User and Functional Requirement Specifications

Signatures indicate agreement and/or approval with the contents of this change request as an accurate definition of the tasks, responsibilities, and activities required for completing the project. The author and approver names and functions are identified in the electronic document repository. The approval information is stored electronically with this document within the electronic document repository (WindChill).

|  |  |  |  |
| --- | --- | --- | --- |
| **Document Version Number** | **Document Revision Date** | **Change Request ID** | **Change Summary**  **(Reference section[s] changed)** |
| A (Windchill) | 09-JUL-2020 | 90656259 | Initial version of Rave Requirements specification:  1) Derived from Rave Requirements Traceability Matrix (RTM) by covering all user requirements and functional requirements listed.  2) Migrating to BTS SLC template.  3) Added 2 new URS IDs: UR-018 & UR-019 and 2 new FRS IDs: EI-002 & EI -003 as per CR 90656259. |

* 1. Table of Contents

|  |
| --- |
| [1.0 Overview](#_Toc31786357)  [1.1 Table of Contents](#_Toc31786358)  [1.2 Purpose](#_Toc31786359)  [1.3 Scope](#_Toc31786360)  [1.4 Responsibilities](#_Toc31786361)  [1.5 References](#_Toc31786362)  [2.0 Overall Description](#_Toc31786363)  [2.1 Application Perspective](#_Toc31786364)  [2.2 Application Features/Functions](#_Toc31786365)  [2.3 User Characteristics](#_Toc31786366)  [2.4 Constraints](#_Toc31786367)  [2.5 Assumptions and Dependencies](#_Toc31786368)  [3.0 Approtioning of Requirements](#_Toc31786369)  [4.0 Data Integrity Data Process Flow](#_Toc31786370)  [5.0 Specific Requirements](#_Toc31786371)  [5.1 System Functions (SF)](#_Toc31786372)  [5.2 Data Requirements (DA)](#_Toc31786373)  [5.3 Interface and Integration Requirements](#_Toc31786374)  [5.4 Feature Level Requirements](#_Toc31786375)  [5.5 Report and Form Requirements](#_Toc31786376)  [5.6 System Requirements](#_Toc31786377)  [5.7 Regulatory Requirements](#_Toc31786378)  [5.8 Software System Attributes](#_Toc31786379)  [5.9 Hardware Requirements](#_Toc31786380)  [5.10 Safety Requirements](#_Toc31786381)  [5.11 Communications Requirements](#_Toc31786382)  [6.0 Appendices](#_Toc31786383) |

1.0 Overview

The EDC Rave system is used globally (except for Russia) by sites (hospitals), core labs, Clinical Research Organizations (CROs) and Abbott Vascular (AV) to collect, store, and manage anonymized patient data throughout the lifetime of a trial.

The EDC Rave system is used as a repository of clinical trial data and other areas within Clinical Research use this data to support their business processes.

The Rave system is hosted as a Software-as-a-Service (SaaS) solution in the U.S. by the vendor, Medidata.

1.2 Purpose

The purpose of this document is to describe the requirements for the EDC Rave System.

The intended audience for this document is Rave System users, Abbott and Cognizant project team, and the System/Process owner.

1.3 Scope

The EDC Rave system will accomplish the business goal of storing the patients’ clinical trial data for various studies.

1.4 Responsibilities

| Term, Acronym | Definition |
| --- | --- |
| AE | Adverse Events |
| AV | Abbott Vascular |
| BTS | Business Technology Solutions |
| CDRT | Clinical Data Reporting Tool |
| CRO | Clinical Research Organization |
| CRF | Case Report Forms |
| CTMS | Clinical Trial Management System |
| DD | Device Deficiency |
| DM | Device Malfunction |
| eCRF | Electronic Case Report Form |
| EDC | Electronic Data Capture |
| ID | Identifier |
| PDF | Portable Document Format |
| RECON | Reconcilation system |
| SDV | Source Data Verification |

1.5 References

| Document Number | Document Title |
| --- | --- |
| BTSQC 09.05 | BTS IT Computerized System Life Cycle |
| 90534634 | EDC Rave – System Risk Classification |

2.0 Overall Description

The EDC Rave system is a web-based application hosted in the cloud as a Software-as-a-Service (SaaS) solution by the third-party vendor Medidata. The Rave system manages stored clinical trial data, provides the ability to generate reports, and integrates with other downstream Clinical systems (e.g., ClinDART, RECON, CDRT, and CTMS).

