Assessment Tool for Electronic Health Record Security

Guidance for Low-Resource Settings

April 2020

USAID FROM THE AMERICAN PEOPLE

PEPFAR

MEASURE Evaluation

Assessment Tool for Electronic Health Record Security

Guidance for Low-Resource Settings

April 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-20-195

ISBN: 978-1-64232-260-6

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 recognize the project management team and the technical support we received from Jason B. Smith, Manish Kumar, and David La'Vell Johnson of MEASURE Evaluation at the University of North Carolina at Chapel Hill (UNC); Herman Tolentino, Steven Yoon, Tadesse Wuhib, Eric-Jan Manders, Daniel Rosen, Carrie Preston, Nathan Volk, and Adebowale Ojo of the United States Centers for Disease Control and Prevention (CDC); Mark DeZalia at the President's Emergency Plan for AIDS Relief (PEPFAR); and Nega Gebreyesus, Kristen Wares, and Jacob Buehler at USAID.

The MEASURE Evaluation project, funded by USAID and PEPFAR, would like to thank the Monitoring and Evaluation Technical Support Program at the Makerere University School of Public Health in Uganda for its cooperation and support in testing this tool and providing valuable feedback and insight. We would also like to thank the Rakai Health Service Program, The AIDS Support Organization, the Elizabeth Glaser Pediatric AIDS Foundation, the Infectious Disease Institute, the management of Alive Medical Services Clinic, and the Makerere University Joint AIDS Programme, and the implementing partners in Uganda that allowed us to visit their facilities during the piloting of the assessment tool. The testing of this assessment tool would not have been possible without the support of Rachel Kwezi of USAID in Uganda; Ray Ransom of CDC, Uganda; and technical assistance from CDC, PEPFAR, and USAID headquarters.

We acknowledge the team that 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 UNC, for editorial, design, and production support.

Suggested citation: 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

Cover design by Denise Todloski

CONTENTS

FIGURES

TABLES

ABBREVIATIONS

CDC	Centers for Disease Control and Prevention
DNS	domain name system
EAP	Extensible Authentication Protocol
EHR	electronic health record
FedRAMP	Federal Risk and Authorization Management Program
GDPR	General Data Protection Regulation
HIPAA	Health Insurance Portability and Accountability Act of 1996
IT	information technology
LAN	local area network
NIST	National Institute of Standards and Technology
OWASP	Open Web Application Security Project
PEPFAR	United States President's Emergency Plan for AIDS Relief
PHI	Personal Health Information
PII	personally identifiable information
PKI	public key infrastructure
TLS	Transport Layer Security
UNC	University of North Carolina
USAID	United States Agency for International Development
VoIP	Voice over Internet Protocol
VPN	virtual private network
WAN	wide area network

GLOSSARY OF TERMS

Availability: Ensuring timely and reliable access to and use of information.
Source: https://csrc.nist.gov/glossary/term/availability

Baseline risks: Current level of risk that takes into account existing risk mitigation measures.
Source: API STANDARD 780, Security Risk Assessment Methodology for the Petroleum and Petrochemical Industries, First Edition, May 2013

Confidentiality: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
Source: https://csrc.nist.gov/glossary/term/confidentiality

Cryptographic: Pertaining to, or concerned with, cryptography, which is the discipline that embodies the principles, means, and methods for the transformation of data to hide their semantic content, prevent their unauthorized use, or prevent their undetected modification.
Sources: https://csrc.nist.gov/glossary/term/cryptographic and
https://csrc.nist.gov/glossary/term/cryptography

Encryption: The process of changing plaintext into a form (called "ciphertext") that conceals the data's original meaning to prevent them from being known or used. If the transformation is reversible, the corresponding reversal process is called "decryption," which is a transformation that restores encrypted data to their original state.
Source: https://csrc.nist.gov/glossary/term/encryption

Integrity: Guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity.
Source: https://csrc.nist.gov/glossary/term/integrity

Non-repudiation: Protection against an individual falsely denying having performed a particular action. Provides the capability to determine whether a given individual took a particular action, such as creating information, sending a message, approving information, and receiving a message.
Source: https://csrc.nist.gov/glossary/term/non_repudiation

Penetration testing: A test methodology intended to circumvent the security function of a system.
Source: https://csrc.nist.gov/glossary/term/penetration_testing

Personally identifiable information (PII): Information that can be used to distinguish or trace the identity of an individual (e.g., name, Social Security number, biometric records) alone or when combined with other personal or identifying information that is linked or linkable to a specific individual (e.g., date and place of birth, mother's maiden name).
Source: https://csrc.nist.gov/glossary/term/personally_identifiable_information

Risk assessment: Identifies the kinds and levels of risk to which organizations may be exposed; also considers both the likelihood and impact of undesired events.
Source: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf

Risk mitigation strategy: Prioritizing, evaluating, and implementing the appropriate risk-reducing controls and countermeasures recommended from the risk management process.
Source: https://csrc.nist.gov/glossary/term/risk_mitigation

Threat event: An event or situation that has the potential for causing undesirable consequences or impact.
Source: https://csrc.nist.gov/glossary/term/Threat_Event

Threat source: The intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally trigger a vulnerability.
Source: https://csrc.nist.gov/glossary/term/threat_source

Vulnerability testing: 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
Source: Scarfone, K., Souppaya, M., Cody, A., & Orebaugh, A. (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: National Institute of Standards and Technology. Retrieved from https://www.nist.gov/publications/technical-guide-information-security-testing-and-assessment.

INTRODUCTION

The Assessment Tool for Electronic Health Record Security: Guidance for Low-Resource Settings was developed to help ministries of health, implementing partners, software developers, donors, and other stakeholders examine the security of electronic health record (EHR) systems. Designed using internationally accepted best practices, the assessment approach keeps the limited capacity of information security specialists in low-resource settings in mind. The guidance takes into consideration typical EHR implementation scenarios, such as a single instance of an EHR being used for retrospective data entry, while also allowing users to continue to assess security as their EHR systems mature to interconnected point-of-care systems. This document provides instructions on the use of several tools to assess EHR system privacy and security and for instituting continuous monitoring of EHR privacy and security.

BACKGROUND

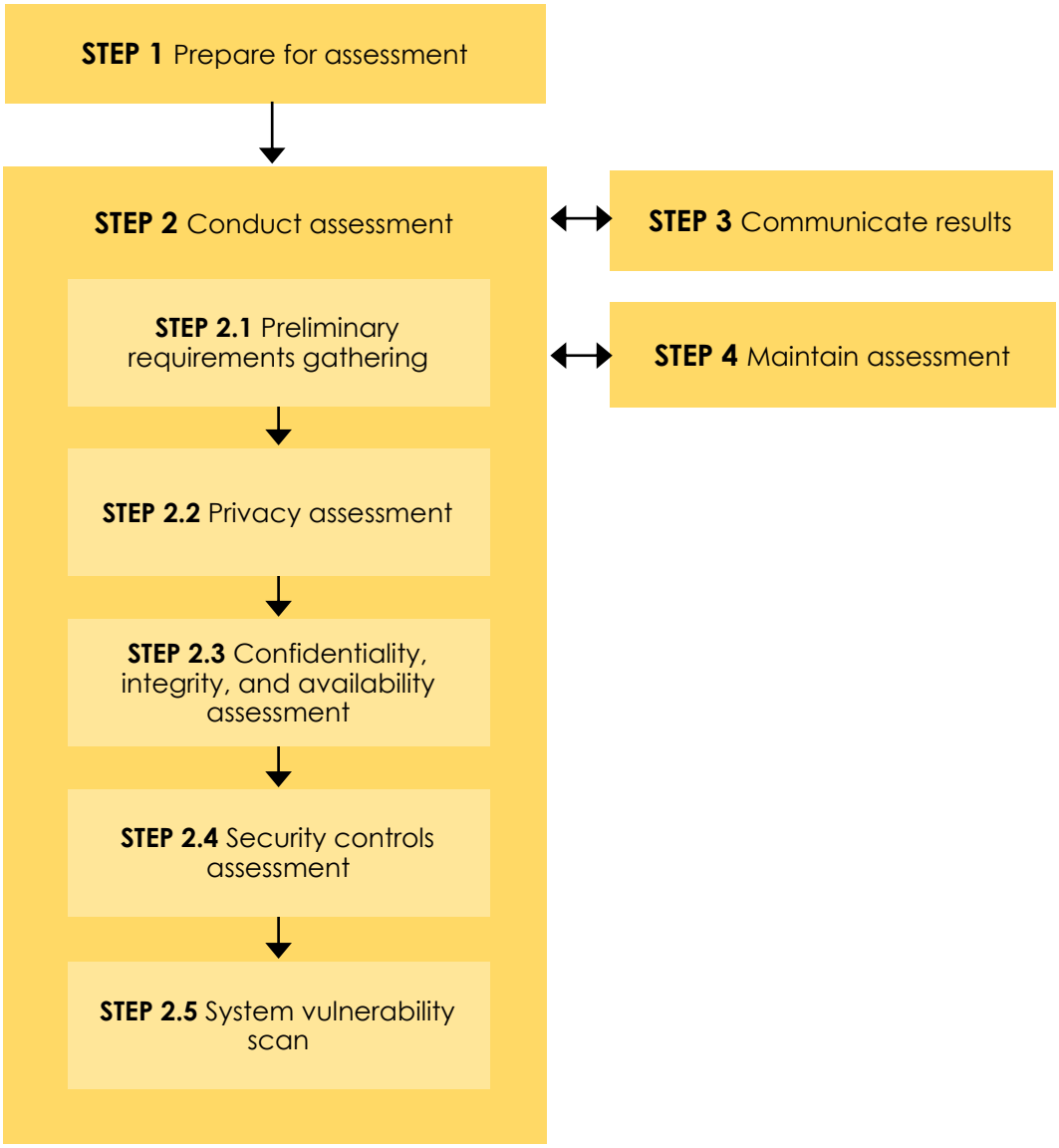
An information system security audit is a type of risk assessment. Risk assessments are a key part of effective risk management. They facilitate decision making at the information systems level and at the organizational and mission/business process levels. Risk management is an ongoing process. Assessments should ideally be performed before system acquisition, during implementation, and as the system is maintained. The approach provided in this document is a type of targeted risk assessment. A targeted risk assessment has a narrowly defined scope to produce answers to specific questions, in this case: what are the risks associated with the use of an EHR and how can these risks be mitigated?

Security assessments are generally qualitative in nature and subjective based on both who is providing the data and who is conducting the assessment. Such assessments should be adapted to organizational needs and capacity to conduct them while not sacrificing the rigor needed to identify system vulnerabilities. The methods and tools described in this document represent internationally accepted best practices, but they are intended to be flexible enough to meet the needs and capabilities of facilities, implementing partners, governments, and donors needing to understand and manage the risks associated with the use of an EHR. The authors included high-priority and medium-priority security controls from several different sources (International Organization for Standardization, National Institute of Standards and Technology [NIST], Health Insurance Portability and Accountability Act of 1996 [HIPAA]) and then further reduced the number of controls based on consensus about what would not likely be applicable in low-resource settings. Users should be aware that risk assessment tools are limited by the methodologies and the tools used; the subjectivity, quality, and trustworthiness of the data collected; the interpretation of the results; and the knowledge and expertise of those conducting the assessment.

OVERVIEW OF THE ASSESSMENT PROCESS

Figure 1 provides an overview of the steps of the assessment process, including preparing for the assessment, conducting the assessment, communicating the assessment results, and maintaining the assessment. The steps are described in the next section.

Figure 1. Overview of the assessment process



Adapted from: Guide for conducting risk assessments (Joint Task Force Transformation Initiative, 2012).

ASSESSMENT PROCESS

This section describes the steps for conducting the assessment that are illustrated in Figure 1.

Step 1. Prepare for the Assessment

Preparing for a risk assessment includes the following tasks:

1.1 Identify the purpose of the assessment
1.2 Identify the scope of the assessment
1.3 Identify the assumptions and constraints of the assessment
1.4 Identify the sources of information to be used and inputs to the assessment

1.1 Identify the Purpose of the Assessment

When conducting an assessment, it is important to understand the information that the assessment is intended to produce and the decisions the assessment is intended to support. The assessment tools in this document aims to help facilities, organizations, implementing partners, governments, and donors determine whether best practices for information security control have been established, and what risks to which they may be vulnerable require attention. If this is an initial assessment, the tool can be used to help identify baseline risks and to inform a risk mitigation strategy. If this is a reassessment, the results can be used for risk monitoring or to assess the impact of previously implemented risk mitigation strategies.

1.2 Identify the Scope of the Assessment

The scope of the assessment considers the applicability of the assessment components to the situation, the time frame to conduct the assessment, and architectural and technology considerations. The following questions should be considered when determining the scope of the assessment:

1. What is contained in the system architecture diagram of the EHR system instance that is to be assessed?
    a. Include all the constituent parts of the EHR system, including secure file shares, mediators, offline tools, etc., that make up the entire system.
    b. Include all systems connected to this instance (i.e., all systems that interact with the EHR system pulling and pushing data to and from the EHR).
    c. Include a list of interfaces with this instance, such as application programming interface connections, secure FTP file servers, HTTPS connections, etc.
    d. Specify which systems are available through the Internet (thereby accessible by anyone) or over a local area network (LAN)/wide area network (WAN)/virtual private network (VPN) (thereby accessible only to credentialed users in a secured network).
2. What type of information is stored in this instance of the EHR?
    a. List all the data elements, such as first name, last name, date of birth, patient identification number, etc.

3. For each system connected to this EHR instance, provide details of the data elements moving between systems.
    a. List them by system.
    b. Specify which data elements in this instance of the EHR are exchanged with other systems.
4. For each system mentioned, specify where it is hosted (on a local cloud, Amazon Web Services, etc.)
5. For each system mentioned, specify which ministry entity owns it or is its custodian.

1.3 Identify the Assumptions and Constraints of the Assessment

The following assumptions and constraints should be noted as part of the pre-assessment process:

- Threat sources—possible sources of data loss
- Threat events—any previous or near-miss incidents that have occurred
- Vulnerabilities and predisposing conditions of which stakeholders are already aware
- Potential impact of data loss

Planners should also identify constraints in key areas relevant to the assessment, including the following:

- Resources available for the assessment.
- Skills and expertise required to conduct the assessment.
- Operational considerations for clinical activities and how they could be impacted during the assessment process.

By considering these issues, organizations can define both the scope of the assessment and the technical assistance needed to perform the assessment.

1.4 Identify the Sources of Information to be Used and Inputs to the Assessment

Descriptive, threat, vulnerability, and impact information can be gathered from multiple sources, including system documentation of both EHR reference implementation and actual implementation; design of and technologies used in the information system of which the EHR is a part; the environment in which the EHR operates; connectivity to and dependence on other technologies; and dependence on common infrastructures or shared services. Much of this information is collected through the privacy assessment conducted in Step 2.3.

Additional sources of information can include incident reports, security logs, user interviews, system administrator interviews, previous security assessment reports or those of connected systems, vulnerability assessments, policies, and vendor or manufacturer vulnerability reports.

It is also critical to review national and regional policies and ensure that the functionality of the EHR system meets those needs. For example, the African Union Convention on Cyber Security and Personal Data Protection (2014) states that a "natural person needs to give consent for their data to be collected." Therefore, the assessment would need to determine whether there is a mechanism or process in place and is documented for a patient's consent to be obtained.

Step 2. Conduct the Assessment

The assessment should ideally be conducted under the guidance of a Certified Information Systems Security Professional or by personnel with sufficient understanding of information security and technology, using the following five-step process:

2.1 Preliminary requirements gathering
2.2 Privacy assessment
2.3 Criticality and sensitivity assessment
2.4 Security and privacy controls assessment
2.5 System vulnerability scan

2.1 Preliminary Requirements Gathering

Using the information collected in Step 1, determine the scope of the assessment, ensuring that it covers the appropriate data, systems, and functions of the EHR being assessed. This information should be shared with the external assessors, if it has been determined that outside assistance is needed after the completion of the preparation step. Organizations and assessors should explicitly agree on the boundaries of the assessment (i.e., what will be included and what will not be included), identify the interfaces that exist in the systems being assessed, and identify what data sharing agreements exist.

2.2 Privacy Assessment

The privacy assessment evaluates whether the system collects personal information or personally identifiable information (PII) and determines whether the privacy of that PII is adequately protected. This PII inventory enables organizations to implement effective administrative, technical, and physical security policies and procedures to protect PII and mitigate the risks of PII exposure. The privacy assessment survey is given in Appendix A1. This survey tool is used to interview personnel familiar with the system, such as system administrators.

2.3 Criticality and Sensitivity Assessment

The goal of performing a criticality and sensitivity assessment is to assist the organization to identify and quantify the risks to the information and system assets, and the level of impact to the system. This information can be used to determine how best to mitigate the risks and effectively preserve the organization's mission. The preservation of confidentiality, integrity, and availability of data and the system are vital to data and system security (International Organization for Standardization, 2016).

The three criteria for this assessment are:

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

The criticality and sensitivity determination is made for each criterion using a scale of low, medium, or high. NIST (2004) describes these determinations in the Federal Information Processing Standards Publication 199. They are provided in Table 1.

Table 1. Criticality and sensitivity determination and definitions

Determination	Definition
Low	The potential impact is low if the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals **Amplification:** A limited adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.
Medium	The potential impact is moderate if the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. **Amplification:** A serious adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life-threatening injuries.
High	The potential impact is high if the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals. **Amplification:** A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life-threatening injuries.

Source: International Organization for Standardization, 2016

The criticality and sensitivity assessment should be done for each instance of an EHR because EHR implementations can contain different information and be used in different ways, which will affect the criticality and sensitivity determinations. Use the guidance provided in Appendix B to determine the criticality and sensitivity for confidentiality, integrity, and availability, and for the overall determination.

2.4 Security and Privacy Controls Assessment

The purpose of the security and privacy controls assessment is to determine the presence and implementation of management, operational, and technical controls. The security controls used in this assessment tool are derived from NIST Special Publication 800-53.. The security controls are organized into families and classes. The classes are: technical, those which use technology; management, those which use administrative or management methods; and operational, which are implemented by people in day-to-day operations. There are 17 security control families (Table 2).

Table 2. List of security control families, thematic area, and classes

Family/type	Family thematic area	Class
Access control	The requirements for using—and prohibitions against the use of—various system resources vary considerably from one system to another	Technical
Awareness and training	Making system users aware of their security responsibilities and teaching correct practices	Operational
Audit and accountability	Adequacy of system controls and ensuring compliance with established policies and operational procedures	Technical
Certification, accreditation, and security assessments	Testing or evaluation of the management, operational, and technical security controls on a system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome, with respect to meeting the security requirements for the system	Management
Configuration management	Activities focused on establishing and maintaining the integrity of information technology (IT) products and systems through the control of processes for initializing, changing, and monitoring the configurations of those products and systems throughout the software development life cycle	Operational
Contingency planning	Planning for events with the potential to disrupt system operations	Operational
Identification and authentication	Controls related to verifying the identity of a user, process, or device, typically as a prerequisite for granting access to resources in a system	Technical
Incident response	Standard operating procedures to mitigate threat events	Operational
Maintenance	Procedures for the maintenance of organizational systems	Operational
Media protection	Defense of digital and non-digital media	Operational
Physical and environmental protection	Measures taken to protect systems, buildings, and related supporting infrastructure against threats associated with their physical environment	Operational
Planning	System security plans developed to provide an overview of the security requirements of the system, and how the security controls and control enhancements meet those security requirement	Management
Personnel security	Personnel security seeks to minimize the risk that staff (permanent, temporary, or contractor) pose to organizational assets through the malicious use or exploitation of their legitimate access to the organization's resources	Operational
Risk assessment	Planning and procedures to regularly assess and mitigate risk	Management
System and services acquisition	Planning and management of security through the software development life cycle	Management
System and communications protection	Physical and logical system and communications protection controls	Technical
System and information integrity	Guarding against improper information modification or destruction; includes ensuring information non-repudiation and authenticity	Operational

Source: NIST. (n.d.). NIST Special Publication 800-53
date

Each family/type contains controls for the security functionality of that family. The security controls assessment tool found in Appendix C, Table C2 has columns for the security control type, control title, the security control assessment criteria, and assessment guidance. For detailed definitions of each security control, see the NIST 800-53 documentation. To make the assessment more manageable, the controls were narrowed down to those that were ranked as Priority 1 and Priority 2 impact by NIST. They are prioritized based on the expected impact to threat mitigation.

Security Requirements Levels for Implementation Scenarios

During the pilot test of this assessment tool, the authors determined that there should be a method for distinguishing which controls were needed based on the risks posed by the type of EHR implementation commonly encountered in low-resource settings. Implementation scenarios take into account the primary use of the EHR (retrospective data entry versus point-of-care service delivery) and how often the system is connected the Internet (which can increase the risk of external threats). Based on the implementation scenarios, the tool developers grouped the security controls into three security requirements levels (Table 3). The security requirements levels can be used to filter the questions included in the assessment, prioritize findings after the assessment, or plan for additional security measures as the implementation scenario changes. The security requirements build on each other, meaning that all "minimum" requirements security controls should be considered for "intermediate" implementation scenarios, and all "minimum" and "intermediate" security controls should be considered for "advanced" implementation scenarios. The security requirements level is listed for each control in Appendix C, Table C2. These are only suggestions; assessors and system administrators should ultimately apply the security controls that they believe are most relevant to their context.

Table 3. Security requirements levels, by implementation scenario

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

To determine the score for each control, the following steps are taken:

1. For each control, the assessor asks the relevant organizational representative the questions in the security control assessment criteria column of the security controls table in Appendix C, Table C2. The relevant representative could be the systems administrator or someone in a similar role. Asking questions about whether the processes or policies are in place is the first step. Appendix C, Table C2 contains questions to guide the assessors on determining the status of each security control in the organization implementing an EHR.
2. If the organizational representative says that the policy or process is in place, the assessor asks to see the relevant documentation or the function in the EHR system itself.
3. The assessor then determines whether the control is being implemented and whether it is functioning as intended.
4. Based on the information gathered in these steps, the assessor assigns a score to each control. Table 4 describes the scores in more detail.

Table 4. Security controls assessment scores

Score	Score definition	Score explanation
1	Not implemented	The organization does not have any documentation for this control, and it is not being implemented.
2	Partially implemented, not documented	The organization meets some of the criteria for the control. The policies and processes are not documented, but rather are informally passed on.
3	Partially implemented, documented	The organization meets some of the criteria for the control. The policies and processes for the control are documented.
4	Fully implemented, documented, and disseminated	The organization meets the criteria for the control, the criteria are fully implemented and functional, and there is corresponding documentation.

In addition to the score, the notes on findings section allows the assessor to contextualize the findings by adding notes from interviews and observations.

2.5 System Vulnerability Scan

Vulnerability testing is a type of technical testing used to identify, validate, and assess technical vulnerabilities and assist organizations to understand and improve the security position of their systems and networks (Scarfone & Souppaya, 2008). It is not meant to take the place of implementing security controls and maintaining system security, but to help organizations confirm that their systems are properly secured, identify any organizational security requirements that are not met, and other security weaknesses that should be addressed. Vulnerability scans are ranked based on their threat level severity and potential impact to the system if exploited.

Although the results of a vulnerability scan of OpenMRS have been provided (https://www.measureevaluation.org/resources/files/openmrs_report3.html.zip/at_download/file), a scan should still be conducted because variations in implementation and interfaces present additional sources of vulnerability. The following list includes open-source tools that can be used to perform a vulnerability scan:

- **Open Web Application Security Project (OWASP)**
  https://owasp.org/www-community/Vulnerability_Scanning_Tools
  OWASP is a nonprofit foundation that works to improve the security of software. Through community-led open-source software projects, hundreds of local chapters worldwide, tens of thousands of members, and leading educational and training conferences, the OWASP Foundation is the source for developers and technologists to secure the web.
- **Federal Risk and Authorization Management Program (FedRAMP)**
  https://marketplace.fedramp.gov/#/products?sort=productName&productNameSearch=security
  FedRAMP is a United States government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.
- **Magic Quadrant for Application Security Testing**
  https://www.gartner.com/doc/reprints?id=1-6JR0995&ct=190419&st=sb
  Gartner Special Reports provide actionable insights on major trends. In a complex, uncertain and volatile world, the pace of digital change is faster than ever. Looking ahead is critical to success. These reports provide insights on major business and technology trends.

Step 3. Communicate Results

Communication throughout the assessment process and after the assessment is completed is critical. Communication during the assessment process helps ensure that the data collected during the assessment are as accurate as possible. Communication about information system security risks after the assessment helps organizations understand the results of the assessment and develop action plans to mitigate risk. It is recommended that the findings of the assessment are communicated to key stakeholders at both facilities and their supervising organizations throughout the course of the assessment so that the final results do not come as a surprise to stakeholders.

3.1 Communication Tools and Methods

After the assessment is completed, the assessors compile the data and choose appropriate methods and tools for communicating the results. Appendix D provides examples of risk communication visualization tools for documenting the results of the different parts of the assessment.

The **privacy assessment** results are used to classify the characteristics of the information maintained in the EHR and provide data to inform the criticality and sensitivity assessment. The results of the privacy assessment can be summarized in the assessment report as the context and characteristics of the EHR, and can also be used as further context support when prioritizing risks to mitigate.

The results of the **criticality and sensitivity assessment** help the organization classify the impact on the confidentiality, integrity, and availability of the EHR if it is compromised. For example, if the confidentiality determination is high, then "the loss of confidentiality could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals" (NIST, 2004).

To share the results of the **security controls assessment,** the assessors summarize the findings and gaps by control families (Appendix D, Table D2 provides a sample form). The assessors can also group the results by the four different score types given in Table 4 above. This will help stakeholders visualize where things are in terms of both EHR implementation and documentation, and where items have not been implemented or documented to a satisfactory level. To communicate the results of the **vulnerability scan,** the assessors classify the vulnerabilities found in the scan as high, medium, low, and informational. The vulnerabilities can then be quantified and summarized, as shown in Appendix D, Table D3.

3.2 Mitigating Identified Risks

After presenting the findings and risks to the organization, it is up to the organization to determine the risk posed by the controls that are not fully satisfied and prioritize which ones to address. If the assessment team is from an external entity, the assessors can guide the organization on which controls are most important to prioritize based on different criteria, such as feasibility, importance, and the ability to build on existing structures and resources. If the assessment has been conducted by the organization itself, these same criteria can be used to prioritize which risks and gaps to tackle first. As described in the *Security Requirements Levels for Implementation Scenarios* section above, the implementation of the EHR can also help the organization prioritize which security controls to focus on based on how the EHR is networked and how it is being used at the facility level. Moreover, as part of prioritizing the risks identified by the assessment, assessors and organizations can refer to the Standard Operating Procedures for a Secure Electronic Health Record (MEASURE Evaluation, 2020), which lists key activities that can be undertaken to implement an EHR securely in low-resource settings.

After the risks have been prioritized, an action plan is developed to address them. The action plan identifies key activities, responsible parties, and deadlines to monitor progress toward risk mitigation.

