Compliance Checklist for safety requirements for electronic health applications

1. Audit identification

Audited Institution: open-emr.org

Project: OpenEMR v7.0

Document name: SRS for Security on e-health applications* (SEC-CAT*)

Date: 27-12-2023

Audit type: ❒ Internal
X External

2. Auditor team

Names:

e-mails: **Phones:**

3. Checklist

	Response alternatives	Yes	No	N/a
✓	**[SEC-CAT-BAC-001]:** The application will implement and apply dual access control prior to deleting users, medical records.		X	
✓	**[SEC-CAT-BAC-002]:** The application must incorporate robust access control mechanisms to prevent circumvention of access control checks by manipulating the URL. The following access control bypass tactics should be avoided and counteracted: **1.** Modification of the URL (parameter manipulation or forced navigation). **2.** Modification of the internal state of the application. **3.** Modification of the HTML page. **4.** Use of attack tools to modify API requests	X		
✓	**[SEC-CAT-BAC-003]:** The application must implement security measures to prevent the elevation of privileges. Prevent situations where a user can act without being authenticated or an administrator can act as a regular user after logging in.	X		
✓	**[SEC-CAT-BAC-004]:** The application must enforce strict and flexible access controls for authorized users, preventing unauthorized access to the API and ensuring record ownership.			X
✓	**[SEC-CAT-BAC-005]:** The application must prevent unauthorized access to data processing devices and assign roles to users to protect the integrity of ePHI against unauthorized alterations.	X		
✓	**[SEC-CAT-BAC-006]:** The system must allow users to be assigned to workgroups and grant access to records based on these groups. This access may be through a workstation, transaction, program, process, or other mechanism.	X		
✓	**[SEC-CAT-BAC-007]:** The system must implement measures to control who uses the data processing system by ensuring that users are authenticated with an individual authenticator before using a group authenticator.	X		
✓	**[SEC-CAT-BAC-008]:** The system is required to establish a formal process for user registration and deregistration, facilitating access to health information systems. This process must guarantee a consistent alignment between the authentication level, the mapping of users to roles, roles to system functions, and the level of access to be granted to the user.	X		
✓	**[SEC-CAT-CRF-001]:** The system must implement a robust FIPS-validated cryptographic infrastructure to encrypt and decrypt electronically protected health information to ensure adequate protection of sensitive information.	X		
✓	**[SEC-CAT-CRF-002]:** The application must ensure the security of integrity and confidentiality during the transmission of ePHI over electronic networks following the technical safeguards standards established in the regulatory framework	X		
✓	**[SEC-CAT-CRF-003]:** The application must ensure secure storage of the session identifier, ensuring that at no time is the generated session ID included in requests via the URL.	X		
✓	**[SEC-CAT-CRF-004]:** The application must ensure message encryption when the SessionIndex is linked to privacy data			X
✓	**[SEC-CAT-CRF-005]:** The application must exclusively store cryptographic representations of passwords, following best practices and using FIPS-validated cryptographic modules	X		
✓	**[SEC-CAT-INJ-001]:** The application must implement data entry validation measures before storing them to guarantee the integrity and security of the information processed, stored, or accessible through end-user point devices.		X	
✓	**[SEC-CAT-INJ-002]:** The application must be secure against SQL injection attacks. It is necessary to avoid possible security problems related to SQL injection and adjust the application to eliminate any risk associated with this attack.	X		
✓	**[SEC-CAT-INJ-003]:** The application must implement effective restrictions on the types of files that users can upload to prevent the upload of dangerous files that may be automatically processed in the application environment.	X		
✓	**[SEC-CAT-INJ-004]:** The application must implement protection measures against command injections. Depending on the application's architecture, the application must be modified to escape/sanitize special character input or configure the system to protect against command injection attacks.		X	
✓	**[SEC-CAT-INJ-005]:** The application must implement protection measures against Cross-Site Scripting (XSS) vulnerabilities to prevent malicious code injection attacks.		X	

