

**SOFTWARE DESIGN SPECIFICATION  
FOR  
VANDERBILT RESEARCH ELECTRONIC DATA CAPTURE (REDCAP)  
INFORMED CONSENT MODULE  
SERVING**



**VICTR DEPARTMENT  
VANDERBILT UNIVERSITY  
NASHVILLE, TN**



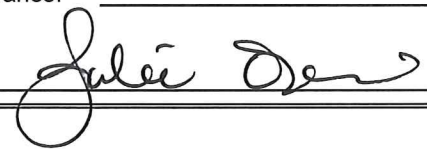
DOCUMENT NUMBER: SDS-REDCAP-PART11-001  
DATE ISSUED: 8/24/2018  
REVISION: 0

PREPARED BY  
RUSSELL BARBARE  
VALIDATION ENGINEER  
OFNI SYSTEMS

---

Vanderbilt Research Electronic Data Capture (REDCap) Informed Consent Module Software Design Specification		Doc. #: SDS-REDCap-Part11-001 Rev. #: 0
Department VICTR	Author Russell Barbare	Page 2 of 14

### SIGNATURES

Author: <u>Russell Barbare</u>	
Signature: <u></u>	Date: <u>27 August 2018</u>
System Owner: <u>Paul A. Harris</u>	
Signature: <u></u>	Date: <u>27 August 2018</u>
Quality Assurance: <u>Julie Ozier</u>	
Signature: <u></u>	Date: <u>28 August 2018</u>

### REVISION HISTORY

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

Vanderbilt Research Electronic Data Capture (REDCap) Informed Consent Module Software Design Specification		Doc. #: SDS-REDCap-Part11-001 Rev. #: 0
Department VICTR	Author Russell Barbare	Page 3 of 14

## TABLE OF CONTENTS

1.1	INTRODUCTION.....	41
1.1.1	Objectives .....	41
1.2	Scope.....	41
1.3	Assumptions/Restrictions.....	41
2	ACRONYMS AND REFERENCES.....	51
2.1	Acronyms and Definitions.....	51
2.2	References .....	51
3	COMPUTER SYSTEM DESCRIPTION .....	51
3.1	System Software .....	51
3.2	System Hardware Description .....	51
3.3	System Security .....	51
3.4	System Interactions .....	61
3.5	System Performance .....	61
3.6	System Availability .....	61
3.7	Physical Environment.....	61
4	PRIMARY BUSINESS FUNCTIONALITY .....	61
4.1	Informed Consent .....	61
5	REGULATORY REQUIREMENTS .....	61
5.1	Procedural .....	61
5.2	Software .....	81

<b>Vanderbilt Research Electronic Data Capture (REDCap) Informed Consent Module Software Design Specification</b>		Doc. #: SDS-REDCap-Part11-001 Rev. #: 0
Department VICTR	Author Russell Barbare	Page 4 of 14

## 1. Introduction

### 1.1. Objectives

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

The Software Design Specification for the Research Electronic Data Capture (REDCap) Informed Consent Module describes the system elements, functions and configuration necessary to properly operate the system within functional requirements outlined in Functional Requirement Specification for the Research Electronic Data Capture (REDCap) Informed Consent Module (FRS). By meeting requirements outlined in this document, REDCap will correctly and reliably perform its intended functionality.

### 1.2. Scope

This Software Design Specification applies to the Research Electronic Data Capture (REDCap) informed consent module. The SDS details how REDCap will technologically meet requirements outlined in the Functional Requirement Specification for the Research Electronic Data Capture (REDCap) Informed Consent Module (FRS), including applicable requirements for electronic records and signatures outlined in 21 CFR 11.

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). The functional requirements for the system are detailed in the Functional Requirements Specification for the Research Electronic Data Capture (REDCap) Informed Consent Module (SDS-REDCap-Part11-001). Demonstrating successful installation and operation of requirements described in FRS 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.

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

<b>Vanderbilt Research Electronic Data Capture (REDCap) Informed Consent Module Software Design Specification</b>		Doc. #: SDS-REDCap-Part11-001 Rev. #: 0
Department VICTR	Author Russell Barbare	Page 5 of 14

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

### **2.2. References**

21 CFR Part 11 "Electronic Records; Electronic Signatures"

FRS-REDCap-Part11-001, Functional Requirement Specification for the Research Electronic Data Capture (REDCap)

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

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

## **3. Computer 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.

<b>Vanderbilt Research Electronic Data Capture (REDCap) Informed Consent Module Software Design Specification</b>		Doc. #: SDS-REDCap-Part11-001 Rev. #: 0
Department VICTR	Author Russell Barbare	Page 6 of 14

#### 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 Informed Consent forms.

#### 4.1. Informed Consent

Requirements for the informed consent form:

##### 4.1.1. Subjects can complete an informed consent form.

REDCap generates a unique link to each survey automatically. The link is the same for every survey responder. The link can be viewed by the project manager under Manage Survey Participants > Public Survey Link > Public Survey URL. To complete the form, subjects navigate to the link, fill out all required fields, and consent by checking the consent box and submitting the information.

