System Acceptance Certificate and Validation Summary

TrialKit Web version 7

Includes current versions of Android and iOS mobile apps

28 October 2023

By: Crucial Data Solutions, Inc.

Table of Contents:

Summary

TrialKit TrialKit Web version 7 was developed using the following languages and framework:

Web – C# in .NET and MVC

The database is written with PL/pgSQL for PostgreSQL

Development was performed by qualified and trained staff following an approved software development lifecycle including analysis, design, development, validation, and release of the final product.

The development and validation process is regulated by SOPs and related guidelines and templates which are under version control by Quality Assurance. Those documents used during this validation are:

- FM-5910 - Validation Plan
- P-2070 - ER/ES Compliance
- SOP-G-3050 - Controlled Documents
- SOP-QA-3170 - Computer System Security
- SOP-QA-3190 - Product Change Control
- SOP-QA-3150 – Ticket Management
- SOP-PD-3410 - SDLC and Computer System Validation Process
- SOP-QA-3120 - Computer System Validation Documentation Management Process

Overall validation activities are performed by Quality Assurance and the Software Validation Group in compliance with SOPs listed above and 21 CFR Part 11 detailed in Appendix A.

The complete coverage of TrialKit TrialKit Web version 7 system functionality is demonstrated by the traceability
between the User Requirements, Functional Requirements, Test Case results (Test Executions), and User Acceptance Tests. This traceability is maintained in two ways:

- For newly developed features (if applicable) in TrialKit TrialKit Web version 7, all traceable items were linked to each other by the use of standard functionality within the CDS's Application Lifecycle Management system (ALM).
- For features part of this version, traceability is maintained through a matrix hosted in CDS's ALM All Functional Requirements were tested by the Software Validation Group and Software Development through formal Test Cases. All traceability has been approved by Quality Assurance when reviewing Test Executions or by directly approving the Traceability Matrix.

To guarantee the independence of testing, Quality Assurance reviewed the testing process to ensure that a Software Developer could only test requirements that they did not code themselves.

Quality Assurance provided oversight to all testing activities, reviewing test strategy, verifying qualifications and independence of testers and provided guidance and instruction regarding the depth of testing, testing coverage, and the capture of objective evidence of actual test results.

Testing was performed in accordance with applicable SOPs and Guidelines and based on a Validation/QA Plan describing the test strategy, expected results, defect handling, and responsibilities for testing.

Test actions for all listed requirements were based on Test Cases or documented in individual tickets. Test Case templates and test results were tracked in CDS's ALM and reviewed exhaustively by Quality Assurance.

All defects related to this software release were tracked using CDS's ALM system. Defects found and fixed during the validation have been retested through formal Test Executions, and the information is provided as a comment in the ticket.

Operational Qualification and Study Validation

In Addition to verification activities directly supporting the changes in this version, a comprehensive re-validation has been performed and documented to cover the following functional areas across 228 Test steps across the functional areas listed below, using a simulated default study configuration. The results of these tests and steps are kept on file by CDS.

- User Access controls
  - Sign In
  - Sign out
  - Session Timeout
  - Adding users and updating status
  - Study and site access
  - Roles and permissions
- Subject Record Management
  - Subject ID Creation and sequencing
  - Scheduled visit design
  - Log Forms
  - Version control
- Subject Form Data
  - Data saving - Clinician
  - Data saving - Patient
  - Edit checks
  - Conditional Actions
  - Form permissions
  - Field blinding
  - Local Lab Ranges
  - Randomization
  - Product assignments
  - Data exports
- Audit histories (subject records)
  - Subject form events and data changes
  - Site and user access
  - Roles and permission settings
  - Field blinding
- Field-level SDV/locking
- Query routing and visibility
- Form workflow review
- Key Reports For Driving Protocol Adherence
  - Action Items Report

    - Queries Report
- ePRO access
- ePRO form deployment
- Participant Consent
- Site Documents
- Study Documents
- File Uploads
- Site Payment Tracking