2.1 Application Perspective

The EDC Rave system records patients’ clinical trial data for various clinical studies. The Rave system allows users to generate CRFs for the recorded clinical trials.

### 2.1.1. Operations

Not Applicable.

### 2.1.2. Site Adaptation/Localization Requirements

Not Applicable.

2.2 Application Features/Functions

The EDC Rave system allows sites (hospitals) to record clinical trial data.

The Rave system allows site users to add the subject and related subject data for various studies. The data can be events such as AE, DM, DD, medications, device data, subject follow-up data, etc. CRFs are generated with all the recorded clinical trial data and Rave allows site users to view and download the report as a PDF file.

The EDC Rave system allows the recorded clinical trial data to be sent to other downstream applications.

2.3 User Characteristics

Not applicable.

2.4 Constraints

Not Applicable.

2.5 Assumptions and Dependencies

Not Applicable.

3.0 Approtioning of Requirements

Not Applicable.

4.0 Data Integrity Data Process Flow

The following diagram describes the Rave system data flow to other integrated clinical system applications.



5.0 Specific Requirements

|  | **User Requirements**  EDC Rave system User requirements | |
| --- | --- | --- |
| **UR ID** | **User Requirement Description** | **Feature Criticality** |
| **UR-001** | Sites should be able to collect and view trial-specific patient data as per protocol. | Non-Critical |
| **UR-002** | Email should be triggered to notify Abbott sponsor group about protocol stipulated patient data in the trial.  Trial should be able to trigger forms in appropriate visits, as well as map and calculate patient data, as per protocol. | Non-Critical |
| **UR-003** | Appropriate queries should fire for inconsistent patient data in the trial. | Non-Critical |
| **UR-004** | Trial should be able to capture data within designated time-point, as per protocol. | Non-Critical |
| **UR-005** | Sponsor should be able to track source verification of the data against patient documentation. | Non-Critical |
| **UR-006** | Investigator should be able to provide electronic signature to confirm data validity.  The system should provide capability to sign forms electronically. | Non-Critical |
| **UR-007** | Trial should be able to provide appropriate functionality to users based on their roles and responsibility. | Non-Critical |
| **UR-008** | Trial should be able to provide appropriate data access to users based on their roles and responsibility. | Non-Critical |
| **UR-009** | Sponsor should be able to run reports as needed for tracking various trial parameters. | Non-Critical |
| **UR-010** | Sponsor should be able to migrate patient data when the trial has been updated. | Non-Critical |
| **UR-011** | Sponsor should be able to translate between languages. | Non-Critical |
| **UR-012** | System shall provide the capability to build and execute a risk-based, partial SDV, based on study parameters. | Non-Critical |
| **UR-013** | The system should allow the user to generate eCRF PDF, in both annotated and non-annotated format, with or without subject data. | Other |
| **UR-014** | The system should have the capability to create and manage sites and users (both Site and Sponsor). | Non-Critical |
| **UR-015** | The system should allow users such as Data Managers, Monitors and Study Managers the ability to make changes to the form status in batches; to apply actions such as ‘verify, freeze, and lock’ to multiple eCRFs for multiple subjects. | Other |

|  | **User Requirements**  EDC Rave system User requirements | |
| --- | --- | --- |
| **UR ID** | **User Requirement Description** | **Feature Criticality** |
| **UR-016** | The system shall send the Subject ID and data entry completion status information to CTMS. It’s not applicable for testing - studies not enrolling at this time. | Other |
| **UR-017** | The system should have the capability to code AEs and Medications using Coder module. | Non-Critical |
| **UR-018** | The system shall send Subject details, AEs, and DM information to the RECON system. | Other |
| **UR-019** | ClinDART system shall be able to pull data from Rave system to run reports within ClinDART. | Other |

5.1 System Functions (SF)

Not Applicable.

5.2 Data Requirements (DA)

Not Applicable.