✓	**[SEC-CAT-INJ-006]:** The application must implement an information output validation mechanism for the following software programs and/or applications: [reporting, data tables listing].	X		
✓	**[SEC-CAT-IND-001]:** The system must ensure that data is only processed following the directives provided in the data flow control.			X
✓	**[SEC-CAT-IND-002]:** The system must implement measures to prevent unauthorized and involuntary transfer of information through shared system resources.			X
✓	**[SEC-CAT-IND-003]:** The application must show a system of use of the system and privacy notification before granting access. This notice must contain information about the property of the system, the monitoring, recording, and auditing of use, the penalties for unauthorized use, and the acceptance of these conditions by the user.		X	
✓	**[SEC-CAT-IND-004]:** The system must generate error messages that provide the user with the information necessary for corrective actions without revealing details that can be exploited	X		
✓	**[SEC-CAT-IND-005]:** The application must physically or logically separate the functionality of the user, including user interface services and system management functionality.		X	
✓	**[SEC-CAT-IND-006]:** The application should be designed not to use emerging or non-categorized mobile code.	X		
✓	**[SEC-CAT-IND-007]:** The application should not contain authentication data incorporated into its code, configuration files, scripts, HTML files, or any ASCII file		X	
✓	**[SEC-CAT-IND-008]:** The application should not write sensitive data in the application records. The application must be designed or reconfigured to avoid including sensitive data in the records.	X		
✓	**[SEC-CAT-IND-009]:** The application should not unnecessarily store or retain sensitive information in hidden fields. It is imperative to eliminate this information as soon as possible, or instead, use practices such as token or truncation, following the guidelines of PCI DSS to guarantee safe storage.	X		
✓	**[SEC-CAT-IND-010]:** The application must ensure that the configuration and control files are not stored in the same directory as the user data. The application user data must be located in a directory different from the application code, and user file permits must be established to restrict user access to application configuration.	X		
✓	**[SEC-CAT-IND-011]:** The application should not be housed on a general-purpose server if the application is designated as criticism or high availability by the Information Security Officer (ISSO). Critical applications not shared by other less critical applications must be implemented on servers.		X	
✓	**[SEC-CAT-IND-012]:** The application must implement an adequate limitation of access routes to prevent malicious route manipulation that can lead to unauthorized revelation of files or directories.		X	
✓	**[SEC-CAT-IND-013]:** The application must be protected against vulnerabilities of canonical representation. An adequate canonical form must be selected, and the entire user entry must be canonized before authorization decisions are made.	X		
✓	**[SEC-CAT-IND-014]:** The application must incorporate a "safe failure" approach through safe error management to prevent vulnerabilities derived from incorrect management of return codes and exceptions in all system components.	X		
✓	**[SEC-CAT-IND-015]:** The application should not be vulnerable to race conditions.	X		
✓	**[SEC-CAT-IND-016]:** The application must implement measures to prevent memory use after being released since referring to memory after release can cause program failures, the use of unexpected values, or execute unwanted code.	X		
✓	**[SEC-CAT-IND-017]:** The application should prevent null pointer reference, avoiding trying to access a Null pointer, which could result in unexpected failure or exit.	X		
✓	**[SEC-CAT-IND-018]:** The application must implement controls defined by the organization to protect the system's memory against unauthorized code execution.	X		
✓	**[SEC-CAT-IND-019]:** The application should not be vulnerable to buffer overflow attacks	X		
✓	**[SEC-CAT-IND-020]:** The application should be designed to use components that are not vulnerable to XML attacks.	X		
✓	**[SEC-CAT-IND-021]:** The application must implement repetition-resistant authentication mechanisms for network access for privileged and non-privileged accounts.	X		
✓	**[SEC-CAT-IND-022]:** Applications with SOAP messages requiring integrity must include the following message elements: -Message ID-Service Request-Timestamp-SAML Assertion (optionally included in messages), and all elements of the message must be digitally signed.			X
✓	**[SEC-CAT-IND-023]:** The application must authenticate all the endpoint devices connected to the network before establishing any connection.			X
✓	**[SEC-CAT-IND-024]:** Safe messages with WS-Security must have time stamps indicating when they were created and expired. The application must be designed to use these time stamps and sequence numbers in WS-Security messages.			X
✓	**[SEC-CAT-IND-025]:** The application must verify the validity periods in all messages that WS-SECURITY or SAML statements use. Design and configure the application to use and verify validity periods in all token WS-Security profiles and SAML statements.			X
✓	**[SEC-CAT-SEM-001]:** The application must verify the validity periods in all messages that WS-SECURITY or SAML statements use. Design and configure the application to use and verify validity periods in all token WS-Security profiles and SAML statements.		X	
✓	**[SEC-CAT-SEM-002]:** The application must define and implement due security settings to avoid DDoS attacks		X	