Validation Statement / System Acceptance

After execution of the actions described above, it is concluded that TrialKit TrialKit Web version 7 has been developed according to the CDS Quality System, following written procedures dealing with all relevant phases of the Software Development Lifecycle, and in compliance with the regulatory framework from ICH, FDA and the European Union, including, but not limited to:

- FDA 21 CFR Part 11 Electronic Records; Electronic Signatures; Final Rule – Detailed in appendix below
- FDA Guidance for Industry; Computerized Systems Used In Clinical Investigations
- General Principles of Software Validation; Final Guidance for Industry and FDA Staff
- National regulations as applicable for individual clinical studies

Installation Qualification (IQ)

IQ documentation was developed and approved prior to the implementation.
Successful implementation will be verified by executing the IQ documentation and approved by Quality Assurance as required by SOP-QA-3190

Maintenance Stage

Future software upgrades resulting from identified software defects and/or additional requirements will be initiated by CDS management and are following a predefined process described in written procedures.

Any changes to the system after formal product release will be addressed in accordance with appropriate change control procedures and validated by Quality Assurance before releasing into production.

Any non-compliance and associated corrective actions will be documented via established SOP’s.

Security

TrialKit TrialKit Web version 7 is built on AWS cloud architecture comprised of database, application, and user interface.

Amazon Web Services are used across varying regions for data hosting and network redundancy.

Data is transferred between client and server using 256-bit SSL or greater encryption technology, along with 2-Factor Password-protected and biometric user access controls permissions.

Password security features include but are not limited to defined minimum length, alphanumeric composition, and device tokenization. Network architecture involves utilizing clustered firewalls and security appliances to protect user access that is distributed (balanced) across multiple application servers' farm.

30 days of five-minute interval backups are kept on-site at the primary data center for fast recovery if necessary and sent monthly to a geographically separated location with mirrored security and compliance standards.

The power infrastructure provides uninterrupted power supplies backed up by a generator. A validated disaster recovery and a business contingency plan are in place. The primary data center provides SOC type I and II audit certifications along with a variety of globally-acknowledged security certification programs.

New Features and Changes Included in this release

ID	Name	Level	Risk	Type
4886385717	Web forms 7.0 Final Integrated	Web only	3	Requirement
5066798836	ICS calendar notifications need to indicate the system timezone and instructions to join meeting	Services Only	1	Requirement
4855363612	Study progress report export updated to rename "Tx start date" to "Start Date" and add Randomization Date	Services Only	2	Requirement
5022413672	External variable dependencies get error when they are pointed to an incomplete CA	Services Only	1	Bug
5038983265	Volume batch records with signature is signing users out of the system	Web only	1	Bug
4796008433	Subject Summary report renamed and updated with additional details	Web only	1	Requirement
4811993626	Export Subject Visits report (TKDrive version) from the subject summary	Web+Services	1	Requirement
5080741340	Relocate report buttons on subject manager and add shortcut to dashboard report	Web only	1	Requirement
5033002654	Move log form ID column to the end of the table	Web only	1	Requirement
5180064898	Data change audit api (form/712) needs the user who originally created the form and the date created	Services Only	1	Requirement
5030940105	Update query popup window button text to "Save" with hover text	Web only	1	Requirement
2535345771	Query batch redeployment	Web+Services	2	Requirement

ID	Name	Level	Risk	Type
4796361011	Report builder - ability to include unique record ID for site/study forms	Web+Services	2	Requirement
4843839326	Transaction audit report and data change audit report updated to include time of day in the filtering options	Web+Services	1	Requirement
4880679732	Randomization confirmation email needs to follow user's permanent roles	Web+Services	1	Bug
4955416717	Button to copy host and study details to clipboard	Web only	1	Requirement
5013497833	Subject search is allowing access to casebook if registration form is in error	Web only	2	Bug
5073273976	File repository zip export should export whatever the user is currently filtering in the table	Web+Services	1	Requirement
5163078831	Rerun edit checks to also update visit date	Web only	2	Requirement
5178154231	Decode mutliselect field values in report builder	Web+Services	1	Requirement
5186331775	Action items filter for records ready for review that were previously unlocked by edit check or compuation	Web+Services	2	Requirement
5242855411	API to get study details to work with any study ID passed in (study/712)	Services Only	2	Requirement
4947277037	New dashboard report metrics x 6	Web+Services	1	Requirement
5081003423	Option to Display dashboard report on home page	Data Model+Service	1	Requirement
5108415910	Embed email address links on web page builder	Web only	1	Requirement