Step 4. Maintain the Assessment

The fourth step in the risk assessment process is to maintain the assessment. The objective of this step is to keep specific knowledge of the risks to the EHR and related systems up to date. The results of the assessment inform management decisions and guide risk responses. To support the ongoing review of risk management

decisions (e.g., acquisition decisions, authorization decisions for information systems and common controls, connection decisions), organizations maintain the EHR assessment(s) to incorporate any changes detected through ongoing monitoring. This helps determine the effectiveness of risk responses, identify risk-impacting changes to the EHR and the environments in which it operates, and verify compliance.

Policies Informing Security and Privacy

Table 5 contains a list of international and regional policies relevant to privacy and security that provide additional considerations for the assessment. National policies for the country in which the assessment is conducted should also be reviewed. They may include policies on cybersecurity and those specific to eHealth and patient privacy.

Table 5. International and regional policies

Document name and year	Relevant policies	Notes
African Union Convention on Cyber Security and Personal Data Protection (2014)	• Each state party should have an agency responsible for protecting personal data. This agency is referred to as the "national protection authority." • Processing of personal data about genetics and health can only be done after authorization from the national protection authority. • Data processing requests should include the following: (a) The identity and address of the data controller or, where he or she is not established in the territory of a State Party of the African Union, the identity and address of his or her duly mandated representative. (b) The purpose of the processing and a general description of its functions. (c) The interconnections envisaged or all other forms of harmonization with other processing activities. (d) The personal data processed, their origin, and the category of persons involved in the processing. (e) Period of conservation of the processed data. (f) The service or services responsible for carrying out the processing and the category of persons who, due to their functions or service requirements, have direct access to registered data. (g) The recipients authorized to receive data communication. (h) The function of the person or the service before which the right of access is to be exercised. (i) Measures taken to ensure the security of processing actions and of data. (j) Indication about the use of a subcontractor.	The Security Controls Assessment covers most of the relevant policies in the Convention. The following are some additional issues to consider for the Convention: • What ministry, department, or agency acts as the national protection agency in the country? • Does the EMR have authority to be in use from the national protection agency? • There should be an authority that reviews the requests for data from the EMR. • Are there procedures in place to ensure that the minimum necessary amount of data needed are being collected?

Document name and year	Relevant policies	Notes
	(k) Envisaged transfer of personal data to a third country that is not a member of the African Union, subject to reciprocity. • Natural persons need to give consent for their data to be collected. • Data subjects have the right to information about their data, such as knowing the purpose of their data, being able to request edits and erasures, knowing when the data are going to be transferred to other countries, being aware of recipients who might receive the data, and being informed about the data storage period. • The Convention specifies the minimum required amount of data that need to be collected. • Sensitive data (including health data) can only be processed under the following circumstances: o "The data subject has given his/her written consent, by any means, to the processing and in conformity with extant texts. o Processing is necessary in the public interest, especially for historical, statistical, or scientific purposes." • Data should be protected from alterations and erasures. • Data should not be kept longer than necessary.	
HIPAA Security Information Series (no date)	The Centers for Medicare and Medicaid Services published a Security Series to implement the HIPAA provisions. The focus of this series is how to secure electronically protected health information. The series covers the following topics relevant to this assessment tool: • **Administrative safeguards:** Includes the administrative activities needed to implement the security standards. • **Physical safeguards:** Includes protecting the electronic systems from physical hazards, such as environmental dangers and unauthorized access. • **Technical safeguards:** Includes automated processes that can protect the data and access to the data. • **Risk analysis and risk management**: Includes the specification to conduct an assessment of the risks and vulnerabilities to the confidentiality, integrity, and availability of the electronically protected health information. This part also includes the specification to implement security measures to reduce risks and vulnerabilities.	The assessment tool covers the administrative, physical, and technical safeguards. However, if an organization wants to conduct an assessment using only the Security Series standards, the United States Department of Health and Human Services website has comprehensive tables describing these standards: https://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html. The assessment tool addresses the specification to conduct a risk assessment and produces recommendations for reducing identified risks and vulnerabilities.

Document name and year	Relevant policies	Notes

General Data Protection Regulation (GDPR)	• Data covered: All PII.
	• Data subject rights (similar to both HIPAA and African Union Convention on Cyber Security and Personal Data Protection):
	  ○ Access their own data.
	  ○ Edit their own data or add supplementary statements.
	  ○ Know how their data are being used.
	• Data breach reporting: Organization must notify the overseeing authority if the breach is likely to result in "rights and freedoms of natural persons" (Microsoft & Polsinelli, 2018). Breaches should be reported within 72 hours.
	• Data processing:
	  ○ Controllers must maintain a log of how data are processed.
	  ○ For "high risk" processing activities, organizations should conduct a data protection impact assessment.
	• Security requirements: Requires an assessment of risks to the data being collected, stored, and processed by the organization. The security specifications are broad.
		Many of the stipulations in the General Data Protection Regulation (GDPR) are covered in the assessment tool. In addition to what is found in the controls, the assessment should consider whether the organization keeps a log of how and when data are processed (e.g., reports generation log).

REFERENCES

International Organization for Standardization. (2016). Information technology—Security techniques—Information security management systems—Overview and vocabulary (ISO/IEC 27000:2016[E] Fifthedition). Retrieved from http://www.iso27001security.com/html/27000.html.

Joint Task Force Transformation Initiative. (2012). *Guide for conducting risk assessments.* NIST Special Publication 800-30, Revision 1. Gaithersburg, MD: National Institute of Standards and Technology. Retrieved from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

Microsoft & Polsinelli. (2018). GDPR implementation and HIPAA compliance: An analysis of the GDPR and HIPAA for U.S. health and life sciences organizations. Retrieved from http://download.microsoft.com/download/B/B/F/BBFc0412-E610-49D9-AF83-D76DE35259F7/GDPR_Implementation_and_HIPAA_Compliance_EN_US.pdf.

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

Scarfone, K., Souppaya, M., Cody, A., & Orebaugh, A. (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: National Institute of Standards and Technology. Retrieved from https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=152164.

U.S. Department of Health and Human Services. (n.d.). *Security Rule Guidance Material* (The HIPAA security information series). Retrieved from https://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html.

OTHER RESOURCES

Abdel-Aziz, A. (2011). *Scoping security assessments: A project management approach.* Bethesda, MD: SANS Institute. Retrieved from https://www.sans.org/reading-room/whitepapers/awareness/scoping-security-assessments-project-management-approach-33673.

African Union. (2009). *African charter on statistics.* Addis Ababa, Ethiopia: African Union. Retrieved from https://au.int/sites/default/files/treaties/36412-treaty-0037_-_african_charter_on_statistics_e.pdf.

African Union. (2014). *African Union convention on cyber security and personal data protection.* Addis Ababa, Ethiopia: African Union. Retrieved from https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection.

American Petroleum Institute. (2013). API STANDARD 780, Security Risk Assessment Methodology for the Petroleum and Petrochemical Industries, First Edition, May 2013. Retrieved from https://standards.globalspec.com/std/1603209/ansi-api-std-780

International Organization for Standardization. (2020). ISO27K toolkit. Retrieved from https://www.iso27001security.com/html/toolkit.html.

Joint Task Force Transformation Initiative. (2012). *Guide for conducting risk assessments.* NIST Special Publication 800-30, Revision 1. Gaithersburg, MD: National Institute of Standards and Technology. Retrieved from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf.

Joint Task Force Transformation Initiative. (2014). *Assessing security and privacy controls in federal information systems and organizations building effective assessment plans.* NIST Special Publication 800-53A, Revision 4. Gaithersburg, MD: National Institute of Standards and Technology. Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf.

McAllister, E., Grance, T., & Scarfone, K. (2010*). Guide to protecting the confidentiality of personally identifiable information (PII).* NIST 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). *Standard operating procedures for a secure electronic health record.* Chapel Hill, NC: MEASURE Evaluation, University of North Carolina. Retrieved from https://www.measureevaluation.org/resources/publications/ms-20-194

National Institute of Standards and Technology (NIST). (2006). *Minimum security requirements for federal information and information systems.* FIPS PUB 200. Gaithersburg, MD: NIST. Retrieved from https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.200.pdf.

National Institute of Standards and Technology (NIST). (n.d.) Special Publication 800-53. Retrieved from https://nvd.nist.gov/800-53.

Ngaruro, A. (2017). *MomConnect security findings and recommendations* (tr-17-231). Chapel Hill, NC: MEASURE Evaluation, University of North Carolina. Retrieved from https://www.measureevaluation.org/resources/publications/tr-17-231.

Ross, R., Pillitteri, V., Dempsey, K., Riddle, M., & Guissanie, G. (2020). *Protecting controlled unclassified information in nonfederal systems and organizations.* NIST Special Publication 800-171, Revision 2. Gaithersburg, MD: National Institute of Standards and Technology. Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf.

Scholl, M., Stine, K., Hash, J., Bowen, P., Johnson, A., Dancy Smith, C., & Steinberg, D. I. (2008). *An introductory resource guide for implementing the Health Insurance Portability and Accountability Act (HIPAA) security rule.* NIST Special Publication 800-66, Revision 1. Gaithersburg, MD: National Institute of Standards and Technology. Retrieved from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-66r1.pdf.

Stine, K., Kissel, R., Barker, W. C., Fahlsing, J., & Gulick, J. (2008). *Volume I: Guide for mapping types of information and information systems to security categories.* NIST Special Publication 800-60, Volume I Revision 1. Gaithersburg, MD: National Institute of Standards and Technology. Retrieved from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-60v1r1.pdf.

U.S. Department of Health and Human Services. (2020). Privacy impact assessments. Retrieved from https://www.hhs.gov/pia/index.html.

U.S. Department of Health and Human Services. (2017). *Privacy impact assessment.* Washington, DC: U.S. Department of Health and Human Services. Retrieved from https://www.hhs.gov/sites/default/files/os-hiv.gov_.pdf.

APPENDIX A. EHR SECURITY ASSESSMENT TOOL

Appendix A1. Privacy Assessment Survey

Purpose: To evaluate whether a system collects personally identifiable information (PII) and determine whether the privacy of that PII is adequately protected. This PII inventory enables organizations to implement effective administrative, technical, and physical security policies and procedures to protect PII and mitigate the risks of PII exposure.

Please read and answer the questions below.

1. Date assessment conducted:
2. System name:
3. Is this a new or existing system?
4. Has the system undergone an internal or external security certification and accreditation process?
5. Describe the purpose of the system/how it is used (e.g., retrospective data entry, point-of-care).
6. Describe the type of information the system will collect, maintain (store), share, or process (e.g., antiretroviral therapy clinic data only, complete medical record, labs and findings).
7. Indicate the type of PII that the system will collect, maintain, or process, and the primary purpose.
8. Indicate the categories of individuals about whom PII is collected, maintained, shared, or processed (e.g., antiretroviral therapy patients only, all adult patients, adults and children).
9. How many individuals' PII is in the system?
10. Cite the legal authority to use the PII (if applicable to the country).
11. Are records in the system retrieved by one or more PII data elements?
12. Identify the sources of PII in the system (e.g., directly from an individual about whom the information pertains, government sources, such as a master patient index).
13. Is the PII shared with other organizations?
14. Identify with whom the PII is shared or disclosed and for what purpose.
15. Describe any agreements in place that authorize the information sharing or disclosure.
16. Describe the procedures for accounting for disclosures or security compromise.
17. Describe the process to notify and obtain consent from individuals whose PII is in the system when major changes occur to the system.

18. Is the PII collected verified for accuracy?

19. Describe the process in place to resolve concerns when individuals believe that their PII has been inappropriately obtained, used, or disclosed, or that it is inaccurate.

20. Describe the process in place for periodic reviews of PII contained in the system to ensure the integrity, availability, accuracy, and relevancy of the data.

21. Identify who will have access to the PII in the system and the reason why they require access (e.g., users, administrators, contractors, others).

22. Describe the procedures in place to determine which system users (e.g., administrators, developers, contractors) can access the PII.

23. Are criteria, procedures, controls, and responsibilities regarding access to PII documented?

24. Does access to PII require manager/administrator approval?

25. Describe the retention process and guidelines in place regarding PII (in general for patient records and also for system-generated reports that contain PII).

26. Describe the procedures for disposition of PII at the end of the retention period. Include how long any reports that contain this information will be maintained, and how the information will be disposed of (e.g., shredding, degaussing, overwriting).

27. Who is responsible for ensuring safeguards for the PII?

28. What involvement will outsiders or third-party contractors have with the design and maintenance of the system?

29. Has a third-party or outside contractor confidentiality agreement or a non-disclosure agreement been developed for contractors who work on the system? How are these maintained?

30. Is access to the PII being monitored, tracked, or recorded?

31. Does the website use system/web measurement and customization technology?

32. Describe the type of system/website measurement and customization technologies in use and whether they are used to collect PII (e.g., session cookies, persistent cookies, third-party tools).

Appendix A2. Privacy Assessment Guidance for Assessors

This table will assist assessors to understand the intent of the questions in the privacy assessment survey.

Question	Guiding information
1. Date assessment conducted:	These questions allow an understanding of the scope of the assessment in terms of: • The validity of the assessment responses for a given time period. • The exact system and its boundaries, for which the assessment responses are applicable. • An understanding of whether there is a previous system that this system is replacing or has replaced.
2. System name:	
3. Is this a new or existing system?	
4. Has the system undergone an internal or external security certification and accreditation process?	Describe any processes used to certify that the personally identifiable information (PII) being collected in the system adheres to best practices, guidelines, regulations, laws, etc.
5. Describe the purpose of the system/how it is used (e.g., retrospective data entry, point-of-care).	Provide a general description of the system for the purpose of outlining how it supports the organization's business function, including describing the way the system operates to achieve this, any interconnections with other programs, and information on where the system operates in the organization (e.g., is it a critical point-of-care system or a reporting system or a retrospective data entry type of system?). The description should be as comprehensive as necessary to get a full understanding of the system.
6. Describe the type of information the system will collect, maintain (store), share, or process (e.g., antiretroviral therapy clinic data only, complete medical records, labs and findings).	Describe the types of information in the system and explain why and how they are used by the organization. The description should be as comprehensive as necessary to get a full understanding of the system.
7. Indicate the type of PII that the system will collect, maintain, or process, and the primary purpose.	PII means information that can be used to distinguish or trace an individual's identity, such as name, Social Security number, biometric records, etc., alone, or when combined with other personal or identifying information that is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, home address, etc. This helps get a full picture of the sensitive data contained in the system that could be a security risk. It is important to catalogue because data considered non-PII can become PII if combined with additional sources of data; therefore, these data also need to be protected. Additional considerations should take into account employment, ethnicity, or sexual orientation for vulnerable or at-risk populations.

Question	Guiding information
8. Indicate the categories of individuals about whom PII is collected, maintained, shared, or processed (e.g., antiretroviral therapy patients only, all adult patients, adults and children).	Describe whether the data collected pertain to children, adults, key populations, etc., for the purpose of identifying applicable security controls and additional measures needed to protect these data (e.g., if data about children are collected, then it is important to check that there is appropriate adult consent being provided/captured and that all applicable regulations/laws, etc., pertaining to children's data are followed).
9. How many individuals' PII is in the system?	This helps determine how much sensitive information is contained in the system and the level of risk exposure.
10. Cite the legal authority to use the PII (if applicable to the country).	Provide details on any best practice, guidelines, regulations, or laws applicable to the collection and use of PII of which you are aware. Have any of them been applied to these data? It is important that the assessor be aware of legal authorities and regulations that may apply to PII.
11.Are records on the system retrieved by one or more PII data elements?	Describe how the data are referenced in the system. This will provide details on how non-PII can be combined to identify information; these are also key pieces of sensitive information stored in the system.
12. Identify the sources of PII in the system (e.g., directly from an individual about whom the information pertains, government sources, such as a master patient index).	Describe where the PII came from to determine whether it came from public sources, other systems, or directly from the individual. Also for the purpose of determining whether appropriate approvals/consent was provided.
13. Is the PII shared with other organizations?	Identify the name of each external system, person, or organization with whom PII is shared, what PII is shared, the purpose of the sharing, and how share the PII is shared(such as on a case-by-case basis, via monthly reporting, bulk transfer, or direct access). Describe whether any of these data are shared with external systems or organization for the purpose of determining whether a data-sharing agreement exists or is needed.
14. Identify with whom the PII is shared or disclosed and for what purpose.	For each external system/person/organization listed above, provide a detailed description of the reason for sharing that information, including what that external entity says that they will use it for.
15. Describe any agreements in place that authorize the information sharing or disclosure.	List any memoranda of understanding or data-sharing agreements with external entities and obtain copies of these documents.
16. Describe the procedures for accounting for disclosures/security compromise.	Describe any processes in place to report a security compromise to the management of the organization, any external government

Question	Guiding information
	authorities, and the owners of the PII (i.e., individual people).
17. Describe the process to notify and obtain consent from individuals whose PII is in the system when major changes occur to the system.	If any major changes to the system occur, such as retiring of the system or transfer to a different external entity, such as another service provider/nongovernmental organization or government ministry, how do the owners of the PII get notified of this for the purpose of ensuring disclosure and transparency?
18. Is the PII collected verified for accuracy?	How does the organization/system ensure that the PII being collected is correct and does not contain any mistakes, such as transcription errors in a system used for retrospective data entry? Are there are any internal validations or regular data quality assessment procedures?
19. Describe the process in place to resolve an individual's concerns when he or she believes that his or her PII has been inappropriately obtained, used, or disclosed, or that it is inaccurate.	Describe the process in place for individuals to report inappropriate use of their PII. In the event that an individual or source entity needs to update the information or correct it, describe how this is done.
20. Describe the process in place for periodic reviews of PII contained in the system to ensure the integrity, availability, accuracy, and relevancy of the data.	Describe any organizational processes that are undertaken to check the quality of the PII contained in the system.
21. Identify who will have access to the PII in the system and the reason why they require access (e.g., users, administrators, contractors, others).	List the roles of users who can access and see the PII and the reason for accessing it (e.g., to enter PII, update PII, generate reports, perform system maintenance).
22. Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) can access the PII.	For each role above, describe the method of approval to allow access to the data (e.g., through e-mail approval from organization management, through a request from the ministry of health or a donor). Are there any rules (written and unwritten) applied to accessing the PII in the system?
23. Are criteria, procedures, controls, and responsibilities regarding access to PII documented?	
24. Does access to PII require manager/administrator approval?	Describe any specific approvals specifically applied to PII data in the system.
25. Describe the retention process and guidelines in place for the PII (in general for patient records and also for system-generated reports that contain PII).	Describe how long PII is kept in the system and any guidelines for how this should be done.
26. Describe the procedures for disposition of PII at the end of the retention period. Include how long any reports that contain this information will be maintained, and how the information disposed of (e.g., shredding, degaussing, overwriting).	If the system is to be retired and no longer used, describe what happens to the PII contained (e.g., is the database deleted, are the data saved on an external drive and archived somewhere?). Also describe how long reports generated by the system containing PII are maintained and how they are disposed of.

Question	Guiding information
27. Who is responsible for ensuring safeguards for the PII?	In the system/organization, is there anyone designated as being responsible for the security of the PII?
28. What involvement will outsiders or third-party contractors have with the design and maintenance of the system?	Describe any agreements with external parties that develop and maintain the system about the expectations of access to and use of the PII.
29. Has a third-party or outside contractor confidentiality agreement or a nondisclosure agreement been developed for contractors who work on the system? How are these maintained?	
30. Is access to the PII being monitored, tracked, or recorded?	Describe whether the system maintains a record of actions being performed on the PII (e.g., log file).
31. Does the website use system/web measurement and customization technology?	Describe whether any of these technologies that can collect additional information are being used by the system and why they have been deployed.
32. Describe the type of system/website measurement and customization technologies in use and whether they are used to collect PII (e.g., session cookies, persistent cookies, third-party tools).	

APPENDIX B. CRITICALITY AND SENSITIVITY

Appendix B. Table B1 will help assessors determine the criticality and sensitivity of their EHRs. This guidance is based on Federal Information Processing Standards (FIPS)199 (NIST, 2004) but is tailored for assessing EHRs (and is likely relevant to other health information systems that contain PII). Because EHRs are used in the provision of care, some assumptions are made about the type of data stored in the system. The factors that impact criticality and sensitivity are:

- **Confidentiality:** The amount of PII collected. The EHR should capture the minimum PII needed in the provision of care and for business processes. PII that identifies a unique individual, such as a national identifier, is more sensitive than other types of identifiers. The quantity of PII in the system also *increases* (never decreases) impact, so an EHR that contains thousands of records will be more impacted by a breach than an EHR that contains under 100 records.
    - FIPS199 provides the following examples of harm to individuals:
        - "A breach of the confidentiality of PII at the low impact level would not cause harm greater than inconvenience, such as changing a telephone number. The types of harm that could be caused by a breach involving PII at the moderate impact level include financial loss due to identity theft or denial of benefits, public humiliation, discrimination, and the potential for blackmail. Harm at the high impact level involves serious physical, social, or financial harm, resulting in potential loss of life, loss of livelihood, or inappropriate physical detention."
    - The determination of confidentiality may vary, depending on the legal status and cultural and social norms for vulnerable populations for which the data are collected, such as people living with HIV/AIDS, orphaned children, sex workers, men who have sex with men, etc.
- **Integrity:** If the integrity of the system was compromised, what adverse impact might that have on the provision of care? The more providers rely on the system for clinical decision making, the more critical it is that there is no unauthorized manipulation of the data, because this could negatively impact patient safety due to medical errors.
- **Availability:** Similar to integrity, the criticality and sensitivity designation of availability is dependent on how the system is used by providers. If providers are unable to provide safe, accurate, and timely care without the system, the determination will be high.

Appendix B. Table B1 provides guidance on how to determine criticality and sensitivity for each of these criteria based on the context of the EHR implementation.

Appendix B. Table B1. Determining criticality and sensitivity of an EHR

Assessment criteria	Considerations	Determination guidance
Confidentiality: Refers to the system's ability to provide assurance that the data and information are not made available or disclosed to unauthorized individuals, entities, or processes	• What type of information is stored in the system? • If information in the system was accessed inappropriately, how much harm could be done, either financially or via stigma and discrimination? For example, if insurance information is stored in the system, it is more likely to be used inappropriately than if other demographic information is stored in the system.	• **Low:** If the EHR is used in the provision of care or to retrospectively record care, it will not be considered as low because it will contain PII that can be used to uniquely identify patients. • **Medium**: If the EHR is being used for the analysis of an outbreak, to track a spread of disease, or for an administrative purpose only, then it could be considered as medium. An EHR that contains patient- level data could be considered as medium if a compromise of integrity results in significant harm to individuals that does not involve major, financial loss, loss of life, or serious life-threatening injuries. • **High:** Most EHRs, whether used retrospectively or at the point of care, would receive this determination because they contain identifying information for patients, along with diagnoses and designations of vulnerable populations. The breach of data could cause harm to patients and could lead to substantial reputational and financial loss for patients and the implementing organization. Note: The system may contain diagnoses and information that are highly sensitive. Take into consideration the known stigma in the country where the system is being used and laws that may protect or threaten patients. For example, an HIV diagnosis is generally considered highly sensitive and could cause significant harm to patients if compromised (loss of employment, ostracism from their community). If the loss of data could lead to imprisonment or violence against a patient, then it should also be considered high. Making a determination between medium and high can be subjective. The assessor should use input from multiple stakeholders to make the final determination.

Assessment criteria	Considerations	Determination guidance
Integrity: Includes authentication, nonrepudiation, and accountability, and refers to the system's ability to be accurate and complete and provide protection from unauthorized modification.	• What would be the consequences of unauthorized modifications being made to the system? • How important is it to track who makes changes to the system? For example, if an EHR is being used for ordering procedures and labs, it is likely more important to track who makes changes to those than when the EMR is being used for retrospective data entry. • What would be the impact on patient safety if the integrity of the system was compromised?	• **Low:** Integrity c be considered as low for systems used for retrospective data entry. In this case, errors may be caught through data quality checks and as part of the reporting process. Point-of-care systems that are used in data entry but not for providing feedback to clinicians for clinical decision making may also be designated as low if there is duplicated paper-based documentation. • **Medium:** A point-of-care system that is used for clinical decision making without duplicate paper documentation could be designated as medium, provided that a compromise to system integrity would not result in patient harm and medical errors that are serious or life-threatening. • **High:** In cases where an EHR is used in clinical decision making and compromise would lead to medical errors and would impact patient safety, then integrity should be designated as high. An example would be an EHR that receives lab results electronically that a provider uses to determine treatment recommendations or to make diagnoses that are potentially serious or life-threatening.
Availability: Refers to a system's ability to be accessible and usable on demand by an authorized entity.	• Is the system being used to make clinical care decisions? For example, if an EHR is being used to make clinical care decisions, such as dosing for a medication, it is more likely important to ensure that previous dosing and side effects are available to the clinician at the time of prescribing. Moreover, if the system stores information on severe allergies to medications for patients, the availability of this information is important in a setting in which the system is used for prescribing.	• **Low:** EHRs used for retrospective data entry would be considered as low because they are not used in clinical decision making and paper records are available. For a point-of-care system, the impact may also be considered as low if, in the event of compromised availability, there is a limited adverse effect on the organization's ability to provide services, minor financial loss, and minor harm to patients. • **Moderate:** An EHR's availability designation may be considered as moderate in a point-of-care implementation if there are alternate data sources, such as paper records; the data are not used in critical clinical decision making (e.g., someone will die or be seriously harmed if the clinician does not have the right information at the right time); and the availability of the system does not compromise patient

Assessment criteria	Considerations	Determination guidance
	• Are other sources of the information stored in other places (such as paper records)? • Consider how long the system could be down before clinical workflow would be negatively impacted.	• safety in a manner that is serious or life-threatening. • **High:** An EHR's availability designation would be considered as high if a compromise in availability would have a severe or catastrophic adverse impact, such as the inability to provide care, major financial loss, or life-threatening injury or harm to patients.

Additional Considerations

In many developed countries, EHRs are closely tied to insurance, billing, and financial systems. In such cases, the assessor would need to consider how compromised confidentiality, integrity, or availability could impact financial losses. In a country that has enacted laws in which compromise of confidentiality, integrity, or availability could result in litigation by patients, legal prosecution, or fines, the financial impact should be considered in the assessment.

Determining the Overall Impact

The overall impact designation is based on the highest designation received in the three assessment areas. For example, if confidentiality is medium but integrity and availability are low, the overall designation would still be medium.

APPENDIX C. SECURITY CONTROLS

Security Controls Assessment Instructions

Appendix C. Table C1 contains the security controls to be assessed. The controls are grouped by control type, and each control has assessment criteria and additional assessment guidance to assist users in understanding the scope of the control. Each security control also has suggested questions that assessors can use when interviewing facility staff, system administrators, IT staff, and system developers. These questions are meant to be starting points for understanding whether the organization or system meets a control, do not cover the entire breadth of the control, and should be followed up with further probing questions, as needed.

The security requirements level was assigned in this assessment tool based on the Implementation Scenarios Risk (see the *Security Requirements Levels for Implementation Scenarios* section in the main text above). Assessors can choose to filter out the security controls based on their Implementation Scenario Risk category to reduce the burden of this assessment. (See Appendix C. Table C1 below and the *Security Requirements Levels for Implementation Scenarios* section in the main text above for more details.)

Appendix C. Table C1. Security requirements level by implementation scenario

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

There is some highlighting in the suggested questions to indicate additional instructions for the assessors. Green highlighting indicates that the question is for developers of the EHR. Yellow highlighting indicates additional instructions for the assessors.

