[4. SECURITY REQUIREMENTS 3](#_Toc151383436)

[4.1. Risk Management 3](#_Toc151383437)

[4.2. Security Policy 3](#_Toc151383438)

[4.3. Organizing Information Security 3](#_Toc151383439)

[4.4. Asset Management 3](#_Toc151383440)

[4.5. Human Resources Security 3](#_Toc151383441)

[4.6. Physical and Environmental Security 3](#_Toc151383442)

[4.7. Communications and Operations Management 3](#_Toc151383443)

[4.8. Access Control 4](#_Toc151383444)

[4.8.2. User Access Management 4](#_Toc151383445)

[4.2.8.1. User Registration 4](#_Toc151383446)

[4.8.2.2. Privilege Management 5](#_Toc151383447)

[a) Role-Based Access Control 5](#_Toc151383448)

[b) Workgroup-Based Access Control 5](#_Toc151383449)

[c) Discretionary Access Control 6](#_Toc151383450)

[4.8.3. User Responsibilities 6](#_Toc151383451)

[4.8.4. Network Access Control 6](#_Toc151383452)

[4.8.5. Operating System Access Control 6](#_Toc151383453)

[4.8.6. Application and Information Access Control 6](#_Toc151383454)

[4.8.7. Workstation Access Control 7](#_Toc151383455)

[4.8.8. Mobile Computing and Teleworking 7](#_Toc151383456)

[4.9. Information Systems Acquisition, Development and Maintenance 7](#_Toc151383457)

[4.9.2. Correct Processing of Information 7](#_Toc151383458)

[4.9.2.1. Input Data Validation 7](#_Toc151383459)

[4.9.2.2. Output Data Validation 7](#_Toc151383460)

[4.9.3. Cryptographic Controls 8](#_Toc151383461)

[4.9.4. Security of File Systems 8](#_Toc151383462)

[4.9.5. Security in Development and Support Processes 8](#_Toc151383463)

[4.9.6. Vulnerability Management 8](#_Toc151383464)

[4.10. Information Security Incident Management 8](#_Toc151383465)

[4.10.1. Reporting Incidents and Weaknesses 8](#_Toc151383466)

[4.10.2. Management of Incidents and Improvements 8](#_Toc151383467)

[4.11. Business Continuity Management 8](#_Toc151383468)

[4.12. Compliance 8](#_Toc151383469)

# SECURITY REQUIREMENTS

## Risk Management

* Does not apply.

## Security Policy

* Does not apply

## Organizing Information Security

* Does not apply

## Asset Management

* Does not apply

## Human Resources Security

* Security Requirement 13 – Verifying the Identity of Users All organizations connecting to the EHRi or hosting components of the EHRi must verify the identity and address of each permanent or temporary staff member or contractor who will become a registered user of a PoS system connected to the EHRi or who will have access to hosted components of the EHRi.

## Physical and Environmental Security

* Does not apply

## Communications and Operations Management

* Security Requirement 30 – Encrypting PHI During Transmission: The EHRi and PoS systems connected to the EHRi must apply industry-standard cryptographic algorithms and protocols during transmission of PHI to maintain the confidentiality and integrity of this data whenever it is transmitted outside the physical security perimeters that protects information processing facilities supporting EHRi servers, applications or data.
* Security Requirement 37 – Logging Transactions in the EHRi: The EHRi must create a secure audit record each time a user:

a) Accesses, creates or updates PHI of a patient/person via the EHRi;

b) Overrides the consent directives of a patient/person via the EHRi;

c) Accesses, via the EHRi, data that is locked or masked by instruction of a patient/person; or

d) Accesses, creates or updates registration data on an EHRi user.