✓	**[SEC-CAT-SEM-003]:** The application must implement measures to validate the deserialization of non-reliable data and ensure the resulting data are valid before processing them.	X		
✓	**[SEC-CAT-SEM-004]:** The application must be protected against Vulnerabilities of CROSS-SITE REQUEST FORGERY (CSRF) through the configuration to use unpredictable challenge tokens and verify the HTTP referrer, ensuring that the application was issued from the site itself. In addition, mitigating controls must be implemented as necessary, such as using web reputation services	X		
✓	**[SEC-CAT-SEM-005]:** The application must be configured to deactivate non-essential capabilities.	X		
✓	**[SEC-CAT-SEM-006]:** The application should avoid showing users what is not required to users. It is necessary to configure it so that it does not reveal technical details about architecture in error events.		X	
✓	**[SEC-CAT-SEM-007]:** The application must identify and authenticate uniquely non-organizational users (or processes that act in the name of non-organizational users).			X
✓	**[SEC-CAT-SEM-008]:** The application must identify and authenticate uniquely organizational users (or processes that act in the name of organizational users).	X		
✓	**[SEC-CAT-SEM-009]:** The applications that issue SAML statements must use random numbers approved by FIPS to generate SAML session in Saml's AuthnStatement element.			X
✓	**[SEC-CAT-SEM-010]:** The application must ensure that each party that makes statements (Asserting Party) provides unique identifiers for each SAML statement (Security Assertion Markup Language). It is required to design and configure each SAML statement authority to use unique affirmation identifiers.			X
✓	**[SEC-CAT-SEM-011]:** The application must guarantee the use of encrypted statements or equivalent confidentiality protections when the statement data is transmitted through an intermediary, and the confidentiality of the statements of statements is necessary during the transmission through the intermediary.			X
✓	**[SEC-CAT-SEM-012]:** The application should use both the <NotBefore> y <NotOnOrAfter> elements and the <OneTimeUse> element when using the <Conditions> element in a SAML Assertion.			X
✓	**[SEC-CAT-SEM-013]:** The application should use the NotOnOrAfter condition when using the SubjectConfirmation element in a SAML assertion.			X
✓	**[SEC-CAT-SEM-014]:** The application must configure session cookies with the following properties: o Establish the HTTPOnly flag in session cookies. o Ensure that the safe flag (Secure) is activated in session cookies.		X	
✓	**[SEC-CAT-VOC-001]:** Keep updated on the components or libraries of the application		X	
✓	**[SEC-CAT-VOC-002]:** The libraries or software components that do not have the support or maintenance must be removed or replaced		X	
✓	**[SEC-CAT-VOC-003]:** The application must provide notifications or alerts when product updates and safety-related patches are available		X	
✓	**[SEC-CAT-IAF-001]:** The application must identify user actions that can be carried out in the system without requiring identification or authentication	X		
✓	**[SEC-CAT-IAF-002]:** All organizations that connect to the Health Electronic Registry Information System (EHRI) must submit to possible users of Systems Point of Sale (POS) that link to EHRI to a formal process of registration of Users			X
✓	**[SEC-CAT-IAF-003]:** The application, when using PKI-based authentication, must validate certified by building a certification chain (including state information) to an accepted trust anchor, so the application must be designed to create a certification chain to a Trust Anchor accepted when using PKI -based authentication.			X
✓	**[SEC-CAT-IAF-004]:** The application, when using PKI-based authentication, must validate certified by building a certification chain (including state information) to an accepted trust anchor, so the application must be designed to create a certification chain to a Trust Anchor accepted when using PKI -based authentication.			X
✓	**[SEC-CAT-IAF-005]:** The application must implement procedures to verify that the person or entity that seeks access to protected electronic health information is what it claims to be.	X		
✓	**[SEC-CAT-IAF-006]:** The application must: o The application must impose a limit of 3 Invalid login attempts by a user during 15 minutes and o Automatically block the account for 1 hour; Block the account or node until an administrator releases it; delay the next login notice for 1 hour; Notify the system administrator; Take permanent account blocking when the maximum number of failed attempts is exceeded.	X		
✓	**[SEC-CAT-IAF-007]:** The application must implement procedures to verify that the person or entity that seeks access to protected electronic health information is what it claims to be.	X		
✓	**[SEC-CAT-IAF-008]:** The application must implement robust multifactor authentication, using at least two authentication factors (for example, CAC, Alt. Token) to access non-privileged networks and accounts.	X		
✓	**[SEC-CAT-IAF-009]:** The application should allow users to use a single identity credential (unique login), whether patients or suppliers, when the portal provides access to other applications or services with separate authentication mechanisms.	X		
✓	**[SEC-CAT-IAF-009]:** The application should allow users to use a single identity credential (unique login), whether patients or suppliers, when the portal provides access to other applications or services with separate authentication mechanisms.	X		
✓	**[SEC-CAT-IAF-010]:** The application must consider and select robust levels of identity assurance following the roles of the users, defining the necessary mechanisms to prove the identity of the record initially.	X		