##### 4.1.2. Subjects can electronically sign an informed consent form.

Completing an informed consent form electronically signs the form as the last step, so completing the form properly and signing it are the same action.

### 5. Regulatory Requirements

#### 5.1. Procedural

The regulatory requirements fully or partially met by procedural controls are:

##### 5.1.1. System Validation (21 CFR 11.10(a))

The REDCap informed consent module will be validated. This Software Design Specification is part of the validation package. The validation project was described in Validation and Compliance Plan. System requirements were documented in the Functional Requirement Specification (FRS-REDCap-Part11-001). The system testing that will demonstrate that REDCap accurately, reliably and consistently meets these requirements will be documented in the Installation and Operational Qualification Protocol (IOQ-REDCap-Part11-001) and the testing results will be summarized in Validation Summary Report (VSR-REDCap-Part11-001).

This documentation provides the objective evidence that REDCap accurately, reliably and consistently meets these requirements described in FRS-REDCap-Part11-001 meets the regulatory requirement of 21 CFR 11:

<b>Vanderbilt Research Electronic Data Capture (REDCap) Informed Consent Module Software Design Specification</b>		Doc. #: SDS-REDCap-Part11-001 Rev. #: 0
Department VICTR	Author Russell Barbare	Page 7 of 14

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

#### 5.1.2. Protection of Records (21 CFR 11.10(c))

REDCap and all associated system data is protected with established policies and procedures for data backup and recovery, data archiving and business continuity to ensure accurate and ready retrieval of electronic data.

This system requirement meets the following requirement of 21 CFR 11:

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

At a minimum, these procedures will include:

##### 5.1.2.1. REDCap is backed up.

REDCap keeps 7 days' worth of daily backups and 6 months' worth of monthly backups. The backups are generated nightly by a script scheduled via nightly cron job. The logs are sent to Splunk for alerts and archival.

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

Automatic uploading to cloud storage and/or automatic file repository uploading can be set by the project administrator.

#### 5.1.3. Limited System Access/User Password Controls (21 CFR 11.10(d))

11.10(d) Limiting system access to authorized individuals.

Interpretation:

REDCap logins are created by REDCap administrators from lists provided by the project administrators. It is the responsibility of the project administrators to ensure that users do not share accounts.

#### 5.1.4. System Training (21 CFR 11.10(i))

Personnel developing REDCap will be adequately to perform their assigned tasks.

The functionality meets the following requirement of 21 CFR 11:

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.

##### 5.1.4.1. Vanderbilt has appropriate hiring procedures for REDCap developers.

#### 5.1.5. System Documentation (21 CFR 11.10(k))

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

<b>Vanderbilt Research Electronic Data Capture (REDCap) Informed Consent Module Software Design Specification</b>		Doc. #: SDS-REDCap-Part11-001 Rev. #: 0
Department VICTR	Author Russell Barbare	Page 8 of 14

currently maintain documents that require signatories.

#### 5.1.6. Software Version Control

Software version control is handled by a Vanderbilt-hosted GitHub site: <https://github.com/vanderbilt/REDCap>. The site is private and further information on it will not be included in this validation.

5.1.6.1. Vanderbilt has software version control for REDCap.

The version used in this validation is 8.6.2.

### 5.2. Software

The regulatory requirements fully or partially met by software controls are:

#### 5.2.1. Accurate Record Generation (21 CFR 11.10(b))

REDCap has the ability to generate accurate and complete copies of records in both human readable and electronic form suitable for inspection, review and copying by regulatory agencies.

This functionality meets the following requirement of 21 CFR 11:

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.

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

Project administrators can download all completed survey forms from the File Repository as pdf files.

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

The log is available to REDCap project administrators under the Logging application. The log records data exports, form management, changes to user accounts, record changes, and page views.

#### 5.2.2. Limited System Access/User Password Controls (21 CFR 11.10(d))

REDCap allows users to update their passwords. REDCap also provides the ability for administrators to control user access and security group membership, define password complexity and time limits, add new users and reset the passwords of existing users.

The functionality meets the following requirements of 21 CFR 11:

11.10(d) Limiting system access to authorized individuals.

This functionality also supplements these additional requirements of 21 CFR 11:

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(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

<b>Vanderbilt Research Electronic Data Capture (REDCap) Informed Consent Module Software Design Specification</b>		Doc. #: SDS-REDCap-Part11-001 Rev. #: 0
Department VICTR	Author Russell Barbare	Page 9 of 14

any attempts at their unauthorized use to the system security unit, and, as appropriate, to organizational management.

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

This will be tested by verifying that users cannot log in with a blank or incorrect password.

5.2.2.2. REDCap passwords expire.

REDCap ensures that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging). User passwords expire after a certain period of time.

5.2.2.3. REDCap passwords have minimum complexity requirements.

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

5.2.2.5. Invalid login attempts are logged.

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

#### 5.2.3. Audit Trails (21 CFR 11.10(e))

REDCap will produce an audit trail, recording all changes to all records.

The audit trail meets the following requirements of 21 CFR 11:

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.

