	Compliance Checklist for safety requirements for electronic health appli	cati	ons	5
1.	Audit identification			
	ted Institution: open-emr.org			
	ect: OpenEMR v7.0			
	ment name: SRS for Security on e-health applications* (SEC-CAT*) 27-12-2023			
_	t type:			
1244	X External			
2.	Auditor team			
Nan				
e-ma		Phor	ies:	
3.	Checklist			
	Response alternatives	Yes	No	N/a
	✓ [SEC-CAT-BAC-001]: The application will implement and apply dual access control prior to deleting		X	
	users, medical records. ✓ ISEC-CAT-RAC-0021: The application must incorporate robust access control mechanisms to prevent			
	✓ [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).	X		
	2. Modification of the internal state of the application.			
	3. Modification of the HTML page.			
	 4. Use of attack tools to modify API requests ✓ [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	X		
	as a regular user after logging in.			
	✓ [SEC-CAT-BAC-004]: The application must enforce strict and flexible access controls for authorized users,			X
	preventing unauthorized access to the API and ensuring record ownership.			Λ
	✓ [SEC-CAT-BAC-005]: The application must prevent unauthorized access to data processing devices and	X		
	assign roles to users to protect the integrity of ePHI against unauthorized alterations. ✓ [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	X		
	other mechanism.			
	✓ [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	X		
	authenticator.			
	✓ [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	X		
	level of access to be granted to the user.			
	✓ [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	X		
	information. ✓ [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	X		
	the regulatory framework			
	✓ [SEC-CAT-CRF-003]: The application must ensure secure storage of the session identifier, ensuring that	X		
	at no time is the generated session ID included in requests via the URL.	71		
	✓ [SEC-CAT-CRF-004]: The application must ensure message encryption when the SessionIndex is linked			X
	to privacy data ✓ [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		X	
	point devices.			
	✓ [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	X		
	associated with this attack.	Λ		
	✓ [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	X		
	environment.			
	✓ [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 accomply a provided to		X	
	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.		Λ	
	✓ [SEC-CAT-INJ-005]: The application must implement protection measures against Cross-Site Scripting		τ,	
	(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		v	
	monitoring, recording, and auditing of use, the penalties for unauthorized use, and the acceptance of these		X	
	conditions by the user.			
✓	[SEC-CAT-IND-004]: The system must generate error messages that provide the user with the information	X		
√	necessary for corrective actions without revealing details that can be exploited			
•	[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	v		
	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	X		
√	as token or truncation, following the guidelines of PCI DSS to guarantee safe storage.		 	
•	[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	X		
	configuration.			
✓	[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		X	
	applications not shared by other less critical applications must be implemented on servers.			
✓	[SEC-CAT-IND-012]: The application must implement an adequate limitation of access routes to prevent		X	
	malicious route manipulation that can lead to unauthorized revelation of files or directories.		-1-	
✓	[SEC-CAT-IND-013]: The application must be protected against vulnerabilities of canonical	37		
	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	X		
	in all system components.			
✓	[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,	X		
✓	or execute unwanted code.			
V	[SEC-CAT-IND-017]: The application should prevent null pointer reference, avoiding trying to access a	X		
√	Null pointer, which could result in unexpected failure or exit. [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	X		
,	network access for privileged and non-privileged accounts.			
✓	[SEC-CAT-IND-022]: Applications with SOAP messages requiring integrity must include the following			v
	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			X
	WS-Security messages.			
✓	[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			X
	in all token WS-Security profiles and SAML statements.			
,			i 1	
✓	[SEC-CAT-SEM-001]: The application must define, document, and implement configurations, including		v	
√	security, hardware, software, services, and networks, adjusting them in the most restrictive way consistent		X	
✓ ✓			X	

SEC-CAT-SEM-003: The application must be protected against Vulnerabilities of CROSS-SITE REQUEST FORCERY (CSRF) through the configuration to use unpredictable challenge tokens and verify the HTTP referer, ensuring that the application must be protected against Vulnerabilities of CROSS-SITE REQUEST FORCERY (CSRF) through the configuration to use unpredictable challenge tokens and verify the HTTP referer, ensuring that the application must be sent sent of the sent sent sent that the sent sent sent sent sent sent sent sen					
SEC-CAT-SEA-001 : The application must be protected against Vulnerabilities of CROSS-SITE REQUEST FORCERY (CSRF) through the configuration to use unspredicable 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 SEC-CAT-SEA-005 : 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. SEC-CAT-SEA-005 : The application must identify and authenticate uniquely organizational users (or processes that act in the name of one-organizational users). SEC-CAT-SEA-005 : The application must identify and authenticate uniquely organizational users (or processes that act in the name of organizational users). SEC-CAT-SEA-005 : The application must identify and authenticate uniquely organizational users of processes that cit in the name of organizational users.	✓		X		
REQUEST FORGERY (CSRE) 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 **SEC-CAT-SEM-006]: The application must be configured to deactivate non-essential capabilities. **X **SEC-CAT-SEM-006]: The application on treveal technical details about architecture in error events. **SEC-CAT-SEM-007]: The application of reveal technical details about architecture in error events. **SEC-CAT-SEM-007]: The application must identify and authenticate uniquely organizational users (or processes that act in the name of organizational users). **SEC-CAT-SEM-007]: The application must identify and authenticate uniquely organizational users (or processes that act in the name of organizational users). **SEC-CAT-SEM-007]: The application stati issue SAMI. statements statements must use random numbers approved by IFBS to generate SAMI. session in Samis AuthEnsidement element. **SEC-CAT-SEM-007]: The application must ensure that each party that makes statements (Asserting Party) provides unique identifiers for each SAMI. statement (Security Assertion Markup Language). It is required to design and configure each SAMI. statement (Security Assertion Markup Language). It is required to design and configure each SAMI. statement (Security Assertion Markup Language). It is required to design and configure each SAMI. statement state through an intermediary, and the confidentiality protections when the statement data is transmitted through an intermediary. **SEC-CAT-SEM-013]: The application should use the NotOnOrAfter condition when using the Subject Confirmation element in SAMI. sestrion. **SEC-CAT-SEM-013]: The application should use the NotOnOrAfter condition when using the Subject Confirmation element when using the Conditions or olimate is the subject of the application was accepted trust anchor, so the application mus			<u> </u>		
