FUNCTIONAL REQUIREMENTS SPECIFICATION FOR VANDERBILT RESEARCH ELECTRONIC DATA CAPTURE (REDCAP) INFORMED CONSENT MODULE SERVING

VICTR DEPARTMENT
VANDERBILT UNIVERSITY
NASHVILLE, TN

DOCUMENT NUMBER: FRS-REDCAP-PART11-001
DATE ISSUED: 8/24/2018
REVISION: 0

PREPARED BY
RUSSELL BARBARE
VALIDATION ENGINEER
OFNI SYSTEMS

SIGNATURES

Author: Russell Barbare

Signature: Russell Barbare Date: 27 August 2018

System Owner: Paul A. Harris

Signature: Paul A. Harris Date: 27 August 2018

Quality Assurance: Julie Ozier

Signature: Julie Ozier Date: 28 August 2018

REVISION HISTORY

Rev #	Description	Date Approved
0	Initial Issue.	28 August 2018

TABLE OF CONTENTS

1. Introduction

1.1. Objectives

This is the Functional Requirement Specification for the Research Electronic Data Capture (REDCap) Informed Consent Module (FRS-REDCap-Part11-001), for use by VICTR at Vanderbilt University (Nashville, TN). The Research Electronic Data Capture (REDCap) system, hereafter referred to as REDCap, is used to collect electronic data online. The informed consent module collects informed consent forms. REDCap is a proprietary web server system and has been categorized as a GAMP category 5 GxP system.

The Functional Requirement Specification details the capabilities and functions that the REDCap informed consent module must be capable of performing. This specification will provide general, as well as specific requirements to be used in the design, validation and use of the system. By meeting requirements outlined in this document, the REDCap informed consent module will correctly and reliably perform its intended functionality.

1.2. Scope

This Functional Requirement Specification applies to the Research Electronic Data Capture (REDCap) informed consent module. The FRS will address what functions the REDCap informed consent module must be able to perform to fulfill 21 CFR 11 requirements for computer systems.

The validation project was outlined in the Validation and Compliance Plan for the Research Electronic Data Capture (REDCap) Informed Consent Module (VCP-REDCap-Part11-001). Details on how the system or system component will be developed and how it will operate will be defined in the Software Design Specification for the Research Electronic Data Capture (REDCap) Informed Consent Module (SDS-REDCap-Part11-001). Demonstrating successful installation and operation of these requirements will be described in the Installation and Operational Qualification Protocol for the Research Electronic Data Capture (REDCap) Informed Consent Module (IOQ-REDCap-Part11-001). The validation project will be summarized in the Validation Summary Report for the Research Electronic Data Capture (REDCap) Informed Consent Module (VSR-REDCap-Part11-001).

1.3. Assumptions/Restrictions

This validation applies to the REDCap informed consent module, and not the workstation or computer environment.

Vanderbilt University has contracted with Ofni Systems to create the validation package and perform validation testing.

The initial validation will be limited to 21 CFR Part 11 requirements and the functions of the informed consent module, but not to project-specific user or institutional requirements. Additional validations may be performed under this validation plan.

21 CFR 11 requirements cannot be met entirely by software - procedural controls are also necessary. This validation will indicate what procedural controls are necessary. Procedural controls that Vanderbilt has in place will be documented; procedural controls that users should have in place will be identified.

21 CFR 11 requires controls for both the developers and the users/administrators of electronic systems. Since REDCap is used both by Vanderbilt personnel and by other persons, businesses, and institutions not affiliated with Vanderbilt University, this validation will indicate which controls are the responsibility of the developers and which are the responsibility of the other users. Both internal and external users of REDCap must ensure that they meet the user responsibilities in order to meet have 21 CFR 11 compliance.

REDCap is configurable; some of the possible configurations will not meet 21 CFR 11 requirements unless specific settings are used or additional testing is performed. The initial validation will identify which settings are needed; system administrators or equivalent must ensure that individual instances have the appropriate settings.

2. Acronyms and References

2.1. Acronyms and Definitions

CFR - Code of Federal (US) Regulations

FRS - Functional Requirement Specification

GxP - Abbreviation which includes current Good Manufacturing, Clinical and Laboratory Practices

Informed Consent (form) - A document for recording informed consent as defined in ICH E6(R1)

IOQ - Installation/Operational Qualification

Informed Consent - The process as defined by ICH E6(R1) whereby a subject is informed about a clinical trial and consents to it.

Open System - An environment in which system access is not controlled by persons who are responsible for the content of electronic records that are on the system.