The audit trail for REDCap will be verified on each data entry form to ensure that data recorded during the test cases was accurately recorded on the audit trail. In addition, the audit trail will be challenge tested to demonstrate that the audit trail is:

5.2.3.1. The audit trail is secure.

Users have read-only access to the audit trail, but audit trail records in REDCap cannot be altered by any system user, including Administrative users. The audit trail is stored within the program database, which is not accessible to any system user, including Administrative users.

5.2.3.2. The audit trail is computer generated.

Audit trail records are automatically generated by the computer, without any input from the user.

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

Audit Trail records have an accurate Time/Date stamp.

5.2.3.4. 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.

<b>Vanderbilt Research Electronic Data Capture (REDCap) Informed Consent Module Software Design Specification</b>		Doc. #: SDS-REDCap-Part11-001 Rev. #: 0
Department VICTR	Author Russell Barbare	Page 10 of 14

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

For the informed consent, each signing of the form gets saved as a separate entry.

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

The document repository is write-only with no overwrite. All consent forms are retained indefinitely.

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

The pdf files can be downloaded.

#### 5.2.4. Operational System Checks (21 CFR 11.10(f))

REDCap uses operational system checks to enforce permitted sequencing of steps and events, as appropriate.

The functionality meets the following requirements of 21 CFR 11:

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

Operational System Checks for REDCap will be tested on the appropriate forms and workflow, described previously in this document.

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

Project administrators can define fields as required.

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

REDCap uses authority checks to ensure before system users perform certain actions that they are authorized to perform those actions within the system. In REDCap, this is implemented through user-level security, which assigns each User ID to a specific group with a designated collection of privileges.

This functionality allows REDCap to meet the following requirement of 21 CFR 11:

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.

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

Project administrators with the appropriate permissions have access to the User Rights and Data Access Groups tabs. User Rights allows creating, editing, and deleting roles; editing user rights; and assigning and removing users from roles. Roles with users cannot be deleted. Data Access Groups allow creation or deletion of Data Access Groups and adding users to or removing users from them. Once a user is assigned to a Data Access Group, the user will be able to see only the project records created by themselves and others in that group.

#### 5.2.6. Device Checks (21 CFR 11.10(h))

Device checks are not applicable to this system.

#### 5.2.7. Use of Electronic Signatures (21 CFR 11.10(j) and 21 CFR 11.200(2))

<b>Vanderbilt Research Electronic Data Capture (REDCap) Informed Consent Module Software Design Specification</b>		Doc. #: SDS-REDCap-Part11-001 Rev. #: 0
Department VICTR	Author Russell Barbare	Page 11 of 14

Users signing informed consent have to agree to an accountability clause before signing. The functionality meets the following requirement of 21 CFR 11:

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.

11.200(2) Electronic signatures that are not based upon biometrics shall be used only by their genuine owners

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

5.2.8. Controls for Open Systems (21 CFR 11.30)

REDCap will 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.

The functionality meets the following requirements of 21 CFR 11:

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.

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

Secure Socket Layer (SSL) in web browsers is an end-to-end encryption method, indicated by the use of https addresses instead of http addresses. This will be tested by verifying that http access to redcap.vanderbilt.edu is redirected to https access.

5.2.9. Electronic Signature and Meaning (21 CFR 11.50 and 11.70)

Electronic signatures within REDCap include the printed name of the signer, the date/time the signature was added and the meaning of the electronic signature.

The functionality meets the following requirements of 21 CFR 11:

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.

Electronic signatures will meet the following technical requirements:

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

First name and last name are mandatory; project administrators can optionally add middle name, title, Junior/Senior, I/II/III/... entry as text or select entry boxes.

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

<b>Vanderbilt Research Electronic Data Capture (REDCap) Informed Consent Module Software Design Specification</b>		Doc. #: SDS-REDCap-Part11-001 Rev. #: 0
Department VICTR	Author Russell Barbare	Page 12 of 14

The top of the consent form says "Consent Forms".

5.2.9.3. Signed informed consents are read-only.

The functionality meets the following requirements of 21 CFR 11:

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.

#### 5.2.10. 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)(1) 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.

(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.

#### 5.2.11. 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

<b>Vanderbilt Research Electronic Data Capture (REDCap) Informed Consent Module Software Design Specification</b>		Doc. #: SDS-REDCap-Part11-001 Rev. #: 0
Department VICTR	Author Russell Barbare	Page 13 of 14

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.

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

Possible identification components that are designed to be used only by the individual are a signature field or a text field asking for information unique to the individual. Such information includes their birthday, birth town, or the last four digits of their social security number.

#### 5.2.12. Electronic Signature Passwords (21 CFR 11.300)

Regulatory requirement:

11.300(a) 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:

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

<b>Vanderbilt Research Electronic Data Capture (REDCap) Informed Consent Module</b> <b>Software Design Specification</b>		Doc. #: SDS-REDCap-Part11-001 Rev. #: 0
Department VICTR	Author Russell Barbare	Page 14 of 14

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:

Since REDCap does not use identification codes in combination with passwords for electronic signatures in the informed consent forms, these requirements are not applicable to the informed consent forms.