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 whe reputation services FISEC-CAT-SEM-005]: The application must be configured to deactivate non-essential capabilities. X FISEC-CAT-SEM-005]: The application must be configured to deactivate non-essential capabilities. X X FISEC-CAT-SEM-005]: The application must denotify and authenticate uniquely non-organizational users (or processes that act in the name of non-organizational users). FISEC-CAT-SEM-005]: The application must identify and authenticate uniquely organizational users (or processes that act in the name of organizational users). FISEC-CAT-SEM-001]: The application must identify and authenticate uniquely organizational users (or processes that act in the name of organizational users). FISEC-CAT-SEM-011: The application must stream that cach party that makes statements (Asserting Party) provides unique identifiers for each SAM. Issaement (Security Assertion Markup Language). It is required to design and configure each SAM. Issaement authority to use unique affirmation identifiers. FISEC-CAT-SEM-011: The application must guarantee the use of encrypted statements or equivalent confidentiality of the statements of statements is necessary during the transmission through the intermediary. And the confidentiality of the statements of statements is necessary during the transmission through the intermediary. FISEC-CAT-SEM-011: The application should use the NonOnOrAfter condition when using the SubjectConfirmation element in a SAML assertion. FISEC-CAT-SEM-011: The application should use the NonOnOrAfter condition when using the SubjectConfirmation element in a SAML assertion. FISEC-CAT-VOC-001: Keep updated on the components or libraries of the application when using the mass flags that the saft flag (Secure) is activated in session cookies. FISEC-CAT-1AF-001: The application must identify user actions that can be carried out in the	✓		l	}	
the H11P reterret, ensuring that the application was assued from the site itself: in adultion, mitigating controls must be implemented as necessary, such as using whe reputation services and capabilities. SISC_CAT-SEM-005 The application must be configured to deactivate non-essential capabilities. X SISC_CAT-SEM-005 The application must denote and authenticate uniquely non-organizational users (or processes that act in the name of non-organizational users). X SISC_CAT-SEM-007 The application must identify and authenticate uniquely organizational users (or processes that act in the name of on-organizational users). SISC_CAT-SEM-008 The application must identify and authenticate uniquely organizational users (or processes that act in the name of organizational users). X SISC_CAT-SEM-009 The application must identify and authenticate uniquely organizational users (or processes that act in the name of organizational users). SISC_CAT-SEM-019 The application must identify and authenticate uniquely organizational users (or processes that act in the name of organizational users). X SISC_CAT-SEM-011 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 (Security Assertion Markup Language). It is required to design and configure each SAML statement (as the arms mist intermediary, and the confidentiality of the statements of statements is necessary during the transmitted through an intermediary, and the confidentiality of the statements of statements is necessary during the transmitisotion through the intermediary. X SISC_CAT-SEM-012 The application should use the NonConforAter condition when using the Sabject Confirmation element in a SAML assertion. SISC_CAT-SEM-013 The application should use the NonConforAter condition when using the state of the particular process and the state of the state of the state o			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 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). SEC-CAT-SEM-008 : The application shall sixes SAML statements uniquely organizational users (or processes that act in the name of organizational users). SEC-CAT-SEM-008 : The application must clausers and authenticate uniquely organizational users (or processes that act in the name of organizational users). SEC-CAT-SEM-018 : The application must causer 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 (Security Assertion Markup Language). It is required to design and configure each SAML statement authority to use unique affirmation identifiers. X SEC-CAT-SEM-018 : The application must continue the confidentiality of the statements of statements is necessary during the transmission through an intermediary. X SEC-CAT-SEM-018 : The application should use the NotOnOrAfter condition when using the SobjectConfirmation element in a SAML assertion. SEC-CAT-SEM-018 : The application should use the NotOnOrAfter condition when using the SobjectConfirmation element in a SAML assertion. SEC-CAT-SEM-018 : The application must provide notifications or alters when product updates and safety-related patches are available SEC-CAT-SEM-018 : The application must provide notifications or alters when product updates and safety-re				}	
SEC-CAT-SEM-006 : The application should avoid showing users what is not required to users, it is necessary to configure its obstait idoes not reveal technical details about architecture in error events.			<u> </u>	igsquare	
necessary to configure it so that it does not reveal technical details about architecture in error events. SEC-CAT-SEM-091]: The application must identify and authenticate uniquely non-organizational users for processes that act in the name of non-organizational users). SEC-CAT-SEM-098]: The application must identify and authenticate uniquely organizational users for processes that act in the name of non-organizational users). SEC-CAT-SEM-098]: The application must identify and authenticate uniquely organizational users for processes that act in the name of organizational users). SEC-CAT-SEM-091]: The application must users and the confidence of the processes that act in the name of organizational users). SEC-CAT-SEM-091]: The application shall statement authority to use unique affirmation identifiers. SEC-CAT-SEM-091]: The application must guarantee the use of enzypted statements or equivalent confidentiality protections when the statement data is transmitted through an intermediary, and the confidentiality protections when the statement data is transmitted through an intermediary, and the confidentiality of the statement with the confidentiality of the statement will be confidentially of the statement of statements is necessary during the transmission through the intermediary. SEC-CAT-SEM-0912]: The application should use both the «Notlefore» y «NotloftorArfer» elements and the «One Time the element in a SAML assertion. SEC-CAT-VEC-091]: The application should use to Month of the statement of statements of the process of statements of the proplection of the statement of statements of the superior organization of the subject of the proplection of the statement of the proplection of the statement of the proplection of the statement of the properties: SEC-CAT-VEC-091]: The application must provide notifications or alerts when product updates and safety-related patches are available SEC-CAT-VEC-093]: The application must identify user actions that can be carried out in the system without requ			X		
