**Security Functional Requirements:**

For each security objective, we have developed a set of context-specific templates and example security functional requirements that can be generated using these templates.

|  | **ID** | **Description** | **Example** |
| --- | --- | --- | --- |
| **Confidentiality** | **C1** | **Authorized access**  *Given:*  <subject> = user  <resource> = sensitive information  <action> = create/read/update/delete/share type actions  *Add Security Requirements:*   * The system shall enforce access privileges that <enable|prevent> <subject> to <action> for <resource>. [see AY1, C2, I1, I2, I4] | **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 monitor the status and location of system components that may contain unencrypted discharge instructions data. * The system shall transmit discharge instructions in encrypted format to and from authorized users. |
| **C2** | **Confidentiality during storage**  *Given:*  <resource> = sensitive information  *Add Security Requirements:*   * The system shall encrypt <resource> and store <resource> in encrypted format using an industry-approved encryption algorithm. [see AY3, I2, I4] * The system shall monitor the status and location of system components that may contain unencrypted <resource> data. |
| **C3** | **Confidentiality during transmission**  *Given:*  <subject> = user  <resource> = sensitive information  <action> = send/receive/transmit  *Add Security Requirements:*   * The system shall transmit <resource> in encrypted format to and from the authorized <subject>. [see C1, I4] |
| **Integrity** | **I1** | **Maintaining integrity during read-type actions**  *Given:*  <subject> = system, user or role  <resource> = sensitive information  <action> = read / view / display / send / receive  *Add Security Requirements:*   * The system shall ensure consistent understanding of <resource > by the <subject> during <action>. [see AY1] * The system shall have provision to report errors in <resource> during <action>. [see AY1] | **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. |
| **I2** | **Maintaining integrity during write-type actions**  *Given:*  <subject> = system, user or role  <resource> = sensitive information  <action> = create / update / auto-populate / merge  *Add Security Requirements:*   * The system shall ensure that all mandatory information is provided for the <resource> before <action>. * The system shall protect against loss of information during <action>. * The system shall have provision to report errors in <resource> during <action>. [see AY1] * The system shall have provision to report errors in <resource> after <action>. [see AY1] * The system shall have provision to correct errors in <resource> if errors are detected. [see AY1] * The system shall ensure synchronization of <resource> if multiple <subject>s can perform <action> on <resource> simultaneously. [see AY1] | **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. |
| **I3** | **Maintaining integrity during delete actions**  *Given:*  <subject> = system, user or role  <resource> = sensitive information  <action> = delete  *Add Security Requirements:*   * The system shall ensure that <action> on <resource> is performed in accordance with the retention policy. [see AY1] | **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. |
| **I4** | **Maintaining integrity of unchangeable resources**  *Given:*  <resource> = write-once information (e.g., log files)  *Add Security Requirements:*   * The system shall not allow modification of <resource> by any user. [see AY1] | **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** | **A1** | **Maintaining availability of data**  *Given:*  <time> = length of time, typically one year  <keywords> = retention | archive | history  <resource> = information  <action> = read / view / display / send / receive / access  *Add Security Requirements:*   * The system shall store and make available <object> for a period of at least <time period>. [see C1] * The system shall provide the capability for an administrator to purge data that is at least <time period> old and in accordance with organizational retention policy. [see I4] | **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] |
| **A2** | **Maintaining appropriate response time**  *Given:*  <time> = short duration, typically less than 10 seconds  <action> = any action present  *Add Security Requirements:*   * The system shall respond to user <action> within <time period>. * The system shall provide monitoring capabilities to ensure that response time falls within <time period>. | **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. |
| **A3** | **Maintaining service availability**  *Given:*  <time duration> = time of day for service/system to be available  <service> = any system component present  <action> = optional action  *Add Security Requirements:*   * The system shall ensure <service> to user <action> during <time period>. * The system shall provide monitoring capabilities to ensure that <service> is available to users / other system components during <time period> | **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. |
| **A4** | **Provide backup and recovery capabilities**  *Given:*  <keyword> = backup, recovery  *Add Security Requirements:*   * 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.   [See C1] | **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. |
| **A5** | **Limit resources to ensure capacity and performance** constraints  *Given:*  <resource> = any resource  <limiter> = limit on the number of records or size of the record  *Add Security Requirements:*   * The system shall limit the number of records presented to the user for <resource> when the request limit of <limiter> is reached. * The system shall notify the user that the maximum number of records was returned. | **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** | **IA1** | **Need to select context for roles or other attributes** **affecting accessibility to data**.  *Given:*  Statement to choose a specific role or attribute for system access.  *Add Security Requirement:*   * The system shall ensure the user has selected <context> prior to performing any further action within the system. [see C1, AY3] | **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 ensure the user selects their current clinic location prior to performing any further action within the system. |
| **IA2** | **Unique accounts**  *Given:*  Statement implying users need to be uniquely identified  *Add Security Requirement:*   * Each user should be assigned a unique identifier that can be used for the purpose of authentication. [see AY3] | **Statement:** All users are registered and uniquely identified.  **Security Requirement:**   * Each user should be assigned a unique identifier that can be used for the purpose of authentication. * The system should implement a mechanism to authenticate each user. * System shall integrate with an existing single sign-on mechanism. |
| **IA3** | **Authentication**  *Given:*  Statement implying need for user authentication  *Add Security Requirement:*   * The system should implement a mechanism to authenticate each user. * System shall integrate with an existing single sign-on mechanism. |
| **Accountability** | **AY1** | **Logging transactions with sensitive data**  *Given:*  <subject> = user or role  <resource> = sensitive information  <action> = create/read/update/delete  *Add Security Requirements:*   * The system shall log every time <subject> [performs the] <action> <on|for> <resource>. [see C1, I4] * At a minimum, the system shall capture the following information for the log entry: <subject> identification, timestamp, <action>, <resource>, and identification of the owner of <resource>. [see IA2, C1, I4] | **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>. |
| **AY2** | **Logging authentication events**  *Given:*  <subject> = user or role  <action> = logging-in, logging-out  *Add Security Requirements:*   * The system shall log every time <subject> logs into and logs out of the system. [see C1, I4] * At a minimum, the system shall capture the following information for the log entry: <subject> identification, timestamp, <action>. [see IA2, C1, I4] | **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. |
| **AY3** | **Logging system events**  *Given:*  <action> = system-level action that cannot be traced to a specific user account  *Add Security Requirements:*   * The system shall log every time <action> happens. [see C1, I4] * At a minimum, the system shall capture the following information for the log entry: timestamp, <action>. [see C1, I4] | **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 |
| **Privacy** | **PR1** | **Usage of personal information**  *Given:*  <subject> = user or role  <resource> = sensitive information  <action> = create/read/update/delete/disclose  *Add Security Requirements:*   * The system shall allow the owner of <resource> to be notified of potential authorized uses of <resource>. [see C1] * The system shall allow the owner of <resource> to be notified when the <resource> is <action> by <subject>. [see I2, AY1] * The system shall have the ability to get consent from the owner of <resource> before accessing <resource> for authorized use. [see C1, AY1] * The system shall allow access to <resource> for authorized use without prior consent only under exceptional circumstances as defined by applicable privacy policy. [see I2, AY1] * The system shall have provision for the owner of <resource> to withdraw consent for <action> <on|> <resource>. [see C1, AY1] * The system shall have provision for de-identifying the <resource> before <action> by <subject>, if required. [see C1, AY1] | **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. * The system shall have provision for the owner of historical patient data to withdraw consent for accessing historical patient data. * The system shall have provision for de-identifying the patient data before access by nurses, if required. |