* Security Requirement 38 – Preserving the History of PHI in the EHRi: The EHRi must be capable of displaying the former content of a record at any point in the past, as well the associated details of who entered, accessed or modified the data, and at what time.
* Security Requirement 39 – Preserving the History of PHI in PoS Systems: All PoS systems connected to the EHRi should be capable of displaying the former content of a record at any point in the past, as well as the associated details of who entered, accessed or modified the data, and at what time.
* Security Requirement 41 – Logging Access to PHI in PoS Systems: All PoS systems connected to the EHRi must record in an audit log every instance of a user accessing, updating or archiving PHI.
* Consideration ID-15 – Consider the Definition of Minimum Requirements and Specifications for Audit and Logging Capabilities to be Used by Member Organizations: Member organizations should consider use of common logging and auditing functions to facilitate trust relationships and to meet accountability obligations.
* Security Requirement 42 – Minimum Content of Audit Logs: The EHRi audit log and the audit logs of PoS systems connecting to the EHRi must contain:

a) The user ID of the accessing user;

b) The role the user is exercising63;

c) The organization of the accessing user (at least in those cases where an individual accesses information on behalf of more than one organization);

d) The patient ID of the data subject (patient/person);

e) The function performed by the accessing user;

f) A timestamp;

g) 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

h) In the case of changes to consent directives made by a substitute decision-maker, the identity of the decision-maker.

* Security Requirement 46 – Reporting Every Access to a Patient/Person's HER: The EHRi must be capable of identifying all users who have accessed or modified a given patient/person's record(s) over a given period of time.
* Security Requirement 47 – Reporting Every Access by a User: The EHRi must be capable of identifying all patients/persons whose records have been accessed or modified by a given user over a given period of time.
* Security Requirement 48 – Analyzing EHRi Audit Logs for Patients/Persons at Elevated Risk: The EHRi must provide functions for analyzing logs and audit trails to allow the identification of all users who have accessed or modified such record(s) over a given period of time.
* Security Requirement 49 – Securing Access to EHRi Audit Logs: The EHRi must secure access to audit records and must safeguard access to system audit tools and audit trails to prevent misuse or compromise.

## Access Control

### User Access Management

#### 4.2.8.1. User Registration

* Security Requirement 53 – Registering Users: All organizations connecting to the EHRi must subject potential users of PoS systems that connect to the EHRi to a formal user-registration process. These user-registration procedures must ensure:

a) The level of user identification that is provided is consistent with the assurance required, given the value of the information assets and the functions that will become available to the user;

b) Each potential user has a legitimate relationship with the organization; and

c) Each potential user has a legitimate need to access PHI via the EHRi.

* Security Requirement 54 – Assigning Identifiers to Users: All organizations connecting to the EHRi must ensure that users of PoS systems that connect to the EHRi are assigned an identifier (User ID) that, in combination with other identifiers (e.g. facility identifiers, jurisdictional identifiers), can uniquely identify the user within the EHRi. PoS systems must support the unique identification of users.
* Security Requirement 55 – Time-Limited User Registration: All organizations connecting to the EHRi must ensure that the registration of users of PoS systems that connect to the EHRi is time-limited (after which, the user’s registration must be renewed).

#### 4.8.2.2. Privilege Management

#### Role-Based Access Control

* + Security Requirement 57 – Granting Access to Users by Role: The EHRi and all PoS systems connected to the EHRi must support role-based access control (RBAC) capable of mapping each user to one or more roles and each role to one or more system functions.
  + Consideration CH26 – Select identity-proofing level of assurance by role: Consider what robust mechanism(s) should be used to initially prove the identity of the registrant and whether that level of assurance is required and/or adequate for all roles accessing the solution.
  + Consideration CH27 – Use a single identity credential where possible: Consider the use of a single identity (i.e. single sign-on) for users (i.e. patients or providers) where the portal provides access to other applications/services that have separate authentication mechanisms.
  + Consideration ID-14 – Consider Establishing Authentication Protocols for Use Among Member Organizations

#### Workgroup-Based Access Control

* + Security Requirement 59 – Granting Access to Users in Workgroups: The EHRi and all PoS systems connected to the EHRi must be capable of assigning users to working groups and granting access to records based on working groups.
  + Security Requirement 60 – Timely Revocation of Access Privileges: The EHRi and all PoS systems connected to the EHRi must support the revocation of user access privileges in a timely manner (i.e. immediately prevent the user from logging on after access privileges have been revoked).