SDS - Software Design Specification

SOP - Standard Operating Procedure

VICTR - Vanderbilt Institute for Clinical and Translational Research

2.1.1. Project Administrator / User / Subject

REDCap has a flexible user / group / permission structure. Implementation of 21 CFR 11 security permissions practically requires at least three levels of access:

Project Administrator - A REDCap user who has rights to add or remove REDCap users. Requires a REDCap user ID and password.

User - A REDCap user who has rights to make system changes or review data for one or more REDCap trials. Requires a REDCap user ID and password.

Subject - A REDCap user who is a trial patient or subject. For a REDCap trials in which they are a clinical trial subject (as defined in ICH E6(R1)), Subjects cannot make any changes to the design, user lists, or settings and can only enter and view their own data.

Patient is synonymous with Subject in this hierarchy. REDCap Project Administrators may create additional security groups and/or levels but practical implementation of 21 CFR 11 requires at least these three authority levels. In order to delineate these terms from the more common usages of administrator, user, and subject, they will be capitalized; lowercase 'users' includes all of the above.

2.2. References

21 CFR Part 11 "Electronic Records; Electronic Signatures"

GAMP 5, A Risk-Based Approach to Compliant GxP Computerized Systems

International Conference on Harmonisation of Technical Requirements for Registration of Pharmaceuticals for Human Use, Guideline for Good Clinical Practice E6(R1)

IOQ-REDCap-Part11-001, Installation and Operational Qualification Protocol for the Research Electronic Data Capture (REDCap) Informed Consent Module

SDS-REDCap-Part11-001, Software Design Specification for the Research Electronic Data

Capture (REDCap) Informed Consent Module

VCP-REDCap-Part11-001, Validation and Compliance Plan for the Research Electronic Data Capture (REDCap)

3. System Description

3.1. System Software

REDCap is a proprietary web server system used to collect electronic data online. REDCap is considered to be an Open System, as defined in 21 CFR 11.3(9).

3.2. System Hardware Description

REDCap is a web server system designed and hosted by Vanderbilt University. REDCap is accessible through any web-connected device that meets the minimum requirements.

3.3. System Security

The system has a flexible user / group / permission structure to control user rights. Users entering data into the data collection forms can be controlled by a variety of methods.

3.4. System Interactions

The REDCap informed consent module does not interact with any other validated computer systems beyond those described in this document.

3.5. System Performance

There are no system performance requirements for REDCap.

3.6. System Availability

The system is available except during scheduled maintenance. REDCap will be maintained by the VICTR group.

3.7. Physical Environment

REDCap operates on standard Vanderbilt University servers hosted in a controlled environment. Users connect to REDCap via the internet, with no environmental controls. Environmental controls will not be tested.

4. Primary Business Functionality

The primary business function is to collect electronic data online. For the purposes of this validation, the validated business function will be collection of signed Inform Consent forms.

4.1. Informed Consent

Requirements for the informed consent form:

4.1.1. Subjects can complete an informed consent form.

4.1.2. Subjects can electronically sign an informed consent form.

5. Re□ulatory Requirements

This validation will demonstrate that the informed consent module of REDCap can be 21 CFR 11 compliant. Full compliance requires additional responsibilities on the part of the software users. Section 5.1 and its subsections will cover the general division of responsibilities and types of proof necessary to fulfill them properly; proof than Vanderbilt can supply will be verified as part of this validation. Other subsections under Section 5 will detail the specific responsibilities.

For the regulatory requirements, the collected data in the database is the record, the archived pdf is the audit trail and the informed consent form, and the First Name, Last Name, date/time stamp, consent form title, and any additional authentication the Sponsor requires is the electronic signature.

5.1. General Divisions of Responsibility

5.1.1. Software Developers versus Software Users

21 CFR 11 puts the primary responsibilities on the parties using the electronic system, not the developer. There are two general exceptions to this:

1) Certain sections of 21 CFR 11 specifically name other responsible parties.

2) Many sections of 21 CFR 11 require controls that can only be reasonably fulfilled using software. Therefore, the software developers are responsible for implementing controls that can be compliant.

The individual sections below will identify the responsible parties. Responsibilities of Vanderbilt will be verified as part of this validation; other responsibilities should be performed by the administrator(s) of the projects.

5.1.1.1. Generic Vanderbilt Responsibilities

In general, Vanderbilt is responsible for:

1) Any responsibilities assigned to software developers by 21 CFR 11.