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

Control type: Access control				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
Account management	**Minimum**	Does the organization: manage information system accounts, including the following: *identifying account types (i.e., individual, group, system, application, guest/anonymous, and temporary); * establishing conditions for group membership; * identifying authorized users of the information system and specifying access privileges; * requiring appropriate approvals for requests to establish accounts; * establishing, activating, modifying, disabling, and removing accounts; * specifically authorizing and monitoring the use of guest/anonymous and temporary accounts; * notifying account managers when temporary accounts are no longer required and when information system users are terminated, transferred, or information system usage or need-to-know/need-to-share changes; * deactivating: (i)	Information system account types include, for example, individual, shared, group, system, guest/anonymous, emergency, developer/manufacturer/vendor, temporary, and service. Some of the account management requirements listed above can be implemented by organizational information systems. The identification of authorized users of the information system and the specification of access privileges reflects the requirements in other security controls in the security plan. Users requiring administrative privileges on information system accounts receive additional scrutiny by appropriate organizational personnel (e.g., system owner, mission/business owner, or chief information security officer) responsible for approving such accounts and privileged access. Organizations may choose to define access privileges or other attributes by account, by type of account, or a combination of both. Other attributes required for authorizing access include, for example, restrictions on time-of-day, day-of-week, and point-of-origin. In defining other account attributes, organizations should consider system-related requirements (e.g., scheduled maintenance, system upgrades) and	1.1. Once the EHR was been successfully installed, explain how you first logged into the system. 1.2. Did you use a default admin password to first login? Explain the steps you follow to assign access to users in the system. 1.3. Does anyone authorize each user's access before it is activated/granted? 1.4. When individuals who have access to the EHR leave the organization, is their access to the system removed? 1.5. Explain the steps taken to deactivate a user no longer working with the organization. 1.6. How many users have access to the EHR? 1.7. Does each user have a username and password? 1.8. Are these unique? A unique username and password is not known or shared with any other individual. 1.9. How many EHR system administrators are there?

Control type: Access control				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
		temporary accounts that are no longer required; and (ii) accounts of terminated or transferred users; and granting access to the system based on: * a valid access authorization; * intended system usage; and * other attributes as required by the organization or associated mission/business functions. Define the frequency of information system account reviews. Review information system accounts in accordance with organization-defined frequency.	mission/business requirements, (e.g., time zone differences, customer requirements, remote access to support travel requirements). Failure to consider these factors could affect information system availability. Temporary and emergency accounts are accounts intended for short-term use. Organizations establish temporary accounts as a part of normal account activation procedures when there is a need for short-term accounts without the demand for immediacy in account activation. Organizations establish emergency accounts in response to crisis situations and with the need for rapid account activation. Therefore, emergency account activation may bypass normal account authorization processes. Emergency and temporary accounts are not to be confused with infrequently used accounts (e.g., local login accounts used for special tasks defined by organizations or when network resources are unavailable). Such accounts remain available and are not subject to automatic disabling or removal dates. Conditions for disabling or deactivating accounts include, for example: (i) when shared/group, emergency, or temporary accounts are no longer required; or (ii) when individuals are transferred or terminated. Some types	1.10. Has the system admin default password been changed? 1.11 Does each EHR system administrator have a unique username and password? A unique username and password are not known or shared with any other individual. 1.12 How are roles and privileges in the system assigned to users? 1.13 Can you provide an example of a role and the associated privileges that role has in the system?

Control type: Access control				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
			of information system accounts may require specialized training.	
Access control policy and procedures	**Minimum**	Has the organization developed and formally documented an access control policy that addresses: purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, compliance; disseminated a formally documented access control policy to elements in the organization having associated access control roles and responsibilities; defined the frequency of access control policy reviews and updates; reviewed or updated the access control policy in accordance with organization-defined frequency; defined the frequency of access control procedure reviews and updates; and reviewed or updated access control procedures in accordance with organization-defined frequency?	This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the Access Control family. Policy and procedures reflect applicable laws, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organizational level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program, in general, and for specific information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.	2.1. Are any of the account management procedures (i.e., information/steps in 1 above) documented anywhere? If yes, can you please provide us with the document? 2.2. If yes, who created them and have they been reviewed and approved by any staff members? What are the titles of those staff who created or reviewed or approved the documents? 2.3. When was the last time the documents were reviewed or approved? Are they reviewed and approved on a regular basis?

Control type: Access control				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
Access enforcement	**Minimum**	Does the EHR enforce approved authorizations for logical access to the system, in accordance with applicable policy?	Access control policies (e.g., identity-based policies, role-based policies, control matrices, cryptography) control access between active entities or subjects (i.e., users or processes acting on behalf of users) and passive entities or objects (e.g., devices, files, records, domains) in information systems. In addition to enforcing authorized access at the information system level and recognizing that information systems can host many applications and services in support of organizational missions and business operations, access enforcement mechanisms can also be employed at the application and service levels to provide increased information security.	3.1. **Instructions to assessors:** If documentation exists based on the answer to 2.1 above, check what is documented against the information and steps outlined in 1 to make sure they match. Identify any gaps or differences between what was described and what is documented.
Separation of duties	**Minimum**	Does the organization: separate duties of individuals as necessary to prevent malevolent activity without collusion; document separation of duties; and implement separation of duties through assigned information system access authorizations?	Separation of duties addresses the potential for abuse of authorized privileges and helps reduce the risk of malevolent activity without collusion. Separation of duties includes, for example: (i) dividing mission functions and information system support functions among different individuals or roles; (ii) conducting information system support functions with different individuals (e.g., system management, programming, configuration management, quality assurance and testing, and network security); and (iii) ensuring that security personnel administering access control	4.1. If a user is a clinical health worker (or nurse, doctor, or data entry clerk), what modules can they access or see in the system? 4.2. If a user is a clinical health worker (or nurse, doctor, data entry clerk), what modules can they not access or see in the system? 4.3. Do any of the above users access or see the same modules as a user who is the system administrator? Describe which modules are different for each user.

Control type: Access control				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
			functions do not also administer audit functions.	4.4. Are there other user roles defined in the system and what are their associated permissions/privileges? 4.5. Are user roles and their associated permissions/privileges documented? Please provide these documents.
Least privilege	**Minimum**	Does the organization employ the concept of least privilege, allowing only authorized access for users (and processes acting on behalf of users) that are necessary to accomplish assigned tasks in accordance with organizational missions and business functions?	Organizations employ least privilege for specific duties and information systems. The principle of least privilege is also applied to information system processes, ensuring that the processes operate at privilege levels no higher than necessary to accomplish required organizational mission/business functions. Organizations consider the creation of additional processes, roles, and information system accounts, as necessary, to achieve least privilege. Organizations also apply least privilege to the development, implementation, and operation of organizational information systems.	5.1. **Instructions to assessors:** Check to see whether user roles in the system can access only the modules they need (i.e., check to see if each role is able to access modules not relevant to its job duties). Provide details.
Unsuccessful login attempts	**Minimum**	Does the organization define the maximum number of consecutive invalid login attempts to the information system by a user and the time period in which the consecutive invalid attempts occurred? Does the EHR enforce the organization-	This control applies regardless of whether the login occurs via a local or network connection. Due to the potential for denial of service, automatic lockouts initiated by information systems are usually temporary and are automatically released after a predetermined time period established by organizations. If a delay algorithm is selected, organizations	6.1. What happens if when attempting to login to the EHR, a user uses an invalid credential? Please provide details—does the system provide any error messages? Invalid credentials are either a username or password. 6.2. How many times can a user enter invalid credential in the system

Control type: Access control				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
		defined limit of consecutive invalid login attempts by a user during the organization-defined time period? Does the organization define action to be taken by the system when the maximum number of unsuccessful login attempts is exceeded as: lock out the account/node for a specified time period; lock out the account/note until released by an administrator; delay the next login prompt according to organization-defined delay algorithm? Does the EHR automatically lock the account/node for the organization-defined time period, lock the account/node until released by an administrator, or delay the next login prompt for the organization-defined delay period when the maximum number of unsuccessful login attempts is exceeded; perform the organization-defined actions when the maximum number of unsuccessful login attempts is exceeded, regardless of	may choose to employ different algorithms for different information system components based on the capabilities of those components. Responses to unsuccessful login attempts can be implemented at both the operating system and the application levels.	before it locks that user out? Please provide details. System lockout is when a system no longer accepts the username or password combination to be used to try to access the system. 6.3. **Instructions to assessors:** At each facility, please try to enter invalid credentials and provide details on what happens. If possible, provide screenshots/pictures of what happens. 6.4. **Instructions to assessors:** If the system provides a lockout message, try using the invalid credential at least two more times and provide details of what happens. Does the system continue to display a lockout message or does it allow a user to log in to the system?

Control type: Access control				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
		whether the login occurs via a local or network connection?		
System use notification	**Minimum**	Does the organization approve the information system use notification message or banner to be displayed by the information system before granting access to the system? Does the system display the approved system use notification message or banner before granting access to the system that provides privacy and security notices consistent with applicable laws, directives, policies, regulations, standards, and guidance and states that: users are accessing a government information system; system usage may be monitored, recorded, and subject to audit; unauthorized use of the system is prohibited and subject to criminal and civil penalties; and use of the system indicates consent to monitoring and recording; and retain the notification message or banner on the	System use notifications can be implemented using messages or warning banners displayed before individuals log in to information systems. System use notifications are used only for access via login interfaces with human users and are not required when such human interfaces do not exist. Organizations consider system use notification messages/banners displayed in multiple languages based on specific organizational needs and the demographics of information system users.	7.1. Does the system display anywhere in the system (usually on the login page) a message that outlines the terms of use for the system? Provide details. 7.2. **Instructions to assessors:** At each facility, please verify whether this message is present. Provide screenshots/pictures, where possible.

Control type: Access control				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
		screen until the user takes explicit actions to login to or further access the information system?		
Session termination	**Minimum**	Does the EHR automatically terminate a user's session after organization-defined conditions or trigger events require session disconnect?	This control addresses the termination of user-initiated logical sessions. A logical session (for local, network, and remote access) is initiated when a user (or process acting on behalf of a user) accesses an organizational information system. Such user sessions can be terminated (and thereby terminate user access) without terminating network sessions. Session termination terminates all processes associated with a user's logical session, except those processes that are specifically created by the user (i.e., session owner) to continue after the session is terminated. Conditions or trigger events requiring automatic session termination can include, for example, organization-defined periods of user inactivity, targeted responses to certain types of incidents, and time-of-day restrictions on information system use.	8.1. If a user is logged in to the system and is performing other duties not on the application, does the system time out after a period of time because of not being used? Please provide details. What is the duration of time before the system times out or logs out the user? 8.2. Are there other conditions under which a user can be automatically logged out or timed out of the system? Provide details. 8.3. **Instructions to assessors:** At each facility, verify whether and how long it takes for the application to log a user out or time out due to lack of activity in the application. Provide details of findings.
Remote access	**Minimum**	Does the organization document the allowed methods of remote access to the information system; have established usage restrictions and implementation	Remote access is access to organizational information systems by users (or processes acting on behalf of users) communicating through external networks (e.g., the Internet). Remote access methods include, for example, dial-up, broadband,	9.1. Can you access the system from a different location via the Internet, LAN, WAN, or other method that allows access remotely? If yes, please provide details.

Control type: Access control				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
		guidance for each allowed remote access method; monitor for unauthorized remote access to the information system; authorize remote access to the information system before connection; and enforce requirements for remote connections to the information system?	and wireless. Organizations often employ encrypted VPNs to enhance confidentiality and integrity over remote connections. The use of encrypted VPNs does not make the access non-remote; however, the use of VPNs, when adequately provisioned with appropriate security controls (e.g., employing appropriate encryption techniques for confidentiality and integrity protection), may provide sufficient assurance to the organization that it can effectively treat such connections as internal networks. Still, VPN connections traverse external networks, and the encrypted VPN does not enhance the availability of remote connections. Also, VPNs with encrypted tunnels can affect the organizational capability to adequately monitor network communications traffic for malicious code. Remote access controls apply to information systems other than public web servers or systems designed for public access. This control addresses authorization before allowing remote access without specifying the formats for such authorization. Although organizations may use interconnection security agreements to authorize remote access connections, such agreements are not required by this control. Enforcing access	9.2. If yes, is this process documented? If yes, please provide the documents.

Control type: Access control				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
			restrictions for remote connections is addressed in Access Control.	
Wireless access	**Minimum**	Does the organization have established usage restrictions and implementation guidance for wireless access; monitor for unauthorized wireless access to the information system; authorize wireless access to the information system before connection; and enforce requirements for wireless connections to the information system?	Wireless technologies include, for example, microwave, packet radio (UHF/VHF), 802.11x, and Bluetooth. Wireless networks use authentication protocols (e.g., Extensible Authentication Protocol/ Transport Layer Security [EAP/TLS, PEAP), which provide credential protection and mutual authentication.	10.1. Can the system be accessed via wireless connection (e.g., via Bluetooth)? If yes, provide details. 10.2. If yes to 10.1, please also provide details on how these connections are secured; for example, does the connection use wireless networks authentication protocols (e.g., EAP/TLS, PEAP), which provide credential protection and mutual authentication. Credential protection refers to the use of technologies, such as single sign-on, two-factor authentication (i.e., methods to secure usernames and passwords). Mutual authentication, also called two-way authentication, refers to two parties authenticating each other at the same time, which is built into protocols, such SSH and TLS. 10.3. Does any documentation exist that details the above? Please provide. 10.4. **Instructions to assessors:** Verify whether any wireless connection uses SSH, TLS, and credential protection.

Control type: Access control				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
Access control for mobile devices	**Minimum**	Does the organization have established usage restrictions and implementation guidance for: organization-controlled portable and mobile devices; authorize connection of mobile devices meeting organizational usage restrictions and implementation guidance to organizational information systems; enforce requirements for the connection of mobile devices to organizational information systems; disable information system functionality that provides the capability for automatic execution of code on mobile devices without user direction; issue specially configured mobile devices to individuals traveling to locations that the organization deems to be of significant risk in accordance with organizational policies and procedures; have defined inspection and preventative measures to be applied to mobile devices returning from locations that the organization deems to be	A mobile device is a computing device that: (i) has a small form factor such that it can easily be carried by a single individual; (ii) is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); (iii) possesses local, non-removable or removable data storage; and (iv) includes a self-contained power source. Mobile devices can also include voice communication capabilities, on-board sensors that allow the device to capture information, or built-in features for synchronizing local data with remote locations. Examples include smart phones, E-readers, and tablets. Mobile devices are typically associated with a single individual, and the device is usually in close proximity to the individual; however, the degree of proximity can vary, depending on the form factor and size of the device. The processing, storage, and transmission capability of the mobile device can be comparable to or merely a subset of desktop systems, depending on the nature and intended purpose of the device. Due to the large variety of mobile devices with different technical characteristics and capabilities, organizational restrictions may vary for the different classes/types of such devices. Usage restrictions and specific	11.1. Can this instance of the EHR be accessed via a mobile device? If yes, please provide details. 11.2. Has the organization issued any of the system users with mobile devices for the purpose of accessing the application? 11.3. Is there documentation describing how mobile devices can access the application, including policies and restrictions? If yes, please provide this documentation.

Control type: Access control				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
		of significant risk; and apply organization-defined inspection and preventative measures to mobile devices returning from locations that the organization deems to be of significant risk in accordance with organizational policies and procedures?	implementation guidance for mobile devices include, for example, configuration management, device identification and authentication, implementation of mandatory protective software (e.g., malicious code detection, firewall), scanning devices for malicious code, updating virus protection software, scanning for critical software updates and patches, conducting primary operating system (and possibly other resident software) integrity checks, and disabling unnecessary hardware (e.g., wireless, infrared). Organizations are cautioned that the need to provide adequate security for mobile devices goes beyond the requirements in this control. Many safeguards and countermeasures for mobile devices are reflected in other security controls in the catalog allocated in the initial control baselines as starting points for the development of security plans and overlays using the tailoring process. There may also be some degree of overlap in the requirements articulated by the security controls in the different families of controls. Access Control addresses mobile devices that are not organization-controlled.	
Use of external information systems and	**Minimum (access to the system)**	Does the organization identify individuals authorized to access the information system	External information systems are information systems or components of information systems that are outside the	12.1. Does this application share data with external systems, such as a health management information

Control type: Access control				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
information flow enforcement	**Intermediate (sharing data with external systems)**	from the external information systems; process, store, or transmit organization-controlled information using the external information systems? Does the organization establish terms and conditions, consistent with any trust relationships established with other organizations owning, operating, or maintaining external information systems, allowing authorized individuals to access the information system from the external information systems; and process, store, or transmit organization-controlled information using the external information system; define an applicable policy for controlling the flow of information in the system and between interconnected systems; define approved authorizations for controlling the flow of information in the system and between interconnected systems in accordance with applicable policy; enforce approved	authorization boundary established by organizations and for which organizations typically have no direct supervision and authority over the application of required security controls or the assessment of control effectiveness. External information systems include, for example: (i) personally owned information systems/devices (e.g., notebook computers, smart phones, tablets, personal digital assistants); (ii) privately owned computing and communications devices resident in commercial or public facilities (e.g., hotels, train stations, convention centers, shopping malls, or airports); (iii) information systems owned or controlled by nongovernment organizations; and (iv) information systems that are not owned by, operated by, or under the direct supervision and authority of organizations. This control also addresses the use of external information systems for the processing, storage, or transmission of organizational information, including, for example, accessing cloud services (e.g., infrastructure as a service, platform as a service, or software as a service) from organizational information systems. For some external information systems (i.e., information systems operated by other national agencies, including organizations subordinate to those agencies), the trust	system, human resource information system, laboratory information system, other EHRs, etc.? Provide names of each system and details of who owns/manages each of the external systems. Please provide details. 12.2 Are there sharing policies or processes that define how an external system can access this application? 12.3 If yes to the above, explain the process of information sharing in a step-by-step way. How do data get moved from the EHR to the other system? Is it manually/via APIS, via emailed files, via a data exchange stack? Please provide details for each connection between the EHR and the other system. 12.4. Are any of the above information flows documented anywhere? 12.5. Are individuals external to the organization allowed to access the system; for example, for data review purposes or to get data for reporting to donors/external partners? Please provide details. 12.6. Are there sharing policies or processes that define how an

Control type: Access control				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
		authorizations for controlling the flow of information in the system and between interconnected systems in accordance with applicable policy?	relationships that have been established between those organizations and the originating organization may be such that no explicit terms and conditions are required. Information systems in these organizations would not be considered external. These situations occur when, for example, there are preexisting sharing/trust agreements (either implicit or explicit) established between national agencies or organizations subordinate to those agencies, or when such trust agreements are specified by applicable laws, directives, or policies. Authorized individuals include, for example, organizational personnel, contractors, or other individuals with authorized access to organizational information systems and over which organizations have the authority to impose rules of behavior with regard to system access. Restrictions that organizations impose on authorized individuals need not be uniform, as those restrictions may vary, depending on the trust relationships between organizations. Therefore, organizations can choose to impose different security restrictions on contractors. This control does not apply to the use of external information systems to access public interfaces to organizational information systems. Organizations establish terms and conditions for the use	individual external to the organization can access this application or how the organization shares data with other systems? 12.7. Is information shared internally from the system? If so, what types of information are shared? Does the information contain PII? 12.8. How is the information transmitted and stored when shared from the system? 12.9. How is the information from the system disposed of after it is shared?

Control type: Access control				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
			of external information systems in accordance with organizational security policies and procedures. Terms and conditions address at a minimum: the types of applications that can be accessed on organizational information systems from external information systems; and the highest security category of information that can be processed, stored, or transmitted on external information systems. If terms and conditions with the owners of external information systems cannot be established, organizations may impose restrictions on organizational personnel using those external systems. Information flow control regulates where information is allowed to travel in an information system and between information systems (as opposed to who is allowed to access the information) and without explicit regard to subsequent accesses to that information. Flow control restrictions include, for example, keeping export-controlled information from being transmitted in the clear to the Internet, blocking outside traffic that claims to be from within the organization, restricting web requests to the Internet that are not from the internal web proxy server, and limiting information transfers between organizations based on data structures	

Control type: Access control				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
			and content. Transferring information between information systems representing different security domains with different security policies introduces risk that such transfers violate one or more domain security policies. In such situations, information owners/stewards provide guidance at designated policy enforcement points between interconnected systems. Organizations consider mandating specific architectural solutions when required to enforce specific security policies. Enforcement includes, for example: (i) prohibiting information transfers between interconnected systems (i.e., allowing access only); (ii) employing hardware mechanisms to enforce one-way information flows; and (iii) implementing trustworthy regrading mechanisms to reassign security attributes and security labels.	
Information sharing	**Minimum**	Has the organization defined the circumstances where user discretion is required to facilitate information sharing; facilitated information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the	This control applies to information that may be restricted in some manner (e.g., privileged medical information, contract-sensitive information, proprietary information, personally identifiable information, classified information about special access programs or compartments) based on some formal or administrative determination. Depending on the specific information-sharing	13.1. Describe the steps/process taken when a request to share data is received by the system administrator or a user at a facility. 13.2. Has the organization established criteria or events that would allow the sharing of data with other systems or stakeholders? Please provide details. Provide documentation if it exists.

Control type: Access control				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
		information for the organization-defined circumstances; defined the information-sharing circumstances and automated mechanisms or manual processes required to assist users in making information-sharing or collaboration decisions; and employed organization-defined circumstances and automated mechanisms or manual processes to assist users in making information-sharing or collaboration decisions?	circumstances, sharing partners may be defined at the individual, group, or organizational level. Information may be defined by content, type, security category, or special access program/compartment.	

Control type: Identification and authentication				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
Identification and authentication (organizational users)	**Minimum**	Does the EHR uniquely identify and authenticate organizational users (or processes acting on behalf of organizational users)?	Organizational users include employees or individuals who organizations deem to have equivalent status of employees (e.g., contractors, guest researchers). This control applies to all accesses other than: (i) accesses that are explicitly identified and documented in Access Control; and	14.1. Describe the process the EHR uses to uniquely identify and authenticate organizational users. Individual authenticators include, for example, passwords, tokens,

Control type: Identification and authentication				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
			(ii) accesses that occur through authorized use of group authenticators without individual authentication. Organizations may require unique identification of individuals in group accounts (e.g., shared privilege accounts) or for detailed accountability of individual activity. Organizations employ passwords, tokens, or biometrics to authenticate user identities, or in the case of multifactor authentication, or some combination thereof. Access to organizational information systems is defined as either local access or network access. Local access is any access to organizational information systems by users (or processes acting on behalf of users) in which such access is obtained by direct connections without the use of networks. Network access is access to organizational information systems by users (or processes acting on behalf of users) in which such access is obtained through network connections (i.e., nonlocal accesses). Remote access is a type of network access that involves communication through external networks (e.g., the Internet). Internal networks include LANs and WANs. In addition, the use of encrypted VPNs for network connections between organization-controlled endpoints and non-organization-	biometrics, public key infrastructure (PKI) certificates, and key cards.

Control type: Identification and authentication				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
			controlled endpoints may be treated as internal networks from the perspective of protecting the confidentiality and integrity of information traversing the network. Multifactor authentication requires the use of two or more different factors to achieve authentication. The factors are defined as (i) something you know (e.g., password, personal identification number); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric). Multifactor solutions that require devices separate from information systems gaining access include, for example, hardware tokens providing time-based or challenge-response authenticators and smart cards. In addition to identifying and authenticating users at the information system level (i.e., at login), organizations also employ identification and authentication mechanisms at the application level, when necessary, to provide increased information security. Identification and authentication requirements for those other than organizational users are described in Identification and Authentication.	
Identifier management	**Minimum**	Does the organization define the time period for preventing reuse of user or	Common device identifiers include, for example, media access control, Internet protocol (IP) addresses, or device-unique	15.1. Provide details on how the organization or the EHR manages

Control type: Identification and authentication				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
		device identifiers; define the time period of inactivity after which a user identifier is to be disabled; manage information system identifiers for users and devices by receiving authorization from a designated organizational official to assign a user or device identifier, selecting an identifier that uniquely identifies an individual or device, assigning the user identifier to the intended party or the device identifier to the intended device, preventing reuse of user or device identifiers for the organization-defined time period, or disabling the user identifier after the organization-defined time period of inactivity?	token identifiers. Management of individual identifiers is not applicable to shared information system accounts (e.g., guest and anonymous accounts). Typically, individual identifiers are the usernames of the information system accounts assigned to those individuals. In such instances, the account management activities of -Access Control use account names provided by Identification and Authentication Control. This control also addresses individual identifiers not necessarily associated with information system accounts (e.g., identifiers used in physical security control databases accessed by badge reader systems for access to information systems). Preventing reuse of identifiers implies preventing the assignment of previously used individual, group, role, or device identifiers to different individuals, groups, roles, or devices.	user identifiers and credentials including the following: • Whether a time period is defined for preventing reuse of user or device identifiers or time period of inactivity after which a user identifier is to be disabled. • How authorization is received from a designated organizational official to assign a user or device identifier to access the system. • How an identifier is selected so that it uniquely identifies an individual or device. • How the user identifier is assigned to the intended user or the device identifier for access to the system. • How reuse of user or device identifiers is prevented. • How the user identifier is disabled after the organization-defined time period of inactivity.
Authenticator management	**Minimum**	Does the organization define the time period (by authenticator type) for changing or refreshing authenticators; manage information system authenticators for users and devices by: verifying, as part	Individual authenticators include, for example, passwords, tokens, biometrics, PKI certificates, and key cards. Initial authenticator content is the actual content (e.g., the initial password) as opposed to requirements about authenticator content (e.g., minimum password length). In many cases,	16.1. Provide details on how the EHR authentication is managed, including the following: • System or processes used to perform authentication. • How security of the authentication system is ensured.

Control type: Identification and authentication				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
		of the initial authenticator distribution, the identity of the individual or device receiving the authenticator; establishing initial authenticator content for authenticators defined by the organization; ensuring that authenticators have sufficient strength of mechanism for their intended use; establishing and implementing administrative procedures for initial authenticator distribution; establishing and implementing administrative procedures for lost, compromised, or damaged authenticators; establishing and implementing administrative procedures for revoking authenticators; changing default content of authenticators on information system installation; establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators (if deemed to be appropriate by the organization); changing or	developers ship information system components with factory default authentication credentials to allow for initial installation and configuration. Default authentication credentials are often well known, easily discoverable, and present a significant security risk. The requirement to protect individual authenticators may be implemented via other controls for authenticators stored in organizational information systems (e.g., passwords stored in hashed or encrypted formats, files containing encrypted or hashed passwords accessible with administrator privileges). Information systems support individual authenticator management by organization-defined settings and restrictions for various authenticator characteristics, including, for example, minimum password length, password composition, validation time window for time synchronous one-time tokens, and number of allowed rejections during the verification stage of biometric authentication. Specific actions that can be taken to safeguard authenticators include, for example, maintaining possession of individual authenticators, not loaning or sharing individual authenticators with others, and reporting lost, stolen, or compromised authenticators immediately.	• How or whether default content of authenticators were changed on information system installation. • What administrative procedures for lost or compromised or damaged authenticators have been implemented.