✓	**[SEC-CAT-IAF-011]:** The application must consider and select robust levels of identity assurance following the roles of the users, defining the necessary mechanisms to prove the identity of the record initially.	X		
✓	**[SEC-CAT-IAF-012]:** The application must implement safe login procedures that protect against login attempts by brute force.		X	
✓	**[SEC-CAT-IAF-013]:** The application should consider that by authenticating the user, at least the two factors of the authentication mechanism are implemented.	X		
✓	**[SEC-CAT-IAF-014]:** The application must require the re-authentication of users and devices when information systems' authenticators, roles, or security categories change.		X	
✓	**[SEC-CAT-IAF-015]:** In case of an error during the login, the application should not offer specific help messages that can benefit an unauthorized user	X		
✓	**[SEC-CAT-IAF-016]:** The application should not show system or application identifiers until the login process has been successfully completed.	X		
✓	**[SEC-CAT-IAF-017]:** The application should not allow passwords to be transmitted in clear text on a network, following section 9.4.2 J) of safe login procedures.	X		
✓	**[SEC-CAT-IAF-018]:** During the login procedures, the application should not show the password that is being entered.	X		
✓	**[SEC-CAT-IAF-019]:** The application must prohibit password reuse for a minimum of five generations	X		
✓	**[SEC-CAT-IAF-020]:** The application should allow the use of a temporary password for the session in the system, with an immediate change to a permanent password.		X	
✓	**[SEC-CAT-IAF-021]:** The application must, when a successful login is completed, show the following information: **1.** Date and time of the last successful login. **2.** Details of any login and login attempts since the last successful session.		X	
✓	**[SEC-CAT-IAF-022]:** The application must apply a minimum 24 -hour/1 day password life policy.	X		
✓	**[SEC-CAT-IAF-023]:** The application must apply a maximum 60-day password restriction.	X		
✓	**[SEC-CAT-IAF-024]:** The application must ensure that changing the password requires changing at least eight characters.		X	
✓	**[SEC-CAT-IAF-025]:** The application must comply with the following password complexity policies: o Require at least a special character. o Apply a minimal password length of 15 characters. o Demand at least one capital character. o Make at least a lowercase character. o Impose password complexity by requiring at least a numerical character.	X		
✓	**[SEC-CAT-IAF-026]:** The application must prevent users, except the administrator or the user associated with the password, from making password changes.	X		
✓	**[SEC-CAT-IAF-027]:** Do not send or implement predetermined credentials, especially for administrators.	X		
✓	**[SEC-CAT-IAF-028]:** The application must limit the number of concurrent sessions for each account to three.		X	
✓	**[SEC-CAT-IAF-029]:** The application must limit the number of concurrent sessions for each account to three.	X		
✓	**[SEC-CAT-IAF-030]:** The EHRI application must restrict the duration of connections to application services to provide additional security in access to those applications.		X	
✓	**[SEC-CAT-IAF-031]:** The application must implement electronic procedures that automatically finish an electronic session after a default inactivity period.	X		
✓	**[SEC-CAT-IAF-032]:** The application must automatically end the administrator user session and close the administrator's session after a 10-minute inactivity period is exceeded.	X		
✓	**[SEC-CAT-IAF-033]:** The application must automatically end the un-privileged user session and close the session of not-privileged users after a 15-minute inactivity period has elapsed.	X		
✓	**[SEC-CAT-IAF-034]:** The application must automatically end the un-privileged user session and close the session of not-privileged users after a 15-minute inactivity period has elapsed.	X		
✓	**[SEC-CAT-IAF-035]:** The application must ensure that, at the end of a session, all network connections linked to that session are closed, and the session ID and cookies data are destroyed.	X		
✓	**[SEC-CAT-IAF-036]:** The application must be able to revoke the user's access privileges on time, which implies immediately preventing the user from accessing the system once their privileges have been revoked.	X		
✓	**[SEC-CAT-IAF-037]:** The application must finish the existing user sessions by eliminating an account. Configure the application to close user sessions whose accounts have been deleted.	X		
✓	**[SEC-CAT-IAF-038]:** The application must automatically delete or deactivate temporary user accounts 72 hours after creation. Configure the temporary accounts so they are deleted or deactivated automatically after 72 hours of the account's creation.			X
✓	**[SEC-CAT-IAF-039]:** The application must automatically deactivate the user accounts after an inactivity period of 35 days.		X	
✓	**[SEC-CAT-SDF-001]:** The application must acquire components only from official sources through safe links. Preference must be given to signed packages to reduce the possibility of including a modified or malicious component.		X	
✓	**[SEC-CAT-SDF-002]:** The application must incorporate a "software supply chain safety tool" to verify that the components do not contain known vulnerabilities		X	