SEC-CAT-SEM-091]: The application must dentity and authenticate uniquely non-organizational users (or processes that act in the name of non-organizational users). SEC-CAT-SEM-098]: The application must identity and authenticate uniquely organizational users (or processes that act in the name of non-organizational users). SEC-CAT-SEM-098]: The application must identity and authenticate uniquely organizational users (or processes that act in the name of organizational users). SEC-CAT-SEM-098]: The application must charge that cach party that makes statements after the design and configure each SAML statement (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. SEC-CAT-SEM-011]: The application must guarantee the use of encrypted statements or equivalent confidentiality protections when the statement data its transmitted through an intermediary, and the confidentiality of the statements of statements is necessary during the transmission through the intermediary. SEC-CAT-SEM-011]: The application should use both the <000Bfores < >\cdot SCAT-SEM-011]: The application should use both the <000Bfores < >\cdot SCAT-SEM-011]: The application should use both the <000Bfores < >\cdot SCAT-SEM-011]: The application should use to thick exhibitions of the subject Confirmation element in a SAML assertion. SEC-CAT-SEM-012]: The application should use to the SCAT-SEM-013]: The application should use to the SCAT-SEM-013]: The application should use that the scate flag (Sec-CAT-SEM-013): The large state of the secure is a state of the application with the state flag (Sec-CAT-SEM-013): The large state of the secure is a state of the secure is a state of the secure of the subject of the secure of the secure is a state of the secure of the subject of the secure of the secu	✓	[SEC-CAT-SEM-006]: The application should avoid showing users what is not required to users. It is	l	v	
SEC-CAT-SEM-008]: The application must identify and authenticate uniquely organizational users (or processes that act in the name of organizational users). SEC-CAT-SEM-009]: The applications that issue SAML statements must use random numbers approved by FIF8 to generate SAML session in SAML statement element. SEC-CAT-SEM-010]: The application state issue SAML statements must use random numbers approved to FIF8 to generate SAML session in SAML statement element. SEC-CAT-SEM-010]: The application must user statement element of confidentiality protections what statement security to use unique affirmation identifiers. SEC-CAT-SEM-011]: The application must grantened the use of encrypted statements or equivalent confidentiality protections when the statement data is transmitted through an intermediary, and the confidentiality of the statements is necessary during the transmission through the intermediary. SEC-CAT-SEM-012]: The application should use both the NoBelfore y NotOnOrAfter selements and the NoTime User element when using the Conditions-element in a SAML Assertion. SEC-CAT-SEM-013]: The application should use the NotOnOrAfter condition when using the Subject-Confirmation element in a SAML assertion. SEC-CAT-VG-01]: Representation must configure session cookies with the following properties: SEC-CAT-VG-01]: Representation must configure session cookies. Establish the HTPOnly flag in session cookies. Establish the HTPOnly flag in session cookies. SEC-CAT-VG-02]: The libraries or software components that do not have the support or maintenance must be removed or replaced on the components or libraries of the application. SEC-CAT-VG-03]: The application must provide notifications or alerts when product updates and safety-related patches are available. SEC-CAT-VG-03]: The application must provide notifications or alerts when product updates and safety-related patches are available. SEC-CAT-VG-04]: The papplication when using PKI-based authentication, must validate certi		necessary to configure it so that it does not reveal technical details about architecture in error events.		Λ	
(or processes that act in the name of non-organizational users). SEC-CAT-SEM-098]: The application must identify and authenticate uniquely organizational users (or processes that act in the name of organizational users). SEC-CAT-SEM-099]: The applications that issue SAML statements must use random numbers approved by FIPS to generate SAML session in Saml's AuthnStatement element. SEC-CAT-SEM-091]: 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. SEC-CAT-SEM-011]: The application must guarantee the use of encrypted statements or equivalent confidentiality protections when the statement and its transmitted through an intermediary, and the confidentiality of the statements of statements is necessary during the transmission through the intermediary. SEC-CAT-SEM-012]: The application should use the NoOnOrAfter condition when using the subject confirmation element in a SAML assertion. SEC-CAT-SEM-013]: The application should use the NoOnOrAfter condition when using the subject confirmation element in a SAML assertion. SEC-CAT-VOC-001]: The paplication must configure session cookies. SEC-CAT-VOC-002]: The libraries or software components that do not have the support or maintenance must be removed or replaced SEC-CAT-VOC-003]: The application must identify user actions that can be carried out in the system without requiring identification or authentication SEC-CAT-IAF-003]: The application must identify user actions that can be carried out in the system without requiring identification or availation of the system without requiring identification or availation of the system of registration of Users SEC-CAT-IAF-003]: The application must ingent to the Health Electronic Registry Information System (ElRI) must submit to possible users of Systems Point of Sale (POS	✓	[SEC-CAT-SEM-007]: The application must identify and authenticate uniquely non-organizational users			v
processes that act in the name of organizational users). SISE_CAT-SEM-1902 The applications that issue SAML statements must use random numbers approved by FIPS to generate SAML session in Saml's AuthnStatement element. SISE_CAT-SEM-1915 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. SISE_CAT-SEM-1911 : The application must guarnetize the use of encrypted statements or equivalent confidentiality protections when the statement data is transmitted through an intermediary, and the confidentiality of the statements is necessary during the transmission through the intermediary. SISE_CAT-SEM-1912 : The application should use both the NotBefores y eNotOnOrAfters centents and the <ometion-lower alerts="" and="" application="" are="" available="" both="" configure="" cookies="" cookies.="" during="" enotonorafters="" following="" intermediary.="" must="" notbefores="" notifications="" of="" or="" patches="" pibraction="" product="" properties:="" provide="" safety-related="" session="" should="" sise_cat-sem-1913 :="" sise_cat-sem-1914 :="" sise_cat-voc-0012 :="" td="" the="" updates="" use="" when="" with="" y="" ="" <=""><td></td><td>(or processes that act in the name of non-organizational users).</td><td>l</td><td> </td><td>Λ</td></ometion-lower>		(or processes that act in the name of non-organizational users).	l		Λ
SEC-CAT-SEM-019]: The application shalt issue SAML statements must use random numbers approved by FIPS to generate SAML session in Saml's AuthnStatement element. SEC-CAT-SEM-019]: 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 (Security Assertion Markup Language). It is required to design and configure each SAML statement (Security Assertion Markup Language). It is required to design and configure each SAML statement (Security Assertion Markup Language). It is required to design and configure each SAML statement to recommend through an intermediary. It is confidentially of the statements of statements is necessary during the transmission through the intermediary. SEC-CAT-SEM-011]: The application should use the NotOnOrAfter clements and the "OneTimeUse" element in a SAML assertion. SEC-CAT-SEM-014]: The application should use the NotOnOrAfter condition when using the SubjectConfirmation element in a SAML assertion. SEC-CAT-SEM-014]: The application must configure session cookies. SEC-CAT-VOC-001]: The libraries or software components or libraries of the application was to replaced by the stream of	✓	[SEC-CAT-SEM-008]: The application must identify and authenticate uniquely organizational users (or	37		