Control type: Identification and authentication				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
		refreshing authenticators in accordance with the organization-defined time period by authenticator type; protecting authenticator content from unauthorized disclosure and modification; and requiring users to take, and having devices implement, specific measures to safeguard authenticators?	Authenticator management includes issuing and revoking, when no longer needed, authenticators for temporary access, such as that required for remote maintenance. Device authenticators include, for example, certificates and passwords.	
Device identification and authentication	**Minimum**	Does the EHR define the specific types of devices for which identification and authentication is required before establishing a connection to the information system; and uniquely identify and authenticate the organization-defined devices before establishing a connection to the information system?	Organizational devices requiring unique device-to-device identification and authentication may be defined by type, device, or a combination of type/device. Information systems typically use either shared known information (e.g., media access control or transmission control protocol/internet protocol addresses) for device identification or organizational authentication solutions (e.g., IEEE 802.1x and EAP, Radius server with EAP-TLS authentication, Kerberos) to identify/authenticate devices on local or WANs. Organizations determine the required strength of authentication mechanisms by the security categories of information systems. Because of the challenges of applying this control on large scale, organizations are encouraged to only apply the control to a	17.1. Describe how a device trying to connect to the EHR is uniquely identified and authenticated before establishing a connection to the EHR. 17.2. Describe how the organization ensures that a valid user logging in to the system is doing so from an organization-authorized device.

Control type: Identification and authentication				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
			limited number (and type) of devices that truly need to support this capability.	
Authenticator feedback	**Minimum**	Does the EHR obscure feedback of authentication information during the authentication process to protect the information from possible exploitation or use by unauthorized individuals?	The feedback from information systems does not provide information that would allow unauthorized individuals to compromise authentication mechanisms. For some types of information systems or system components, for example, desktops or notebooks with relatively large monitors, the threat (often referred to as shoulder surfing) may be significant. For other types of systems or components, for example, mobile devices with two- to four-inch screens, this threat may be less significant, and may need to be balanced against the increased likelihood of typographic input errors due to the small keyboards. Therefore, the means for obscuring the authenticator feedback is selected accordingly. Obscuring the feedback of authentication information includes, for example, displaying asterisks when users type passwords into input devices or displaying feedback for a very limited time before fully obscuring it.	18.1. Does the EHR obscure feedback of authentication information during the authentication process to protect the information from possible exploitation or use by unauthorized individuals; for example, displaying asterisks when users type passwords into the input system, and displaying feedback for a very limited time before fully obscuring it? 18.2. **Instructions to assessors:** At each facility, verify the method of obfuscation. Provide details of findings and, if possible, provide a screenshot/picture.
Cryptographic module authentication	**Minimum or Intermediate**	Does the EHR use mechanisms for authentication to a cryptographic module that meet the requirements of applicable national laws,	Authentication mechanisms may be required in a cryptographic module to authenticate an operator accessing the module and to verify that the operator is authorized to assume the requested role and perform services in that role.	19.1. Has the EHR implemented any cryptographic methods? Provide details and documents.

Control type: Identification and authentication				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
		directives, policies, regulations, standards, and guidance for such authentication?		
Identification and authentication (non-organizational users)	**Minimum**	Does the EHR uniquely identify and authenticate non-organizational users (or processes acting on behalf of non-organizational users)?	Organizations use risk assessments to determine authentication needs and consider scalability, practicality, and security in balancing the need to ensure ease of use for access to information and information systems with the need to protect and adequately mitigate risk.	20.1. Describe how non-organizational users of the EHR are identified and authenticated if they need access to the system.
Identification and authentication policy and procedures	**Minimum**	Has the organization developed and formally documented identification and authentication policy that address purpose, scope, roles and responsibilities, management commitment, and coordination among organizational entities and compliance; disseminated the policy to stakeholders in the organization with associated identification and authentication roles and responsibilities; developed and formally documented identification and authentication procedures; developed procedures to facilitate implementation of	This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the Identification and Authentication family. Policy and procedures reflect applicable laws, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organizational level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program, in general, and for specific information	21.1. Are any of the identification and authentication methods and policies we discussed just now documented? 21.2. Has the organization established policy and procedures for the effective implementation of security controls for system authentication in line with existing local/regional laws, government directive, and industry standards as related to EHRs? Provide details and documents. 21.3. **Instructions to assessors:** Share specific local and regional laws and government directions and find out from the system administrator whether these have been documented and implemented. Provide details and documents of findings.

Control type: Identification and authentication				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
		the identification and authentication policy and associated identification and authentication controls; and disseminated identification and authentication procedures to elements in the organization with associated identification and authentication roles and responsibilities?	systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.	

Control type: Audit and accountability				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
Audit events and audit generation	**Minimum**	Does the organization define the list of events the information system must be capable of auditing based on a risk assessment and mission/business needs; coordinate the security audit function with other organizational entities requiring audit-related information to enhance mutual support and help	An event is any observable occurrence in an organizational information system. Organizations identify audit events as those events that are significant and relevant to the security of information systems and the environments in which those systems operate to meet specific and ongoing audit needs. Audit events can include, for example, password changes, failed logins, or failed accesses related to information systems, administrative privilege usage, or third-	22.1. Does the application have capabilities for logging events (for example, password changes, failed logins, or failed accesses related to information systems, administrative privilege usage, Personal Identification Verification credential usage or third-party credential usage, changes to the data) that occur in the system? Please obtain an example of a log file. Provide details on how we can access and find the

Control type: Audit and accountability				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
		guide the selection of auditable events; provide a rationale for why the list of auditable events is deemed to be adequate to support after-the-fact investigations of security incidents; define the subset of auditable events defined that are to be audited in the information system and the frequency of (or situation requiring) auditing for each identified event; and determine, based on current threat information and ongoing assessment of risk, the subset of auditable events defined to be audited in the information system, and the frequency of (or situation requiring) auditing for each identified event? Does the EHR provide audit record generation capability, at organization-defined information system components, for the list of auditable events defined by the organization; allow	party credential usage. In determining the set of auditable events, organizations consider the auditing appropriate for each of the security controls to be implemented. To balance auditing requirements with other information system needs, this control also requires identifying that subset of auditable events that are audited at a given point in time. For example, organizations may determine that information systems should have the capability to log every file access both successful and unsuccessful, but not activate that capability, except for specific circumstances due to the potential burden on system performance. Auditing requirements, including the need for auditable events, may be referenced in other security controls and control enhancements. Organizations also include auditable events that are required by applicable national laws, directives, policies, regulations, and standards. Audit records can be generated at various levels of abstraction, including at the packet level as information traverses the network. Selecting the appropriate level of abstraction is a critical aspect of an audit capability and can facilitate the identification of root causes to problems. Organizations consider in the definition of auditable events, the auditing necessary to cover related events, such as the steps	log file at each facility when we visit it. 22.2. Is the capability for logging events turned on at each facility/site at which the application is installed? 22.3. Does the organization specify what types of system events should be audited? If so, is this documented anywhere? 22.4. Does the system audit the types of events specified by the organization?

Control type: Audit and accountability				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
		designated organizational personnel to select which auditable events are to be audited by specific components of the system; generate audit records for the list of audited events defined in AU-2 with the content as defined in AU-3?	in distributed, transaction-based processes (e.g., processes that are distributed across multiple organizations), and actions that occur in service-oriented architectures.	
Content of audit records	**Minimum**	Does the EHR produce audit records that contain sufficient information to, at a minimum, establish what type of event occurred; when (date and time) the event occurred; where the event occurred; the source of the event; the outcome (success or failure) of the event; and the identity of any user/subject associated with the event?	Audit record content that may be necessary to satisfy the requirement of this control includes, for example, time stamps, source and destination addresses, user/process identifiers, event descriptions, success/fail indications, filenames involved, and access control or flow control rules invoked. Event outcomes can include indicators of event success or failure and event-specific results (e.g., the security state of the information system after the event occurred).	23.1. What information is captured about the events in the system, such as the type of event or when it occurred? 23.2. What information is contained in the logs? 23.3. Describe how the EHR identifies potential security-relevant error conditions, including generation of error messages that provide information necessary for corrective actions without revealing sensitive or potentially harmful information in error logs and administrative messages that could be exploited by adversaries (e.g., when a user enters the wrong password, the system should indicate that the password is wrong, but that credentials are wrong; or when there is an error in a patient record, the error log does not contain the patient identifiers).

Control type: Audit and accountability				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
				23.4. **Instructions to assessors:** At each facility, navigate to the location of the log file and verify its presence or absence. Provide details of findings and, if possible, download or provide a screenshot of the log file at each facility to get a record of the contents.
Protection of audit information	**Minimum**	Does the EHR protect audit information and audit tools from unauthorized access, modification, and deletion?	Audit information includes all information (e.g., audit records, audit settings, and audit reports) needed to successfully audit information system activity. This control focuses on technical protection of audit information. Physical protection of audit information is addressed by media protection controls and physical and environmental protection controls.	24.1. Who can access the audit/log file?
Audit review, analysis, and reporting	**Minimum or Intermediate**	Does the organization define the frequency of information system audit record reviews and analyses; review and analyze information system audit records for indications of inappropriate or unusual activity in accordance with the organization-defined frequency; and report findings of inappropriate or unusual activities to	Audit review, analysis, and reporting covers information security-related auditing performed by organizations, including, for example, auditing that results from monitoring of account usage, remote access, wireless connectivity, mobile device connection, configuration settings, system component inventory, use of maintenance tools and nonlocal maintenance, physical access, temperature and humidity, equipment delivery and removal, communications at the information system boundaries, use of	25.1. When is the audit file reviewed? Is there a process to regularly review it or is it reviewed when there is an issue? 25.2. Describe the process established for audit review, analysis, and reporting.

Control type: Audit and accountability				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
		designated organizational officials?	mobile code, and use of Voice over Internet Protocol (VoIP). Findings can be reported to organizational entities that include, for example, the incident response team, help desk, and information security group/department. If organizations are prohibited from reviewing and analyzing audit information or are unable to conduct such activities (e.g., in certain national security applications or systems), the review/analysis may be carried out by other organizations granted such authority.	
Audit and accountability policy and procedures	**Minimum or Intermediate**	Has the organization formally documented an audit and accountability policy that addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance; disseminated the formal policy to elements in the organization with associated audit and accountability roles and responsibilities; developed and formally documented audit and accountability policy procedures that implement the policy and associated audit and	This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the Audit and Accountability family. Policy and procedures reflect applicable laws, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organizational level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or, conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program, in general, and for specific information	26.1. Does the organization have a security events checklist for what to look for in the audit logs that would raise concern? Please provide details. 26.2. Have the audit and accountability processes described above been documented anywhere? If yes, please provide them.

Control type: Audit and accountability				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
		accountability controls; disseminated the formally documented audit and accountability procedures to stakeholders in the organization with associated audit and accountability policy roles and responsibilities?	systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.	
Audit storage capacity	**Intermediate**	Does the organization allocate audit record storage capacity and configure auditing to reduce the likelihood of audit record storage capacity being exceeded?	Organizations consider the types of auditing to be performed and the audit processing requirements when allocating audit storage capacity. Allocating sufficient audit storage capacity reduces the likelihood of such capacity being exceeded and resulting in the potential loss or reduction of auditing capability.	27.1. Does the application automatically set storage limits for the audit log? 27.2. Is this functionality turned on for this instance of the EHR? 27.3. Describe what happens if the audit/log file exceeds the maximum allocated storage. 27.4. **Instructions to assessors:** At each facility, navigate to the location of the log file and capture the size of the audit/log file. Provide details of findings and, if possible, download or screenshot the log file at each facility to get a record of the contents.
Response to audit processing failures	**Intermediate**	Does the EHR define designated organizational officials to be alerted in the event of an audit processing failure, alert designated organizational officials in the event of an audit processing	Audit processing failures include, for example, software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded. Organizations may choose to define additional actions for different audit processing failures (e.g., by	28.1. What happens if there is an audit/log file failure? Does anyone get notified? If yes, how? Audit processing failures include, for example, software/hardware errors, failures in the audit capturing mechanisms, and audit storage

Control type: Audit and accountability				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
		failure, define additional actions to be taken in the event of an audit processing failure, and take the additional organization-defined actions in the event of an audit processing failure?	type, by location, by severity, or a combination of such factors). This control applies to each audit data storage repository (i.e., distinct information system component where audit records are stored), the total audit storage capacity of organizations (i.e., all audit data storage repositories combined), or both.	capacity being reached or exceeded. 28.2. On notification of an audit process failure, what steps does the system administrator take? Provide details. 28.3. Are these steps documented anywhere? Please provide documents.
Time stamps	**Minimum**	Does the EHR use internal system clocks to generate time stamps for audit records?	Time stamps generated by the information system include date and time. Time is commonly expressed in Coordinated Universal Time (UTC), a modern continuation of Greenwich Mean Time (GMT), or local time with an offset from Coordinated Universal Time. Granularity of time measurements refers to the degree of synchronization between information system clocks and reference clocks (e.g., clocks synchronizing within hundreds of milliseconds or within tens of milliseconds). Organizations may define different time granularities for different system components. Time service can also be critical to other security capabilities, such as access control and identification and authentication, depending on the nature of the mechanisms used to support those capabilities.	29.1. To be determined by the vulnerability scan.

Control type: Audit and accountability				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
Non-repudiation	**Minimum**	Does the EHR protect against an individual falsely denying having performed a specific action?	Types of individual actions covered by non-repudiation include, for example, creating information, sending and receiving messages, and approving information (e.g., indicating concurrence or signing a contract). Non-repudiation protects individuals against later claims by (i) authors of not having authored specific documents; (ii) senders of not having transmitted messages; (iii) receivers of not having received messages; or (iv) signatories of not having signed documents. Non-repudiation services can be used to determine whether information originated from a specific individual, or whether an individual took specific actions (e.g., sending an e-mail, signing a contract, approving a procurement request) or received specific information. Organizations obtain non-repudiation services by employing various techniques or mechanisms (e.g., digital signatures, digital message receipts).	30.1. Do users at any time share the same username and password? 30.2. Have there been instances where individuals used a username/password that did not belong to them? 30.3. Provide details of any steps taken to avoid the above. If there is documentation, please provide it. 30.4. **Instructions to assessors:** At each facility, ask at least two users whether the credentials they are using belong to them. Ask whether they have shared them with anyone else in the past. Ask when they received that credential and from whom.

Control type: Awareness and training				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
Security awareness training	**Minimum**	Does the organization provide basic security awareness training to all information system users (including managers, senior executives, and contractors) as part of initial training for new users and when required by system changes; define the frequency of refresher security awareness training; and provide refresher security awareness training in accordance with the organization-defined frequency?	Organizations determine the appropriate content of security awareness training and security awareness techniques based on the specific organizational requirements and the information systems to which personnel have authorized access. The content includes a basic understanding of the need for information security and user actions to maintain security and to respond to suspected security incidents. The content also addresses awareness of the need for operations security. Security awareness techniques can include, for example, displaying posters, offering supplies inscribed with security reminders, generating e-mail advisories/notices from senior organizational officials, displaying login screen messages, and conducting information security awareness events.	31.1. What instructions are given to system users about system security? 31.2. Has the organization performed security awareness training for system users? 31.3. If user roles exist in the system, are users provided with training specifically about that role? 31.4. Are training refreshers provided to remind users about the importance of maintaining system security? 31.5. Please provide details of the contents of any security training provided. If possible, provide the training materials.
Security awareness and training policy and procedures	**Minimum**	Has the organization developed and formally documented awareness and training policy that addresses purpose, scope, roles and responsibilities, management commitment; disseminated formal documented awareness and training policy to elements in the organization with associated awareness and training roles and	This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the Awareness and Training family. Policy and procedures reflect applicable laws, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organizational level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for	32.1. Are the training procedures documented? Please provide them. 32.2. **Instructions to assessors:** At each facility, ask at least two users whether they are aware of any security processes or procedures. Provide details of these interviews. 32.3. At each facility, ask at least two users when they last received security training. Provide details of these interviews.

Control type: Awareness and training				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
		responsibilities; developed and formally documented awareness and training procedures that implemented the policy and associated awareness and training controls; disseminated formal documented awareness and training procedures to stakeholders in the organization with associated awareness and training roles and responsibilities?	organizations or, conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program, in general, and for specific information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.	

Control type: Configuration management				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
Baseline configuration	**Minimum**	Does the organization develop and document a baseline configuration of the information system; and maintain, under configuration control, a current baseline configuration of the information system?	This control establishes baseline configurations for information systems and system components, including communications and connectivity-related aspects of systems. Baseline configurations are documented, formally reviewed, and agreed-on sets of specifications for information systems or configuration items in those systems. Baseline configurations	33.1. Describe the baseline configurations of the EHR system installed at this facility. Baseline configurations include information about information system components (e.g., standard laptop versions, operating system current versions, current version numbers of the EHR application installed,

Control type: Configuration management				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
			serve as a basis for future builds, releases, and changes to information systems. Baseline configurations include information about information system components (e.g., standard software packages installed on workstations, notebook computers, servers, network components, or mobile devices; current version numbers and patch information on operating systems and applications; and configuration settings/parameters); network topology; and the logical placement of those components in the system architecture. Maintaining baseline configurations requires creating new baselines as organizational information systems change over time. Baseline configurations of information systems reflect the current enterprise architecture.	including build/patch number currently deployed, configuration settings/parameters). Are these baseline configurations documented? 33.2. Describe the application architecture and network topology (i.e., the logical placement of those system components in the system architecture). For example, is the system installed as a client server or cloud implementation? Is the database installed on the same server as the frontend application? Is it a standalone implementation or is it implemented on a LAN or WAN? Please provide documentation of the application architecture and network topology and baseline configurations.
Configuration change control	**Minimum**	Does the organization determine the types of changes to the information system that are configuration controlled; approve configuration-controlled changes to the system with explicit consideration for security impact analyses; document approved configuration-controlled changes to the system; retain	Configuration change controls for organizational information systems involve the systematic proposal, justification, implementation, testing, review, and disposition of changes to the systems, including system upgrades and modifications. Configuration change control includes changes to baseline configurations for components and configuration items of information systems; changes to configuration settings for IT products (e.g., operating systems,	34.1. Describe how changes to installed versions of the EHR are managed (e.g., who can make updates to the trunk, how is branching and merging done, how are rollbacks done). 34.2. Are changes managed via any version control system, such as Jira, GitHub, Subversion, Mercurial, BitBucket, etc.? Provide links to the change management system.

Control type: Configuration management				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
		and review records of configuration-controlled changes to the system; audit activities associated with configuration-controlled changes to the system; define the configuration change control element (e.g., committee, board) responsible for coordinating and providing oversight for configuration change control activities, the frequency with which the configuration change control element convenes, or configuration change conditions that prompt the configuration change control element to convene; coordinate and provide oversight for configuration change control activities through the organization-defined configuration change control element that convenes at the organization-defined frequency or for any organization-defined configuration change conditions?	applications, firewalls, routers, and mobile devices); unscheduled or unauthorized changes; and changes to remediate vulnerabilities. Typical processes for managing configuration changes to information systems include, for example, Configuration Control Boards that approve proposed changes to systems. For new development information systems or systems undergoing major upgrades, organizations consider the inclusion of representatives from development organizations on the Configuration Control Boards. Auditing of changes includes activities before and after changes are made to organizational information systems and the auditing activities required to implement such changes.	34.3. Has the organization or facility made any changes to the baseline configuration of the EHR installed? How are those changes managed?

Control type: Configuration management				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
Configuration settings	**Intermediate**	Does the organization define security configuration checklists to be used to establish and document mandatory configuration settings for the information system technology products employed; define security configuration checklists that reflect the most restrictive mode consistent with operational requirements; establish and document mandatory configuration settings for IT products employed in the information system using organization-defined security configuration checklists; implement the security configuration settings; identify, document, and approve exceptions from the mandatory configuration settings for individual components in the information system based on explicit operational requirements; and monitor and control changes to the configuration settings in accordance with organizational policies and procedures?	Configuration settings are the set of parameters that can be changed in hardware, software, or firmware components of the information system that affect the security posture or functionality of the system. IT products for which security-related configuration settings can be defined include, for example, mainframe computers, servers (e.g., database, electronic mail, authentication, web, proxy, file, domain name), workstations, input/output devices (e.g., scanners, copiers, and printers), network components (e.g., firewalls, routers, gateways, voice and data switches, wireless access points, network appliances, sensors), operating systems, middleware, and applications. Security-related parameters are those parameters impacting the security state of information systems, including the parameters required to satisfy other security control requirements. Security-related parameters include, for example: (i) registry settings; (ii) account, file, directory permission settings; and (iii) settings for functions, ports, protocols, services, and remote connections. Organizations establish organization-wide configuration settings and subsequently derive specific settings for information systems. The established settings become part of the system's configuration baseline. Common secure	35.1. Does the organization specify certain settings in the system that are used to control security (e.g., application settings, such as account settings, timeout settings, privileges; settings for workstations and input/output devices; network settings; registry settings, account, file, directory permission settings; and settings for functions, ports, protocols [http versus https, services, and remote connections])? If so, what are those settings? Please share any related documentation.

Control type: Configuration management				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
			configurations (also referred to as security configuration checklists, lockdown and hardening guides, security reference guides, security technical implementation guides) provide recognized, standardized, and established benchmarks that stipulate secure configuration settings for specific IT platforms and products and instructions for configuring those information system components to meet operational requirements. Common secure configurations can be developed by a variety of organizations including, for example, IT product developers, manufacturers, vendors, consortia, academia, industry, government agencies, and other organizations in the public and private sectors.	
Security impact analysis	**Intermediate**	Does the organization analyze changes to the information system to determine potential security impacts before change implementation?	Organizational personnel with information security responsibilities (e.g., Information System Administrators, Information System Security Officers, Information System Security Managers, and Information System Security Engineers) conduct security impact analyses. Individuals conducting security impact analyses possess the necessary skills and technical expertise to analyze the changes to information systems and the associated security ramifications. Security impact analysis may include, for example, reviewing security plans to understand	36.1. Describe how changes are reviewed to ensure that security functionality is not impacted. Provide documents. 36.2. When application/system changes are made, what types of security controls are verified? Provide detail and documents.

Control type: Configuration management				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
			security control requirements and reviewing system design documentation to understand control implementation and how specific changes might affect the controls. Security impact analyses may also include assessments of risk to better understand the impact of the changes and determine whether additional security controls are required. Security impact analyses are scaled in accordance with the security categories of the information systems.	
Access restrictions for change	**Minimum**	Does the organization define, document, approve, and enforce physical and logical access restrictions associated with changes to the information system?	Any changes to the hardware, software, or firmware components of information systems can potentially have significant effects on the overall security of the systems. Therefore, organizations permit only qualified and authorized individuals to access information systems for the purposes of initiating changes, including upgrades and modifications. Organizations maintain records of access to ensure that configuration change control is implemented and to support after-the-fact actions should organizations discover any unauthorized changes. Access restrictions for change also include software libraries. Access restrictions include, for example, physical and logical access controls, workflow automation, media libraries, abstract layers (e.g., changes implemented in third-party	37.1. Who has authority to request changes to the application? Provide details and documents. 37.2. Who has authority to make changes in the system?

Control type: Configuration management				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
			interfaces rather than directly in the information systems), and change windows (e.g., changes occur only during specified times, making unauthorized changes easy to discover).	
Information system component inventory	**Minimum**	Has the organization defined the information deemed necessary to achieve effective property accountability; and developed, documented, and maintained an inventory of information system components that accurately reflects the current information system; is consistent with the authorization boundary of the information system; is at the level of granularity deemed necessary for tracking and reporting; includes organization-defined information deemed necessary to achieve effective property accountability; and is available for review and audit by designated organizational officials?	Organizations may choose to implement centralized information system component inventories that include components from all organizational information systems. In such situations, organizations ensure that the resulting inventories include system-specific information required for proper component accountability (e.g., information system association, information system owner). Information deemed necessary for effective accountability of information system components includes, for example, hardware inventory specifications, software license information, software version numbers, component owners, and for networked components or devices, machine names and network addresses. Inventory specifications include, for example, manufacturer, device type, model, serial number, and physical location.	38.1. On how many computers/laptops has the EHR been installed or who can access the EHR through the LAN/WAN? Is a list of all laptops, their locations, etc. maintained at each facility? If yes, provide details and documents.
Software usage restrictions	**Minimum or Intermediate**	Does the organization use software and associated documentation in accordance with contract agreements and	Software license tracking can be accomplished by manual methods (e.g., simple spreadsheets) or automated methods (e.g., specialized tracking	39.1. Describe the agreement between the organization and creators/developers of the EHR. Are there specific terms of use,

Control type: Configuration management				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
		copyright laws; track the use of software and associated documentation protected by quantity licenses to control copying and distribution; and control and document the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work?	applications), depending on organizational needs.	including restrictions? If yes, provide details and documents.
User-installed software	**Minimum or Intermediate**	Does the organization have established organization-defined policies governing the installation of software by users; enforce software installation policies through organization-defined methods; and monitor policy compliance at an organization-defined frequency?	If provided the necessary privileges, users have the ability to install software in organizational information systems. To maintain control over the types of software installed, organizations identify permitted and prohibited actions regarding software installation. Permitted software installations may include, for example, updates and security patches to existing software and downloading applications from organization-approved app stores. Prohibited software installations may include, for example, software with unknown or suspect pedigrees or software that organizations consider potentially malicious. The policies that organizations select governing user-installed software may be organization-developed or provided by some external entity. Policy	40.1. On laptops where the EHR is installed or accessed via LAN/WAN, is any other software installed? If yes, provide details and documents. 40.2. Are the EHR users restricted from installing third-party software on the same machine where the EHR is installed or accessed? If yes, provide details and documents.

Control type: Configuration management				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
			enforcement methods include procedural methods (e.g., periodic examination of user accounts), automated methods (e.g., configuration settings implemented on organizational information systems), or both.	
Configuration management plan	**Intermediate**	Does the organization develop, document, and implement a configuration management plan for the information system that addresses roles, responsibilities, and configuration management processes and procedures; define the configuration items for the information system and when in the system development life cycle the configuration items are placed under configuration management; and establish the means for identifying configuration items throughout the system development life cycle and a process for managing the configuration of the configuration items?	Configuration management plans satisfy the requirements in configuration management policies while being tailored to individual information systems. Such plans define detailed processes and procedures for how configuration management is used to support system development life cycle activities at the information system level. Configuration management plans are typically developed during the development/acquisition phase of the system development life cycle. The plans describe how to move changes through change management processes; how to update configuration settings and baselines; how to maintain information system component inventories; how to control the development, test, and operational environments; and how to develop, release, and update key documents. Organizations can employ templates to help ensure consistent and timely development and implementation of configuration management plans. Such templates can represent a master	41.1. Is any of the above regarding baseline configurations, processes for changing configurations, or security configurations for the system environment documented in a plan? If yes, request a copy of the plan.