ID	Name	Level	Risk	Type
5124720797	SDTM annotations on PDF annotated forms	Web only	2	Requirement
5203127855	Blinded log fields need to be masked in log table	Web only	2	Requirement
5233038059	Action Items, open queries table needs to filter for query type (attn issuer/attn site)	Web+Services	2	Requirement
5241436877	Updated Common Navigation Buttons	Web only	2	Requirement
5243033755	Data exports need to display the file ID and name for upload fields	Web only	2	Requirement
5305657324	Study configuration option to enable participant payments	Web+Services	2	Requirement
5201244289	TMF text wrapping	Web only	1	Bug
5316546253	Form with "/" in the name cannot be exported to PDF from the longitudinal view	Web only	1	Bug
5379459428	New form property to "Prevent form editing" of completed forms	Web only	1	Requirement
5108442612	TrialKit Learning Center option in Account menu	Web only	1	Requirement
5017059424	Add forms list to the scheduled visit and event exports	Services Only	1	Requirement
5323176002	Firefox browser showing review progress bar at 50% in subject manager if the review is at 0%	Web only	1	Bug
5312994154	Study configuration functionality updated with more organized layout	Web only	1	Requirement
5360050268	Form builder- form with several tabs/pages needs to wrap	Web only	1	Requirement
4763363452	SDTM Metadata visit design definitions	Web only	2	Requirement

ID	Name	Level	Risk	Type
5340117111	Increase tab size and font on multi-tab forms	Web only	1	Requirement
5353566314	Change to menu interactions from hover to on-click	Web only	1	Requirement
5364223634	Remove dynamic CAs in Site Manager	Web only	1	Requirement
5349836680	Field property 'Med code field' support for memo fields	Web only	1	Requirement
5368940453	Fixed table on old forms is clearing results	Web only	2	Bug
4880834197	CSV exports need to include text labels that set to be included in exports	Web only	2	Requirement
5377751790	.MOV file extension not opening in browser preview	Web only	1	Bug
5073929194	Lab range checks in form render	Web Service + iOS	2	Requirement

5155216683	Due forms list should hide forms that don't have view rights	Services Only	2	Requirement
5132446641	Form property to control editing of completed forms for patient users	Web Service + iOS	2	Requirement

5383266779	Permission to Allow editing participant completed forms	Web Service + iOS	2	Requirement
5247709467	Deleted forms in form builder need to remove events from the event diary table	Web Service + iOS	2	Requirement
5222313175	Event triggers are not using the subject's current version	Services Only	2	Bug
5193412865	Nmible Participant payments integration	Services Only	2	Requirement
5232296597	Payments button for Participant payment access	Web Service + iOS	1	Requirement
5155168496	User host redirect if user is part of an archived or the user is suspended on the target host	Web Service + iOS	3	Requirement
2535205281	Payment Configuration	Web Service + iOS	2	Requirement

Approvals

System Administration	Quality Assurance	Executive Approval
Dek Mauleon	Cody Wilke	Paul Grady
Director, System Administration	Director, Quality Assurance	CEO
Dek Mauleon	Cody Wilke	Paul Grady
28 Oct 2023	27 Oct 2023	27 Oct 2023

Appendix A

21 CFR Part 11 Statement

Electronic Records;
Electronic Signature;
Final Rule

Including Crucial Data Solutions (CDS) Comments For
TrialKit TrialKit Web version 7 and all underlying subversions/minor releases

CDS Comments in Blue

21 CFR Part 11 - Table of Contents

Subpart A – General Provisions

Sec. 11.1 Scope

(a) The regulations in this part set forth the criteria under which the agency considers electronic records, electronic signatures, and handwritten signatures executed to electronic records to be trustworthy, reliable, and generally equivalent to paper records and handwritten signatures executed on paper.