✓	**[SEC-CAT-SDF-003]:** The application must have a process for reviewing code and configuration changes to minimize the possibility of malicious code or configuration introduction in the software pipeline.		X	
✓	**[SEC-CAT-SDF-004]:** The application must ensure that its continuous integration channel/continuous deployment (CI/CD) has adequate segregation, safe configuration, and access control to guarantee the integrity of the code that flows through construction and implementation processes.		X	
✓	**[SEC-CAT-SDF-005]:** The application must guarantee that the non-signed or non-encrypted serialized data are not sent to non-reliable customers without integrity verification or digital signature to detect manipulations or reproductions of the serialized data.			X
✓	**[SEC-CAT-SDF-006]:** The application must be able to show the previous content of a record at any point in the past, as well as the associated details of who entered, agreed, or modified the data and at what time.		X	
✓	**[SEC-CAT-SDF-007]:** The application must implement policies and procedures to protect protected electronic health information (EPHI) against improper alterations or destruction.	X		
✓	**[SEC-CAT-LMF-001]:** The application must implement a comprehensive security management process to guarantee the non-repudiation, confidentiality, integrity, and availability of all protected electronic health information (EPHI) created, received, maintained, or transmitted. This process must include the periodic review of system activity records, such as audit records, access reports, and security monitoring reports.	X		
✓	**[SEC-CAT-LMF-002]:** The application must implement a comprehensive security management process to guarantee the non-repudiation, confidentiality, integrity, and availability of all protected electronic health information (EPHI) created, received, maintained, or transmitted. This process must include the periodic review of system activity records, such as audit records, access reports, and security monitoring reports.	X		
✓	**[SEC-CAT-LMF-003]:** The application must have an audit reduction capacity that supports research after security incidents. The application must be configured to offer an audit reduction capacity that supports forensic investigations.	X		
✓	**[SEC-CAT-LMF-004]:** The application must generate audit records when successful/unsuccessful attempts are made to grant privileges. Configure the application to audit successful and unsuccessful attempts to grant privileges.	X		
✓	**[SEC-CAT-LMF-005]:** The application must generate audit records for successful and unsuccessful attempts to modify privileges, security levels, and information categories.	X		
✓	**[SEC-CAT-LMF-006]:** The application must generate audit records for successful and failed attempts to eliminate privileges, security levels, database safety objects, and information categories.	X		
✓	**[SEC-CAT-LMF-007]:** The application must generate audit records for privileged activities, accesses at the system level, successful/non-success to objects, and all direct access to the information system. The application in registration tickets corresponding to each type of activity mentioned must be configured.	X		
✓	**[SEC-CAT-LMF-008]:** The application must register the actions of users related to access and data changes. It includes identifying specific data elements that require protection and auditing all access and modification of data.	X		
✓	**[SEC-CAT-LMF-009]:** The application must audit the execution of privileged functions. Configure the application to record registration inputs when privileged functions are executed. At least ensure the specific action performed on the date and time of the event is registered.	X		
✓	**[SEC-CAT-LMF-010]:** The application must generate safe audit records every time a user: 1. Access, create, or update the personal health information (PHI) of a patient/person through the application; 2. cancels the consent directives of a patient/person through the application 3. Access, through the application, to data blocked or masked by instruction of a patient/person; 4. Access, create, or update user registration data in the application	X		
✓	**[SEC-CAT-LMF-011]:** The application must generate audit records that show the start and end of the user's access time to the system and events related to the beginning, closure, and duration of sessions.	X		
✓	**[SEC-CAT-LMF-012]:** The application must initiate the audit of sessions at the beginning. Configure the application to start registering application events as soon as the application starts.	X		
✓	**[SEC-CAT-LMF-013]:** The application must register closing events of the application. Configure the application or application server to record the closing events of the application in the event records.	X		
✓	**[SEC-CAT-LMF-014]:** The application must generate audit records when successful or failed login attempts occur.	X		