2) Ensuring that the technical controls for 21 CFR 11 compliance that should be met by software can be met by the REDCap informed consent module.

Vanderbilt has agreed to:

3) Validate the non-project-specific functions of the system that are required for 21 CFR 11 compliance.

4) Provide that validation to Project Administrators who require 21 CFR 11 compliance.

For item 2), note that software is not required to be compliant under all possible settings. Instead, there must be some combination of settings that allows compliance, those settings must be enacted for projects that are expected to be compliant, and the compliant settings must be verified for projects.

5.1.1.2. Generic Project Administrators' Responsibilities

In general, project Administrators are responsible for:

1) Any responsibilities directly assigned to the project Administrators by 21 CFR 11.

2) Ensuring that all settings required for compliance are enacted and documented (validated) for the individual project.

3) Retaining the validation documents provided from Vanderbilt.

For Vanderbilt projects, these responsibilities are considered Vanderbilt responsibilities.

5.1.2. Software Settings

The software is not required to be compliant under all possible settings of the software. Instead, there must be some combination of settings that allow compliance, those settings must be enacted for compliant projects, and the compliant settings must be verified for compliant projects. The REDCap informed consent module is compliant under the correct settings and those will be identified in this validation. It is the responsibility of the administrators of the individual projects to enact and verify those settings for each project.

5.1.3. Software versus Procedures

Software cannot meet 21 CFR 11 requirements by itself – there have to be procedures also. This includes procedures both by Vanderbilt and by the organizations using the individual projects of REDCap. Sections below will indicate where procedures are necessary and which party is responsible for having them.

5.1.4. Electronic Signatures

Electronic signatures are optional under 21 CFR 11 but are necessary for informed consent. For this validation, the only electronic signatures used are for Subjects to sign the informed consent.

5.1.5. Optional Requirements

The following requirements of 21 CFR 11 are optional and are not used in REDCap:

Continuous electronic signing, an implied part of 11.200(a)(1), is not implemented in REDCap.

Signing-on-behalf-of (11.200(a)(3)) is not implemented in REDCap.

REDCap does not use biometrics (11.200(b)).

REDCap does not use physical authentication devices such as ID cards (11.300(c) and 11.300(e)).

5.2. Controls for Closed Systems (21 CFR 11 B Sec. 11.10)

REDCap will meet or exceed all technological and procedural requirements for systems in order to be compliant with 21 CFR Part 11 guidelines for Open Systems.

5.2.1. System Validation (21 CFR 11.10(a))

Regulatory requirement:

11.10(a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.

Interpretation:

Validation is required for the functions of the system that are important for patient safety, regulatory, or business functions.

5.2.1.1. Vanderbilt Responsibilities

The functions of the REDCap informed consent module that allow it to be 21 CFR 11 compliant will be validated as part of this validation; the completed validation documents are proof of the validation.

5.2.1.2. Project Administrators' Responsibilities

Project Administrators have the responsibility to:

Validate all custom parts of a project, including but not limited to the data collection forms.

Verify and document that all settings needed for 21 CFR 11 compliance listed in this validation package are set.

5.2.2. Accurate Record Generation (21 CFR 11.10(b))

Regulatory requirement:

11.10(b) The ability to generate accurate and complete copies of records in both human readable and electronic form suitable for inspection, review, and copying by the agency. Persons should contact the agency if there are any questions regarding the ability of the agency to perform review and copying of the electronic records.

Interpretation:

All user-entered data and all significant meta-data are available in human readable form and can be exported in formats that are readily viewable without using REDCap.

5.2.2.1. Vanderbilt Responsibilities

5.2.2.1.1. REDCap informed consent forms can be exported in human-readable and non-proprietary readable electronic format(s).

5.2.2.1.2. Significant REDCap meta-data can be exported in human-readable and readable non-proprietary electronic format(s).

5.2.2.2. Project Administrator Responsibilities

Verify that completed informed consent forms can be downloaded.

5.2.3. Protection of Records (21 CFR 11.10(c))

Regulatory requirement:

11.10(c) Protection of records to enable their accurate and ready retrieval throughout the records retention period.

Interpretation:

Records must be held on a system that is backed up can be recovered in a reasonable amount of time. Records that have a specific regulatory retention period are held for the retention period.

5.2.3.1. Vanderbilt Responsibilities

5.2.3.1.1. REDCap is backed up.

5.2.3.1.2. REDCap allows project administrators to enter a server to automatically archive informed consents to.

5.2.3.2. Project Administrator Responsibilities

If there are REDCap projects hosted outside of Vanderbilt, those projects must be covered by a backup and recovery policy.