5.3 Interface and Integration Requirements

### 5.3.1. User Interfaces

|  | **User Interfaces**  EDC Rave Systemuser interfaces requirements | |
| --- | --- | --- |
| **UI ID** | **Functional Specification Description** | **Feature Criticality** |
| **UI-001** | The system shall provide the ability to build eCRFs to allow users to enter, save, and view data. | Non-Critical |
| **UI-002** | The system shall execute functional rules for the trial, including complex edit checks, custom functions, derivations, and email rules. | Non-Critical |
| **UI-003** | The system shall execute data checks for the trial, including range checks, edit checks, and custom functions. | Non-Critical |
| **UI-004** | The system shall have appropriate forms folder (visit) mapping, per the protocol. | Non-Critical |
| **UI-005** | The system shall have verification functionality for the trial to allow source data verification tracking. | Non-Critical |
| **UI-006** | The system shall implement electronic signatures on specific forms/folders. | Non-Critical |

|  | **User Interfaces**  EDC Rave Systemuser interfaces requirements | |
| --- | --- | --- |
| **UI ID** | **Functional Specification Description** | **Feature Criticality** |
| **UI-007** | The system shall implement groups’ rights and roles for the trial. | Non-Critical |
| **UI-008** | The system shall provide the ability to grant users access to data fields, based on user roles. | Non-Critical |
| **UI-009** | The system shall allow users to use standard, ad hoc, and custom reporting tools. | Non-Critical |
| **UI-010** | The system shall provide an interface for migrating existing subject data from one CRF version to another (this is a process in the Architect module). | Non-Critical |
| **UI-011** | The system shall allow the capability to enable users to translate Rave text strings from one language to another (e.g., from a reference locale, such as English, to a target locale, such as Japanese; Translation Workbench module). | Non-Critical |
| **UI-012** | The system shall provide the capability to build and execute a risk-based, partial SDV based on study parameters. | Non-Critical |
| **UI-013** | The system shall allow the user to generate PDFs with trial CRFs, with and without subject data. | Other |
| **UI-014** | The system shall have the capability to create and manage sites and users. | Non-Critical |
| **UI-015** | The system shall allow users to change the status of the forms individually or in batches. | Other |
| **UI-016** | The system shall provide the capability for users to perform medical coding on AEs and Medications using the Coder module. | Non-Critical |

### 5.3.2. Hardware Integration

Not Applicable.

### 5.3.3. Software Interfaces

Not Applicable.

### 5.3.4. Communication Interface

Not Applicable.

### 5.3.5. Internal Interface Requirements

Not Applicable.

### 5.3.6. External Interface Requirements

|  | **External Interfaces**  EDC Rave Systemexternal interfaces requirements | |
| --- | --- | --- |
| **EI ID** | **Functional Specification Description** | **Feature Criticality** |
| **EI-001** | The system shall provide the capability to export data entry completion status and subject IDs to CTMS. | Other |
| **EI-002** | The system shall provide the capability to export Subject details, AEs, and DM information to the RECON system. | Other |
| **EI-003** | The system shall provide the capability for the ClinDART system to pull data to run reports. | Other |

5.4 Feature Level Requirements

Not Applicable.

5.5 Report and Form Requirements

Not Applicable.

5.6 System Requirements

### 5.6.1. Performance Requirements

Not Applicable.

### 5.6.2. Database Requirements

Not Applicable.