Control type: Configuration management				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
			configuration management plan for the organization at large, with subsets of the plan implemented on a system-by-system basis. Configuration management approval processes include the designation of key management stakeholders responsible for reviewing and approving proposed changes to information systems, and personnel who conduct security impact analyses before the implementation of changes to the systems. Configuration items are the information system items (hardware, software, firmware, and documentation) to be configuration-managed. As information systems continue through the system development life cycle, new configuration items may be identified and some existing configuration items may no longer need to be under configuration control.	
Configuration management policy and procedures	**Intermediate**	Has the organization: developed and formally documented a policy that addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities and compliance; disseminated the policy to stakeholders in the organization with associated	This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the Configuration Management family. Policy and procedures reflect applicable laws, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organizational level may make the need for system-specific policies and procedures unnecessary. The	42.1. Is any of the above documented as policies and procedures, etc.? If yes, obtain a copy of the policies and procedures?

Control type: Configuration management				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
		configuration management roles and responsibilities; developed and formally documented configuration management procedures; implemented the policy and associated configuration management controls; and disseminated procedures to stakeholders in the organization with associated configuration management roles and responsibilities?	policy can be included as part of the general information security policy for organizations or, conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program, in general, and for specific information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.	

Control type: Contingency planning				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
Information system backup	**Minimum**	Does the organization define the frequency of conducting user-level information backups to support recovery time objectives and recovery point objectives; define the frequency of conducting system-level information backups to support recovery time objectives and recovery point objectives; define the	System-level information includes, for example, system-state information, operating system and application software, and licenses. User-level information includes any information other than system-level information. Mechanisms employed by organizations to protect the integrity of information system backups include, for example, digital signatures and cryptographic hashes. Protection of system backup information while in transit is beyond the scope of this control.	43.1. Describe how information in the application is backed up at each facility. How is this set up? Is it an automatic or manual process? What is the location of the file? How often are backups taken? Provide details and documents. 43.2. **Instructions to assessors:** At each facility, for each laptop or

Control type: Contingency planning				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
		frequency of conducting information system documentation backups (including security-related information) to support recovery time objectives and recovery point objectives; back up user-level information in accordance with the organization-defined frequency; back up system-level information in accordance with the organization-defined frequency; and back up information system documentation in accordance with the organization-defined frequency?	Information system backups reflect the requirements in contingency plans and other organizational requirements for backing up information.	server with the EHR installed, navigate to the location of the backup file and capture the size of the file. Provide details of findings or screenshot the file location at each facility/laptop.
Information system recovery and reconstitution	**Minimum**	Does the organization provide automated mechanisms or manual procedures for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure?	Recovery is executing information system contingency plan activities to restore organizational mission/business functions. Reconstitution takes place following recovery and includes activities for returning organizational information systems to fully operational states. Recovery and reconstitution operations reflect mission and business priorities, recovery point/time and reconstitution objectives, and established organizational metrics consistent with contingency plan requirements. Reconstitution includes the deactivation of any interim	44.1. If a failure or disruption to the functioning of the system occurs and data are lost or corrupted, describe the process for recovering those data back to the system. Provide details of the last time this happened.

Control type: Contingency planning				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
			information system capabilities that may have been needed during recovery operations. Reconstitution also includes assessments of fully restored information system capabilities, reestablishment of continuous monitoring activities, potential information system reauthorizations, and activities to prepare the systems against future disruptions, compromises, or failures. Recovery/reconstitution capabilities employed by organizations can include both automated mechanisms and manual procedures.	
Telecommuni-cations services	**Intermediate**	Does the organization establish alternate telecommunications services to support the information system; define in the time period in which resumption of information system operations should take place; establish necessary alternate telecommunications service agreements to permit the resumption of telecommunications services for essential missions and business functions in the organization-defined time period when the primary telecommunications capabilities are unavailable?	This control applies to telecommunications services (data and voice) for primary and alternate processing and storage sites. Alternate telecommunications services reflect the continuity requirements in contingency plans to maintain essential mission/business functions despite the loss of primary telecommunications services. Organizations may specify different time periods for primary/alternate sites. Alternate telecommunications services include, for example, additional organizational or commercial ground-based circuits/lines or satellites in lieu of ground-based communications. Organizations consider such factors as availability, quality of service, and access when entering into alternate telecommunications agreements.	45.1. If the application is networked via LAN, WAN, or Internet at a facility, what happens if the network service is disrupted? Provide details of service-level agreements describing maximum downtime, alternate connection possibilities, the process for connecting secondary networking service, etc. Provide documents.

Control type: Contingency planning				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
Alternate storage site	**Minimum**	Has the organization established an alternate storage site and initiated necessary alternate storage site agreements to permit the storage and recovery of information system backup information?	Alternate storage sites are sites that are geographically distinct from primary storage sites. An alternate storage site maintains duplicate copies of information and data in the event that the primary storage site is not available. Items covered by alternate storage site agreements include, for example, environmental conditions at alternate sites, access rules, physical and environmental protection requirements, and coordination of delivery/retrieval of backup media. Alternate storage sites reflect the requirements in contingency plans so that organizations can maintain essential mission/business functions despite disruption, compromise, or failure in organizational information systems.	46.1. Does the organization provide alternate backup locations if the primary backup is not available? Provide details and documents. An alternate storage site maintains duplicate copies of information and data in the event that the primary storage site is not available. 46.2. At each facility, for each laptop/computer with the EHR installed, verify the location and connection to the alternate storage. The connection should be always available in case the primary backup fails (such as connection to an external hard drive or network connection to remote storage). Provide details of findings and, if possible, provide screenshots/pictures at each facility/laptop.
Alternate processing site	**Intermediate**	Has the organization established an alternate processing site; defined the time period for achieving the recovery time objectives in which processing should be resumed at the alternate processing site; included necessary alternate	Alternate processing sites are sites that are geographically distinct from primary processing sites. An alternate processing site provides processing capability in the event that the primary processing site is not available. Items covered by alternate processing site agreements include, for example, environmental conditions at alternate sites, access rules, physical and	47.1. What happens if the live or production version of the system is no longer available? Is there an alternative to allow continuing to access to and use of the system?

Control type: Contingency planning				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
		processing site agreements to permit the resumption of information system operations for essential missions and business functions in the organization-defined time period; and ensured that the equipment and supplies required to resume operations are available at the alternate site or that contracts are in place to support delivery to the site in time to support the organization-defined time period for resumption?	environmental protection requirements, and coordination for the transfer/assignment of personnel. Requirements are specifically allocated to alternate processing sites that reflect the requirements in contingency plans to maintain essential mission/business functions despite disruption, compromise, or failure in organizational information systems.	
Contingency training and contingency plan testing	**Intermediate**	Does the organization provide initial contingency training to personnel with contingency roles and responsibilities with respect to the information system, define the frequency of refresher contingency training, and provide refresher training in accordance with organization-defined frequency? Does the organization define the contingency plan tests or exercises to be conducted, define the frequency of contingency plan tests or exercises, test/exercise the	Contingency training provided by organizations is linked to the assigned roles and responsibilities of organizational personnel to ensure that the appropriate content and level of detail is included in such training. For example, regular users may only need to know when and where to report for duty during contingency operations and if normal duties are affected; system administrators may require additional training on how to set up information systems at alternate processing and storage sites; and managers/senior leaders may receive more specific training on how to conduct mission-essential functions in designated offsite locations and how to establish communications with other governmental entities for the purposes of coordination on contingency-related	48.1. If the EHR is being used for point-of-care service delivery, what happens if the system goes down (either the EHR or the network connection to access the EHR)? How do you continue providing care and documentation? 48.2. Does the facility/organization test its contingency plans? If so, how often are they tested? Is this documented anywhere? 48.3. How do you test the contingency plan or provide training on the contingency

Control type: Contingency planning				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
		contingency plan using organization-defined tests/exercises in accordance with organization-defined frequency, and review the contingency plan test/exercise results and take corrective actions?	activities. Training for contingency roles/responsibilities reflects the specific continuity requirements in the contingency plan. Methods for testing contingency plans to determine the effectiveness of the plans and to identify potential weaknesses in the plans include, for example, walk-through and tabletop exercises, checklists, simulations (parallel, full interrupt), and comprehensive exercises. Organizations conduct testing based on the continuity requirements in contingency plans and include a determination of the effects on organizational operations, assets, and individuals arising due to contingency operations. Organizations have flexibility and discretion in the breadth, depth, and timelines of corrective actions.	plan (e.g., tabletop testing, simulation, checklists)? A tabletop test is a simulation meeting to determine actionable next steps and plans in response to an emergency situation.
Contingency plan	**Minimum**	Has the organization developed a contingency plan for the information system that identifies essential missions and business functions and associated contingency requirements; provides recovery objectives, restoration priorities, and metrics; addresses contingency roles, responsibilities, assigned individuals with contact information; addresses	Contingency planning for information systems is part of an overall organizational program for achieving continuity of operations for mission/business functions. Contingency planning addresses both information system restoration and implementation of alternative mission/business processes when systems are compromised. The effectiveness of contingency planning is maximized by considering such planning throughout the phases of the system development life cycle. Performing contingency planning on hardware, software, and firmware development can be an effective means of	49.1. Has a contingency plan detailing the above been developed? Provide details and documents.

Control type: Contingency planning				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
		maintaining essential missions and business functions despite an information system disruption, compromise, or failure; addresses eventual, full information system restoration without deterioration of the security measures originally planned and implemented; and is reviewed and approved by designated officials in the organization; defined key contingency personnel (identified by name and/or by role) and organizational stakeholders designated to receive copies of the contingency plan; and distributed copies of the contingency plan to organization-defined key contingency personnel and organizational elements. Determine whether coordinated contingency planning activities with incident handling activities: defined the frequency of contingency plan reviews; reviewed the contingency plan for the information system in accordance with	achieving information system resiliency. Contingency plans reflect the degree of restoration required for organizational information systems because not all systems may need to fully recover to achieve the level of continuity of operations desired. Information system recovery objectives reflect applicable laws, directives, policies, standards, regulations, and guidelines. In addition to information system availability, contingency plans also address other security-related events, resulting in a reduction in mission or business effectiveness, such as malicious attacks compromising the confidentiality or integrity of information systems. Actions addressed in contingency plans include, for example, orderly/graceful degradation, information system shutdown, fallback to a manual mode, alternate information flows, and operating in modes reserved for when systems are under attack. By closely coordinating contingency planning with incident handling activities, organizations can ensure that the necessary contingency planning activities are in place and activated in the event of a security incident.	

Control type: Contingency planning				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
		the organization-defined frequency; revised the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing?		
Contingency planning policy and procedures	**Minimum**	Has the organization developed and formally documented a contingency planning policy that addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities and compliance; developed procedures to facilitate implementation of the contingency planning policy and associated contingency planning controls; and disseminated procedures to stakeholders in the organization with associated contingency planning roles and responsibilities?	This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the Contingency Planning family. Policy and procedures reflect applicable laws, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organizational level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or, conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program, in general, and for specific information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.	50.1. Have policies and procedure detailing the above been developed? Provide details and documents.

Control type: Incident response				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
Incident handling	**Minimum**	Does the organization implement an incident handling capability for security incidents that includes preparation; detection and analysis; containment; eradication; and recovery; coordinate incident handling activities with contingency planning activities; incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises; and implement the resulting changes to incident response procedures, training, and testing/exercise accordingly?	Organizations recognize that incident response capability is dependent on the capabilities of organizational information systems and the mission/business processes being supported by those systems. Therefore, organizations consider incident response as part of the definition, design, and development of mission/business processes and information systems. Incident-related information can be obtained from a variety of sources, including, for example, audit monitoring, network monitoring, physical access monitoring, user/administrator reports, and reported supply chain events. Effective incident handling capability includes coordination among many organizational entities, including, for example, mission/business owners, information system owners, authorizing officials, human resources offices, physical and personnel security offices, legal departments, operations personnel, procurement offices, and the risk executive (function).	51.1. Describe how a system administrator gets to know about a real or suspected security incident. A security incident can include system hacking, network breach, compromising of public/private keys, inappropriate physical access to the system, etc. 51.2. If someone in the facility learns of a security incident, what is the process for handling the incident? 51.3. Described how lessons learned from a security incident are disseminated to ensure that they do not occur again.
Incident reporting	**Minimum**	Has the organization defined a time period required to report suspected security incidents to the organizational incident response capability; required personnel to report suspected	The intent of this control is to address both specific incident reporting requirements in an organization and the formal incident reporting requirements for government agencies and their subordinate organizations. Suspected	52.1. Describe how a real or suspected security incident is communicated in the organization to senior-level leaders and stakeholders, such as the ministry of health, donors, partners, etc.?

Control type: Incident response				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
		security incidents to the organizational incident response capability in the organization-defined time period; and reported security incident information to designated authorities?	security incidents include, for example, the receipt of suspicious e-mail communications that can potentially contain malicious code. The types of security incidents reported, the content and timeliness of the reports, and the designated reporting authorities reflect applicable laws, directives, regulations, policies, standards, and guidance.	
Incident monitoring	**Minimum**	Does the organization track and document information on system security incidents?	Documenting information on system security incidents includes, for example, maintaining records about each incident, the status of the incident, and other pertinent information necessary for forensics, and evaluating incident details, trends, and handling. Incident information can be obtained from a variety of sources, including, for example, incident reports, incident response teams, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports.	53.1. How are security incidents documented and tracked? What kind of information is collected for each incident? Provide details on how these are implemented and the reports they provide. 53.2. What sources are used to monitor for security incidents? Incident information can be obtained from a variety of sources, including, for example, incident reports, incident response teams, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports.
Incident response assistance	**Intermediate**	Does the organization provide an incident response support resource that offers advice and assistance to users of the information system for the handling and reporting of	Incident response support resources provided by organizations include, for example, help desks, assistance groups, and access to forensics services, when required.	54.1. Does the organization have incident response support resources that offer advice and assistance to users of the information system for the handling and reporting of

Control type: Incident response				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
		security incidents, and ensure that the incident response support resource is an integral part of the organization's incident response capability?		security incidents (e.g., incident response guidance)?
Incident response training	**Minimum**	Does the organization identify personnel with incident response roles and responsibilities with respect to the information system; provide incident response training to personnel with incident response roles and responsibilities with respect to the information system; provide incident response training material to address the procedures and activities necessary to fulfill identified organizational incident response roles and responsibilities; define the frequency of refresher incident response training; and provide refresher incident response training in accordance with the organization-defined frequency?	Incident response training provided by organizations is linked to the assigned roles and responsibilities of organizational personnel to ensure that the appropriate content and level of detail is included in such training. For example, regular users may only need to know who to call or how to recognize an incident on the information system; system administrators may require additional training on how to handle/remediate incidents; and incident responders may receive more specific training on forensics, reporting, system recovery, and restoration. Incident response training includes user training on the identification and reporting of suspicious activities, both from external and internal sources.	55.1. Describe incident response training and its contents, if provided. 55.2. **Instructions to assessors:** At each facility, ask at least two users whether they are aware of any incident response processes or procedures. Provide details of these interviews. 55.3. **Instructions to assessors:** At each facility, ask at least two users when they last received incident response training. Provide details of these interviews.
Incident response testing	**Intermediate**	Does the organization define incident response tests/exercises; define the frequency of incident response	Organizations test incident response capabilities to determine the overall effectiveness of the capabilities and to identify potential weaknesses or	56.1. Describe how the organization tests its incident response procedures.

Control type: Incident response				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
		tests/exercises; test/exercise the incident response capability for the information system using organization-defined tests/exercises in accordance with organization-defined frequency; document the results of incident response tests/exercises; and determine the effectiveness of the incident response capability?	deficiencies. Incident response testing includes, for example, the use of checklists, walkthrough or tabletop exercises, simulations (parallel/full interrupt), and comprehensive exercises. Incident response testing can also include a determination of the effects on organizational operations (e.g., reduction in mission capabilities), organizational assets, and individuals due to incident response.	
Incident response plan	**Intermediate**	Has the organization developed an incident response plan that provides the organization with a roadmap for implementing its incident response capability; describes the structure and organization of the incident response capability; provides a high-level approach for how the incident response capability fits into the overall organization; meets the unique requirements of the organization, which relate to mission, size, structure, and functions; defines reportable incidents; provides metrics for measuring the incident response capability in the organization; defines the resources and management support needed to effectively	It is important that organizations develop and implement a coordinated approach to incident response. Organizational missions, business functions, strategies, goals, and objectives for incident response help determine the structure of incident response capabilities. As part of a comprehensive incident response capability, organizations consider the coordination and sharing of information with external organizations, including, for example, external service providers and organizations involved in the supply chain for organizational information systems.	57.1. Is there an incident response plan that details the above? Provide details and documents.

Control type: Incident response				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
		maintain and mature an incident response capability; and is reviewed and approved by designated officials in the organization?		
Incident response policy and procedures	**Intermediate**	Has the organization developed and formally documented an incident response policy that addresses purpose, scope, roles and responsibilities, management commitment, and coordination among organizational entities and compliance; disseminated the policy to stakeholders in the organization with associated incident response roles and responsibilities; developed and formally documented incident response procedures; developed procedures to facilitate implementation of the incident response policy and associated incident response controls; and disseminated incident response procedures to stakeholders in the organization with associated incident response roles and responsibilities?	This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the Incident Response family. Policy and procedures reflect applicable laws, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organizational level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or, conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program, in general, and for specific information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.	58.1. Are there documented incident response policies and procedures? Provide details and documents.

Control type: Maintenance				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
Controlled maintenance	**Minimum**	Does the organization schedule, perform, document, and review records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications or organizational requirements; control all maintenance activities, whether performed onsite or remotely and whether the equipment is serviced on site or removed to another location; require that a designated official explicitly approve the removal of the information system or system components from organizational facilities for offsite maintenance or repairs; sanitize equipment to remove all information from associated media before removal from organizational facilities for offsite maintenance or repairs; and check all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions?	This control addresses the information security aspects of the information system maintenance program and applies to all types of maintenance to any system component (including applications) conducted by any local or nonlocal entity (e.g., in-contract, warranty, in-house, software maintenance agreement). System maintenance also includes those components not directly associated with information processing or data/information retention, such as scanners, copiers, and printers. Information necessary for creating effective maintenance records includes, for example: (i) date and time of maintenance; (ii) name of individuals or group performing the maintenance; (iii) name of escort, if necessary; (iv) a description of the maintenance performed; and (v) information system components/equipment removed or replaced (including identification numbers, if applicable). The level of detail included in maintenance records can be informed by the security categories of organizational information systems. Organizations consider supply chain issues associated with replacement components for information systems.	59.1. Describe how the organization manages the system and laptop maintenance process, including how it is scheduled, performed, and documented, and whether it is performed remotely or local, etc. 59.2. Describe how the potential impact to security controls is determined after each maintenance cycle, including verification that the controls are still functioning properly following maintenance or repair actions. 59.3. What happens if a computer needs to be taken offsite for maintenance? Is there a process for this?

Control type: Maintenance				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
Maintenance personnel	**Minimum**	Has the organization established a process for maintenance personnel authorization; maintained a current list of authorized maintenance organizations or personnel; and ensured that personnel performing maintenance on the information system either have the required access authorizations or are supervised by designated organizational personnel with the required access authorizations and technical competence deemed necessary to supervise information system maintenance?	This control applies to individuals performing hardware or software maintenance on organizational information systems, and physical environment controls addresses physical access for individuals whose maintenance duties place them in the physical protection perimeter of the systems (e.g., custodial staff, physical plant maintenance personnel). Technical competence of supervising individuals relates to the maintenance performed on the information systems, and having required access authorizations refers to maintenance on and near the systems. Individuals not previously identified as authorized maintenance personnel, such as IT manufacturers, vendors, systems integrators, and consultants, may require privileged access to organizational information systems, for example, when required to conduct maintenance activities with little or no notice. Based on organizational assessments of risk, organizations may issue temporary credentials to these individuals. Temporary credentials may be for one-time use or for very limited time periods.	60.1. Provide details of the individuals who perform maintenance processes, including a current list of authorized maintenance organizations or personnel, how access to the computers and system to perform these actions is provided, etc.
Non-local maintenance	**Minimum**	Does the organization authorize, monitor, and control non-local	Non-local maintenance and diagnostic activities are those activities conducted	61.1. Are maintenance processes performed by organizational staff?

Control type: Maintenance				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
		maintenance and diagnostic activities; document, in the organizational policy and security plan for the information system, the acceptable conditions for allowing the use of non-local maintenance and diagnostic tools; allow the use of non-local maintenance and diagnostic tools only as consistent with organizational policy and as documented in the security plan; employ strong identification and authentication techniques in the establishment of non-local maintenance and diagnostic sessions; maintain records for non-local maintenance and diagnostic activities; or does the information system in certain cases terminate all sessions and network connections when non-local maintenance or diagnostics is completed?	by individuals communicating through a network, either an external network (e.g., the Internet) or an internal network. Local maintenance and diagnostic activities are those activities carried out by individuals physically present at the information system or information system component and not communicating across a network connection. Typically, strong authentication requires authenticators that are resistant to replay attacks and employ multifactor authentication. Strong authenticators include, for example, PKI where certificates are stored on a token protected by a password, passphrase, or biometric.	If not, please provide details of how third-party entities are authorized to perform maintenance and what types of controls are in place to monitor their services.
Timely maintenance	**Minimum**	Does the organization define security-critical information system components or key IT components for which it will obtain maintenance support or spare parts; define the time period in which support or spare parts should be obtained after a failure; obtain maintenance support or spare	Organizations specify the information system components that result in increased risk to organizational operations and assets, individuals, other organizations, or the nation when the functionality provided by those components is not operational. Organizational actions to obtain	62.1. Describe how often maintenance processes are done. Are they on a regular schedule? Is ad hoc maintenance done in response to critical security flaws in the system or on the laptops? Provide details and documents of the last time this was done.

Control type: Maintenance				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
		parts for the organization-defined list of security-critical information system components or key IT components in the organization-defined time period of failure?	maintenance support typically include having appropriate contracts in place.	
System maintenance policy and procedures	**Minimum**	Has the organization developed and formally documented a system maintenance policy that addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance; disseminated the policy to stakeholders in the organization with associated system maintenance roles and responsibilities; developed and formally documented system maintenance procedures; developed procedures to facilitate implementation of the system maintenance policy and associated system maintenance controls; and disseminated system maintenance procedures to stakeholders in the organization having associated system maintenance roles and responsibilities?	This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the Maintenance family. Policy and procedures reflect applicable laws, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organizational level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or, conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program, in general, and for specific information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.	63.1. Are there documented maintenance policies and procedures? Provide details and documents.

Control type: Media protection				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
Media use	**Minimum**	Does the organization restrict or prohibit the use of types of information system media on their information systems or system components using defined security safeguards?	Information system media includes both digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes, for example, paper and microfilm. This control also applies to mobile devices with information storage capability (e.g., smart phones, tablets, E-readers). This control restricts the use of certain types of media on information systems, for example, restricting or prohibiting the use of flash drives or external hard disk drives. Organizations can employ technical and nontechnical safeguards (e.g., policies, procedures, rules of behavior) to restrict the use of information system media. Organizations may restrict the use of portable storage devices, for example, by using physical cages on workstations to prohibit access to certain external ports, or disabling or removing the ability to insert, read, or write to such devices. Organizations may also limit the use of portable storage devices to approved devices only, including, for example, devices provided by the organization, devices provided by other approved organizations, and devices that are not personally owned.	64.1. Does any of the EHR data stored on media include both digital and non-digital media? Digital media includes, for example, diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes, for example, paper and microfilm (for example, printed reports from the EHR). Provide details and documents. 64.2 Are there any restrictions on what type of media can be used to store data from the EHR? If so, please provide details.

Control type: Media protection				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
			Last, organizations may restrict the use of portable storage devices based on the type of device; for example, prohibiting the use of writeable, portable storage devices, and implementing this restriction by disabling or removing the capability to write to such devices.	
Media access	**Minimum**	Does the organization define digital and non-digital media requiring restricted access, define individuals authorized to access the media, define security measures taken to restrict access, and restrict access to organization-defined information system media to organization-defined authorized individuals using organization-defined security measures?	Information system media includes both digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes, for example, paper and microfilm. Restricting non-digital media access includes, for example, denying access to patient medical records in a community hospital unless the individuals seeking access to such records are authorized healthcare providers. Restricting access to digital media includes, for example, limiting access to design specifications stored on compact disks in the media library to the project leader and the individuals on the development team.	65.1. Describe how individuals are authorized to access the media. Provide details for digital and non-digital media (including printed reports from the EHR). 65.2. Describe security measures taken to restrict media access. Provide details for digital and non-digital media.
Media marking	**Minimum**	Does the organization define removable media types and information system output that require marking; mark	The term security marking refers to the application or use of human-readable security attributes. The term security labeling refers to the application or use	66.1. Describe how both digital and non-digital media are marked, using, for example, human-readable

Control type: Media protection				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
		removable media and information system output in accordance with organizational policies and procedures, indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; define removable media types and information system output exempt from marking, controlled areas designated for retaining removable media and information output exempt from marking, and have removable media and information system output exempt from marking remain in designated controlled areas?	of security attributes with regard to internal data structures in information systems. Information system media includes both digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes, for example, paper and microfilm. Security marking is generally not required for media containing information determined by organizations to be in the public domain or to be publicly releasable. However, some organizations may require markings for public information, indicating that the information is publicly releasable. Marking of information system media reflects applicable laws, directives, policies, regulations, standards, and guidance.	markings, designations for public versus internal release of media, etc.
Media storage	**Minimum**	Does the organization define types of digital and non-digital media physically controlled and securely stored in designated controlled areas, and controlled areas designated to physically control and securely store the media; physically control and securely store organization-defined information system media in organization-defined	Information system media includes both digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes, for example, paper and microfilm. Physically controlling information system media includes, for example, conducting inventories, ensuring that	67.1. Describe how digital and non-digital media are physically controlled and securely stored. Are controlled areas designated to physically control and securely store the media? Provide details for digital and non-digital media.

Control type: Media protection				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
		controlled areas using organization-defined security measures; and protect information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures?	procedures are in place to allow individuals to check out and return media to the media library, and maintaining accountability for all stored media. Secure storage includes, for example, a locked drawer, desk, or cabinet, or a controlled media library. The type of media storage is commensurate with the security category or classification of the information residing on the media. Controlled areas are areas for which organizations provide sufficient physical and procedural safeguards to meet the requirements established for protecting information or information systems. For media containing information determined by organizations to be in the public domain, to be publicly releasable, or to have limited or no adverse impact on organizations or individuals if accessed by other than authorized personnel, fewer safeguards may be needed. In these situations, physical access controls provide adequate protection.	
Media transport	**Minimum**	Does the organization define the types of digital and non-digital media protected and controlled during transport outside of controlled areas, and security measures (e.g., locked container, encryption) for such	Information system media includes both digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes,	68.1. In the event that digital and non-digital media need to be moved, describe how this is done, including security measures taken, personnel assigned to transport the media, etc.