by FIPS to generate SAML session in Saml's AuthnStatement element. SEC-CAT-SEM-010; The application must ensure that each party that makes statements (Asserting Party) provides unique identifiers for each SAML statement (Security Assertino Markup Language). It is required to design and configure each SAML statement authority to use unique affirmation identifiers. SEC-CAT-SEM-011]: The application must guarantee the use of encrypted statements or equivalent confidentiality protections when the statement and its transmitted through an intermediary, and the confidentiality of the statements is necessary during the transmission through the intermediary. X		processes that act in the name of organizational users).	Λ		
by FIPS to generate SAMI, session in SamIs AuthnStatement element. SEC-CAT-SEM-010]: The application must ensure that each party that makes statements (Asserting Party) provides unique identifiers for each SAMI, statement (Security Assertion Markup Language). It is required to design and configure each SAMI. statement (Security Assertion Markup Language). It is required to design and configure each SAMI. statement (Security Assertion Markup Language). It is required to design and configure each SAMI. statement authority to use unique affirmation identifiers. SEC-CAT-SEM-011]: The application must guarantee the use of encrypted statements or equivalent confidentiality protections when the statements and the statements of statements is necessary during the transmission through the intermediary. SEC-CAT-SEM-012]: The application should use both the <nobefore> y <noionorafter> elements and the <one <conditions="" element="" the="" timeuses="" using="" when=""> element in a SAMI. Assertion. SEC-CAT-SEM-013]: The application should use the NoIOnOrAfter condition when using the SubjectConfirmation element in a SAMI assertion. SEC-CAT-VOC-001]: Keep updated on the components or libraries of the application SEC-CAT-VOC-001]: The ilpraries or software conoponents that do not have the support or maintenance must be removed or replaced SEC-CAT-VOC-001]: The application must provide notifications or alerts when product updates and safety-related patches are available SEC-CAT-IAF-003]: The application must identify user actions that can be carried out in the system without requiring identification or authentication SEC-CAT-IAF-003]: The application subt connect to the Health Electronic Registry Information System (EHR) must submit to possible users of Systems Point of Sale (POS) that link to EHRI to a formal process of registration of Users 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</one></noionorafter></nobefore>	✓	[SEC-CAT-SEM-009]: The applications that issue SAML statements must use random numbers approved	1		**
SEC-CAT-SEM-010 : The application must ensure that each party that makes statements (Asserting Party) provides unique identifiers for each SAML statement authority to use unique affirmation identifiers. SEC-CAT-SEM-011 : The application must guarantee the use of encrypted statements or equivalent confidentiality or the statements of statement at its transmitted through an intermediary, and the confidentiality of the statements of statement at its transmitted through an intermediary, and the confidentiality of the statements of statements is necessary during the transmission through the intermediary. SEC-CAT-SEM-012 : The application should use both the <nobefore> y <notonafter> clements and the <onetimeuse> element when using the <conditions> element in a SAML Assertion. SEC-CAT-SEM-014 : The application should use the NotOnOrAfter condition when using the SubjectConfirmation element in a SAML assertion. SEC-CAT-SEM-014 : The application must configure session cookies. </conditions></onetimeuse></notonafter></nobefore>			l	}	X
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. 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 protections when the statements is necessary during the transmission through the intermediary. SEC-CAT-SEM-012 : The application should use both the <nobefore's <conditions—selement="" <notooorafters="" <one="" a="" and="" application="" assertion.="" clements="" components="" condition="" configure="" cookies="" element="" following="" in="" libraries="" must="" notonorafter="" of="" on="" or="" properties:="" reep="" saml="" sec-cat-sem-013 :="" sec-cat-sem-014 :="" sec-cat-voc-001 :="" session="" should="" subjectconfirmation="" td="" the="" timeuse's="" updated="" use="" using="" when="" with="" x="" y="" ="" <=""><td>✓</td><td></td><td></td><td></td><td></td></nobefore's>	✓				
to design and configure each SAML statement authority to use unique affirmation identifiers. 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. SEC-CAT-SEM-012: The application should use both the <nobforto-xfartpoond-afartpoond< td=""><td></td><td>- 11</td><td>l</td><td> </td><td>X</td></nobforto-xfartpoond-afartpoond<>		- 11	l		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 protections when the statements is necessary during the transmission through the intermediary. SEC-CAT-SEM-012]: The application should use both the NotPottonOrAfter older of the statements of statements is necessary during the transmission through the intermediary. SEC-CAT-SEM-013]: The application should use both the NotPottonOrAfter condition when using the Souther Confidence in a SAML Assertion. SEC-CAT-SEM-014]: The application should use the NotOnOrAfter condition when using the SubjectConfirmation element in a SAML assertion. SEC-CAT-VOC-001]: The properties of software components that do not have the support or maintenance must be removed or replaced. SEC-CAT-VOC-001]: The libraries or software components that do not have the support or maintenance must be removed or replaced. SEC-CAT-VOC-003]: The application must provide notifications or alerts when product updates and safety-related patches are available. SEC-CAT-IAF-003]: The application must identify user actions that can be carried out in the system without requiring identification or authentication. SEC-CAT-IAF-003]: The application must identify user actions that can be carried out in the system without requiring identification or authentication. SEC-CAT-IAF-003]: The application must in the subject of the s			l		
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. SEC-CAT-SEM-012]: The application should use both the <nobford-7>> NOBFORD-7</nobford-7>	√				
confidentiality of the statements of statements is necessary during the transmission through the intermediary. 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. SEC-CAT-SEM-013 : The application should use the NotOnOrAfter condition when using the SubjectConfirmation element in a SAML assertion. SEC-CAT-SEM-014 : The application should use the NotOnOrAfter condition when using the SubjectConfirmation element in a SAML assertion. SEC-CAT-VC-0012 : The properties of the application with the HTTPOnJ flag in session cookies. X SEC-CAT-VC-002 : The libraries or software components or libraries of the application X SEC-CAT-VC-003 : The application must provide notifications or alerts when product updates and safety-related patches are available SEC-CAT-VC-003 : The application must identify user actions that can be carried out in the system without requiring identification or authentication SEC-CAT-IAF-003 : The application must identify user actions that can be carried out in the system without requiring identification or authentication SEC-CAT-IAF-003 : The application must identify user actions that can be carried out in the system without requiring identification or authentication 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. SEC-CAT-IAF-004 : The application must impose a limit of 3 Invalid login attempts by a user during 15 minutes and 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; Block the account or node until an administrator releases it; delay the next login notice for 1 hour; Bloc</conditions></onetimeuse></notonorafter></notbefore>			l	}	X