5.7 Regulatory Requirements

### 5.7.1. Electronic Record and Electronic Signature Requirements

**NOTE:** All text in brackets “[ ]” indicates applicable 21 CFR policy reference.

|  |  | **Record Access and Retrievability**  These functions are required if the system maintains quality records  N/A – The system does not contain electronic records used for quality decisions. | | |
| --- | --- | --- | --- | --- |
| **Reg.** | **ERS ID** | **Functional Specification Description** | **Requirement Type** | **Feature Criticality** |
| ERES | R500 | The system shall be in compliance with 21 CFR Part 11 Record Access and Retrievability requirements. | User | Non-Critical |
| ERES | R500.001 | The system shall provide access to complete records and documents in human readable form.  [11.10(b)] | Functional | Non-Critical |
| ERES, DI | R500.002A | The system shall be able to retrieve active and historical data, metadata, audit trail and signature information.  [11.10(b), 11.10(c)] | Functional | Non-Critical |
| ERES | R500.002B | The system shall provide (e.g. reports) indication if any data has been changed (e.g. corrected) since the original entry. | Functional / Procedural | Non-Critical |
| N/A | R500.003 | The System must maintain the integrity and security of electronic quality records and any associated electronic signatures for the retention period of the record. | This is a duplicate FRS of RS R500.007 Not Applicable. | |
| ERES | R500.004 | The system shall be capable of detecting invalid or altered records.  [11.10(a)] | Functional | Non-Critical |
| ERES | R500.005 | The system shall provide the ability to derive original results from raw data retained as a quality record.  [11.10(c)] | Functional | Non-Critical |
| ERES | R500.006 | The system shall maintain the integrity and security of electronic quality records and any associated electronic signatures when data is migrated.  [11.10(c)] | Functional | Non-Critical |
| ERES | R500.007 | The system must maintain the integrity and security of electronic quality records and any associated electronic signatures for the retention period of the record, if required by predicate rule. [11.10(c), 11.10(e), 11.30, 11.50(b)] | Functional  And/or  Procedural | Non-Critical |

|  |  | **Security**  These functions are required if the system maintains quality records  N/A – The system does not maintain quality records. | | |
| --- | --- | --- | --- | --- |
| **Reg.** | **ERS ID** | **Functional Specification Description** | **Requirement Type** | **Feature Criticality** |
| ERES | R510 | The system shall be in compliance with 21 CFR Part 11 Security requirements. | User | Non-Critical |
| ERES; PII | R510.008 | The system shall prohibit access by unauthorized users.  [11.10(d), 11.10(g)] | Functional | Non-Critical |
| ERES; PII | R510.009 | The system shall require a minimum of 2 components (e.g., user ID and password) for access.  [11.10(d)] | Functional | Non-Critical |
| ERES; PII | R510.010 | The system shall require individual account access (except for read only access).  [11.10(d), 11.10(g)] | Functional  And/or  Procedural | Non-Critical |
| ERES; PII | R510.011 | The system shall prevent the reuse of user accounts.  [11.10(a), 11.300(a)] | Functional  And/or  Procedural | Non-Critical |
| ERES; PII | R510.012 | The system shall prevent the use of automated logins or the use of login scripts by individual users.  [11.10(g)] | Procedural | Non-Critical |
| ERES; PII | R510.013A | The system shall define system access and security levels for authorized individuals.  [11.10(d)] | Functional | Non-Critical |
| ERES; PII | R510.013B | System and data administrators (with capability to delete records) shall be independent from the group using the system. | Procedural | Non-Critical |
| ERES; PII | R510.014 | The system shall provide controls (e.g., time outs, auto-logout) for system access if devices are left unattended.  [11.10(g)] | Functional | Non-Critical |
| ERES; PII | R510.015 | The system shall define an “unauthorized attempts” threshold (e.g., 6 failed attempts) and report upon detection of reaching this threshold to appropriate authority.  [11.300(d)] | Functional | Non-Critical |
| ERES; PII | R510.016 | The system shall require all users to change their system access passwords (or second component) at least every 90 days.  [11.300(b)] | Functional and  Procedural | Non-Critical |
| ERES; PII | R510.017 | All remote or interfaced systems are authenticated prior to the transfer or processing of data.  [11.10(h)] | Functional | Non-Critical |
| ERES; PII | R510.018 | Instruments or other automated input devices, interfaces or connections to the system are checked to ensure that they are properly identified and connected to the system.  [11.10(h)] | Functional | N/A |
| ERES; PII | R510.019 | Device (e.g., terminals) checks are in place to determine the validity of the source of data input or operational instruction, as appropriate.  [11.10(h)] | Functional | Non-Critical |