Project administrators are responsible for determining the regulatory retention period of their informed consent forms and retaining them for that duration.

5.2.4. Limited System Access (21 CFR 11.10(d))

Regulatory requirement:

11.10(d) Limiting system access to authorized individuals.

Interpretation:

All levels of system access are controlled and limited to authorized users.

5.2.4.1. Vanderbilt Responsibilities

5.2.4.1.1. Access to REDCap project design, settings, or controls requires an active user ID and password.

5.2.4.1.2. REDCap passwords expire.

5.2.4.1.3. REDCap passwords have minimum complexity requirements.

5.2.4.1.4. Repeated successive invalid login attempts will lock out the REDCap user ID.

5.2.4.1.5. Invalid login attempts are logged.

5.2.4.1.6. REDCap logs out or locks after a period of inactivity.

5.2.4.2. Project Administrators' Responsibilities

Project Administrators are responsible for:

Having policies stating that REDCap user IDs are unique to one user and that passwords cannot be shared.

Creating and maintaining appropriate user and group accounts and privileges.

5.2.5. Audit Trails (21 CFR 11.10(e))

Regulatory requirement:

11.10(e) Use of secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying.

Interpretation:

User data entry and significant metadata, e.g., significant changes to system settings, must be tracked.

5.2.5.1. Vanderbilt Responsibilities

5.2.5.1.1. The audit trail is secure.

5.2.5.1.2. The audit trail is computer generated.

5.2.5.1.3. The audit trail has an accurate time/date stamp.

5.2.5.1.4. The audit trail records actions that create, modify, and delete electronic records.

For the informed consent, each signing of the form gets saved as a separate entry. Recording creation is therefore automatic and modification and deletion of data can be identified by comparing the different informed consent forms.

5.2.5.1.5. Changes to a record do not obscure previously recorded audit trail information.

5.2.5.1.6. The audit trail is retained for a period at least as long as that required for the subject electronic records.

5.2.5.1.7. The audit trail is accessible for agency review and copying.

5.2.5.2. Project Administrators' Responsibilities

If project Administrators wish to capture Subject data other than the informed consent, they are responsible for validating the audit trail for those data.

5.2.6. Operational System Checks (21 CFR 11.10(f))

Regulatory requirement:

11.10(f) Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.

Interpretation:

The primary tested workflow is creation of signed informed consents. Operational checks for those will be tested as part of informed consent creation.

5.2.6.1. Vanderbilt Responsibilities

5.2.6.1.1. REDCap has operational checks to ensure informed consents are complete and correct.

Input checks will be tested under this requirement.

5.2.6.2. Project Administrators' Responsibilities

See the general responsibilities in Section 5.1.1.2.

5.2.7. Authority Checks/User Level Security (21 CFR 11.10(g))

Regulatory requirement:

11.10(g) Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.

Interpretation:

There should be a security framework that allows control over the actions that all system users can perform and any specific settings necessary should be implemented.

5.2.7.1. Vanderbilt Responsibilities

5.2.7.1.1. REDCap has the ability to control permissions for users with user IDs.

5.2.7.2. Project Administrators' Responsibilities

Project Administrators are responsible for implementing appropriate permissions for the users who have access to the project.

5.2.8. Device Checks (21 CFR 11.10(h))

Regulatory requirement:

11.10(h) Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.

Interpretation:

Device checks are not applicable to this system.

5.2.9. System Training (21 CFR 11.10(i))

Regulatory requirement:

11.10(i) Determination that persons who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks.

Interpretation:

Persons who use REDCap have the education, training, and/or experience to run the system properly.

5.2.9.1. Vanderbilt Responsibilities

5.2.9.1.1. Vanderbilt has appropriate hiring procedures for REDCap developers.

5.2.9.2. Project Administrators' Responsibilities

Project Administrators are responsible for having appropriate hiring and training procedures for REDCap users.

5.2.10. Use of Electronic Signatures (21 CFR 11.10(j))

Regulatory requirement:

11.10(j) The establishment of, and adherence to, written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification.

Interpretation:

Users signing informed consent have to agree to an accountability clause before signing.

5.2.10.1. Vanderbilt Responsibilities

5.2.10.1.1. Users signing informed consent have to agree to an accountability clause before signing.

5.2.10.2. Project Administrators' Responsibilities

See the general responsibilities in Section 5.1.1.2.