SEC-CAT-SEM-012]: The application should use both the «NotDtefore» y «NotOnOrAfter» elements and the «OneTimeUse» element when using the «Conditions» element in a SAML Assertion. SEC-CAT-SEM-013]: The application should use the NotOnOrAfter condition when using the SubjectConfirmation element in a SAML assertion.			l	}	21
the <onetimeuse> element when using the <conditions> element in a SAML Assertion. SEC-CAT-SEM-013 : The application should use the NotOnOrAfter condition when using the SubjectConfirmation element in a SAML assertion. SEC-CAT-SEM-014 : The application must configure session cookies with the following properties: SEC-CAT-WOC-001]: Keep updated on the components or libraries of the application X </conditions></onetimeuse>	_			$\vdash \vdash \vdash$	
SEC-CAT-SEM-013]: The application should use the NotOnOrAfter condition when using the SubjectConfirmation element in a SAML assertion.	,		ı		X
SubjectConfirmation element in a SAML assertion. SEC-CAT-SEM-014]: The application must configure session cookies with the following properties: SEMENDAM TO SEM	1			$\vdash \vdash \vdash$	
SEC-CAT-SEM-014]: The application must configure session cookies with the following properties: Establish the HTTPOnly flag in session cookies. X	,		l		X
Ensure that the safe flag (Secure) is activated in session cookies. SEC-CAT-VOC-001]: Keep updated on the components or libraries of the application X	./			$\vdash \vdash \vdash$	
SEC-CAT-VOC-001]: Keep updated on the components or libraries of the application SEC-CAT-VOC-002]: The libraries or software components that do not have the support or maintenance must be removed or replaced SEC-CAT-VOC-003]: The application must provide notifications or alerts when product updates and safety-related patches are available SEC-CAT-IAF-001]: The application must identify user actions that can be carried out in the system without requiring identification or authentication 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 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. SEC-CAT-IAF-004]: The application, when using authentication based on public key infrastructure (PKI), must enforce authorized access to the corresponding private key, so the application. SEC-CAT-IAF-004: 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. The application must impose a limit of 3 Invalid login attempts by a user during 15 minutes and 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. 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. SEC-CAT-IAF-007: The application should allow users to use a single identity c	V		l	v	
SEC-CAT-VOC-0012: Keep updated on the components or libraries of the application X			l	Λ	
SEC-CAT-VOC-002]: The libraries or software components that do not have the support or maintenance must be removed or replaced SEC-CAT-VOC-003]: The application must provide notifications or alerts when product updates and safety-related patches are available 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-001]: 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 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. SEC-CAT-IAF-004]: The application, when using authentication based on public key infrastructure (PKI), must enforce authorized access to the corresponding private key, so the application or relevant access control mechanism must be configured to guarantee authorized access to the private key (s) of the application. X SEC-CAT-IAF-006]: 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. SEC-CAT-IAF-006]: 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. SEC-CAT-IAF-007]: The application must implement provide secses to the private secked. SEC-CAT-IAF-008]: 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. SEC-CAT-IAF-009]: The application must implement provides access to other application, using at least				37	
SEC-CAT-IAF-001 : The application must provide notifications or alerts when product updates and safety-related patches are available				X	
SEC-CAT-IAF-003]: The application must provide notifications or alerts when product updates and safety-related patches are available SEC-CAT-IAF-001]: The application must identify user actions that can be carried out in the system without requiring identification or authentication SEC-CAT-IAF-001]: The application shat 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 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. SEC-CAT-IAF-004]: The application, when using authentication based on public key infrastructure (PKI), must enforce authorized access to the corresponding private key, so the application or relevant access control mechanism must be configured to guarantee authorized access to the private key (s) of the application. SEC-CAT-IAF-004]: 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. SEC-CAT-IAF-006]: The application must: The application must impose a limit of 3 Invalid login attempts by a user during 15 minutes and Automatically block the account for 1 hour, Rotify that the person or entity that seeks access to protected electronic health information is what it claims to be. SEC-CAT-IAF-006]: 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. 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.	✓		l	X	
SEC-CAT-IAF-001]: The application must identify user actions that can be carried out in the system without requiring identification or authentication 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				 	
SEC-CAT-IAF-001]: The application must identify user actions that can be carried out in the system without requiring identification or authentication X	✓		l	X	
without requiring identification or authentication 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 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. SEC-CAT-IAF-004]: The application, when using authentication based on public key infrastructure (PKI), must enforce authorized access to the corresponding private key, so the application or relevant access control mechanism must be configured to guarantee authorized access to the private key (s) of the application. 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. SEC-CAT-IAF-006]: The application must: The application must impose a limit of 3 Invalid login attempts by a user during 15 minutes and 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. 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. SEC-CAT-IAF-009]: The application must implement probust multifactor authentication, using at least two authentication factors (for example, CAC, Alt. Token) to access non-privileged networks and accounts. SEC-CAT-IAF-009]: The application should allow users to use a single identity credential (unique login), whether patients or		•	<u> </u>	لتنا	
