EHR. Users should have unique accounts to associated devices, such as computers that access the EHR or have it installed. Documented policies help ensure that security controls are followed. Expressly prohibit sharing of accounts, including administrative accounts. This ensures that authorized user privileges are associated with each unique user identifier.
Threats addressed: Unauthorized access to the EHR and devices containing PHI
☐ T3. Establish emergency access
Considerations: Consider which staff will access the EHR in the event of a system malfunction or other emergency and how they will access it. This will depend on the criticality of the EHR (how long can the facility go without system access before operations and patient safety are negatively impacted?), the geographic spread of your facilities, and availability of security and IT staff. An example would be to back up the server remotely if physical access is not possible.
Threats addressed: Loss of EHR accessibility

☐ T4. Enforce automatic logoff
Considerations: The EHR should enforce an automated session lock that returns to a login screen after a predetermined period of inactivity or upon receiving a request from a user. Retain the session lock until the user reestablishes access using the established identification and authentication procedures. This should be employed for software as well as servers, workstations, and laptops.
Threats addressed: Unauthorized access to EHR and devices containing PHI
☐ T5. Encrypt EHR data
Considerations: Policies and procedures need to include encryption of PHI. Staff should be trained to encrypt the data they are sending electronically. Many EHRs and computers have built-in encryption functionality that can be used (e.g., BitLocker on Microsoft computers and servers). Any media used to share PHI, such as a backup drive, should be encrypted. IPs should evaluate actual costs, ease of implementing, and effectiveness of encryption technology and periodically reexamine these as data sharing and system interconnectedness increase.
Threats addressed: Unauthorized access to EHR and devices containing PHI
☐ T6. Implement hardware, software, and procedural mechanisms that record or examine information system activities
Considerations: This will serve to operationalize audit and accountability policies. All parts of the information system that are involved in key audit events, such as the creation, storage, and transmission of PHI, should be identified and have audit capabilities. Other key events include password changes, failed logons, or failed accesses related to information systems, administrative privilege usage, Personal Identification Verification credential usage, third-party credential usage, or changes to the data. Key audit events should be reviewed periodically for unusual activity. The frequency and scope of the audits should be informed by a security risk analysis (the higher the risks or the more critical the integrity and availability of the system is, the more frequently analysis is needed). Reports should be shared with appropriate staff to help identify inappropriate use of the system.
Threats addressed: Failure to detect unauthorized activity
☐ T7. Protect the EHR from improper alteration or destruction
Considerations: Users should be restricted from improper altering or destroying EHR data using role settings. Data authentication methods and data quality methods should be used to ensure that data are not altered or destroyed improperly.
Threats addressed: Improper alteration or destruction of data
☐ T8. Ensure the integrity of usernames and passwords
Considerations: Access control should ensure that databases storing usernames and passwords are encrypted. Passwords should be obfuscated when entered. Users should not be able to store password information for a web-based EHR in the browser.
Threats addressed: Unauthorized access to information systems

Physical Safeguards

☐ P1. Maintain an inventory of physical systems, devices, and media used to access, create, transmit, or store EHR data
Considerations: Inventory should include locations of devices (computers, servers, networking equipment, universal power supply), software installed, and serial numbers. Inventory should be added at acquisition, and it should be periodically reviewed and updated in case of changes to facilities or other incidents that may impact inventory. Inventory should be verified as part of normal maintenance procedures.
Threats addressed: Identify locations that need physical access control