Control type: Media protection				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
		media transported outside controlled areas; protect and control organization-defined information system media during transport outside controlled areas using organization-defined security measures; maintain accountability for information system media during transport outside controlled areas; identify personnel authorized to transport information system media outside controlled areas; and restrict the activities associated with transport of information system media to authorized personnel.	for example, paper and microfilm. This control also applies to mobile devices with information storage capability (e.g., smart phones, tablets, E-readers), that are transported outside controlled areas. Controlled areas are areas or spaces for which organizations provide sufficient physical or procedural safeguards to meet the requirements established for protecting information or information systems. Physical and technical safeguards for media are commensurate with the security category or classification of the information residing on the media. Safeguards to protect media during transport include, for example, locked containers and cryptography. Cryptographic mechanisms can provide confidentiality and integrity protections depending on the mechanisms used. Activities associated with transport include the actual transport and activities such as releasing media for transport and ensuring that media enters the appropriate transport processes. For the actual transport, authorized transport and courier personnel may include individuals from outside the organization. Maintaining accountability of media during transport includes, for example,	

Control type: Media protection				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
			restricting transport activities to authorized personnel, and tracking or obtaining explicit records of transport activities as the media moves through the transportation system to prevent and detect loss, destruction, or tampering. Organizations establish documentation requirements for activities associated with the transport of information system media in accordance with organizational assessments of risk to include the flexibility to define different recordkeeping methods for the different types of media transport as part of an overall system of transport-related records.	
Media sanitization	**Minimum**	Does the organization sanitize information system media, both digital and non-digital, before disposal, release out of organizational control, or release for reuse; and employ sanitization mechanisms with strength and integrity commensurate with the classification or sensitivity of the information?	This control applies to all information system media, both digital and non-digital, subject to disposal or reuse, regardless of whether the media is considered removable. Examples include media found in scanners, copiers, printers, notebook computers, workstations, network components, and mobile devices. The sanitization process removes information from the media such that the information cannot be retrieved or reconstructed. Sanitization techniques, including clearing, purging, cryptographic erase, and destruction, prevent the disclosure of information to unauthorized	69.1. In the event that the media need to be disposed, release for reuse, etc., describe how information system media, both digital and non-digital, are sanitized before disposal or release, including what sanitization mechanisms are used and their associated strength and integrity based on the type of information contained. For example, is PII/PHI sanitized differently than other systems of data? How are printed reports with PII/PHI disposed of?

Control type: Media protection				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
			individuals when such media are reused or released for disposal. Organizations determine the appropriate sanitization methods, recognizing that destruction is sometimes necessary when other methods cannot be applied to the media requiring sanitization. Organizations use discretion on the employment of approved sanitization techniques and procedures for media containing information deemed to be in the public domain or publicly releasable or deemed to have no adverse impact on organizations or individuals if released for reuse or disposal. Sanitization of non-digital media includes, for example, removing a classified appendix from an otherwise unclassified document, or redacting selected sections or words from a document by obscuring the redacted sections or words in a manner equivalent to removing them from the document.	
Media protection policy and procedures	**Minimum**	Has the organization developed and formally documented a media protection policy that addresses purpose, scope, roles and responsibilities, management commitment, and coordination among organizational entities and	This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the Media Protection family. Policy and procedures reflect applicable laws, directives, regulations, policies, standards, and guidance.	70.1. Are there documented media protection policies and procedures? Provide details and documents.

Control type: Media protection				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
		compliance; disseminated the policy to stakeholders in the organization with associated media protection roles and responsibilities; developed and formally documented media protection procedures; developed procedures to facilitate implementation of the media protection policy and associated media protection controls; and disseminated media protection procedures to stakeholders in the organization with associated media protection roles and responsibilities?	Security program policies and procedures at the organizational level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or, conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program, in general, and for specific information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.	

Control type: Physical and environmental protection				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
Physical access authorizations	**Minimum**	Does the organization identify areas in the facility that are publicly accessible; develop and keep current lists of personnel with authorized access to the facility where the information system resides (except for those areas in the	This control applies to organizational employees and visitors. Individuals (e.g., employees, contractors, and others) with permanent physical access authorization credentials are not considered visitors. Authorization credentials include, for example, badges, identification cards, and smart	71.1. Describe how personnel and visitors are granted physical access authorization to enter the area with the computers on which the EHR is installed. 71.2. Is there a designation between physical spaces determined

Control type: Physical and environmental protection				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
		facility officially designated as publicly accessible); issue authorization credentials (e.g., badges, identification cards, smart cards); define the frequency for review and approval of the physical access list and authorization credentials for the facility; review and approve the access list and authorization credentials in accordance with the organization-defined frequency; and remove from the access list personnel no longer requiring access?	cards. Organizations determine the strength of authorization credentials needed (including level of forge-proof badges, smart cards, or identification cards) consistent with government standards, policies, and procedures. This control only applies to areas in facilities that have not been designated as publicly accessible.	appropriate for public access versus those determined as restricted, such as the areas that house the computers that can access the EHR via LAN/WAN or computers on which the EHR is installed?
Physical access control	**Minimum**	Does the organization enforce physical access authorizations for all physical access points (including designated entry/exit points) to the facility where the information system resides (excluding those areas in the facility officially designated as publicly accessible); verify individual access authorizations before granting access to the facility; control entry to the facility containing the information system using physical access devices (e.g., keys, locks, combinations, card readers) or guards; control	This control applies to organizational employees and visitors. Individuals (e.g., employees, contractors, and others) with permanent physical access authorization credentials are not considered visitors. Organizations determine the types of facility guards needed, including, for example, professional physical security staff or other personnel, such as administrative staff or information system users. Physical access devices include, for example, keys, locks, combinations, and card readers. Safeguards for publicly accessible areas in organizational facilities include, for example, cameras, monitoring by	72.1. Describe how the organization manages physical access to entry and exit points in buildings where devices with the EHR are installed and used. For example, is entry and exit to the facility containing the EHR controlled using keys, locks, combinations, card readers, guards, etc.?

Control type: Physical and environmental protection				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
		access to areas officially designated as publicly accessible in accordance with the organization's assessment of risk; control access to secure keys, combinations, and other physical access devices; define the frequency for conducting inventories of physical access devices; inventory physical access devices in accordance with the organization-defined frequency; define the frequency of changes to combinations and keys; and change combinations and keys in accordance with the organization-defined frequency, and when keys are lost, combinations are compromised, or individuals are transferred or terminated?	guards, and isolating selected information systems or system components in secured areas. Physical access control systems comply with applicable government laws, directives, policies, regulations, standards, and guidance. Organizations have flexibility in the types of audit logs employed. Audit logs can be procedural (e.g., a written log of individuals accessing the facility and when such access occurred), automated, or some combination thereof. Physical access points can include facility access points, interior access points to information systems or components requiring supplemental access controls, or both. Components of organizational information systems (e.g., workstations, terminals) may be located in areas designated as publicly accessible, with organizations safeguarding access to such devices.	
Access control for transmission medium	**Minimum or Intermediate**	Does the organization control physical access to information system distribution and transmission lines in organizational facilities?	Physical security safeguards applied to information system distribution and transmission lines help prevent accidental damage, disruption, and physical tampering. Physical safeguards may also be necessary to help prevent eavesdropping or in transit modification of unencrypted transmissions. Security safeguards to control physical access to system	73.1. Describe the physical security safeguards that the organization has applied to information system wires and cables to help prevent accidental damage, disruption, and physical tampering. Security safeguards to control physical access to system distribution and transmission lines include, for example: (i) locked wiring closets, (ii) disconnected or

Control type: Physical and environmental protection				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
			distribution and transmission lines include, for example: (i) locked wiring closets, (ii) disconnected or locked spare jacks, and (iii) protection of cabling by conduit or cable trays.	locked spare jacks, and (iii) protection of cabling by conduit or cable trays.
Access control for output devices	**Minimum**	Does the organization control physical access to information system output devices to prevent unauthorized individuals from obtaining the output?	Controlling physical access to output devices includes, for example, placing output devices in locked rooms or other secured areas and allowing access to authorized individuals only, and placing output devices in locations that can be monitored by organizational personnel. Monitors, printers, copiers, scanners, facsimile machines, and audio devices are examples of information system output devices.	74.1. Describe how physical access to information system output devices is controlled to prevent unauthorized individuals from obtaining the outputs that are connected to laptops with the EHR being used or accessed. Monitors, printers, copiers, scanners, facsimile machines, and audio devices are examples of information system output devices. For example, how is access to printers that print reports from the EHR controlled?
Monitoring physical access	**Minimum**	Does the organization monitor physical access to the information system to detect and respond to physical security incidents; define the frequency to review physical access logs; review physical access logs in accordance with the organization-defined frequency; and coordinate results of reviews and investigations with the organization's incident response capability?	Organizational incident response capabilities include investigations of and responses to detected physical security incidents. Security incidents include, for example, apparent security violations or suspicious physical access activities. Suspicious physical access activities include, for example: (i) accesses outside of normal work hours, (ii) repeated accesses to areas not normally accessed, (iii) accesses for unusual lengths of time, and (iv) out-of-sequence accesses.	75.1. Describe how physical access to the computers and the EHR are monitored to detect and respond to physical security incidents. Security incidents include, for example, apparent security violations or suspicious physical access activities. Suspicious physical access activities include, for example: (i) accesses outside of normal work hours, (ii) repeated accesses to areas not normally accessed, (iii) accesses for unusual lengths of time, and (iv) out-of-sequence accesses.

Control type: Physical and environmental protection				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
Power equipment and cabling	**Minimum**	Does the organization protect power equipment and power cabling for the information system from damage and destruction?	Organizations determine the types of protection necessary for power equipment and cabling employed at different locations both internal and external to organizational facilities and environments of operation. This includes, for example, generators and power cabling outside buildings, internal cabling and uninterruptable power sources in an office or data center, and power sources for self-contained entities, such as vehicles and satellites.	76.1. Describe how power equipment and power cabling that supports the system are protected from damage and destruction. Such equipment and cabling includes, for example, generators and power cabling outside buildings and internal cabling and uninterruptable power sources in an office or data center.
Emergency shutoff	**Intermediate**	Has the organization provided the capability of shutting off power to the information system or individual system components in emergency situations; defined the location of emergency shutoff switches or devices by information system or system component; placed emergency shutoff switches or devices in an organization-defined location by information system or system component to facilitate safe and easy access for personnel; and protected the emergency power shutoff capability from unauthorized activation?	This control applies primarily to facilities containing concentrations of information system resources, including, for example, data centers, server rooms, and mainframe computer rooms.	77.1. If an emergency situation occurs to the physical location, is there a way to perform an emergency shut off of power to the system? Provide details.

Control type: Physical and environmental protection				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
Emergency power	**Minimum**	Does the organization provide a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system in the event of a primary power source loss?	This control applies primarily to facilities containing concentrations of information system resources, for example, data centers, server rooms, and mainframe computer rooms.	78.1. In case of an emergency situation resulting in a power failure, does the organization provide a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system in the event of a primary power source loss? Provide details.
Emergency lighting	**Minimum or Intermediate**	Does the organization employ automatic emergency lighting for the information system that activates in the event of a power outage or disruption; employ automatic emergency lighting for the information system that covers emergency exits and evacuation routes in the facility; and maintain the automatic emergency lighting for the information system?	This control applies primarily to facilities containing concentrations of information system resources, including, for example, data centers, server rooms, and mainframe computer rooms.	79.1. In case of an emergency situation resulting in a power failure, is there provision of emergency lighting that activates in the event of a power outage or disruption in the physical location where the system is being used/accessed, including server rooms?
Fire protection	**Minimum**	Does the organization employ fire suppression and detection devices/systems for the information system that are supported by an independent energy source, and maintain fire suppression and detection devices/systems for the information system that are supported by an independent energy source?	This control applies primarily to facilities containing concentrations of information system resources, including, for example, data centers, server rooms, and mainframe computer rooms. Fire suppression and detection devices/systems include, for example, sprinkler systems, handheld fire extinguishers, fixed fire hoses, and smoke detectors.	80.1. Are fire suppression and detection devices/systems available that are supported by an independent energy source in case of a fire incident?

Control type: Physical and environmental protection				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
Temperature and humidity controls	**Minimum or Intermediate**	Does the organization define acceptable temperature and humidity levels in the facility where the information system resides; maintain temperature and humidity levels in the facility where the information system resides in accordance with organization-defined acceptable levels; define the frequency to monitor the temperature and humidity levels; and monitor the temperature and humidity levels in the facility where the information system resides in accordance with the organization-defined frequency?	This control applies primarily to facilities containing concentrations of information system resources, for example, data centers, server rooms, and mainframe computer rooms.	81.1. Are there mechanisms to maintain temperature and humidity levels in the facility where the information system resides to ensure optimal system operation?
Water damage protection	**Minimum or Intermediate**	Does the organization protect the information system from damage resulting from water leakage by providing master shutoff valves that are accessible and working properly, and assign key personnel in the organization to have knowledge of the master water shutoff valves?	This control applies primarily to facilities containing concentrations of information system resources, including, for example, data centers, server rooms, and mainframe computer rooms. Isolation valves can be employed in addition to or in lieu of master shutoff valves to shut off water supplies in specific areas of concern, without affecting entire organizations.	82.1. Are there mechanisms to protect the information system from damage resulting from water leakage; for example, by providing master shutoff valves that are accessible and working properly in the room where the information system is installed (e.g., server room)?
Delivery and removal	**Minimum**	Does the organization define the types of information system components to be authorized,	Effectively enforcing authorizations for entry and exit of information system components may require restricting	83.1. Describe how the EHR data and artifacts are managed, authorized, monitored, and controlled as they

Control type: Physical and environmental protection				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
		monitored, and controlled as such components are entering or exiting the facility; authorize, monitor, and control organization-defined information system components entering and exiting the facility; and maintain records of information system components entering and exiting the facility?	access to delivery areas and possibly isolating the areas from the information system and media libraries.	enter and exit the facility. Are records maintained for this? Provide details.
Physical and environmental protection policy and procedures	**Intermediate**	Has the organization developed and formally documented a physical and environmental protection policy that addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance; disseminated the policy to stakeholders in the organization with associated physical and environmental protection roles and responsibilities; developed and formally documented physical and environmental protection procedures; developed procedures to facilitate implementation of the physical and environmental protection policy and associated physical and environmental protection controls; and disseminated	This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the Physical and Environmental Protection family. Policy and procedures reflect applicable laws, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organizational level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or, conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program, in general, and for specific information systems, if needed. The organizational risk management	84.1. Are there documented physical and environmental protection policies and procedures? Provide details and documents.

Control type: Physical and environmental protection				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
		physical and environmental protection procedures to stakeholders in the organization with associated physical and environmental protection roles and responsibilities?	strategy is a key factor in establishing policy and procedures.	

Control type: Personnel security				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
Position risk designation	**Intermediate**	Does the organization assign a risk designation to all positions in the organization; establish screening criteria for individuals filling organizational positions; define the frequency of risk designation reviews and updates for organizational positions; and review and revise position risk designations in accordance with the organization-defined frequency?	Risk designations can guide and inform the types of authorizations individuals receive when accessing organizational information and information systems. Position screening criteria include explicit information security role appointment requirements (e.g., training, security clearances).	85.1. Describe how risk designation is assigned to all personnel in the organization. For example, are different roles and positions in the organization assessed for risk of how often and how much information they need to access from the system (e.g., system administrators may have a high-risk designation because they have the most access to the system)?
Personnel screening	**Minimum**	Does the organization screen individuals before authorizing access to the information system; define conditions	Personnel screening and rescreening activities reflect applicable laws, directives, regulations, policies, standards, guidance, and specific criteria established for the risk	86.1. Describe how screening of individuals before granting access to the information system is done.

Control type: Personnel security				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
		requiring rescreening and, where rescreening is so indicated, the frequency of such rescreening; rescreen individuals according to organization-defined conditions requiring rescreening and, where rescreening is so indicated, the organization-defined frequency of such rescreening?	designations of assigned positions. Organizations may define different rescreening conditions and frequencies for personnel accessing information systems based on the types of information processed, stored, or transmitted by the systems.	
Personnel transfer	**Minimum**	Does the organization review logical and physical access authorizations to information systems or facilities when personnel are reassigned or transferred to other positions in the organization; define the transfer or reassignment actions and the time period in which the actions should occur following formal transfer or reassignment; and initiate the organization-defined transfer or reassignment actions in an organization-defined time period following formal transfer or reassignment?	This control applies when reassignments or transfers of individuals are permanent or of such extended duration as to make the actions warranted. Organizations define actions appropriate for the types of reassignments or transfers, whether permanent or extended. Actions that may be required for personnel transfers or reassignments to other positions in organizations include, for example: (i) returning old and issuing new keys, identification cards, and building passes; (ii) closing information system accounts and establishing new accounts; (iii) changing information system access authorizations (i.e., privileges); and (iv) providing for access to official records to which individuals had access at previous work locations and in previous information system accounts.	87.1. Describe what happens to an individual's access to the EHR when reassigned or transferred to a different position in the organization or to a different facility.

Control type: Personnel security				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
Third-party personnel security	**Minimum**	Does the organization have established personnel security requirements, including security roles and responsibilities, for third-party providers; have documented personnel security requirements for third-party providers; and monitor third-party provider compliance with personnel security requirements?	Third-party providers include, for example, service bureaus, contractors, and other organizations providing information system development, IT services, outsourced applications, and network and security management. Organizations explicitly include personnel security requirements in acquisition-related documents. Third-party providers may have personnel working at organizational facilities with credentials, badges, or information system privileges issued by organizations. Notifications of third-party personnel changes ensure the appropriate termination of privileges and credentials. Organizations define the transfers and terminations deemed reportable by security-related characteristics that include, for example, functions, roles, and the nature of credentials/privileges associated with individuals transferred or terminated.	88.1. Describe personnel security requirements for third-party providers. For example, what happens when an employee of a third-party provider leaves the provider but previously had access to the system? How is the access removed?
Personnel security policy and procedures	**Minimum or intermediate**	Has the organization developed and formally documented personnel security policy that addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance; disseminated the policy to stakeholders in the organization with associated	This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the Personnel Security family. Policy and procedures reflect applicable laws, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organizational level may make the need for system-specific policies and procedures unnecessary. The	89.1. Are there documented personnel security policies and procedures? Provide details and documents.

Control type: Personnel security				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
		personnel security roles and responsibilities; developed and formally documented personnel security procedures; developed procedures to facilitate implementation of the personnel security policy and associated personnel security controls; and disseminated personnel security procedures to stakeholders in the organization with associated personnel security roles and responsibilities?	policy can be included as part of the general information security policy for organizations or, conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program, in general, and for specific information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.	

Control type: Planning				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
System security plan	**Minimum**	Has the organization developed a security plan for the information system that is consistent with the organization's enterprise architecture; that explicitly defines the authorization boundary for the system; describes the operational context of the information system in terms of mission and business processes; provides the security	Security plans relate security requirements to a set of security controls and control enhancements. Security plans also describe, at a high level, how the security controls and control enhancements meet those security requirements, but do not provide detailed, technical descriptions of the specific design or implementation of the controls or enhancements. Security plans contain sufficient information	90.1. Does the organization have an overall security plan that provides security requirements to a set of security controls and control enhancements? A security plan describes, at a high level, how the security controls and control enhancements meet those security requirements,

Control type: Planning				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
		categorization of the information system, including the supporting rationale; describes the operational environment for the information system; describes the relationships with or connections to other information systems; provides an overview of the security requirements for the system; describes the security controls in place or planned for meeting those requirements, including a rationale for tailoring and supplemental decisions, and is reviewed and approved by the authorizing official or designated representative before plan implementation; defined the frequency of security plan reviews; reviewed the security plan in accordance with the organization-defined frequency; updated the plan to address changes to the information system or environment of operations or problems identified during plan implementation or security control assessments?	(including the specification of parameter values for assignment and selection statements, either explicitly or by reference) to enable a design and implementation that is unambiguously compliant with the intent of the plans and subsequent determinations of risk to organizational operations and assets, individuals, other organizations, and the nation if the plan is implemented as intended. Security plans need not be single documents; the plans can be a collection of various documents, including documents that already exist. Effective security plans make extensive use of references to policies, procedures, and additional documents (e.g., design and implementation specifications) in which more detailed information can be obtained. This reduces the documentation requirements associated with security programs and maintains security-related information in other established management and operational areas related to enterprise architecture, system development life cycle, systems engineering, and acquisition. For example, security plans do not contain detailed contingency plan or incident response plan information, but instead provide, explicitly or by reference, sufficient information to define what needs to be accomplished by those plans.	but does not provide detailed, technical descriptions of the specific design or implementation of the controls or enhancements.

Control type: Planning				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
Rules of behavior	**Minimum**	Has the organization established the rules that describe the information system users' responsibilities and expected behavior for information and information system usage; made the rules available to all information system users; and received a signed acknowledgement from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system?	This control enhancement applies to organizational users. Organizations consider rules of behavior based on individual user roles and responsibilities, differentiating, for example, between rules that apply to privileged users and rules that apply to general users. Establishing rules of behavior for some types of non-organizational users, including, for example, individuals who simply receive data/information from government information systems, is often not feasible, given the large number of such users and the limited nature of their interactions with the systems. The signed acknowledgment portion of this control may be satisfied by the security awareness training and role-based security training programs conducted by organizations, if such training includes rules of behavior. Organizations can use electronic signatures for acknowledging rules of behavior.	91.1. Describe how rules that describe information system user responsibilities and expected behavior for information and information system usage are established. 91.2. Is a signed acknowledgement from users received indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system?
Information security architecture	**Intermediate**	Has the organization developed an information security architecture for the information system that describes the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of organizational information; describes how the information	This control addresses actions taken by organizations in the design and development of information systems. The information security architecture at the individual information system level is consistent with and complements the more global, organization-wide information security architecture described that is integral to and developed as part of the enterprise	92.1. Describe the information security architecture (i.e., overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of organizational information).

Control type: Planning				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
		security architecture is integrated in and supports the enterprise architecture; and describes any information security assumptions about, and dependencies on, external services; reviewed and updated the information security architecture to reflect updates in the enterprise architecture; ensured that planned information security architecture changes are reflected in the security plan, and organizational procurements and acquisitions?	architecture. The information security architecture includes an architectural description, the placement/allocation of security functionality (including security controls), security-related information for external interfaces, information being exchanged across the interfaces, and the protection mechanisms associated with each interface. The security architecture can also include other important security-related information, such as user roles and access privileges assigned to each role, unique security requirements, the types of information processed, stored, and transmitted by the information system, restoration priorities of information and information system services, and any other specific protection needs. In today's modern architecture, it is becoming less common for organizations to control all information resources. There are going to be key dependencies on external information services and service providers. Describing such dependencies in the information security architecture is important to developing a comprehensive mission/business protection strategy. Establishing, developing, documenting, and maintaining under configuration control, a baseline configuration for organizational information systems is critical to implementing and maintaining	

Control type: Planning				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
			an effective information security architecture.	
Security planning policy and procedures	**Intermediate**	Has the organization developed and formally documented a security planning policy that addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance; disseminated the policy to stakeholders in the organization with associated security planning roles and responsibilities; developed and formally documented security planning procedures; developed procedures to facilitate implementation of the security planning policy and associated security planning controls; and disseminated security planning procedures to stakeholders in the organization with associated security planning roles and responsibilities?	This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the Planning family. Policy and procedures reflect applicable laws, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organizational level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or, conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program, in general, and for specific information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.	93.1. Are there documented security plans, information security architecture, expected user behavior policies, and procedures? Provide details and documents.

Control type: Risk assessment				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
Security categorization	**Intermediate**	Does the organization categorize information and the information system in accordance with applicable laws, directives, policies, regulations, standards, and guidance; document the security categorization results (including supporting rationale) in the security plan for the information system; have an authorized official or authorizing official designated representative who reviews and approves the security categorization decision?	Clearly defined authorization boundaries are a prerequisite for effective security categorization decisions. Security categories describe the potential adverse impacts to organizational operations, organizational assets, and individuals if organizational information and information systems are compromised through a loss of confidentiality, integrity, or availability. Organizations conduct the security categorization process as an organization-wide activity with the involvement of chief information officers, senior information security officers, information system owners, mission/business owners, and information owners/stewards. Organizations also consider the potential adverse impact to other organizations and potential national-level adverse impacts. Security categorization processes carried out by organizations facilitate the development of inventories of information assets, and mappings to specific information system components where information is processed, stored, or transmitted.	94.1. Describe how security categorization of information and the information system is done. Security categories describe the potential adverse impact to organizational operations, organizational assets, and individuals if organizational information and information systems are compromised through a loss of confidentiality, integrity, or availability.
Risk assessment	**Intermediate**	Does the organization conduct an assessment of risk of the information system and the information it processes, stores, or transmits that includes the likelihood and magnitude of harm from unauthorized access, use, disclosure, disruption,	Clearly defined authorization boundaries are a prerequisite for effective risk assessments. Risk assessments take into account threats, vulnerabilities, likelihood, and impact to organizational operations and assets, individuals, other organizations, and the nation, based on the operation and use of information systems. Risk	95.1. Describe how risk assessment of the information system and the information it processes, stores, or transmits is done, including the likelihood and magnitude of harm from unauthorized access, use, disclosure,

Control type: Risk assessment				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
		modification, and destruction; define the document in which risk assessment results are documented, selecting from the security plan, risk assessment report, or other organization-defined document; document risk assessment results in the organization-defined document; define the frequency for review of the risk assessment results; review risk assessment results in accordance with the organization-defined frequency; define the frequency that risk assessments are updated; and update the risk assessment in accordance with the organization-defined frequency or when there are significant changes to the information system or environment of operation, or other conditions that may impact the security state of the system?	assessments also take into account risk from external parties (e.g., service providers, contractors operating information systems on behalf of the organization, individuals accessing organizational information systems, outsourcing entities). Risk assessments (either formal or informal) can be conducted at all three tiers in the risk management hierarchy (i.e., organization level, mission/business process level, or information system level) and at any phase in the system development life cycle. Risk assessments can also be conducted at various steps in the Risk Management Framework, including categorization, security control selection, security control implementation, security control assessment, information system authorization, and security control monitoring. Risk assessments can play an important role in security control selection processes, especially during the application of tailoring guidance, which includes security control supplementation.	disruption, modification, or destruction. Provide details and documents. 95.2. If there are risk assessments of the system, how often are they conducted? What tools are used?
Vulnerability scanning	**Intermediate**	Does the organization define the frequency for conducting vulnerability scans on the information system and hosted applications, or an organization-defined process for conducting random vulnerability scans on the information system and hosted	Security categorization of information systems guides the frequency and comprehensiveness of vulnerability scans. Organizations determine the required vulnerability scanning for all information system components, ensuring that potential sources of vulnerabilities, such as networked printers, scanners, and copiers,	96.1. Has a vulnerability scan ever been performed on the information system? Vulnerability scanning includes, for example: (i) scanning for patch levels; (ii) scanning for functions, ports, protocols, and services that

Control type: Risk assessment				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
		applications; scan for vulnerabilities in the information system and hosted applications in accordance with the organization-defined frequency or the organization-defined process for random scans; scan for vulnerabilities in the information system and hosted applications when new vulnerabilities potentially affecting the system/applications are identified and reported; employ vulnerability scanning tools and techniques that use standards to promote interoperability among tools and automate parts of the vulnerability management process that focus on enumerating platforms, software flaws, and improper configurations; formatting and making transparent checklists and test procedures; measuring vulnerability impact; and analyze vulnerability scan reports and results from security control assessments?	are not overlooked. Vulnerability analyses for custom software applications may require additional such approaches as static analysis, dynamic analysis, binary analysis, or a hybrid of the three approaches. Organizations can employ these analysis approaches in a variety of tools (e.g., web-based application scanners, static analysis tools, binary analyzers) and in source code reviews. Vulnerability scanning includes, for example: (i) scanning for patch levels; (ii) scanning for functions, ports, protocols, and services that should not be accessible to users or devices; and (iii) scanning for improperly configured or incorrectly operating information flow control mechanisms. In addition, security control assessments, such as red team exercises, provide other sources of potential vulnerabilities for which to scan.	should not be accessible to users or devices; and (iii) scanning for improperly configured or incorrectly operating information flow control mechanisms. Provide details and documents of results of these scans. 96.2. If a vulnerability scan has been done, how often are vulnerability scans performed on the system?
Risk assessment policy and procedures	**Intermediate**	Has the organization developed and formally documented a risk assessment policy that addresses purpose, scope, roles and	This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the	97.1. Are there documented risk assessment policies and procedures? Provide details and documents.