without requiring identification or authentication ISEC-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 ISEC-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. ISEC-CAT-IAF-004]: The application, when using authentication based on public key infrastructure (PKI), must enforce authorized access to the corresponding private key, so the application or relevant access control mechanism must be configured to guarantee authorized access to the private key (s) of the application. ISEC-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. ISEC-CAT-IAF-006]: 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. ISEC-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. ISEC-CAT-IAF-008]: The application must implement probust multifactor authentication, using at least two authentication factors (for example, CAC, Alt. Token) to access non-privileged networks and accounts. ISEC-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. ISEC-CAT-IAF-009]: The application should allow users to use a single identity credential (uni	✓		X	}	
(EHRI) must submit to possible users of Systems Point of Sale (POS) that link to EHRI to a formal process of registration of Users V [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. V [SEC-CAT-IAF-004]: The application, when using authentication based on public key infrastructure (PKI), must enforce authorized access to the corresponding private key, so the application or relevant access control mechanism must be configured to guarantee authorized access to the private key (s) of the application. V [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. V [SEC-CAT-IAF-006]: The application must implement procedures to verify that the person or entity that permanent account blocking when the maximum number of failed attempts is exceeded. V [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. V [SEC-CAT-IAF-008]: 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. V [SEC-CAT-IAF-008]: 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. V [SEC-CAT-IAF-009]: The application submit implement procedures to verify that the person or entity that seeks access to protected electronic health information is what it claims to be. V [SEC-CAT-IAF-009]: The application should allow users to use a single identity credential (unique login), whether patients or suppliers, when the			<u> </u>	igsquare	
of registration of Users V [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. V [SEC-CAT-IAF-004]: The application, when using authentication based on public key infrastructure (PKI), must enforce authorized access to the corresponding private key, so the application or relevant access control mechanism must be configured to guarantee authorized access to the private key (s) of the application. V [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. V [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 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. V [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. V [SEC-CAT-IAF-009]: 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. V [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. V [SEC-CAT-IAF-010]: The application must consider and select robust levels of identity assurance following the roles of the users, def	✓		l	}	
✓ [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. ✓ [SEC-CAT-IAF-004]: The application, when using authentication based on public key infrastructure (PKI), must enforce authorized access to the corresponding private key, so the application or relevant access control mechanism must be configured to guarantee authorized access to the private key (s) of the application. ✓ [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. ✓ [SEC-CAT-IAF-006]: The application must: ○ 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. ✓ [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. ✓ [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. ✓ [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. ✓ [SEC-CAT-IAF-010]: The application must consider and select robust levels of identity assurance following the roles of the users, defining the necessary me			l	}	X
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. V [SEC-CAT-IAF-004]: The application, when using authentication based on public key infrastructure (PKI), must enforce authorized access to the corresponding private key, so the application or relevant access control mechanism must be configured to guarantee authorized access to the private key (s) of the application. V [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. V [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 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. V [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. V [SEC-CAT-IAF-008]: 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. V [SEC-CAT-IAF-009]: 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. V [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. V [SEC-CAT-IAF-010]: The application must consider and select robust levels o			<u> </u>	لــــــا	
must be designed to create a certification chain to a Trust Anchor accepted when using PKI -based authentication. V [SEC-CAT-IAF-004]: The application, when using authentication based on public key infrastructure (PKI), must enforce authorized access to the corresponding private key, so the application or relevant access control mechanism must be configured to guarantee authorized access to the private key (s) of the application. V [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. V [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 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. V [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. V [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. V [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. V [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.	✓		l	}	
authentication. SEC-CAT-IAF-004 : The application, when using authentication based on public key infrastructure (PKI), must enforce authorized access to the corresponding private key, so the application or relevant access control mechanism must be configured to guarantee authorized access to the private key (s) of the application. 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. SEC-CAT-IAF-006 : The application must: Continue to the private key (s) of the application.			l	}	X
✓ [SEC-CAT-IAF-004]: The application, when using authentication based on public key infrastructure (PKI), must enforce authorized access to the corresponding private key, so the application or relevant access control mechanism must be configured to guarantee authorized access to the private key (s) of the application. ✓ [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. ✓ [SEC-CAT-IAF-006]: The application must: ○ The application must impose a limit of 3 Invalid login attempts by a user during 15 minutes and 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. ✓ [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. ✓ [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. ✓ [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. ✓ [SEC-CAT-IAF-010]: 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. ✓ [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.			l	}	21
must enforce authorized access to the corresponding private key, so the application or relevant access control mechanism must be configured to guarantee authorized access to the private key (s) of the application. 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. The application must impose a limit of 3 Invalid login attempts by a user during 15 minutes and 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. 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. 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. 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. 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.		authentication.			