☐ **P2. Develop, implement, and maintain policies and procedures for the physical protection of facilities and equipment**
Considerations: A facility security plan contains policies and procedures designed to control access to the facility, maintain the facility, and control access to systems and equipment that handle PHI. This should include physical access control procedures to limit entrance to and exit of the area where computers and devices are kept; secure the keys, combinations, and other physical access devices; maintain a list of individuals with authorized access to restricted areas; employ authorization credentials (such as an ID badge); post signage that designates secure areas; and limit access to output devices, such as printers, fax machines, and copiers. This policy should also address the physical environment needed to keep computers working appropriately, such as maintaining universal power supplies, fire extinguishers, temperature and humidity control, air filtration, and protection from water damage. The plan should address any local or country-specific legal requirements addressing physical safety of PHI. The plan should be periodically reviewed and updated as needed. Verification that the policies and procedures are being implemented at all facilities should occur regularly with documented checks.
Threats addressed: Inappropriate access to EHR data, environmental threats to equipment
☐ **P3. Ensure that all locations in the inventory have physical protections in place**
Considerations: Examples include locks on doors and windows where equipment is stored, cameras to monitor entrances and exits, and secure covering for networking equipment and cabling.
Threats addressed: Physical access by unauthorized users
☐ **P4. Ensure the security of keys and combinations to areas where the system is physically located**
Considerations: Policy and procedures should address the security of keys and combinations. This should include when to re-key locks or change combinations when, for example, a key is lost, a combination is compromised, or a staff member is transferred or terminated.
Threats addressed: Physical access by unauthorized users
☐ **P5. Maintain a facility access list**
Considerations: A list should be maintained of staff and others who are allowed access to secure areas, secure systems, keys, and combinations. Include a process for sites to know when headquarters staff or others might be visiting, what access has been approved for them, and how they will be identified. This list should be periodically reviewed so that it is kept up to date.
Threats addressed: Physical access by unauthorized users
☐ **P6. Maintain facility access logs**
Considerations: Develop procedures to create, maintain, and keep a log of who accesses the organization's facilities, when the access occurred, authorization for access, and the reason for the access.
Threats addressed: Physical access by unauthorized users
☐ **P7. Implement policies and procedures for preventing unauthorized physical access**
Considerations: What steps are taken to prevent visitors and patients from viewing another person's PHI, either on purpose or incidentally. This should include restricting areas, locking workstations, and control of paper documents that contain PHI. Policies should be covered in security training and reinforced regularly. Include protection of portable devices that contain PHI, such as laptops, tablets, mobile phones, or flash drives.
Threats addressed: Physical access by unauthorized users

☐ **P8. Implement policies and procedures for the protection of media**
Considerations: Security policies and procedures to physically protect and securely store both paper data printed from the EHR and electronic media inside a facility until they can be securely disposed of or destroyed. Consider restricting the ways that data can be shared or transmitted. Include tracking mechanism for all shared media including printed reports that contain PHI. If a device is to be repurposed, ensure that procedures are in place for removal of PHI.
Threats addressed: Loss of PHI
☐ **P9. Implement policies and procedures for the retention and disposal of devices and media**
Considerations: There should be policies specifying how long to retain PHI. This policy should be informed by local regulations and laws. A disposable process for both electronic and paper media as well as computers and other devices that store PHI should be documented and implemented. The disposable process should ensure that the confidentiality of PHI is not compromised. Ensure that all PHI is removed from devices in the event of offsite maintenance or disposal.
Threats addressed: Unauthorized access to PHI
☐ **P10. Record access to and movement of devices and media**
Considerations: Maintain a record of staff who have authorization to remove devices and media that have or can access PHI from the facility. Transport records should also be maintained. Include backup procedures prior to the movement of equipment if needed.
Threats addressed: Loss of data and data availability

RESOURCES

International Organization for Standardization. (n.d.). ISO/IEC 27001 information security management. Retrieved from https://www.iso.org/isoiec-27001-information-security.html

McAllister, E., Grance, T., & Scarfone, K. (2010). *Guide to protecting the confidentiality of personally identifiable information.* National Institute of Standards and Technology Special Publication 800-122. Gaithersburg, MD: National Institute of Standards and Technology. Retrieved from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-122.pdf

MEASURE Evaluation. (2020). *Assessment Tool for Electronic Health Record Security: Guidance for Low-Resource Settings*. Chapel Hill, NC, USA: MEASURE Evaluation, University of North Carolina. Retrieved from https://www.measureevaluation.org/resources/publications/ms-20-195

National Institute of Standards and Technology (NIST). (2004). *Standards for security categorization of federal information and information systems.* Federal Information Processing Standards Publication 199. Gaithersburg, MD: NIST. Retrieved from https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf

Office of the National Coordinator for Health Information Technology. (n.d.). Security risk assessment tool. Retrieved from https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment-tool

Ruggiero, P., & Heckathorn, M.A. (n.d.). *Data backup options.* Washington, DC: United States Computer Emergency Readiness Team. Retrieved from https://www.us-cert.gov/sites/default/files/publications/data_backup_options.pdf

REFERENCES

Joint Task Force Transformation Initiative. (2013). *Security and privacy controls for federal information systems and organizations*. National Institute of Standards and Technology Special Publication 800-53, Revision 4. Gaithersburg, MD: National Institute of Standards and Technology. Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

Office of the National Coordinator for Health Information Technology. (2015). *Guide to privacy and security of electronic health information*. Washington, DC: U.S. Department of Health and Human Services. Retrieved from https://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf

U.S. Department of Health and Human Services. (n.d.). Security rule guidance material. Retrieved from https://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html

MEASURE Evaluation
University of North Carolina
123 West Franklin Street, Suite 330
Chapel Hill, North Carolina 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. MS-20-194

ISBN 978-1-64232-259-0

USAID FROM THE AMERICAN PEOPLE

PEPFAR

MEASURE Evaluation