|  |  | **Change Control and Audit Trail**  These functions are required if a user or system can create or modify quality records.  N/A – Users cannot create or modify quality records in the system. | | |
| --- | --- | --- | --- | --- |
| **Reg.** | **ERS ID** | **Functional Specification Description** | **Reg.** | **ERS ID** |
| ERES | R520 | The system shall be in compliance with 21 CFR Part 11 Change Control requirements. | User | Non-Critical |
| ERES  PII | R520.020 | The system shall require that all changes to an electronic quality record are documented.  [11.10(e)] | Functional | Non-Critical |
| ERES | R520.021 | The system shall assure that changes to an electronic quality record not obscure previously recorded information.  [11.10(e)] | Functional | Non-Critical |
| ERES | R520.022 | The system shall provide an obvious indication of changes made to an electronic quality record (e.g., version control, highlighted fields).  [11.10(e)] | Functional | Non-Critical |
| ERES  PII  DI | R520.023 | The system shall capture human initiated creation and changes to an electronic quality record in an audit trail at the time of commitment.  [11.10(e)] | Functional | Non-Critical |
| ERES  DI | R520.024 | The system shall provide a link between the audit trail and associated electronic records for the retention period of the record.  [11.10(e)] | Functional  and  Procedural | Non-Critical |
| ERES  PII  DI | R520.025 | The audit trail shall capture the User ID, date and time of actions, indicated at a minimum to the nearest minute, and user action taken (e.g., create, modify, or delete electronic records), and reason for change.  [11.10(e)] | Functional | Non-Critical |
| ERES  PII  DI | R520.026A | The system shall provide access for review of audit trail information.  [11.10(e)] | Functional | Non-Critical |
| ERES  DI | R520.026B | All records that are critical and/or subject to alteration are reviewed on a periodic basis, and/or as part of routine batch release to insure data integrity. | Procedural | Non-Critical |
| ERES  PII  DI | R520.027 | The system shall automatically generate audit trail information.  [11.10(e)] | Functional | Non-Critical |
| ERES  PII  DI | R520.028 | The system shall protect audit trail information so that it cannot be modified or disabled through normal means.  [11.10(e)] | Functional | Non-Critical |

|  |  | **Electronic Signatures**  These functions are required if electronic signatures are applied to the quality records by the system.  N/A – The system does not apply electronic signatures to quality records. | | |
| --- | --- | --- | --- | --- |
| **Reg.** | **ERS ID** | **Functional Specification Description** | **Requirement Type** | **Feature Criticality** |
| ERES | R530 | The system shall be in compliance with 21 CFR Part 11 Change Control requirements. | User | Non-Critical |
| ERES | R530.029 | The system shall provide a separate computer system logon event and e-signature application event.  [11.200(a)(1)] | Functional | Non-Critical |
| ERES | R530.030 | The system shall provide a link between electronic signatures and electronic records, including associated metadata, which cannot be easily refuted for the retention period of the record.  [11.70] | Functional | Non-Critical |
| ERES | R530.031 | The electronic signature manifestation shall be subject to the same controls as the associated electronic record.  [11.50(b)] | Functional | Non-Critical |
| ERES | R530.032 | The system shall prevent re-use of an electronic signature by another individual.  [11.100(a)] | Functional  And/or  Procedural | Non-Critical |
| ERES | R530.0 33A | The system shall require a unique combination of two components for an electronic signature.  [11.200(a)(1)] | Functional  And/or  Procedural | Non-Critical |
| ERES | R530.0 33B | The system shall require that the first component of an electronic signature (e.g., user ID) be unique to one person.  [11.100(a)] | Functional  And/or  Procedural | Non-Critical |
| ERES | R530.0 33C | The system shall assure that the first component of an electronic signature (e.g., user ID) cannot be reassigned to, reused by, or shared with another person.  [11.100(a)] | Functional  and  Procedural | Non-Critical |
| ERES | R530.0 33D | The system shall require that the second component of an electronic signature (e.g., password) be associated with the first component.  [11.300(a)] | Functional  and  Procedural | Non-Critical |
| ERES | R530.0 33E | The system shall assure that the second component of an electronic signature (e.g., password) cannot be entered through automated means.  [11.200(g)(1)(i)] | Procedural | Non-Critical |
| ERES | R530.034 | The system shall present the following information in the manifestation of an electronic signature in human readable form.   * *Printed full name of the signer* * *Date of the signature execution* * *Accurate time of the signature execution and* * *Meaning* of the signature (e.g. approval, rejection).   [11.50(a)] | Functional | Non-Critical |
| ERES | R530.035 | The system shall present the manifestation of the electronic signature on all printed and displayed forms of its associated electronic record.  [11.50(b)] | Functional | Non-Critical |
| ERES | R530.036 | The system shall maintain the security and integrity of the electronic signature.  [11.70] | Functional | Non-Critical |
| ERES | R530.037 | Users are required to change their signature passwords (or second component) at least every 90 days.  [11.300(b)] | Functional | Non-Critical |
| ERES | R530.038A | The system shall define a period of inactive time, after which a session must be considered non-continuous.  [11.200(a)(1)(ii)] | Functional | Non-Critical |
| ERES | R530.038B | If there are multiple signings in a continuous session, the initial signing shall require all components (user ID and password).  [11.200(1)(i)] | Functional | Non-Critical |
| ERES | R530.038C | Non-continuous signing sessions shall require entry of both components (user ID and password) for each signing.  [11.200(1)(ii)] | Functional | Non-Critical |
| ERES | R530.039 | The system shall require users to change their signature passwords upon first use following administration password assignment.  [11.300(c)] | Functional / Procedural | Non-Critical |
| ERES | R530.040 | The system shall define an “unauthorized attempts” threshold for applying an electronic signature (e.g., 6 failed attempts) and report upon detection of reaching this threshold to appropriate authority.  [11.300(d)] | Functional | Non-Critical |
| ERES | R530.041 | The system shall prevent automated execution of an electronic signature.  [11.10(g), 11.300(d)] | Procedural | Non-Critical |
| ERES | R530.042 | If a physical token is used for electronic signature, it shall lack at least one signature component.  [11.200(a)(1)] | Functional | N/A- System does not use physical tokens. |