mechanism must be configured to guarantee authorized access to the private key (s) of the application. 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. The application must impose a limit of 3 Invalid login attempts by a user during 15 minutes and 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. 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. 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. 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. 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.	✓		l		
✓ [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. ✓ [SEC-CAT-IAF-006]: The application must: ○ The application must impose a limit of 3 Invalid login attempts by a user during 15 minutes and 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. ✓ [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. ✓ [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. ✓ [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. ✓ [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. ✓ [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			l		X
seeks access to protected electronic health information is what it claims to be. ISEC-CAT-IAF-006]: The application must: 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. ISEC-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. ISEC-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. ISEC-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. ISEC-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. ISEC-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			<u> </u>		
 ✓ [SEC-CAT-IAF-006]: The application must: The application must impose a limit of 3 Invalid login attempts by a user during 15 minutes and of 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. ✓ [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. ✓ [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. ✓ [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. ✓ [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. ✓ [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 X 	✓		Y		
The application must impose a limit of 3 Invalid login attempts by a user during 15 minutes and 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. 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. 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. 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. 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. SEC-CAT-IAF-009]: 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			- 1		
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. 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. 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. 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. 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. SEC-CAT-IAF-009 : 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 X	✓	[SEC-CAT-IAF-006]: The application must:	l		
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. 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. 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. 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. 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. SEC-CAT-IAF-009 : 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 X			l		
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. ✓ [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. ✓ [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. ✓ [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. ✓ [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. ✓ [SEC-CAT-IAF-00]: 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			Y		
permanent account blocking when the maximum number of failed attempts is exceeded. ✓ [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. ✓ [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. ✓ [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. ✓ [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.			Λ.	}	
 ✓ [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. ✓ [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. ✓ [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. ✓ [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. ✓ [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 			l		
seeks access to protected electronic health information is what it claims to be. 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. 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. 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. SEC-CAT-IAF-009]: 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		permanent account blocking when the maximum number of failed attempts is exceeded.			
Seeks access to protected electronic health information is what it claims to be. 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. 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. 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. 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	✓	[SEC-CAT-IAF-007]: The application must implement procedures to verify that the person or entity that	v		
authentication factors (for example, CAC, Alt. Token) to access non-privileged networks and accounts. ✓ [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. ✓ [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. ✓ [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 X			Λ		
authentication factors (for example, CAC, Alt. Token) to access non-privileged networks and accounts. ✓ [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. ✓ [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. ✓ [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 X	✓	[SEC-CAT-IAF-008]: The application must implement robust multifactor authentication, using at least two	v		
 ✓ [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. ✓ [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. ✓ [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 	<u></u>	authentication factors (for example, CAC, Alt. Token) to access non-privileged networks and accounts.	Λ	L ∫	
whether patients or suppliers, when the portal provides access to other applications or services with separate authentication mechanisms. ✓ [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. ✓ [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 X	✓		- 		
authentication mechanisms. ✓ [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. ✓ [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 X			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. ✓ [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 X 			l		
whether patients or suppliers, when the portal provides access to other applications or services with separate X authentication mechanisms. ✓ [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 X	✓				
authentication mechanisms. ✓ [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 X			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 X			 I		
following the roles of the users, defining the necessary mechanisms to prove the identity of the record X	✓			\vdash	
	· ·		37		
muaity.		Tollowing the roles of the users, defining the necessary mechanisms to prove the identity of the record	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	X		
	initially.			
✓	[SEC-CAT-IAF-012]: The application must implement safe login procedures that protect against login		X	
	attempts by brute force.		Λ	
✓	[SEC-CAT-IAF-013]: The application should consider that by authenticating the user, at least the two	37		
	factors of the authentication mechanism are implemented.	X		
✓	[SEC-CAT-IAF-014]: The application must require the re-authentication of users and devices when			
•			X	
	information systems' authenticators, roles, or security categories change.			
· ·	[SEC-CAT-IAF-015]: In case of an error during the login, the application should not offer specific help	X		
	messages that can benefit an unauthorized user			
✓	[SEC-CAT-IAF-016]: The application should not show system or application identifiers until the login	X		
	process has been successfully completed.	21		
✓	[SEC-CAT-IAF-017]: The application should not allow passwords to be transmitted in clear text on a	37		
	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		
✓		X		
	[SEC-CAT-IAF-019]: The application must prohibit password reuse for a minimum of five generations	Λ		
✓	[SEC-CAT-IAF-020]: The application should allow the use of a temporary password for the session in the		X	
	system, with an immediate change to a permanent password.			
✓	[SEC-CAT-IAF-021]: The application must, when a successful login is completed, show the following			
	information:		v	
	1. Date and time of the last successful login.		X	
	2. Details of any login and login attempts since the last successful session.			
✓	[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		
▼		Λ		
•	[SEC-CAT-IAF-024]: The application must ensure that changing the password requires changing at least		X	
	eight characters.			
✓	[SEC-CAT-IAF-025]: The application must comply with the following password complexity policies:			
	 Require at least a special character. 			
	 Apply a minimal password length of 15 characters. 	X		
	Demand at least one capital character.			
	Make at least a lowercase character.			
	 Impose password complexity by requiring at least a numerical character. 			
✓	[SEC-CAT-IAF-026]: The application must prevent users, except the administrator or the user associated			
•	with the password, from making password changes.	X		
✓		X		
	[SEC-CAT-IAF-027]: Do not send or implement predetermined credentials, especially for administrators.	Λ		
✓	[SEC-CAT-IAF-028]: The application must limit the number of concurrent sessions for each account to		X	
	three.		21	
✓	[SEC-CAT-IAF-029]: The application must limit the number of concurrent sessions for each account to	X		
	three.	Λ		
✓	[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			
'		X		
	electronic session after a default inactivity period.		\vdash	
✓	[SEC-CAT-IAF-032]: The application must automatically end the administrator user session and close the	X		
	administrator's session after a 10-minute inactivity period is exceeded.	_		
✓	[SEC-CAT-IAF-033]: The application must automatically end the un-privileged user session and close the	X		
	session of not-privileged users after a 15-minute inactivity period has elapsed.	Λ		
✓	[SEC-CAT-IAF-034]: The application must automatically end the un-privileged user session and close the	37		
	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		
✓			\vdash	
'	[SEC-CAT-IAF-036]: The application must be able to revoke the user's access privileges on time, which	X		
<u> </u>	implies immediately preventing the user from accessing the system once their privileges have been revoked.			
