3. Safety requirements

Identification and authentication		
Requirements	**Associated questions**	**Equivalence with HL7**
Identification management/authentication begins with the assignment of an identifier to an entity, which must be verified in an authentication process. Authentication can be based on knowledge that only the individual has (e.g., passwords), on a certified token, an element that has been granted by an authority (e.g., smart card, cryptographic key, etc.), or on properties that characterize the individual (e.g., biometrics, voice, handwriting, etc.).	• Does the system have an access control mechanism for accessing protected information based on username and password (username password)? *(username/password)*? • Does the System have an access control mechanism for accessing protected information based on a digital certificate? • Does the System have an access control mechanism for accessing protected information based on a secure token? • Does the System have an access control mechanism for accessing protected information based on biometric information? • Does the system offer the user the possibility to change their password? • Does the system offer the user the possibility to generate a new password when he/she has forgotten it?	CPS1.1. TI1.

Identification and authentication		
Requirements	**Associated questions**	**Equivalence with HL7**
	• Does the system have a procedure and procedure and mechanism to uniquely identify a patient? For example, to distinguish between people who have similar first and last names that may lead to confusion. In these cases, other identification data, e.g., date and place of birth and parents' names, must be confirmed. • Does the system have the ability to manage more than one ID code for each patient? For example, health facility medical record number, health care network identification code, and national identification code. • Does the system have a connection to a local MPI[6]? • Does the system have a connection to an external PFI within the organization, but not at the national level? • Does the system have a connection to a national external PPM? • Does the system have an authentication mechanism for accessing protected information that is accredited to	

[6] Master Patient Index

Identification and authentication		
Requirements	**Associated questions**	**Equivalence with HL7**
	international authentication standards (e.g., SAML, WS-Trust, Kerberos)? • ¿Does the system have mechanisms to manage digital identities (accounts, keys, tokens) throughout their lifecycle, from registration to termination? • Does the system have layers of Hardware/Software where AAA (authentication, authorization and accounting) validation protocol applies?	
Password renewal, session expiration, invalid or malicious authentication control mechanisms must be contemplated. Passwords must be stored in an encrypted and secure manner and must obey certain rules to ensure the highest possible level of security.	• Does the system have an authorization mechanism that enforces lockout time limits in case of login error and default minimum privileges? • Does the system have a logout mechanism for inactivity of the logged in user? • Does the system have a password management mechanism that follows current security standards (NIST SP 800-57 or similar)? • Does the system employ specific measures to protect remote access services?	CPS1.1. TI1.

Identification and authentication		
Requirements	**Associated questions**	**Equivalence with HL7**
	• Does the system have token generation mechanisms?	
Mechanisms for treatment of dependent persons, minors or persons under guardianship, their identification and authentication must be contemplated.	• Does the system have a mechanism to identify and authenticate patients when one patient is a proxy for another? (minors, wards...)	

Permissions and roles of actors		
Requirements	**Associated questions**	**Equivalence with HL7**
Access control, including permitted actions, may be based on privileges and roles assigned to an entity (or person) by an authority according to the entity's attribute or a set of	• Does the system have an access control policy for authorizing and revoking access rights to information systems?	TI1

Permissions and roles of actors		
Requirements	**Associated questions**	**Equivalence with HL7**
competencies and/or performances that are associated with a professional profile and a task, respectively. Authorization and access control may also be based not only on policies reflecting legislation and regulations including consents established by the subject or their representative, but also by environmental or contextual conditions. Above all, by a good organization of the health care facility.	• Does the system have the ability to easily configure these access rules? • Does the system have a process for granting and revoking appropriate user access? • Does the system have procedures in place to periodically review user access to ensure that only necessary privileges are applied? • Does the system have an authentication system that applies higher levels of authentication to protect resources with higher levels of sensitivity? • Does the system have an established usage guide for mobile computing devices (regardless of ownership) that store, process or transmit system data? • Does the system have mechanisms to enable user stories and roles to contain functional safety constraints? For example, that certain profiles (or roles) can only (or roles) can only access information about patients with whom they have a healthcare relationship. For example, patients in my department, or in my basic health scope, or radiology patients.	

Permissions and roles of actors		
Requirements	**Associated questions**	**Equivalence with HL7**
	• Does the system have mechanisms to ensure that access control is attribute or feature based whereby code verifies user authorization for a feature / data element rather than just its function?	