|  |  | **Open System Functions**  These functions are required if the system is an open system and contains quality electronic records.  N/A – The system is not an open system. | | |
| --- | --- | --- | --- | --- |
| **Reg.** | **ERS ID** | **Functional Specification Description** | **Requirement Type** | **Feature Criticality** |
| ERES | R540 | The system shall be in compliance with 21 CFR Part 11 Open System requirements. | User |  |
| ERES; PII | R540.043 | The system shall provide encryption for records exchanged over an open system.  [11.30] | Functional |  |
| ERES | R540.044 | The system shall use digital signature standards or alternate technology.  [11.30] | Functional |  |
| ERES | R540.045 | Security is provided at both the sending and receiving systems.  [11.30] | Functional |  |

|  |  | **Hybrid System Functions**  These functions are required if this is a hybrid system.  N/A – The system is not a hybrid system. | | |
| --- | --- | --- | --- | --- |
| **Reg.** | **ERS ID** | **Functional Specification Description** | **Requirement Type** | **Feature Criticality** |
| ERES | R550 | The system shall be in compliance with 21 CFR Part 11 Hybrid System requirements. | User |  |
| ERES | R550.046 | The system shall assure that the final revision/editions of paper and electronic quality records have the same electronic content.  [11.10(e)] | Functional  and  Procedural |  |
| ERES | R550.047 | The system shall maintain traceability between an electronic quality record and paper record including any alterations.  [11.10(e)] | Functional  and  Procedural |  |
| ERES | R550.048 | Electronic quality records shall contain an indication when handwritten signatures are associated with it, e.g., printed signature line, comment indicating handwritten signature required.  [11.70] | Functional |  |
| ERES | R550.049 | Quality records generated from databases shall have sufficient information regarding the generation of the printed content of the electronic record to reproduce it (e.g., the query is stored on the paper record).  [11.10(e)] | Functional  and  Procedural |  |

|  |  | **Sequencing**  These functions are required if the system controls successive operations, events, and/or data entry.  N/A – The system does not control successive operations, events, or data entry. | | |
| --- | --- | --- | --- | --- |
| **Reg** | **ERS ID** | **Functional Specification Description** | **Requirement Type** | **Feature Criticality** |
| ERES | R560 | The system shall be in compliance with 21 CFR Part 11 sequencing requirements. | User | Critical |
| ERES, DI | R560.050 | If successive operations, events, and/or data entry are required, the system shall ensure the steps are followed in the correct sequence.  [11.10(f)] | Functional | Critical |