✓	[SEC-CAT-IAF-037]: The application must finish the existing user sessions by eliminating an account.	X		
	Configure the application to close user sessions whose accounts have been deleted.	41		
✓	[SEC-CAT-IAF-038]: The application must automatically delete or deactivate temporary user accounts 72		l T	_
	hours after creation. Configure the temporary accounts so they are deleted or deactivated automatically after			X
	72 hours of the account's creation.			
✓	[SEC-CAT-IAF-039]: The application must automatically deactivate the user accounts after an inactivity			
			X	
	period of 35 days.			
√	[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		X	
	links. Preference must be given to signed packages to reduce the possibility of including a modified or malicious component.		X	
✓ ✓ ✓	links. Preference must be given to signed packages to reduce the possibility of including a modified or		X	

✓	[SEC-CAT-SDF-003]: The application must have a process for reviewing code and configuration changes		X	
	to minimize the possibility of malicious code or configuration introduction in the software pipeline.			
~	[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		X	
	integrity of the code that flows through construction and implementation processes.			
✓	[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			X
	manipulations or reproductions of the serialized data.			
✓	[SEC-CAT-SDF-006]: The application must be able to show the previous content of a record at any point		X	
	in the past, as well as the associated details of who entered, agreed, or modified the data and at what time.			
✓	[SEC-CAT-SDF-007]: The application must implement policies and procedures to protect protected	X		
	electronic health information (EPHI) against improper alterations or destruction.			
✓	[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	X		
	information (EPHI) created, received, maintained, or transmitted. This process must include the periodic	- 1		
	review of system activity records, such as audit records, access reports, and security monitoring reports.			
✓	[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	X		
	information (EPHI) created, received, maintained, or transmitted. This process must include the periodic	- 1		
	review of system activity records, such as audit records, access reports, and security monitoring reports.			
✓	[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	X		
	forensic investigations.			
✓	[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	X		
	privileges.			
✓	[SEC-CAT-LMF-005]: The application must generate audit records for successful and unsuccessful	X		
	attempts to modify privileges, security levels, and information categories.	71		
✓	[SEC-CAT-LMF-006]: The application must generate audit records for successful and failed attempts to	X		
	eliminate privileges, security levels, database safety objects, and information categories.	71		
✓	[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	X		
	application in registration tickets corresponding to each type of activity mentioned must be configured.			
✓	[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	X		
	modification of data.			
✓	[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	X		
	action performed on the date and time of the event is registered.			
✓	[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;	X		
	2. cancels the consent directives of a patient/person through the application	- 1		
	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			
✓	[SEC-CAT-LMF-011]: The application must generate audit records that show the start and end of the user's	X		
	access time to the system and events related to the beginning, closure, and duration of sessions.	41		
✓	[SEC-CAT-LMF-012]: The application must initiate the audit of sessions at the beginning. Configure the	X		
	application to start registering application events as soon as the application starts.	<i>^</i> \		
✓	[SEC-CAT-LMF-013]: The application must register closing events of the application. Configure the	X		
	application or application server to record the closing events of the application in the event records.	71		
✓	[SEC-CAT-LMF-014]: The application must generate audit records when successful or failed login	X		
	attempts occur.	Λ		
·		_	_	

✓	[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		X	
	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.			
✓	[SEC-CAT-LMF-016]: The application must back up the audit records at least every seven days in a system			
•			X	
✓	or component different from the one being audited.			
V	[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		X	
	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.			
V	[SEC-CAT-LMF-018]: The LOG management application must ensure access and protect against	37		
	unauthorized modification delete, and guarantee the integrity of audit tools to prevent improper use or	X		
✓	commitment.			
•	[SEC-CAT-LMF-019]: The application must implement strict control measures for the elimination,	v		
	replication, and consultations of audit records, ensuring total control over the entry, reading, manipulation,	X		
✓	or data disposal.			
•	[SEC-CAT-LMF-020]: The application must transfer audit records to a system or medium different from		X	
✓	the audited system and be configured to write application records in a centralized repository.			
V	[SEC-CAT-LMF-021]: The application must allow the review and centralized analysis of audit records with filtering artisps defined by the application	X		
	with filtering options defined by the organization			
✓	[SEC-CAT-LMF-022]: At least one application administrator must be registered to receive notifications of	37		
	updates or safety alerts when they are automatically available. Administrators must register to receive update	X		
	notifications, allowing them to stop and update applications and components of the application.			
✓	[SEC-CAT-LMF-023]: The application must generate audit records when a concurrent session is produced		X	
	from different workstations.			
✓	[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 years who have accessed on modified the accessed of modified the accessed of the first terms in a six of the six of the six of the first terms in a six of the six of the six of the si			
	1. Identify all users who have accessed or modified the records of a patient/person in a given period. 2. Provide for this table to be for a river year.			
	2. Provide functionality to inform for a given user:			
	The records you can access			
	The records you can access. You can access the experience of the (the registration (c)).	X		
	You can access the specific sections of the (the registration (s). The section of the first the firs			
	The privileges you have concerning each of these records.			
	2			
	3. Identify all patients/people whose records have been accessed or modified by a specific user in a given			
	period. The greatest process of a security execution case of an attenuation retential greatest for violeting the			
	4. The system must generate a security event in case of an attempt or potential success for violating the			
	login controls.			
✓	[SEC-CAT-LMF-025]: The application must notify the administrator, audit, and record the modifications	X		
	made in the application configuration.			
✓	[SEC-CAT-LMF-026]: The application must notify the system administrators and system security officers	37		
	(ISSO) of account activation actions. The application must be configured to send notifications to the system	X		
	administrator and the ISSO when application accounts are enabled.			
✓	[SEC-CAT-LMF-027]: The application must notify the system administrators and system security officers	37		
	(ISSO) of account deactivation actions. The application must be configured to send notifications to the	X		
	system administrator and the ISSO when application accounts are enabled.			

✓	[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