Security Objectives:

Project documentation often contains security-relevant statements that are indicative of the security requirements of a system. To identify security-relevant statements in project documentation, it can be helpful to think in terms of security objectives of the software system.

The following table provides a guide for understanding security objectives and a guide to identifying statements that imply the need for each security objective.

Confidentiality (C)	The degree to which the "data is disclosed only as intended"
	Statements that indicate a need for confidentiality: • presence of read-type verbs (read, view, display, share, alert, use, export, retrieve, report etc) when accessing a sensitive resource • securing or restricting access to a sensitive resource • specification of user roles and access rules (e.g., granting or revoking access)
Integrity (I)	"The degree to which a system or component prevents unauthorized access to, or modification of, computer programs or data."
	Statements that indicate a need for integrity: • presence of write-type verbs (create, update, delete, save, auto-populate, review, verify, generate, define, apply etc) when accessing a sensitive resource • accuracy, consistent understanding and interpretation of sensitive information • auto-population or merging of sensitive information • environmental checks (firewall, denial of service, virus checking, app firewalls)
Identification & Authentication (IA)	The need to establish and verify the identity of a user, process or device.
	Statements that indicate a need for identification & authentication: • need to identify / verify the entity (user or system) accessing a sensitive resource • need to identify / verify the source of data (e.g., patient originated data vs. clinic originated data)
Availability (A)	"The degree to which a system or component is operational and accessible when required for use."
	Statements that indicate a need for availability: • time or location constraints on information (e.g., real-time information) • data retention, historical or longitudinal data (available over a period of time) • checks and limits on resource utilization • backups, replication or archiving of resources
Accountability	Degree to which actions affecting software assets "can be traced to the actor responsible for the action"
	Statements that indicate a need for accountability: • recording of actions (e.g., accessing a resource) related to sensitive resources • recording of events (e.g., alerts and notifications) related to sensitive resources • ability to reconstruct history of actions and events • preventing someone or a component from denying they performed an action • transactions of data (create, read, update, delete, merge, unmerge, assign, …)
Privacy (PR)	The degree to which an actor can understand and control how their information is used.
	Statements that indicate a need for privacy: • ability of an individual to exercise control over the collection, use and dissemination of his or her personally identifiable information (e.g., by providing consent) • gathering, usage, disclosure, and management of user or client data • masking of the identity of specific users or individuals • legal and compliance issues related to personally identifiable information

Security Functional Requirements:

For each security objective, we now present a set of example security functional requirements that can be incorporated into a system depending on the system's security needs.

	Example
Confidentiality	**Statement:** The system shall provide a means to edit discharge instructions for a particular patient. **Security Requirements:** • The system shall enforce access privileges that enable authorized users to edit discharge instructions for a particular patient. • The system shall encrypt discharge instructions and store discharge instructions in encrypted format using an industry-approved encryption algorithm. • The system shall transmit discharge instructions in encrypted format to and from authorized users. • The system shall monitor the status and location of system components that may contain unencrypted discharge instructions data.
Integrity	**Statement:** All users should be able to see and view deleted and active documents. **Security Requirements:** • The system shall ensure consistent understanding of deleted and active documents by the user during viewing. • The system shall have provision to report errors in deleted and active documents during viewing.
	Statement: There must therefore be some capacity within the EHRi to merge multiple instances of patient records into a single record. **Security Requirements:** • The system shall ensure that all mandatory information is provided for the patient records before merging. • The system shall protect against loss of information during merging patient records. • The system shall have provision to report errors in patient records during merging. • The system shall have provision to report errors in patient records after merging. • The system shall have provision to correct errors in patient records if errors are detected. • The system shall ensure synchronization of patient records if multiple users can perform merging on patient records simultaneously.
	Statement: Add functionality to be able to delete unpublished versions of an intake. **Security Requirements:** • The system shall ensure that deleting unpublished versions of an intake is performed in accordance with the retention policy.
	Statement: The system shall prevent modifications to the audit records. **Security Requirements:** • The system shall not allow modification of audit records by any user.
Availability	**Statement:** VLER DAS stores event descriptions in an audit log for a minimum of six (6) years. **Security Requirement:** • The system shall store and make available audit event descriptions for a period of at least 6 years. • The system shall provide the capability for an administrator to purge data that is at least 6 years old and in accordance with organizational retention policy. [see I4]
	Statement: respond to requests for access to a patient or person’s PHI within a reasonable time. **Security Requirement:** • The system shall respond to user access to a patient within a reasonable time. • The system shall provide monitoring capabilities to ensure that response time falls within reasonable time period.

	Example
	Statement: If the system claims to be available 24 by 7 then the system shall have ability to run a backup concurrently with the operation of the application. **Security Requirement:** • The system shall ensure system availability to the user 24 by 7. • The system shall provide monitoring capabilities to ensure that system is available to users 24 by 7.
	Statement: If the system claims to be available 24 by 7 then the system shall have ability to run a backup concurrently with the operation of the application. **Security Requirement:** • The system shall have the capability to produce backups and recover the system from the backups. The backup and recovery selections must take into account system recovery time objectives as well as system data recovery point objectives.
	Statement: VLER DAS receives a maximum of 500 results in reverse chronological order by Creation Date. **Security Requirements:** • The system shall limit the number of records presented to the user for VLER DAS results when the request limit of 500 results is reached. • The system shall notify the user that the maximum number of records was returned.
Identification & Authentication	**Statement:** Include a prompt for staff when they log into OSCAR that asks them to choose their current clinic location before they proceed to the appointment schedule for that day. **Security Requirement:** • The system shall not ensure the user selects their current clinic location before any further action is taken within the system.
Accountability	**Statement:** The system should provide the ability to check medications against a list of drugs noted to be ineffective for the patient in the past. **Security Requirements:** • The system shall log every time the user checks medications against a list of drugs noted to be ineffective for the patient in the past. • At a minimum, the system shall capture the following information for the log entry: user identification, timestamp, check, medication, <patient identification>. • The system shall prevent all users from modifying the log entry. • The system shall allow only the authorized auditors to view the log entry.
	Statement: The EHRi and all POS systems connected to the EHRi must robustly authenticate users. **Security Requirements:** • The system shall log every time the user logs into and logs out of the system. • At a minimum, the system shall capture the following information for the log entry: user identification, timestamp, login/logout. • The system shall prevent all users from modifying the log entry. • The system shall allow only authorized auditors to view the log entry.
	Statement: The system shall be able to generate a backup copy of the application data, security credentials, and log or audit files. **Security Requirements:** • The system shall log every time backup happens. • At a minimum, the system shall capture the following information for the log entry: timestamp, backup • The system shall prevent all users from modifying the log entry. • The system shall allow only authorized auditors to view the log entry.

	Example
Privacy	**Statement:** Nurses require access to historical patient data to support patient interaction and care planning. **Security Requirements:** • The system shall allow the owner of historical patient data to be notified of potential authorized uses of historical patient data. • The system shall allow the owner of historical patient data to be notified when the historical patient data is accessed by nurses. • The system shall have the ability to get consent from the owner of historical patient data before accessing historical patient data for authorized use. • The system shall allow access to historical patient data for authorized use without prior consent only under exceptional circumstances as defined by applicable privacy policy.