#### Discretionary Access Control

* Security Requirement 61 – Granting Access By Association: The EHRi and all PoS systems connected to the EHRi:

a) Must be capable of associating users (i.e. healthcare providers) with the records of patients/persons and allowing future access based on this association (i.e., they must be capable of granting discretionary access to records based on a registered user with legitimate and pre-existing access to a patient’s record(s) granting access rights for that (those) record(s) to another registered user); and

b) Must not allow users to grant other users access to a record if the granting users themselves do not possess such access with respect to the record.

Note that granting other users access to a record does not override the role-based access control restrictions of those other users.

* Security Requirement 62 – Reporting the Access Privileges of a User: The EHRi must, and PoS systems connected to the EHRi should, provide functionality that can report, for a given user:

a) Which records the user can access;

b) Which portions of the record(s) the user can access; and

c) Which privileges (e.g. viewing, modification) the user has with respect to each of these records.

### 4.8.3. User Responsibilities

* Does not apply

### Network Access Control

* Does not apply

### Operating System Access Control

* + Security Requirement 69 – Restricting Connection Times to EHRi Applications: Where appropriate, the EHRi should restrict connection duration to EHRi application services to provide additional security for access to those applications.

### Application and Information Access Control

* Security Requirement 70 – Robustly Authenticating Users: The EHRi and all PoS systems connected to the EHRi must robustly authenticate users.

### Workstation Access Control

* Security Requirement 71 – Restricting Access to Unattended Workstations: All PoS systems connected to the EHRi must protect unattended workstations against an unauthorized person using the workstation while the PoS is active, such as with an automatic timeout after a period of inactivity. First,the best approach is to place workstations in a physically secure area in the first place. (está relacionado con cerrar sesión cuando hay inactividad en la app)
* Consideration MC21 – Establish and Enforce Session Timeouts: When designing or acquiring mobile applications intended to access or store PHI, organizations should ensure that the application has the ability to enforce a mandatory session timeout when left unattended.

### Mobile Computing and Teleworking

* Does not apply.

## Information Systems Acquisition, Development and Maintenance

### Correct Processing of Information

* Security Requirement 75 – Uniquely Identifying Patients/Persons: The EHRi and PoS systems connected to the EHRi must:

a) Ensure that patients/persons are assigned an identifier (patient ID) that can uniquely identify the patient/person within the EHRi or within the PoS system; and

b) Be capable of merging two or more EHR records if it is determined that multiple records for the same patient/person have been unintentionally created.

### Input Data Validation

* Security Requirement 76 – Validating Input Data: The EHRi and all PoS systems connected to the EHRi must include, wherever feasible, measures to safeguard against user error by validating data input to ensure that it is correct and appropriate. The following controls should be considered:

a) Input checks to detect the following errors:

i. out-of-range values;

ii. invalid characters in data fields;

iii. missing or incomplete data;

iv. exceeding upper and lower data volume limits;

v. unauthorized or inconsistent control data.

b) Procedures for responding to validation errors.

### Output Data Validation

* + Does not apply

### Cryptographic Controls

* + Consideration MC17 – Uniquely Identify the Individual Using a Mobile Device: Establish approved mechanisms that will allow the organization to uniquely identify the user of a shared mobile device, prior to granting access to confidential information.
  + Consideration MC22 – Ensure Communications Channel Encryption: Organizations should ensure that all mobile communications channels that transmit or receive confidential information are encrypted.

### Security of File Systems

* + Does not apply

### Security in Development and Support Processes

* + Does not apply

### Vulnerability Management

* + Does not apply

## Information Security Incident Management

### Reporting Incidents and Weaknesses

* Does not apply

### Management of Incidents and Improvements

* Does not apply

## Business Continuity Management

* Does not apply

## Compliance

* Does not apply