Control type: Risk assessment				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
		responsibilities, management commitment, coordination among organizational entities, and compliance; disseminated the policy to stakeholders in the organization with associated risk assessment roles and responsibilities; developed and formally documented risk assessment procedures; developed procedures to facilitate implementation of the risk assessment policy and associated risk assessment controls; and disseminated risk assessment procedures to stakeholders in the organization with associated risk assessment roles and responsibilities?	Risk Assessment family. Policy and procedures reflect applicable laws, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organizational level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or, conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program, in general, and for specific information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.	

Control type: Security assessment and authorization				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
Security assessments	**Minimum**	Has the organization developed a security assessment plan for the information system that describes the scope of the assessment, including security	Organizations assess security controls in organizational information systems and the environments in which those systems operate as part of: (i) initial and ongoing security authorizations, (ii) annual assessments, (iii) continuous monitoring,	98.1. Has a security assessment of the system ever been done (e.g., something similar to this assessment)? If yes, provide details and documents of results

Control type: Security assessment and authorization				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
		controls and control enhancements under assessment, assessment procedures to be used to determine security control effectiveness, and assessment environment, assessment team, and assessment roles and responsibilities; defined the frequency of assessing the security controls in the information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system; assessed the security controls in the information system at the organization-defined frequency; produced a security assessment report that documents the results of the security control assessment and that the results of the security control assessment are provided in writing to the authorizing official or authorizing official designated representative?	and (iv) system development life cycle activities. Security assessments do the following: (i) ensure that information security is built into organizational information systems; (ii) identify weaknesses and deficiencies early in the development process; (iii) provide essential information needed to make risk-based decisions as part of security authorization processes; and (iv) ensure compliance with vulnerability mitigation procedures. Organizations can use other types of assessment activities, such as vulnerability scanning and system monitoring, to maintain the security posture of information systems during the entire life cycle. Security assessment reports document assessment results in sufficient detail as deemed necessary by organizations to determine the accuracy and completeness of the reports, and whether the security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting security requirements. Security assessment results are provided to the individuals or roles appropriate for the types of assessments being conducted. For example, assessments conducted in support of security authorization decisions are provided to authorizing officials or authorizing official designated	of these assessments. How frequently is this done?

Control type: Security assessment and authorization				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
			representatives. To satisfy annual assessment requirements, organizations can use assessment results from the following sources: (i) initial or ongoing information system authorizations; (ii) continuous monitoring; or (iii) system development life cycle activities. Organizations ensure that security assessment results are current, relevant to the determination of security control effectiveness, and obtained with the appropriate level of assessor independence. Existing security control assessment results can be reused to the extent that the results are still valid and can also be supplemented with additional assessments as needed. Subsequent to initial authorizations, organizations assess security controls during continuous monitoring. Organizations establish the frequency for ongoing security control assessments in accordance with organizational continuous monitoring strategies. External audits (e.g., audits by external entities such as regulatory agencies) are outside the scope of this control.	
System interconnections	**Advanced**	Does the organization identify connections to external information systems (i.e., information systems outside the authorization boundary); authorize connections from the	This control applies to dedicated connections between information systems (i.e., system interconnections) and does not apply to transitory, user-controlled connections, such as e-mail and website browsing. Organizations	99.1. Describe how connections to external information systems (i.e., information systems outside the authorization boundary) are identified.

Control type: Security assessment and authorization				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
		information system to external information systems through the use of Interconnection Security Agreements; document, for each connection, the interface characteristics, security requirements, and the nature of the information communicated; and monitor the information system connections on an ongoing basis to verify enforcement of security requirements?	carefully consider the risks that may be introduced when information systems are connected to other systems with different security requirements and security controls, both in organizations and external to organizations. Authorizing officials determine the risk associated with information system connections and the appropriate controls employed. If interconnecting systems have the same authorizing official, organizations do not need to develop Interconnection Security Agreements. Instead, organizations can describe the interface characteristics between those interconnecting systems in their respective security plans. If interconnecting systems have different authorizing officials in the same organization, organizations can either develop Interconnection Security Agreements or describe the interface characteristics between systems in the security plans for the respective systems. Organizations may also incorporate Interconnection Security Agreement information into formal contracts, especially for interconnections established between government agencies and nongovernmental (i.e., private sector) organizations. Risk considerations also include information systems sharing the same networks. For	99.2. How are these connections authorized from the information system to the external information systems (e.g., through the use of Interconnection Security Agreements)? 99.3. How are the connections monitored on an ongoing basis to verify enforcement of security requirements? 99.4. Is there documentation for each connection that includes the interface characteristics, security requirements, and the nature of the information communicated? Provide details and documents.

Control type: Security assessment and authorization				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
			certain technologies (e.g., space, unmanned aerial vehicles, and medical devices), there may be specialized connections in place during preoperational testing. Such connections may require Interconnection Security Agreements and be subject to additional security controls.	
Security authorization	**Advanced**	Has the organization assigned a senior-level executive or manager to the role of authorizing official for the information system, and has the authorizing official authorized the information system for processing before commencing operations; defined the frequency of security authorization updates; and updated the security authorization in accordance with an organization-defined frequency?	Security authorizations are official management decisions, conveyed through authorization decision documents, by senior organizational officials or executives (i.e., authorizing officials) to authorize operation of information systems and to explicitly accept the risk to organizational operations and assets, individuals, other organizations, and the nation based on the implementation of agreed-on security controls. Authorizing officials provide budgetary oversight for organizational information systems or assume responsibility for the mission/business operations supported by those systems. Through the security authorization process, authorizing officials assume responsibility and are accountable for security risks associated with the operation and use of organizational information systems. Accordingly, authorizing officials are in positions with levels of authority commensurate with understanding and	100.1. Describe who gave official authorization of the information system for processing before commencing operations was done. Provide details and documents.

Control type: Security assessment and authorization				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
			accepting such information security-related risks. Continuous monitoring programs can satisfy three-year reauthorization requirements, so separate reauthorization processes are not necessary. Through the employment of comprehensive continuous monitoring processes, critical information contained in authorization packages (i.e., security plans, security assessment reports, and plans of action and milestones) is updated on an ongoing basis, providing authorizing officials and information system owners with an up-to-date status of the security state of organizational information systems and environments of operation. To reduce the administrative cost of security reauthorization, authorizing officials use the results of continuous monitoring processes to the maximum extent possible as the basis for rendering reauthorization decisions.	
Continuous monitoring	**Intermediate**	Does the organization establish a continuous monitoring strategy and program; define the frequency for reporting the security state of the information system to appropriate organizational officials; define organizational officials to whom the security state of the information system should be reported; implement	Continuous monitoring programs facilitate ongoing awareness of threats, vulnerabilities, and information security to support organizational risk management decisions. The terms continuous and ongoing imply that organizations assess and analyze security controls and information security-related risks at a frequency sufficient to support organizational risk-based decisions. The results of continuous monitoring programs	101.1. Describe how continuous monitoring of threats, vulnerabilities, and information security is done, including the frequency for reporting the security state of the information system to appropriate organizational officials, organizational officials to whom the security state of the information system should be

Control type: Security assessment and authorization				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
		a continuous monitoring program that includes a configuration management process for the information system and its constituent components, a determination of the security impact of changes to the information system and environment of operation; ongoing security control assessments in accordance with the organization's continuous monitoring strategy, and reporting the security state of the information system to appropriate organizational officials in accordance with organization-defined frequency?	generate appropriate risk response actions by organizations. Continuous monitoring programs also allow organizations to maintain the security authorizations of information systems and common controls over time in highly dynamic environments of operation with changing mission/business needs, threats, vulnerabilities, and technologies. Having access to security-related information on a continuing basis through reports and dashboards gives organizational officials the capability to make more effective and timely risk management decisions, including ongoing security authorization decisions. Automation supports more frequent updates to security authorization packages, hardware/software/firmware inventories, and other system information. Effectiveness is further enhanced when continuous monitoring outputs are formatted to provide information that is specific, measurable, actionable, relevant, and timely. Continuous monitoring activities are scaled in accordance with the security categories of information systems.	reported, how configuration management is done, how security impact of changes to the information system and environment of operation is done, how ongoing security control assessments are done, and how reporting of the security state of the information system to appropriate organizational officials is done. 101.2. What tools are used for continuous monitoring (e.g., a tool that monitors the Wi-Fi network to detect any unauthorized connections)?
Penetration testing	**Advanced**	Does the organization conduct penetration testing on organization-defined information systems or system components?	Penetration testing is a specialized type of assessment conducted on information systems or individual system components to identify vulnerabilities that could be exploited by adversaries. Such testing	102.1. Has penetration testing ever been performed on the system? Penetration testing is a specialized type of assessment conducted on a system to

Control type: Security assessment and authorization				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
			can be used to either validate vulnerabilities or determine the degree of resistance organizational information systems have to adversaries in a set of specified constraints (e.g., time, resources, skills). Penetration testing attempts to duplicate the actions of adversaries in carrying out hostile cyberattacks against organizations and provides a more in-depth analysis of security-related weaknesses and deficiencies. Organizations can also use the results of vulnerability analyses to support penetration testing activities. Penetration testing can be conducted on the hardware, software, or firmware components of an information system and can exercise both physical and technical security controls. A standard method for penetration testing includes, for example: (i) pretest analysis based on full knowledge of the target system; (ii) pretest identification of potential vulnerabilities based on pretest analysis; and (iii) testing designed to determine the exploitability of identified vulnerabilities. All parties agree to the rules of engagement before the commencement of penetration testing scenarios. Organizations correlate the penetration testing rules of engagement with the tools, techniques, and procedures that are anticipated to be	identify vulnerabilities that could be exploited by adversaries. Such testing can be used to either validate vulnerabilities or determine the degree of resistance organizational information systems have to adversaries in a set of specified constraints (e.g., time, resources, skills). The difference between penetration testing and vulnerability testing is that penetration testing simulates an attack on the system using hacking methods to discover other unknown vulnerabilities, and vulnerability testing examines what known system vulnerabilities exist.

Control type: Security assessment and authorization				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
			employed by adversaries carrying out attacks. Organizational risk assessments guide decisions on the level of independence required for personnel conducting penetration testing.	
Internal system connections	**Intermediate**	Does the organization authorize internal connections of organization-defined information system components/classes of components to the information system; and document, for each internal connection, the interface characteristics, security requirements, and the nature of the information communicated?	This control applies to connections between organizational information systems and (separate) constituent system components (i.e., intra-system connections), including, for example, system connections with mobile devices, notebook/desktop computers, printers, copiers, facsimile machines, scanners, sensors, and servers. Instead of authorizing each individual internal connection, organizations can authorize internal connections for a class of components with common characteristics or configurations (e.g., all digital printers, scanners, and copiers with a specified processing, storage, and transmission capability or all smart phones with a specific baseline configuration).	103.1. Describe any internal connection to internal components, their interface characteristics, security requirements, and the nature of the information communicated. Internal connections are connections between the EHR and other internal components (e.g., mobile devices, notebook/desktop computers, printers, copiers, facsimile machines, scanners, sensors, servers). For example, if the EHR connects to a printer via an unsecured Wi-Fi, then information being sent from the EHR to the printer is unsecure. Interface characteristics could be secure connections, use of certificates, etc. 103.2. **Instructions to assessors:** At each facility, note any components, systems, or devices that interconnect with the EHR or the laptop where it is being used or accessed, and

Control type: Security assessment and authorization				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
				examine the interface characteristics of that connection (e.g., the Wi-Fi settings of the connection with the printer).
Security assessment and authorization policy and procedures	**Intermediate**	Has the organization developed and formally documented a security assessment and authorization policy that addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance; disseminated the formal policy to stakeholders in the organization; developed and formally documented procedures to facilitate implementation of the security assessment and authorization policy and associated security assessment and authorization controls; disseminated the formal documented procedures to stakeholders in the organization who have associated security assessment and authorization roles and responsibilities?	This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the Control Access family. Policy and procedures reflect applicable laws, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organizational level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or, conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program, in general, and for specific information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.	104.1. Are there documented security assessment and authorization policies and procedures? Provide details and documents.

Instructions to assessors: Many of the questions in this section should be answered by:

- **Developers of the EHR**
- **Organizational IT staff** only, that is, staff not necessarily at the facility; those not highlighted in green.

Control type: System and communications protection				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
Application partitioning	**Intermediate**	Does the EHR separate user functionality (including user interface services) from information system management functionality?	Information system management functionality includes, for example, functions necessary to administer databases, network components, workstations, or servers, and typically requires privileged user access. The separation of user functionality from information system management functionality is either physical or logical. Organizations implement the separation of system management-related functionality from user functionality by using different computers, different central processing units, different instances of operating systems, different network addresses, virtualization techniques, or combinations of these or other methods, as appropriate. This type of separation includes, for example, web administrative interfaces that use separate authentication methods for users of any other information system resources. Separation of system and user functionality may include isolating administrative interfaces on different domains and with additional access controls.	105.1. Describe how the EHR separates user functionality (including user interface services) from information system management functionality. For example, is the database separated from the front-end of the system?
Security function isolation	**Advanced**	Does the her define the security functions of the information system to be isolated from nonsecurity functions and isolate security functions from nonsecurity functions?	The information system isolates security functions from nonsecurity functions by means of an isolation boundary (implemented via partitions and domains). Such isolation controls access to and protects the integrity of the hardware, software, and firmware that perform those security functions. Information systems	**106.1. Describe how the** EHR defines the security functions of the information system to be isolated from non-security functions, including isolation of security functions from non-security functions.

Control type: System and communications protection				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
			implement code separation (i.e., separation of security functions from non-security functions) in several ways, including, for example, through the provision of security kernels via processor rings or processor modes. For non-kernel code, security function isolation is often achieved through file system protections that serve to protect the code on disk and address space protections that protect executing code. Information systems restrict access to security functions through the use of access control mechanisms and by implementing least privilege capabilities. Although the ideal is for all the code in the security function isolation boundary to only contain security-relevant code, it is sometimes necessary to include non-security functions in the isolation boundary as an exception.	
Denial of service protection	**Advanced**	Does the organization define the types of denial of service attacks (or provide references to sources of current denial of service attacks) that can be addressed by the information system? Does the EHR protect against or limit the effects of the organization-defined or referenced types of denial of service attacks?	A variety of technologies exist to limit or, in some cases, eliminate the effects of denial of service attacks. For example, boundary protection devices can filter certain types of packets to protect information system components on internal organizational networks from being directly affected by denial of service attacks. Employing increased capacity and bandwidth combined with service redundancy may also reduce the susceptibility to denial of service attacks.	107.1. Does the EHR protect against denial service attacks? A denial of service attack is where another entity sends too many requests and overwhelms the system.

Control type: System and communications protection				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
Boundary protection	**Advanced**	Does the organization define the external boundary of the information system and define key internal boundaries of the information system? Does the EHR monitor and control communications at the external boundary of the information system and at key internal boundaries in the system, and connect to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture?	Managed interfaces include, for example, gateways, routers, firewalls, guards, network-based malicious code analysis and virtualization systems, or encrypted tunnels implemented in a security architecture (e.g., routers protecting firewalls or application gateways residing on protected subnetworks). Subnetworks that are physically or logically separated from internal networks are referred to as demilitarized zones. Restricting or prohibiting interfaces in organizational information systems includes, for example, restricting external web traffic to designated web servers in managed interfaces and prohibiting external traffic that appears to be spoofing internal addresses. Organizations consider the shared nature of commercial telecommunications services in the implementation of security controls associated with the use of such services. Commercial telecommunications services are commonly based on network components and consolidated management systems shared by all attached commercial customers, and may also include third-party-provided access lines and other service elements. Such transmission services may represent sources of increased risk despite contract security provisions.	108.1. Describe how external boundaries of the information system are defined, including defining key internal boundaries of the information system versus external ones. For example, if the EHR is connected to a laboratory information system, where does the EHR stop versus the laboratory information start? There is usually an interface in the middle. **108.2. Does the EHR** monitor and control communications at the external boundary of the information system and at key internal boundaries in the system, including connection to external networks or information systems only through managed interfaces consisting of boundary protection? Managed interfaces include, for example, gateways, routers, firewalls, guards, network-based malicious code analysis and virtualization systems, or encrypted tunnels implemented in a security architecture (e.g., routers protecting firewalls or application gateways residing on protected subnetworks).

Control type: System and communications protection				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
				Subnetworks that are physically or logically separated from internal networks are referred to as demilitarized zones. Restricting or prohibiting interfaces in organizational information systems includes, for example, restricting external web traffic to designated web servers in managed interfaces and prohibiting external traffic that appears to be spoofing internal addresses.
Transmission confidentiality and integrity	**Advanced**	Does the EHR protect the integrity of transmitted information?	This control applies to both internal and external networks and all types of information system components from which information can be transmitted (e.g., servers, mobile devices, notebook computers, printers, copiers, scanners, facsimile machines). Communication paths outside the physical protection of a controlled boundary are exposed to the possibility of interception and modification. Protecting the confidentiality and integrity of organizational information can be accomplished by physical means (e.g., by employing protected distribution systems) or by logical means (e.g., employing encryption techniques). Organizations relying on commercial providers offering transmission services as commodity services rather than as fully dedicated services (i.e., services that can be highly specialized to individual customer needs), may find it difficult to obtain the	**109.1. Describe how the EHR** protects the integrity of transmitted information by physical or logical means, such as encryption or protected distribution systems.

Control type: System and communications protection				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
			necessary assurances for the implementation of needed security controls for transmission confidentiality and integrity. In such situations, organizations determine what types of confidentiality and integrity services are available in standard, commercial telecommunication service packages. If it is infeasible or impractical to obtain the necessary security controls and assurances of control effectiveness through appropriate contracting vehicles, organizations implement appropriate compensating security controls or explicitly accept the additional risk.	
Network disconnect	**Intermediate**	Does the organization define the time period of inactivity before the information system terminates a network connection associated with a communications session? Does the EHR terminate a network connection associated with a communication session at the end of the session or after the organization-defined time period of inactivity?	This control applies to both internal and external networks. Terminating network connections associated with communications sessions include, for example, de-allocating associated transmission control protocol/internet protocol address/port pairs at the operating system level, or de-allocating networking assignments at the application level if multiple application sessions are using a single, operating system-level network connection. Time periods of inactivity may be established by organizations and include, for example, time periods by type of network access or for specific network accesses.	110.1. Does the organization define the time period of inactivity before the information system terminates a network connection associated with a communications session? **110.2. Describe how the EHR** terminates a network connection associated with a communication session at the end of the session or after the organization-defined time period of inactivity.
Cryptographic key establishment	**Minimum**	Does the organization establish and manage cryptographic keys for required cryptography	Cryptographic key management and establishment can be performed using manual procedures or automated mechanisms with supporting manual procedures. Organizations	111.1. Describe how system certificates or public/private keys are encrypted and managed. Cryptographic key

Control type: System and communications protection				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
and management		employed in the information system?	define key management requirements in accordance with applicable laws, directives, regulations, policies, standards, and guidance, specifying appropriate options, levels, and parameters. Organizations manage trust stores to ensure that only approved trust anchors are in such trust stores. This includes certificates with visibility external to organizational information systems and certificates related to the internal operations of systems.	management and establishment can be performed using manual procedures or automated mechanisms with supporting manual procedures (e.g., does the organization have a key server to manage keys).
Cryptographic protection	**Intermediate**	Does the EHR implement cryptographic protections using cryptographic modules that comply with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance?	Cryptography can be employed to support a variety of security solutions, including, for example, the protection of classified and controlled unclassified information, the provision of digital signatures, and the enforcement of information separation when authorized individuals have the necessary clearances for such information but lack the necessary formal access approvals. Cryptography can also be used to support random number generation and hash generation. This control does not impose any requirements on organizations to use cryptography. However, if cryptography is required based on the selection of other security controls, organizations define each type of cryptographic use and the type of cryptography required (e.g., protection of classified information, provision of digital signatures).	**112.1. Describe how the EHR** implements cryptographic protections (e.g., does the system use hashing for passwords or encrypt the database at rest). Cryptography can be employed to support a variety of security solutions, including, for example, the protection of restricted/classified and unrestricted/unclassified information, the provision of digital signatures, and the enforcement of information separation when authorized individuals have the necessary clearances for such information but lack the necessary formal access approvals. Cryptography can also be used to support random number

Control type: System and communications protection				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
				generation and hash generation.
Public key infrastructure certificates	**Advanced**	Does the organization define a certificate policy for issuing public key certificates, issue public key certificates under the organization-defined certificate policy, or obtain public key certificates under a certificate policy from an approved service provider?	For all certificates, organizations manage information system trust stores to ensure that only approved trust anchors are in the trust stores. This control addresses both certificates with visibility external to organizational information systems and certificates related to the internal operations of systems (e.g., application-specific time services).	113.1. Does the organization or system have a certificate policy? If so, describe how the certificate policy for issuing public key certificates is defined, including how it obtains public key certificates under a certificate policy from an approved service provider.
Mobile code	**Advanced**	Does the organization have defined acceptable and unacceptable mobile code and mobile code technologies; have established usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies; and authorize, monitor, and control the use of mobile code in the information system?	Decisions about the employment of mobile code in organizational information systems are based on the potential for the code to cause damage to the systems if used maliciously. Mobile code technologies include, for example, Java, JavaScript, ActiveX, Postscript, PDF, Shockwave movies, Flash animations, and VBScript. Usage restrictions and implementation guidance apply to both the selection and use of mobile code installed on servers and mobile code downloaded and executed on individual workstations and devices (e.g., smart phones). Mobile code policy and procedures address preventing the development, acquisition, or introduction of unacceptable mobile code in organizational information systems.	114.1. Describe how acceptable and unacceptable mobile code and mobile code technologies are defined by the system/organization, including usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies. How is the use of mobile code authorized, monitored, and controlled in the system?
Voice over Internet Protocol	**Minimum**	Does the organization have an established usage	Establishes usage restrictions and implementation guidance for Voice over	115.1. Does the system have VoIP, such as automated

Control type: System and communications protection				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
		restrictions and implementation guidance for VoIP technologies based on the potential to cause damage to the information system if used maliciously; and authorize, monitor, and control the use of VoIP in the information system?	Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously; and authorizes, monitors, and controls the use of VoIP within the information system.	voicemail reminders? If so, describe the usage restrictions and implementation guidance for VoIP technologies based on their potential to cause damage to the information system if used maliciously and how these restrictions are implemented, including how the organization authorizes, monitors, and controls the use of VoIP in the information system.
Secure name/ address resolution service (authoritative source)	**Advanced**	Does the EHR provide additional data origin and integrity artifacts along with the authoritative data that the system returns in response to name/address resolution queries?	This control enables external clients, including, for example, remote Internet clients, to obtain origin authentication and integrity verification assurances for the host/service name to network address resolution information obtained through the service. Information systems that provide name and address resolution services include, for example, domain name system (DNS) servers. Additional artifacts include, for example, DNS Security digital signatures and cryptographic keys. DNS resource records are examples of authoritative data. The means to indicate the security status of child zones includes, for example, the use of delegation signer resource records in the DNS. Information systems that use technologies other than the DNS to map between host/service names and network addresses provide other means to ensure the authenticity and integrity of response data.	**116.1. Describe how the EHR** provides additional data origin and integrity artifacts along with the authoritative data that the system returns in response to name/address resolution queries.

Control type: System and communications protection				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
Secure name/ address resolution service (recursive or caching resolver)	**Advanced**	Does the EHR perform data origin authentication and data integrity verification on the name/address resolution responses that the system receives from authoritative sources when requested by client systems.	Each client of name resolution services either performs this validation on its own or has authenticated channels to trusted validation providers. Information systems that provide name and address resolution services for local clients include, for example, recursive resolving or caching DNS servers. DNS client resolvers either perform validation of DNS Security signatures, or clients use authenticated channels to recursive resolvers that perform such validations. Information systems that use technologies other than the DNS to map between host/service names and network addresses provide other means to enable clients to verify the authenticity and integrity of response data.	**117.1. Describe how the EHR** performs data origin authentication and data integrity verification on the name/address resolution responses that the system receives from authoritative sources when requested by client systems.
Session authenticity	**Advanced**	Does the EHR provide mechanisms to protect the authenticity of communications sessions?	This control addresses communications protection at the session, versus packet level (e.g., sessions in service-oriented architectures providing web-based services) and establishes grounds for confidence at both ends of communications sessions in ongoing identities of other parties and in the validity of information transmitted. Authenticity protection includes, for example, protecting against man-in-the-middle attacks/session hijacking and the insertion of false information into sessions.	**118.1. Describe how the EHR** provides mechanisms to protect the authenticity of communications sessions.
Fail in known state	**Advanced**	Does the organization define the known-states the information system should fail to in the event	Failure in a known-state addresses security concerns in accordance with the mission/business needs of organizations. Failure in a known secure state helps prevent the loss	**119.1. Describe how the EHR** defines the known-states the information system should fail to in the event of a system failure,

Control type: System and communications protection				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
		of a system failure; define the types of failures for which the information system should fail to an organization-defined known-state; and define the system state information that should be preserved in the event of a system failure? Does the EHR fail to an organization-defined known-state for an organization-defined type of failure or preserve the organization-defined system state information in the event of a system failure?	of confidentiality, integrity, or availability of information in the event of failures of organizational information systems or system components. Failure in a known safe state helps to prevent systems from failing to a state that may cause injury to individuals or destruction to property. Preserving information system state information facilitates system restart and return to the operational mode of organizations with less disruption of mission/business processes.	including defining the types of failures for which the information system should fail to an organization-defined known-state and the system state information that should be preserved in the event of a system failure. **119.2. In the event of the EHR** failure, describe how it returns to an organization-defined known-state for an organization-defined type of failure and preserves organization-defined system state information in the event of a system failure.
Protection of information at rest	**Intermediate**	Does the EHR protect the confidentiality and integrity of information at rest?	This control addresses the confidentiality and integrity of information at rest and covers user information and system information. Information at rest refers to the state of information when it is located on storage devices as specific components of information systems. System-related information requiring protection includes, for example, configurations or rule sets for firewalls, gateways, intrusion detection/prevention systems, filtering routers, and authenticator content. Organizations may employ different mechanisms to achieve confidentiality and integrity protections, including the use of cryptographic mechanisms and file share	**120.1. Describe how the EHR** protects the confidentiality and integrity of information at rest (e.g., database encryption).