|  |  | **Privacy (PII)**  These functions are required if the system contains data regulated for privacy. For applicable IT controls related to the system see the Data Privacy Plan. Document any specific requirements below that are not covered in the above ERES requirements.  All IT controls are further documented within AQ09-05-UG01.  N/A – The system does not contain regulated Privacy data. | | |
| --- | --- | --- | --- | --- |
| **Reg** | **ERS ID** | **Functional Specification Description** | **Requirement Type** | **Feature Criticality** |
| PII | R570 | *The system shall be in compliance with Access, Identification, Authentication and Authorization Controls. (See change control FRS in ERES table.)* | Functional / Procedural | Critical |
| PII | R580 | *The system shall be in compliance with Audit and Accountability. (See audit trail FRS in ERES table)* | Functional / Procedural | Critical |
| PII | R590 | *The system shall be in compliance with Configuration Management Controls for:*  *Least functionality; Sensitivity Level Notification; Geography Considerations.* | Functional / Procedural | Critical |
| PII | R600 | *The system shall be in compliance with Event Logging and Incident Response for:*  *IT System Security Event Logging and IT System Security Incident Monitoring* | Functional / Procedural | Critical |
| PII | R610 | *The system shall be in compliance with Privacy by Design and Privacy by Default FRS that are applicable for: Notice/Consent and Personal Information Edit Capabilities;* | Functional / Procedural | Critical |
| PII | R620 | *The system shall be in compliance with Risk Assessment vulnerability scanning.* | Functional / Procedural | Critical |
| PII | R630 | *The system shall be in compliance with System and Communications Protection* | Functional / Procedural | Critical |

|  |  | **Payment Card Information (PCI)**  These functions are required if the system contains any PCI data or functionality.  N/A – The system does not control successive operations, events, or data entry. | | |
| --- | --- | --- | --- | --- |
| **Reg** | **ERS ID** | **Functional Specification Description** | **Requirement Type** | **Feature Criticality** |
| PCI | R640 | *The system shall comply with Payment Card Information Requirements (PCI)* | User |  |
| PCI | R640.001 | *The system shall Not store sensitive authentication data after authorization (even if encrypted) i,e,*   * *Full magnetic stripe* * *CVC2/CVV2/CID (card-validation code or value; the three-digit or four-digit number printed on the front or back of a payment card used to verify card-not-present transactions) and* * *Personal identification number (PIN) / PIN Block.* | Functional |  |
| PCI | R640.002 | *The system shall ensure that the storage of the following cardholder data is encrypted if stored in conjunction with the primary account number (PAN): cardholder name, service code, expiration date* | Functional |  |
| PCI | R640.003 | *The system shall mask the primary account number when displayed (the first six and last four digits are the maximum number of digits to be displayed) when there is not a specific business need to display the full number* | Functional |  |
| PCI | R640.004 | *The system shall render the primary account number, at minimum, unreadable anywhere it is stored by using any of the following approaches*   * *Strong one-way hash functions (hashed indexes)* * *Truncation* * *Index tokens and pads (pads should be securely stored) and* * *Strong cryptography with associated key management processes and procedures.* | Functional |  |

### 5.7.2. Electronic Record and Information Management (eRIM) Requirements

Not Applicable.

### 5.7.3. Other Regulatory Requirements

Not Applicable.

### 5.7.4. User Roles

For general Rave system user roles and permisssions, refer to 90534640 Design Specification.

Individual trials have specific roles and permisssions and those may be found in Form and Field Restrictions Specifications for each trial.

5.8 Software System Attributes

### 5.8.1. Reliability

Not Applicable.

### 5.8.2. Availability

Not Applicable.

### 5.8.3. Security

Not Applicable.

### 5.8.4. Data Integrity Requirements (DI)

Not Applicable.

### 5.8.5. Maintainability

Not Applicable.

### 5.8.6. Portability

Not Applicable.

5.9 Hardware Requirements

Not Applicable.

5.10 Safety Requirements

Not Applicable.

5.11 Communications Requirements

Not Applicable.

6.0 Appendices

Not Applicable.

END OF DOCUMENT