5.2.11. System Documentation (21 CFR 11.10(k))

Regulatory requirement:

11.10(k) Use of appropriate controls over systems documentation including:

(1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance.

(2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.

Interpretation:

This applies to documents requiring signatories. The REDCap department does not currently maintain documents that require signatories.

5.2.11.1. Vanderbilt Responsibilities

5.2.11.2. Project Administrators' Responsibilities

REDCap-related documents that have signatories must have lifecycle controls.

5.3. Controls for Open Systems (21 CFR 11.30)

Regulatory requirement:

11.30 Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in 11.10, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality.

Interpretation:

REDCap is an open system as defined in 21 CFR 11.3(b)(9). Open systems require additional security for those parts of the system not under owner control.

5.3.1. Vanderbilt Responsibilities

5.3.1.1. Web access to REDCap requires end-to-end encryption.

This means a forced redirect from http to https if necessary.

5.3.2. Project Administrators' Responsibilities

See the general responsibilities in Section 5.1.1.2.

5.4. Electronic Signature Manifestations (21 CFR 11.50)

REDCap will have the ability to secure data through electronic signatures. Data secured with an electronic signature cannot be edited or deleted unless the electronic signature is removed. Application of an electronic signature requires use of the users ID and password. The only module with electronic signature capabilities is the informed consent module.

5.4.1. Electronic Signature Components (21 CFR 11.50(a))

Regulatory requirement:

11.50(a) Signed electronic records shall contain information associated with the signing that clearly indicates all of the following:

(1) The printed name of the signer;

(2) The date and time when the signature was executed; and

(3) The meaning (such as review, approval, responsibility, or authorship) associated with the signature.

Interpretation:

Electronic signatures require the three specified components.

5.4.1.1. Vanderbilt Responsibilities

5.4.1.1.1. Signed informed consent forms will have the printed name of the signer and the date and time the form is signed.

5.4.1.1.2. The informed consent is identified as an informed consent.

5.4.1.2. Project Administrators' Responsibilities

See the general responsibilities in Section 5.1.1.2.

5.4.2. Electronic Signature Compliance (21 CFR 11.50(b))

Regulatory requirement:

11.50(b) The items identified in paragraphs (a)(1), (a)(2), and (a)(3) of this section shall be subject to the same controls as for electronic records and shall be included as part of any human readable form of the electronic record (such as electronic display or printout).

Interpretation:

Electronic signatures are subject to 11.10(a), 11.10(b), 11.10(c), 11.10(d), 11.10(e), 11.10(f), 11.10(g), 11.10(j), and 11.30. 11.10(h), 11.10(i), and 11.10(k) are N/A.

5.4.2.1. Vanderbilt Responsibilities

Electronic signature compliance will be tested under the applicable sections of 11.10 and 11.30.

5.4.2.2. Project Administrators' Responsibilities

See the general responsibilities in Section 5.1.1.2.

5.4.3. Signature/Record Linking (21 CFR 11.70)

Regulatory requirement:

11.70 Electronic signatures and handwritten signatures executed to electronic records shall be linked to their respective electronic records to ensure that the signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means.

Interpretation:

The system should not allow users to transfer, extend, or reduce the signature□s scope once it is applied.

5.4.3.1. Vanderbilt Responsibilities

5.4.3.1.1. Signed informed consents are read-only.

This requirement is functionally identical to the requirement that the audit trail is secure, since the informed consent form functions as its own audit trail.

5.4.3.2. Project Administrators' Responsibilities

See the general responsibilities in Section 5.1.1.2.

5.5. Electronic Signature General Requirements (21 CFR 11.100)

Regulatory requirement:

11.100(a) Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.

11.100(b) Before an organization establishes, assigns, certifies, or otherwise sanctions an individual's electronic signature, or any element of such electronic signature, the organization shall verify the identity of the individual.

11.100(c) Persons using electronic signatures shall, prior to or at the time of such use, certify to the agency that the electronic signatures in their system, used on or after August 20, 1997, are intended to be the legally binding equivalent of traditional handwritten signatures.

11.100(c)(1) The certification shall be submitted in paper form and signed with a traditional handwritten signature, to the Office of Regional Operations (HFC-100), 5600 Fishers Lane, Rockville, MD 20857.

11.100(c)(2) Persons using electronic signatures shall, upon agency request, provide additional certification or testimony that a specific electronic signature is the legally binding equivalent of the signer's handwritten signature.