Control type: System and communications protection				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
			scanning. Integrity protection can be achieved, for example, by implementing Write-Once-Read-Many technologies. Organizations may also employ other security controls, including, for example, secure offline storage in lieu of online storage when adequate protection of information at rest cannot otherwise be achieved and continuous monitoring to identify malicious code at rest.	
System and communications protection policy and procedures	**Intermediate/ Advanced**	Has the organization developed and formally documented a system and communications protection policy that addresses purpose, scope, roles and responsibilities, management commitment, coordination among, organizational entities and compliance; disseminated the policy to stakeholders in the organization with associated system and communications protection roles and responsibilities; developed and formally documented system and communications protection procedures; developed procedures to facilitate implementation	This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the Systems and Communications family. Policy and procedures reflect applicable laws, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organizational level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or, conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program, in general, and for specific information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.	121.1. Are there documented system and communication protection policies and procedures that address the above issues? Provide details and documents.

Control type: System and communications protection				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
		of the system and communications protection policy and associated system and communications protection controls; and disseminated system and communications protection procedures to stakeholders in the organization with associated system and communications protection roles and responsibilities?		

Control type: System and information integrity				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
Flaw remediation	**Intermediate**	Does the organization identify, report, and correct information system flaws; test software updates related to flaw remediation for effectiveness before installation; test software updates related to flaw remediation for potential side effects on organizational information systems before	Organizations identify information systems affected by announced software flaws, including potential vulnerabilities resulting from those flaws, and report this information to designated organizational personnel with information security responsibilities. Security-relevant software updates include, for example, patches, service packs, hot fixes, and anti-virus signatures.	122.1. Describe how system flaws are identified and reported, including testing of software updates related to flaw remediation for effectiveness before installation and software updates related to flaw remediation for potential side effects on organizational information systems before

Control type: System and information integrity				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
		installation; and incorporate flaw remediation in the organizational configuration management process?	Organizations also address flaws discovered during security assessments, continuous monitoring, incident response activities, and system error handling. Organizations take advantage of available resources, such as the Common Weakness Enumeration or Common Vulnerabilities and Exposures databases, in remediating flaws discovered in organizational information systems. By incorporating flaw remediation in ongoing configuration management processes, required and anticipated remediation actions can be tracked and verified. Organization-defined time periods for updating security-relevant software and firmware may vary based on a variety of factors, including, for example, the security category of the information system or the criticality of the update (i.e., severity of the vulnerability related to the discovered flaw). Some types of flaw remediation may require more testing than other types. Organizations determine the degree and type of testing needed for the specific type of flaw remediation activity under consideration and also the types of changes that are to be configuration-managed. In some situations, organizations may determine that the testing of software and firmware updates	installation, and how flaw remediation is incorporated in the organizational configuration management process.

Control type: System and information integrity				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
			is not necessary or practical (e.g., when implementing simple anti-virus signature updates). Organizations may also consider during testing decisions whether security-relevant software or firmware updates are obtained from authorized sources with appropriate digital signatures.	
Malicious code protection	**Minimum**	Does the organization employ malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code transported by electronic mail, electronic mail attachments, Web accesses, removable media, or other common means, or inserted through the exploitation of information system vulnerabilities; employ malicious code protection mechanisms at workstations, servers, or mobile computing devices on the network to detect and eradicate malicious code transported by electronic mail, electronic mail attachments, Web accesses, removable media, or other common means, or inserted through the exploitation of information system vulnerabilities; update malicious code protection mechanisms (including signature definitions) when new releases are	Information system entry and exit points include, for example, firewalls, electronic mail servers, web servers, proxy servers, remote-access servers, workstations, notebook computers, and mobile devices. Malicious code includes, for example, viruses, worms, Trojan horses, and spyware. Malicious code can also be encoded in various formats (e.g., UUENCODE, Unicode), contained in compressed or hidden files, or hidden in files using steganography. Malicious code can be transported by different means, including, for example, web accesses, electronic mail, electronic mail attachments, and portable storage devices. Malicious code insertions occur through the exploitation of information system vulnerabilities. Malicious code protection mechanisms include, for example, anti-virus signature definitions and reputation-based technologies. A variety of technologies and methods exist to limit or eliminate the effects of malicious code. Pervasive configuration	123.1. Describe how malicious code (e.g., spam) protection mechanisms are used at information system entry and exit points to detect and eradicate malicious code (i) during transport by electronic mail, electronic mail attachments, Web accesses, removable media, or other common means; or (ii) inserted through the exploitation of information system vulnerabilities. 123.2. Describe how malicious code protection mechanisms at workstations, servers, or mobile computing devices on the network to detect and eradicate malicious code are used.

Control type: System and information integrity				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
		available in accordance with configuration management policy and procedures defined in Configuration Management; define the frequency of periodic scans of the information system by malicious code protection mechanisms; define one or more of the following actions to be taken in response to malicious code detection: block malicious code, quarantine malicious code, or send an alert to the administrator; configure malicious code protection mechanisms to perform periodic scans of the information system in accordance with organization-defined frequency, and perform real-time scans of files from external sources as the files are downloaded, opened, or executed in accordance with organizational security policy; and take organization-defined actions in response to malicious code detection?	management and comprehensive software integrity controls may be effective in preventing the execution of unauthorized code. In addition to commercial off-the-shelf software, malicious code may also be present in custom-built software. This could include, for example, logic bombs, back doors, and other types of cyber attacks that could affect organizational mission/business functions. Traditional malicious code protection mechanisms cannot always detect such code. In these situations, organizations rely instead on other safeguards, including, for example, secure coding practices, configuration management and control, trusted procurement processes, and monitoring practices to help ensure that software does not perform functions other than the functions intended. Organizations may determine that in response to the detection of malicious code, different actions may be warranted. For example, organizations can define actions in response to malicious code detection during periodic scans, actions in response to detection of malicious downloads, and actions in response to detection of maliciousness when attempting to open or execute files.	

Control type: System and information integrity				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
Security alerts, advisories, and directives	**Minimum**	Does the organization receive information system security alerts, advisories, and directives from designated external organizations on an ongoing basis; generate internal security alerts, advisories, and directives; define personnel (identified by name or role) who should receive security alerts, advisories, and directives; disseminate security alerts, advisories, and directives to organization-identified personnel; and implement security directives in accordance with established time frames, or notify the issuing organization of the degree of noncompliance?	Compliance with security directives is essential due to the critical nature of many of these directives and the potential immediate adverse effect on organizational operations and assets, individuals, other organizations, and the nation, should the directives not be implemented in a timely manner. External organizations include, for example, external mission/business partners, supply chain partners, external service providers, and other peer/supporting organizations.	124.1. Describe how information system security alerts, advisories, and directives from designated external organizations on an ongoing basis are received. 124.2. Describe how security alerts, advisories, and directives to organization-identified personnel are disseminated.
Security function verification	**Intermediate**	Does the organization define the appropriate conditions, including the system transitional states, if applicable, for verifying the correct operation of security functions; define for periodic security function verification the frequency of the verifications; and define information system responses and alternative actions to anomalies discovered during security function verification? Does the EHR verify the correct operation of security functions in accordance with organization-	Transitional states for information systems include, for example, system startup, restart, shutdown, and abort. Notifications provided by information systems include, for example, electronic alerts to system administrators, messages to local computer consoles, and hardware indications, such as lights.	**125.1. Describe how the EHR** verifies the correct operation of security functions and how it responds to security function anomalies.

Control type: System and information integrity				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
		defined conditions and in accordance with organization-defined frequency (if periodic verification), and respond to security function anomalies in accordance with organization-defined responses and alternative actions?		
Software, firmware, and information integrity	**Advanced**	Does the organization employ integrity verification tools to detect unauthorized changes to software, firmware, and information?	Unauthorized changes to software, firmware, and information can occur due to errors or malicious activity (e.g., tampering). Software includes, for example, operating systems (with key internal components, such as kernels, drivers), middleware, and applications. Firmware includes, for example, the Basic Input Output System. Information includes metadata, such as security attributes associated with information. State-of-the-practice integrity-checking mechanisms (e.g., parity checks, cyclical redundancy checks, cryptographic hashes) and associated tools can automatically monitor the integrity of information systems and hosted applications.	**126.1. Describe how integrity verification tools** to detect unauthorized changes to software, firmware, and information are implemented. Unauthorized changes to software, firmware, and information can occur due to errors or malicious activity (e.g., tampering). Software includes, for example, operating systems (with key internal components, such as kernels, drivers), middleware, and applications. Firmware includes, for example, the Basic Input Output System. Information includes metadata such as security attributes associated with information. State-of-the-practice integrity-checking mechanisms (e.g., parity checks, cyclical redundancy checks, cryptographic hashes) and associated tools can

Control type: System and information integrity				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
				automatically monitor the integrity of information systems and hosted applications.
Information input validation	**Intermediate**	Does the EHR check the validity of information inputs?	Checking the valid syntax and semantics of information system inputs (e.g., character set, length, numerical range, and acceptable values) verifies that inputs match specified definitions for format and content. Software applications typically follow well-defined protocols that use structured messages (i.e., commands or queries) to communicate between software modules or system components. Structured messages can contain raw or unstructured data interspersed with metadata or control information. If software applications use attacker-supplied inputs to construct structured messages without properly encoding such messages, then the attacker could insert malicious commands or special characters that can cause the data to be interpreted as control information or metadata. Consequently, the module or component that receives the tainted output will perform the wrong operations or otherwise interpret the data incorrectly. Prescreening inputs before passing to interpreters prevents the content from being unintentionally interpreted as commands. Input validation helps ensure accurate and	**127.1. Describe how the EHR** checks the validity of information inputs, including checking the valid syntax and semantics of information system inputs (e.g., character set, length, numerical range, and acceptable values), and verifies that inputs match specified definitions for format and content. Software applications typically follow well-defined protocols that use structured messages (i.e., commands or queries) to communicate between software modules or system components.

Control type: System and information integrity				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
			correct inputs and prevent attacks, such as cross-site scripting and a variety of injection attacks.	
Information handling and retention	**Minimum**	Does the organization handle both information in and output from the information system in accordance with applicable laws, directives, policies, regulations, standards, and operational requirements; and retain both information in and output from the information system in accordance with applicable laws, directives, policies, regulations, standards, and operational requirements?	Information handling and retention requirements cover the full life cycle of information, in some cases extending beyond the disposal of information systems.	128.1. **Instructions to assessors:** Information gathered via the privacy assessment will be used for this question because the type of information stored in the system will likely determine how long it needs to be retained. Describe how both information in and output from the system are handled and retained as regards local policies and organizational requirements. Information handling and retention requirements cover the full life cycle of information, in some cases extending beyond the disposal of information systems.
Memory protection	**Intermediate/ Advanced**	Does the EHR implement organization-defined security safeguards to protect its memory from unauthorized code execution?	Some adversaries launch attacks with the intent of executing code in non-executable regions of memory or in memory locations that are prohibited. Security safeguards employed to protect memory include, for example, data execution prevention and address space layout randomization. Data execution prevention safeguards can either be hardware-enforced or software-enforced, with hardware	**129.1. Describe how the EHR** implements security safeguards to protect its memory from unauthorized code execution.

Control type: System and information integrity				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
			providing the greater strength of mechanism.	
System and information integrity policy and procedures	**Intermediate/ Advanced**	Has the organization developed and formally documented a system and information integrity policy that addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance; disseminated the policy to stakeholders in the organization with associated system and information integrity roles and responsibilities; developed and formally documented system and information integrity procedures; developed procedures to facilitate implementation of the system and information integrity policy and associated system and information integrity controls; and disseminated system and information integrity procedures to stakeholders in the organization with associated system and information integrity roles and responsibilities?	This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the System and Information Integrity family. Policy and procedures reflect applicable laws, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organizational level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or, conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program, in general, and for specific information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.	130.1. Are there documented system and information integrity policies and procedures? Provide details and documents.

Control type: System and services acquisition				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
Allocation of resources	**Minimum**	Does the organization include a determination of the information security requirements for the information system in mission/business process planning; determine, document, and allocate the resources required to protect the information system as part of its capital planning and investment control process; and establish a discrete line item for information security in organizational programming and budgeting documentation?	Resource allocation for information security includes funding for the initial information system or information system service acquisition and funding for sustaining the system/service.	131.1. Describe how resource allocation for information **security** includes funding for the initial information system or information system service acquisition and funding for sustaining the system/service, including how security is determined for mission/business process planning.
System development life cycle	**Intermediate**	Does the organization manage the information system using a system development life cycle methodology that includes information security considerations; define and document information system security roles and responsibilities throughout the system development life cycle; and identify individuals having information system security roles and responsibilities?	A well-defined system development life cycle provides the foundation for the successful development, implementation, and operation of organizational information systems. To apply the required security controls in the system development life cycle requires a basic understanding of information security, threats, vulnerabilities, adverse impact, and risk to critical mission/business functions. Organizations include qualified personnel, such as chief information security officers, security architects, security engineers, and information system security officers, in system development life cycle activities to ensure	132.1. Describe how the system is managed using a system development life cycle methodology that includes information security considerations, including defining and documenting information system security roles and responsibilities throughout the system development life cycle and identifying individuals with information system security roles and responsibilities.

Control type: System and services acquisition				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
			that security requirements are incorporated in organizational information systems. It is equally important that developers include individuals on the development team who possess the requisite security expertise and skills to ensure that needed security capabilities are effectively integrated in the information system. Security awareness and training programs can help ensure that individuals having key security roles and responsibilities have the appropriate experience, skills, and expertise to conduct assigned system development life cycle activities. The effective integration of security requirements in enterprise architecture also helps ensure that important security considerations are addressed early in the system development life cycle and that those considerations are directly related to the organizational mission/business processes. This process also facilitates the integration of the information security architecture in the enterprise architecture, consistent with organizational risk management and information security strategies.	
Development process, standards, and tools	**Intermediate**	Does the organization require the developer of the information system, system component, or information system service to follow a documented development process that explicitly	Development tools include, for example, programming languages and computer-aided design systems. Reviews of development processes can include, for example, the use of maturity models to determine the potential effectiveness of such processes. Maintaining the integrity of	133.1. **Instructions to assessors:** These questions should be answered by **the developers of the EHR** and **IT staff of the organization.** (This question applies to any customization, enhancements, or changes to the

Control type: System and services acquisition				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
		addresses security requirements; identifies the standards and tools used in the development process; documents the specific tool options and tool configurations used in the development process; and documents, manages, and ensures the integrity of changes to the process and tools used in development; and review the development process, standards, tools, and tool options and configurations to determine whether the process, standards, tools, and tool options and configurations selected and employed can satisfy organization-defined security requirements?	changes to tools and processes enables accurate supply chain risk assessment and mitigation, and requires robust configuration control throughout the life cycle (including design, development, transport, delivery, integration, and maintenance) to track authorized changes and prevent unauthorized changes.	system done by the organization to add, remove, or change the system.) Both parties should provide details and documents. Describe how the EHR development process explicitly addresses security requirements, identifies the standards and tools used in the development process, documents the specific tool options and tool configurations used in the development process, and ensures the integrity of changes to the process and tools used in development 133.2. Describe the review of development processes, standards, tools, and tool options and configurations to determine whether those selected and employed can satisfy security requirements.
Acquisition process	**Intermediate**	Does the organization include the following requirements or specifications, explicitly or by reference, in information system acquisition contracts based on an assessment of risk and in accordance with applicable laws, directives, policies, regulations, and	Information system components are discrete, identifiable IT assets (e.g., hardware, software, or firmware) that represent the building blocks of an information system. Information system components include commercial IT products. Security functional requirements include security capabilities, security functions, and security mechanisms. Security strength requirements associated with such	134.1. Describe how the security functional requirements and specifications, security-related documentation requirements, and developmental and evaluation-related assurance requirements are included in acquisition contracts for purchase or use of the system. Provide details and documents.

Control type: System and services acquisition				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
		standards: security functional requirements and specifications, security-related documentation requirements, and developmental and evaluation-related assurance requirements?	capabilities, functions, and mechanisms include the degree of correctness, completeness, resistance to direct attack, and resistance to tampering or bypass. Security assurance requirements include (i) development processes, procedures, practices, and methodologies; and (ii) evidence from development and assessment activities providing grounds for confidence that the required security functionality has been implemented and the required security strength has been achieved. Security documentation requirements address all phases of the system development life cycle. Security functionality, assurance, and documentation requirements are expressed in terms of security controls and control enhancements that have been selected through the tailoring process. The security control tailoring process includes, for example, the specification of parameter values through the use of assignment and selection statements and the specification of platform dependencies and implementation information. Security documentation provides user and administrator guidance on the implementation and operation of security controls. The level of detail required in security documentation is based on the security category or classification level of the information system and the degree to	

Control type: System and services acquisition				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
			which organizations depend on the stated security capability, functions, or mechanisms to meet overall risk response expectations (as defined in the organizational risk management strategy). Security requirements can also include organizationally mandated configuration settings specifying allowed functions, ports, protocols, and services. Acceptance criteria for information systems, information system components, and information system services are defined in the same manner as such criteria for any organizational acquisition or procurement.	
Security engineering principles	**Intermediate**	Does the organization apply information system security engineering principles in the specification of the information system; apply information system security engineering principles in the design of the information system; apply information system security engineering principles in the development of the information system; apply information system security engineering principles in the implementation of the information system; and apply information system security engineering	Organizations apply security engineering principles primarily to new development information systems or systems undergoing major upgrades. For legacy systems, organizations apply security engineering principles to system upgrades and modifications to the extent feasible, given the current state of hardware, software, and firmware in those systems. Security engineering principles include, for example: (i) developing layered protections; (ii) establishing sound security policy, architecture, and controls as the foundation for design; (iii) incorporating security requirements in the system development life cycle; (iv) delineating physical and logical security boundaries; (v) ensuring that system developers are trained on how to build secure software; (vi) tailoring security	**135.1. Instructions to assessors:** This question should be answered by **the developers of the EHR** and **IT staff of the organization.** (This question applies to any customization, enhancements, or changes to the system done by the organization to add, remove, or change the system.) Both parties should provide details and documents. Describe how system security engineering principles are applied to (i) system specification; (ii) design; (iii) development; (iv) implementation; and (v) modification of the information system.

Control type: System and services acquisition				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
		principles in the modification of the information system?	controls to meet organizational and operational needs; (vii) performing threat modeling to identify use cases, threat agents, attack vectors, and attack patterns and compensating controls and design patterns needed to mitigate risk; and (viii) reducing risk to acceptable levels, thereby enabling informed risk management decisions.	
External information system services	**Advanced**	Does the organization require that providers of external information system services comply with organizational information security requirements and employ appropriate security controls in accordance with applicable laws, directives, policies, regulations, standards, and guidance; define and document government oversight, and user roles and responsibilities on external information system services; and monitor security control compliance by external service providers?	External information system services are services that are implemented outside the authorization boundaries of organizational information systems. This includes services that are used by, but not a part of, organizational information systems. Organizations establish relationships with external service providers in a variety of ways, including, for example, through joint ventures, business partnerships, contracts, interagency agreements, lines of business arrangements, licensing agreements, and supply chain exchanges. The responsibility for managing risks from the use of external information system services remains with the authorizing officials. For services external to organizations, a chain of trust requires that organizations establish and retain a level of confidence that each participating provider in the potentially complex consumer-provider relationship provides adequate protection for the services rendered. The extent and nature of this chain of trust varies based on the relationships between	136.1. **Instructions to assessors:** This question should be answered by **the developers of the EHR** and **IT staff of the organization.** (This question applies to any customization, enhancements, or changes to the system done by the organization to add, remove, or change the system.) Both parties should provide details and documents. Describe how the services from external information systems are monitored for security control compliance for the purpose of oversight and verification.

Control type: System and services acquisition				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
			organizations and the external providers. Organizations document the basis for trust relationships so that the relationships can be monitored over time. External information system services documentation includes government, service providers, end user security roles and responsibilities, and service-level agreements. Service-level agreements define expectations of performance for security controls, describe measurable outcomes, and identify remedies and response requirements for identified instances of noncompliance.	
Developer security testing and evaluation	**Intermediate**	Does the organization require that information system developers/integrators, in consultation with associated security personnel (including security engineers) create and implement a security test and evaluation plan; implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the security testing and evaluation process; and document the results of the security testing/evaluation and flaw remediation processes?	Developmental security testing/evaluation occurs at all post-design phases of the system development life cycle. Such testing/evaluation confirms that the required security controls are implemented correctly, operating as intended, enforcing the desired security policy, and meeting established security requirements. Security properties of information systems may be affected by the interconnection of system components or changes to those components. These interconnections or changes (e.g., upgrading or replacing applications and operating systems) may adversely affect previously implemented security controls. This control provides additional types of security testing/evaluation that developers can conduct to reduce or eliminate potential flaws. Testing custom software applications	137.1. Describe how security test and evaluation plans are created and implemented, including implementation of verifiable flaw remediation processes to correct weaknesses and deficiencies identified during the security testing and evaluation process, and documentation of results of the security testing/evaluation and flaw remediation processes.

Control type: System and services acquisition				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
			may require such approaches as static analysis, dynamic analysis, binary analysis, or a hybrid of the three approaches. Developers can employ these analysis approaches in a variety of tools (e.g., web-based application scanners, static analysis tools, binary analyzers) and in source code reviews. Security assessment plans provide the specific activities that developers plan to carry out, including the types of analyses, testing, evaluation, and reviews of software and firmware components, the degree of rigor to be applied, and the types of artifacts produced during those processes. The depth of security testing/evaluation refers to the rigor and level of detail associated with the assessment process (e.g., black box, gray box, or white box testing). The coverage of security testing/evaluation refers to the scope (i.e., number and type) of the artifacts included in the assessment process. Contracts specify the acceptance criteria for security assessment plans, flaw remediation processes, and the evidence that the plans/processes have been diligently applied. Methods for reviewing and protecting assessment plans, evidence, and documentation are commensurate with the security category or classification level of the information system. Contracts may specify documentation protection requirements.	

Control type: System and services acquisition				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
Developer-provided training	**Intermediate**	Does the organization require the developer of the information system, system component, or information system service to provide organization-defined training on the correct use and operation of the implemented security functions, controls, and mechanisms?	This control applies to external and internal (in-house) developers. Training of personnel is an essential element to ensure the effectiveness of security controls implemented in organizational information systems. Training options include, for example, classroom-style training, web-based/computer-based training, and hands-on training. Organizations can also request sufficient training materials from developers to conduct in-house training or offer self-training to organizational personnel. Organizations determine the type of training necessary and may require different types of training for different security functions, controls, or mechanisms.	138.1. Describe developer-provided training on the correct use and operation of the security functions, controls, and mechanisms.
Developer security architecture and design	**Intermediate**	Has the organization required the developer of the information system, system component, or information system service to produce a design specification and security architecture that is consistent with and supportive of the organization's security architecture, which is established in and is an integrated part of the organization's enterprise architecture; accurately and completely describes	This control is primarily directed at external developers, although it could also be used for internal (in-house) development. By contrast, the Planning control is primarily directed at internal developers to help ensure that organizations develop an information security architecture and that the security architecture is integrated or tightly coupled to the enterprise architecture. This distinction is important if/when organizations outsource the development of information systems, information system components, or information system services to external entities, and there is a requirement to demonstrate consistency with the	139.1. **Instructions to assessors:** This question should be answered by **the developers of the EHR** and **IT staff of the organization.** (This question applies to any customization, enhancements, or changes to the system done by the organization to add, remove, or change the system.) Both parties should provide details and documents. Are the developers of the system required to follow any security frameworks for software development? If so, which frameworks? Provide details of design specifications and security

Control type: System and services acquisition				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
		the required security functionality, and the allocation of security controls among physical and logical components; and expresses how individual security functions, mechanisms, and services work together to provide required security capabilities and a unified approach to protection?	organization's enterprise architecture and information security architecture.	architecture that describe the security architecture, including accurately and completely describing the required security functionality, and the allocation of security controls among physical and logical components; and express how individual security functions, mechanisms, and services work together to provide required security capabilities and a unified approach to protection.
System and services acquisition policy and procedures	**Intermediate**	Has the organization developed and formally documented a system and services acquisition policy that addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance; disseminated the policy to stakeholders in the organization with associated system and services acquisition roles and responsibilities; developed and formally documented system and services acquisition procedures; developed procedures to	This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the System and Services Acquisition family. Policy and procedures reflect applicable laws, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organizational level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or, conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program, in general, and for specific information systems, if needed. The organizational risk management strategy is a	140.1. **Instructions to assessors:** This question should be answered by **the developers of the EHR** and **IT staff of the organization.** (This question applies to any customization, enhancements, or changes to the system done by the organization to add, remove, or change the system.) Both parties should provide details and documents. Are there documented system and services for acquisition policies and procedures? Provide details and documents.

Control type: System and services acquisition				
Title	**Security requirements level based on the implementation scenario**	**Security control assessment criteria**	**Assessment guidance**	**Questions**
		facilitate implementation of the system and services acquisition policy and associated system and services acquisition controls; and disseminated system and services acquisition procedures to stakeholders in the organization with associated system and services acquisition roles and responsibilities?	key factor in establishing policy and procedures.	

APPENDIX D. COMMUNICATING THE ASSESSMENT RESULTS: SAMPLE VISUALS

Appendix D. Table D1. Sample table of criticality and sensitivity assessment findings

Criteria	Criticality and sensitivity assessment 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.	**Medium:** The loss and cost accrued to the stakeholders' interest if the system's confidentiality is compromised would be **serious** disruption, **significant** financial loss, and **substantial** reputational loss requiring legal action for correction.	*Insert a brief description of the overall determination. Here is sample text from a system collecting, storing, and transmitting personal health information:* Overall, the [*insert system name*] system should be considered a **medium impact system** based on the assessment of the confidentiality, integrity, and availability criteria because it collects, stores, and transmits sensitive personal and health information. Systems that collect, store, and transmit sensitive personal information are typically assessed at 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 substantial reputational loss, requiring legal action for correction.
Integrity: Includes authentication, nonrepudiation, and accountability, and refers to the system's ability to be accurate and complete and provide protection from unauthorized modification.	**Low:** 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.	**Low:** 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.	

Appendix D. Table D2. Sample security and privacy controls assessment results table

Control type	System findings and gaps
Control Type #1	**Findings:**
	Gaps:
[EXAMPLE] Awareness and training: Controls specifying how to provide users with awareness and training on security procedures, roles, and responsibilities	**[Example] Findings:** Security awareness training for users was generally incorporated in general user training. Topics covered were mainly having one user account per user, keeping passwords private, maintaining confidentiality of personal health information, protecting the server room, and doing regular backups of the data in the system. Refresher training was not done consistently at all sites, but when it was done, it was usually on a quarterly or annual basis.
	[EXAMPLE] Gaps: • Role-based security training

Control type	System findings and gaps
Control Type #1	**Findings:**
	Gaps:
	• Additional security awareness training topics, such as locking computers when not in use, handling reports printed from the system with PII, etc. • Documented security training requirements by role

Appendix D. Table D3. Sample vulnerability scan visual

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 [*insert system name*] system) at the maximum risk for system hacking and data theft.	*Insert number of types of vulnerabilities found by threat level*	*Insert bulleted summary of each vulnerability found by threat level*	*Insert number of occurrences of vulnerabilities found*
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.			
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.			
Informational: These vulnerabilities result from some best practices not being implemented. Their impact on the scan target if exploited presents a minimal risk.			

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-20-195

ISBN: 978-1-64232-260-6