Traceability of actions		
Requirements	**Associated questions**	**Equivalence with HL7**
An EHRS system must have built-in internal audit and traceability mechanisms to record activity related to key events in real time, both from the point of view of user activity and the system itself in terms of internal processes (e.g., alerts or notifications) or administration of its components (backups, information extractions, etc.).	• Does the system have the ability to generate an audit trail for any authentication action/Login (successful or unsuccessful), or password change performed by the user? • Does this user audit log have all the information regarding who, what, when, where?	TI2

Traceability of actions		
Requirements	**Associated questions**	**Equivalence with HL7**
The audit registration should contain all necessary information (who, what, when, where) and be accessible and searchable for a sufficient period of time. In some cases, indefinitely. For example, who wrote, edited, signed a medical report, when, where etc.), where etc.) When does "where" refer to a physical location (it has its importance) or to the location of the information? PE access to lab results, an episode etc.	• Does the system have the ability to generate an audit trail for any actions taken by the user against sensitive data or functionality? • Does this user audit log have all information regarding who, what, when, where? • Does the system have the capability to generate an audit trail against actions of the system itself that affect sensitive data? That is, internal actions that the system performs on its own, without the intervention of a logged user, such as cleaning or archiving old information from a history, synchronization of information, etc. • Does this internal system process audit trail have all information regarding who, what, when, where? • Does the system have the ability to generate an audit log with standard tools? • Does the system keep these audit trails accessible for consultation for more than 6 months?	

Information integrity, availability and confidentiality		
Requirements	**Associated questions**	**Equivalence with HL7**
In any solution, a set of standards and best practices must be applied to ensure that data is accurate, up-to-date and available in accordance with current law and regulations.	• Does the system use appropriate or proven encryption methods to protect sensitive data in transit? • Are communications between application components, including APIs, middleware, and data layers authenticated? • Does the system have policies in place that indicate when encryption should be used (e.g., at rest, in transit, with sensitive or confidential data, etc.)? • Are the security regulations and data protection compliance that apply at the national level of the country where the system is to be implemented taken into account? • Does the system employ technologies to block or restrict unencrypted sensitive information from traveling to untrusted networks? • Do secure databases use database encryption levels? • Does the system require encryption on mobile computing devices (i.e., laptops, tablets, etc.)? • Does the system have logical access restrictions to internal system components?	TI1

Information integrity, availability and confidentiality		
Requirements	**Associated questions**	**Equivalence with HL7**
	• Does communication between systems count on identification between parties by means of a Digital Certificate? • Has the system identified and classified sensitive data into levels of protection? • Does the system have the ability to rectify a user's data when it is wrongly associated? • Does the system have change management features? • Does the system have sensitive data identification policies? • Does the system have specific mechanisms for handling and storing sensitive data in an anonymized form?	

Risk Management		
Requirements	**Associated questions**	**Equivalence with HL7**
Every organization or IT project should have a risk management methodology based on best practices and the application of current regulations and standards, such as ISO, COBIT, etc. In this sense, end-to-end IT governance and management practices should be considered.	• Does the system have a person or group with responsibility for an ongoing process of assessing the likelihood of known threats exploiting vulnerabilities and, as a result, the impact on valuable assets? • Does the system have a process to identify and assess reasonably foreseeable internal and external risks to the security, confidentiality and/or integrity of any electronic, paper or other records containing sensitive information? • Are routine risk assessments conducted on the system to identify key objectives to be supported by the information security program? • Is risk documentation carried out?	
The system must have adequate web protection mechanisms (including WAF, port restrictions and DDoS protections).	• Does the system have protection mechanisms for your web application (e.g., WAF, port restrictions and DDoS protections)?	

Standards and regulatory monitoring		
Requirements	**Associated questions**	**Equivalence with HL7**

Elements related to security, encryption, communications, etc. must follow a series of norms or standards recognized at a national or international level, at the same time that the security rules and regulations defined by competent bodies such as the GDPR[7]in the European Union.	• Are standards for key management documented and used?
	• Does the system use secure communication standards (TLS 1?3, SSL v3, etc.)?
	• Does the system use SHA 1024 or similar level of communication encryption?
	• Does the system have standards for isolating sensitive data and procedures and technologies to protect them from unauthorized access and tampering?
	• Under which data protection, dissemination and authorization regulations are they governed?
	  ○ ISO 27002-27002
	  ○ GDPR or equivalent
	  ○ OWASP
	  ○ CEW
	  ○ NIST
	• Does the system provider participate with local, national or international security groups, associations and agencies?	

[7] General Data Protection Regulation of the European Comon