✓	**[SEC-CAT-LMF-015]:** The application must ensure that audit records contain information that establishes the following: **1.** When using centralized logging; the application must include a unique identifier in order to distinguish itself from other application logs. **2.** What type of event occurred; **3.** The function performed by the accessing user; **4.** When the event occurred with a time stamp mark that meets a granularity of one second for a minimum degree of precision. **5.** Where the event occurred; **6.** The organization of the accessing user (at least in those cases where an individual accesses information on behalf of more than one organization); **7.** Source of the event that establishes the identity of any individual or process associated with the event; **8.** network addresses and protocols **9.** destination IP addresses **10.** device identity or location, if possible, and system identifier; **11.** The outcome of the event; and **12.** Identity of any individuals, subjects, or objects/entities associated with the event using the username or user ID of the user related to the event **13.** The role the user is exercising; **14.** In the case of access override to blocked or masked records or portions of records, a reason for the override, as chosen by the user making the access and **15.** In the case of changes to consent directives made by a substitute decision-maker, the identity of the decision-maker.		X	
✓	**[SEC-CAT-LMF-016]:** The application must back up the audit records at least every seven days in a system or component different from the one being audited.		X	
✓	**[SEC-CAT-LMF-017]:** The application must maintain audit records for a specific period of time, determined by regulations and medical standards. This retention must cover from 7 to 75 years, depending on the information and legal requirements of the State. Some states may require that medical records be preserved in the hospital to guarantee continuous accessibility.		X	
✓	**[SEC-CAT-LMF-018]:** The LOG management application must ensure access and protect against unauthorized modification delete, and guarantee the integrity of audit tools to prevent improper use or commitment.	X		
✓	**[SEC-CAT-LMF-019]:** The application must implement strict control measures for the elimination, replication, and consultations of audit records, ensuring total control over the entry, reading, manipulation, or data disposal.	X		
✓	**[SEC-CAT-LMF-020]:** The application must transfer audit records to a system or medium different from the audited system and be configured to write application records in a centralized repository.		X	
✓	**[SEC-CAT-LMF-021]:** The application must allow the review and centralized analysis of audit records with filtering options defined by the organization	X		
✓	**[SEC-CAT-LMF-022]:** At least one application administrator must be registered to receive notifications of updates or safety alerts when they are automatically available. Administrators must register to receive update notifications, allowing them to stop and update applications and components of the application.	X		
✓	**[SEC-CAT-LMF-023]:** The application must generate audit records when a concurrent session is produced from different workstations.		X	
✓	**[SEC-CAT-LMF-024]:** EHRI must be able to register and safely report each access to the records of a patient/person, complying with the following requirements: **1.** Identify all users who have accessed or modified the records of a patient/person in a given period. **2.** Provide functionality to inform for a given user: • The records you can access. • You can access the specific sections of the (the registration (s). • The privileges you have concerning each of these records. **3.** Identify all patients/people whose records have been accessed or modified by a specific user in a given period. **4.** The system must generate a security event in case of an attempt or potential success for violating the login controls.	X		
✓	**[SEC-CAT-LMF-025]:** The application must notify the administrator, audit, and record the modifications made in the application configuration.	X		
✓	**[SEC-CAT-LMF-026]:** The application must notify the system administrators and system security officers (ISSO) of account activation actions. The application must be configured to send notifications to the system administrator and the ISSO when application accounts are enabled.	X		
✓	**[SEC-CAT-LMF-027]:** The application must notify the system administrators and system security officers (ISSO) of account deactivation actions. The application must be configured to send notifications to the system administrator and the ISSO when application accounts are enabled.	X		