(b) This part applies to records in electronic form that are created, modified, maintained, archived, retrieved, or transmitted, under any records requirements set forth in agency regulations. This part also applies to electronic records submitted to the agency under requirements of the Federal Food, Drug, and Cosmetic Act and the Public Health Service Act, even if such records are not specifically identified in agency regulations. However, this part does not apply to paper records that are, or have been, transmitted by electronic means.

(c) Where electronic signatures and their associated electronic records meet the requirements of this part, the agency will consider the electronic signatures to be equivalent to full handwritten signatures, initials, and other general signings as required by agency regulations, unless specifically excepted by regulation(s) effective on or after August 20, 1997.

(d) Electronic records that meet the requirements of this part may be used in lieu of paper records, in accordance with 11.2, unless paper records are specifically required.

(e) Computer systems (including hardware and software), controls, and attendant documentation maintained under this part shall be readily available for, and subject to, FDA inspection.

(f) This part does not apply to records required to be established or maintained by 1.326 through 1.368 of this chapter. Records that satisfy the requirements of part 1, subpart J of this chapter, but that also are required under other applicable statutory provisions or regulations, remain subject to this part.

(g) This part does not apply to electronic signatures obtained under 101.11(d) of this chapter.

(h) This part does not apply to electronic signatures obtained under 101.8(d) of this chapter.

(i) This part does not apply to records required to be established or maintained by part 117 of this chapter. Records that satisfy the requirements of part 117 of this chapter, but that also are required under other applicable statutory provisions or regulations, remain subject to this part.

(j) This part does not apply to records required to be established or maintained by part 507 of this chapter. Records that satisfy the requirements of part 507 of this chapter, but that also are required under other applicable statutory provisions or regulations, remain subject to this part.

(k) This part does not apply to records required to be established or maintained by part 112 of this chapter. Records that satisfy the requirements of part 112 of this chapter, but that also are required under other applicable statutory provisions or regulations, remain subject to this part.

(l) This part does not apply to records required to be established or maintained by subpart L of part 1 of this chapter. Records that satisfy the requirements of subpart L of part 1 of this chapter, but that also are required under other applicable statutory provisions or regulations, remain subject to this part.

(m) This part does not apply to records required to be established or maintained by subpart M of part 1 of this chapter. Records that satisfy the requirements of subpart M of part 1 of this chapter, but that also are required under other applicable statutory provisions or regulations, remain subject to this part.

(n) This part does not apply to records required to be established or maintained by subpart O of part 1 of this chapter. Records that satisfy the requirements of subpart O of part 1 of this chapter, but that also are required under other applicable statutory provisions or regulations, remain subject to this part.

(o) This part does not apply to records required to be established or maintained by part 121 of this chapter. Records that satisfy the requirements of part 121 of this chapter, but that also are required under other applicable statutory provisions or regulations, remain subject to this part.

Sec. 11.2 Implementation.

(a) For records required to be maintained but not submitted to the agency, persons may use electronic records in lieu of paper records or electronic signatures in lieu of traditional signatures, in whole or in part, provided that the requirements of this part are met.

(b) For records submitted to the agency, persons may use electronic records in lieu of paper records or electronic signatures in lieu of traditional signatures, in whole or in part, provided that:

(1) The requirements of this part are met; and

(2) The document or parts of a document to be submitted have been identified in public docket No. 92S-0251 as being the type of submission the agency accepts in electronic form. This docket will identify specifically what types of documents or parts of documents are acceptable for submission in electronic form without paper records and the agency receiving unit(s) (e.g., specific center, office, division, branch) to which such submissions may be made. Documents to agency receiving unit(s) not specified in the public docket will not be considered as official if they are submitted in electronic form; paper forms of such documents will be considered as official and must accompany any electronic records. Persons are expected to consult with the intended agency receiving unit for details on how (e.g., method of transmission, media, file formats, and technical protocols) and whether to proceed with the electronic submission.

Sec. 11.3 Definitions.

(a) The definitions and interpretations of terms contained in section 201 of the act apply to those terms when used in this part.