Interpretation:

11.100(a) is inherent in the design of the informed consent document repository - since the consent forms are unalterable in the archive, and the electronic signature is embedded in them, the electronic signature cannot be reused or reassigned. If a person provides invalid names the informed consent is null and void and therefore the signature is also null and void; if a person provides the correct names then the signature is unique to that individual. Therefore, valid electronic signatures cannot be reused or reassigned and will necessarily be unique to the individual.

The clauses of 11.100(b) and 11.100(c) assume that users of electronic signatures are acting on behalf of the organization, i.e., as employees, managers, contractors, etc. This is not the case for the REDCap informed consent module, so 11.100(b) and 11.100(c) are not applicable.

5.5.1. Vanderbilt Responsibilities

For the REDCap informed consent module design, 11.100(a) is functionally identical to the test that the audit trail is retained as long as the subject record. For 11.100(b) and 11.100(c), see the Interpretation above.

5.5.2. Project Administrators' Responsibilities

Project Administrators are responsible for ensuring the setting necessary to enforce one or more of the Vanderbilt Responsibilities above are implemented. Project Administrators may, at their discretion, set up identity checks per 11.100(b). Note that ICH E6 does not require identify verification in order for participants to enter clinical trials and sign informed consents.

5.6. Electronic Signature Components (21 CFR 11.200)

Regulatory requirement:

11.200(a) Electronic signatures that are not based upon biometrics shall:

11.200(a)(1) Employ at least two distinct identification components such as an identification code and password.

11.200(a)(1)(i) When an individual executes a series of signings during a single, continuous period of controlled system access, the first signing shall be executed using at least one electronic signature component that is only executable by, and designed to be used only by the individual.

11.200(a)(1)(ii) When an individual executes one or more signings not performed during a single, continuous period of controlled system access, each signing shall be executed using all of the electronic signature components.

11.200(a)(2) Be used only by their genuine owners;

11.200(a)(3) Be administered and executed to ensure that attempted use of an individual's electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals.

11.200(b) Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.

Interpretation:

The intent of identification components is to ensure that only the correct individual signs the informed consent. As noted under the 11.100 section, if a person provides invalid names the informed consent is null and void and therefore the signature is also null and void; if a person provides the correct names then the correct individual has signed the informed consent. Therefore, valid informed consents will necessarily be signed by the correct individual. Based on this and the other design factors:

11.200(a)(1) is optional. Project administrators may add identification components to the informed consent for if they desire.

11.200(a)(1)(i) is optional. Project administrators may add an identification component that is only executable by the individual.

11.200(a)(1)(ii) is implicit in the design - electronic signatures require all components independently of when they are signed.

11.200(a)(2) is implicit in the design.

11.200(a)(3) is N/A - signing on behalf of another person is an optional feature that the informed consent module does not implement.

11.200(b) is N/A because biometrics are not used.

5.6.1. Vanderbilt Responsibilities

5.6.1.1. REDCap electronic signatures can use identification components, included those that are designed to be used only by the individual.

5.6.2. Project Administrators' Responsibilities

Project Administrators are responsible for ensuring the setting necessary to enforce one or more of the Vanderbilt Responsibilities above are implemented.

5.7. Electronic Signature Passwords (21 CFR 11.300)

Regulatory requirement:

11.300 Persons who use electronic signatures based upon use of identification codes in combination with passwords shall employ controls to ensure their security and integrity. Such controls shall include:

11.300(a) Maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password.

11.300(b) Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).

11.300(c) Following loss management procedures to electronically de-authorize lost, stolen, missing, or otherwise potentially compromised tokens, cards, and other devices that bear or generate identification code or password information, and to issue temporary or permanent replacements using suitable, rigorous controls.

11.300(d) Use of transaction safeguards to prevent unauthorized use of passwords and/or identification codes, and to detect and report in an immediate and urgent manner any attempts at their unauthorized use to the system security unit, and, as appropriate, to organizational management.

11.300(e) Initial and periodic testing of devices, such as tokens or cards, that bear or generate identification code or password information to ensure that they function properly and have not been altered in an unauthorized manner.

Interpretation:

11.300(c), and 11.300(e) are not applicable because REDCap does not use physical authentication devices. Since REDCap does not use identification codes for electronic signatures in the informed consent forms, 11.300(a), 11.300(b), and 11.300(d) are not applicable to the informed consent forms.

5.8. Software Version Control

Though not specifically listed in 21 CFR 11, software version control is practically necessary to maintain software systems in a validated state.

5.8.1. Vanderbilt has software version control for REDCap.

The version used in this validation is 8.6.2.