✓	**[SEC-CAT-LMF-028]:** The application must notify the system administrators and the system security officers (ISSO) when application accounts are created.	X		
✓	**[SEC-CAT-LMF-029]:** The application must notify the system administrators and system information security officers (ISSO) of account elimination actions. The application configuration must include notification to the system administrator and the ISSO when application accounts are deleted.	X		
✓	**[SEC-CAT-LMF-030]:** The application must notify the system administrators and system information security officers (ISSO) of account elimination actions. The application configuration must include notification to the system administrator and the ISSO when application accounts are deleted.	X		
✓	**[SEC-CAT-LMF-030]:** The application must notify system administrators and system security officers (ISSO) when user accounts are modified.	X		
✓	**[SEC-CAT-LMF-031]:** The application must provide functions to analyze records and audit traces to identify all users who have accessed or modified patient/people records during a certain period.	X		
✓	**[SEC-CAT-LMF-032]:** The application must alert the Information Security Officer (ISSO) and the System administration (SA) in case of a failure in audit processing. The application must be configured to send an alarm when the audit system fails or is experiencing failure.		X	
✓	**[SEC-CAT-SRF-001]:** The application must implement protection measures to prevent SSRF vulnerabilities, including network and application layer controls.	X		

Total Answers for yes	88
Total Answers for no	35
Total Answers for N/a	19
Total requirements evaluated	**142**