(b) The following definitions of terms also apply to this part:

(1) Act means the Federal Food, Drug, and Cosmetic Act (secs. 201-903 (21 U.S.C. 321-393)).

(2) Agency means the Food and Drug Administration.

(3) Biometrics means a method of verifying an individual's identity based on measurement of the individual's physical feature(s) or repeatable action(s) where those features and/or actions are both unique to that individual and measurable.

(4) Closed system means an environment in which system access is controlled by persons who are responsible for the content of electronic records that are on the system.

(5) Digital signature means an electronic signature based upon cryptographic methods of originator authentication, computed by using a set of rules and a set of parameters such that the identity of the signer and the integrity of the data can be verified.

(6) Electronic record means any combination of text, graphics, data, audio, pictorial, or other information representation in digital form that is created, modified, maintained, archived, retrieved, or distributed by a computer system.

(7) Electronic signature means a computer data compilation of any symbol or series of symbols executed, adopted, or authorized by an individual to be the legally binding equivalent of the individual's handwritten signature.

(8) Handwritten signature means the scripted name or legal mark of an individual handwritten by that individual and executed or adopted with the present intention to authenticate a writing in a permanent form. The act of signing with a writing or marking instrument such as a pen or stylus is preserved. The scripted name or legal mark, while conventionally applied to paper, may also be applied to other devices that capture the name or mark.

(9) Open system means 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.

Subpart B - Electronic Records

Sec. 11.10 Controls for closed systems.

Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following:

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

Compliant

TrialKit is validated through CDS's internal Validation process, as spelled out in the company SOP's, which ensures accuracy, reliability, and consistent intended performance. TrialKit, functions according to its specifications, as verified in the Validation process.
The audit log or records saved in TrialKit ensures the ability to discern invalid or altered records as well as providing accountability for each action.

(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 such review and copying of the electronic records.

Compliant

TrialKit generates accurate and complete copies of records in both human readable and electronic form through its standard export utility.

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

Compliant

Records are protected and retrievable throughout the study and during their retention period via online or electronic CRFs, tape backup or electronic media archival methods. After the study is

completed, records are provided directly to the Client and retained per CDS official archival process.

(d) Limiting system access to authorized individuals.

Compliant

Software system access is limited to authorized individuals through the use of unique usernames, in addition to passwords and roles. Hardware system access is governed by official policies and procedures.

(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.

Compliant

TrialKit utilizes secure, computer-generated, time-stamped audit trails that identify the time and date of operator entries, previous and current values and the reason for change for all modifications to the system.
The audit log is included in the archival process and is stored in the database records.
Deleted records are removed to a deleted bin, but are not permanently deleted from the system.

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

Compliant

TrialKit guides the user through operational checks as defined in the protocol. Validation or edit checks are used to alert system users of potential deviations from the protocol.

(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.

Compliant

The TrialKit system provides authority checks through the use of unique usernames, passwords, and assigned roles.

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

Compliant

Data from external sources must transmit through the web service API and is treated as any other authenticated user.

(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.

Compliant

This is guaranteed by the employment of qualified personnel and regular internal/external training. All training and skills documentation for CDS employees are maintained in their employee files per SOP-G-3020, Employee Qualifications and Training.
It is the Sponsor's responsibility to guarantee appropriate training of study staff that will use TrialKit functionality for data collection and processing.

(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.

Compliant

It is the Sponsor's responsibility to provide written policies and train to Sponsor's staff participating in the study in using electronic signature functionality.
Also, CDS's End User License Agreement, which is signed by all users of the system, holds individuals accountable and responsible for actions initiated under their electronic signature. Internally, CDS adheres to Policy P-2070, ER/ES Compliance.

(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.

Compliant

CDS employs the following controls over system documentation (SOP-QA-3120, Computer System Validation Documentation Process):

1. **Distribution of and access to controlled documents is restricted**
2. **All system documentation is version controlled and updated with each release.**

Sec. 11.30 Controls for open systems.

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.

Compliant

Procedures 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, are deployed by CDS.
In addition to employing controls for closed systems, CDS implements 256-bit SSL encryption, and username and password for unique digital signature to ensure record authenticity, integrity, and confidentiality.

Sec. 11.50 Signature manifestations.

(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.

Compliant

For each electronic signature (users of the system) the following information is captured in the audit log:

1. **The printed name of the signer.**
2. **The date and time the signature was executed.**
3. **The meaning associated with the signature.**

(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).

Compliant

All above information is included in human readable form in the audit log as well as on the screen or as a result of the archive process.

Sec. 11.70 Signature/record linking.

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.

Compliant

Electronic signatures executed to electronic records are linked to their respective electronic record(s) in the audit log of the form to which the signature was applied, thus ensuring that the signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means. If a top level form is signed, the signature applies to all forms beneath the signed form.

Subpart C - Electronic Signatures

Sec. 11.100 General requirements.

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

Compliant

Each electronic signature is unique to one individual, as CDS does not allow duplicate user IDs. Usernames are not deleted from the underlying relational database management system (RDBMS), which is an integral part of the system; thus ensuring they cannot be 'reassigned.'

(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.

Compliant

Noted and understood for CDS internal use.
It is the Sponsor's responsibility to verify the identity of Sponsor's staff that is participating in the study. In addition, CDS's End User License Agreement, which is signed by all users of the system, holds individuals accountable and responsible for actions initiated under their electronic signature.

(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.
(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.
(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.

Compliant

CDS's End User License Agreement, which is signed by all users of the system hold individuals accountable and responsible for actions initiated under their electronic signature.
For systems documentation to be used within Crucial Data Solutions, Inc., this certification was submitted on May 10, 2015, to the Office of Regional Operations (HFC-100).

Sec. 11.200 Electronic signature components and controls.

(a) Electronic signatures that are not based upon biometrics shall:
(1) Employ at least two distinct identification components such as an identification code and password.

(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 all electronic signature components; subsequent signings shall be executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual.
(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.
(2) Be used only by their genuine owners; and
(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.

Compliant

As CDS does not use biometrics, it employs the following components and controls:

1. **Access to TrialKit requires both a username and password. The username is always unique thus providing two distinct identification components. TrialKit requires both components of the electronic signature to be entered for all signings, regardless if the signature is executed in a single, continuous period of controlled system access or not.**
2. **TrialKit only issues access information to the genuine owner. Users are encouraged not to share their password, use password-protected screen savers and other security measures to protect the integrity of the data.**
3. **CDS's use of a unique username and password combination and processes ensures that attempted use of an individual's electronic signature by anyone other than its genuine owner requires the collaboration of two or more individuals. Using deductive reasoning, it may be proven that attempted use of an individual's electronic signature by anyone other than its genuine owner requires the collaboration of two or more individuals. All passwords are only given to the genuine owner of the password. Collaboration is 'To work together, especially in a joint intellectual effort.' Therefore, to share the password with someone else, the owner must collaborate with someone else. The owner and someone else constitutes two or more persons.**

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

Compliant

Biometric functions provided by the mobile applications only function for a single user on a unique device token. If more than one user has attached to that device, biometric capabilities are disabled.

Electronic signatures obtained via biometrics are stored with the label "Biometrics".

Sec. 11.300 Controls for identification codes/passwords.

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:

(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.

Compliant

TrialKit maintains the uniqueness of each combined username and password by not allowing duplicate usernames.
Usernames are not deleted from the from the underlying relational database management system (RDBMS), which is an integral part of the system; therefore, they cannot be re-assigned. Thus, no two individuals can have the same combination of identification code and password.

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

Compliant

TrialKit uses device logging and expiration - through the use of multi-factor mechanisms - to keep login credentials in check over long periods of time.

(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.

Compliant

CDS does not issue tokens, cards or other devices that bear or generate identification code or password information.

(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.

Compliant

To prevent unauthorized access to the system, TrialKit supports the use of locking user accounts after a defined number of unsuccessful login attempts.

(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.

Compliant

CDS does not issue tokens, cards or other devices that bear or generate identification code or password information.