Verigo
Truth in Transit

747 SW 2nd Ave
IMB 28 Suite 227
Gainesville, FL 32601
United States

Statement of 21 CFR Part 11 Compliance
For Verigo Software System

The relevant points of these rules have been observed and implemented either in the software or in the validation protocol. To achieve full compliance the user is obligated to implement the **Verigo Software System** on a properly maintained operating system and use the relevant administration of the operating system and the software to ensure data access for authorized individuals and sources.

Statement:

This software was evaluated for conformance to functional and performance specifications. The test performed during the evaluation were made in conformance to the software validation test protocol documented in Verigo's Quality Management System and demonstrated that the software conformed to all applicable performance and functional specifications.

	Name	Signature	Date
Tested	William McCombie		19 May 2017
Reviewed	Adam Kinsey	Adam Kinsey	19 May 2017
Approved	Adam Kinsey	Adam Kinsey	19 May 2017

Scope

The Food and Drug Administration (FDA) is issuing regulations that provide criteria for Acceptance by FDA, under certain circumstances, of electronic records, electronic signatures, and handwritten signatures executed to electronic records as equivalent to paper records and handwritten signatures executed on paper. These regulations, which apply to all FDA program areas, are intended to permit the widest possible use of electronic technology, compatible with FDA's responsibility to promote and protect public health. The use of electronic records as well as their submission to FDA is voluntary. The final rule provides criteria under which FDA will consider electronic records to be equivalent to paper records, and electronic signatures equivalent to traditional handwritten signatures. Part 11 (21 CFR part 11) applies to any paper records required by statute or agency regulations and supersedes any existing paper record requirements by providing that electronic records may be used in lieu of paper records. This document describes each of the specific requirements in the FDA documentation and how these are addressed in Verigo's Software System.

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:

Ref	FDA Requirement	Verigo Implementation	☑
a	Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.	All software systems are subject to a functional testing and validation protocol, consisting of automated and manual tests that must be passed before any software is released.	☑
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.	All records are available to authorized users in PDF, CSV, and HTML file formats.	☑
c	Protection of records to enable their accurate and ready retrieval throughout the records retention period.	All records are generated by and communicated to the server database from only authorized users whose credentials have been authenticated. These communications are secured using at least 128-bit AES encryption via the TLS protocol. These records are stored permanently offsite in a secure database hosted by a major cloud services provider, with full database redundancy as well as point-in-time backup restoration. The records may be accessed at any time by authorized users.	☑
d	Limiting system access to authorized individuals	Users must be authenticated by a unique username and password before they are able to access any software system features.	☑

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 system automatically generates audit trails (including timestamp and username) of all user actions pertaining to records in permanent storage that cannot be altered, overwritten, or deleted. These logs of user activity consist of, but are not limited to: Activating and deactivating monitoring devices User logins and logouts Synchronization of data from monitoring devices Creation, editing, and deletion of user accounts and credentials In addition, for redundancy of security, permanent logs are stored in a separate storage location of all database activity, including data creation, editing, and deletion. All logs are permanent and retained indefinitely, unless otherwise requested by the end customer, but under no circumstances less than 5 years.	☑
f	Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate	System logic embedded in user interfaces and process flows enforces that all sequenced operations occur in the correct order. No user can create, delete, or modify records in a particular step that is out of order in the overall sequence.	☑
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	Users must be authenticated by a unique username and password before they are able to access any software system features. System logic also enforces user access to features (such as the ability to create or modify user accounts) according to Role-based Access Control (RBAC).	☑
h	Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction	The source of monitored data can only be a Verigo data logger. The source of records can only be a terminal device that is executing Verigo software and operated by a user that has provided authenticated credentials to an authorized user account. Verigo's mobile app has log error detection, and the web back-end has tamper detection to prevent invalid data from being submitted.	☑

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	All users signing up for a new Verigo account must agree to the following statement in the Term & Conditions: "I assert that I have the education, training, and experience necessary to perform my assigned tasks related to my use of this software system."	☑
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.	All users signing up for a new Verigo account must agree to the following statement in the Term & Conditions: "I assert that I am today and will continue to be in adherence with all written policies of my organization for my use of this software system."	☑
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.	Verigo has procedures in place to ensure control for systems documentation, and systems documentation can only be accessed, changed, or distributed by Verigo personnel with authorized credentials. All documentation is stored within systems with access control, revision control and logging of all changes.	☑
k	(2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.	Verigo records all systems documentation changes in a time-sequenced manner for proper audit trail recording. All documentation is stored within systems with access control, revision control and changes can only be made by Verigo personnel with authorized credentials.	☑

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.

Ref	FDA Requirement	Verigo Implementation	☑
a	11.30 – Controls for open systems	Not applicable. The Verigo Software System is a closed system.	□

Sec. 11.50 - Signature manifestations

Ref	FDA Requirement	Verigo Implementation	☑
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.	Not applicable for the software. The Verigo Software System does not utilize signatures.	□
b	(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).	Not applicable for the software. The Verigo Software System does not utilize signatures.	□

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.

Ref	FDA Requirement	Verigo Implementation	☑
	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.	Not applicable for the software. The Verigo Software System does not utilize electronic signatures.	☐

Sec. 11.100 - General requirements

Ref	FDA Requirement	Verigo Implementation	☑
a	Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else	Not applicable for the software. The Verigo Software System does not utilize electronic signatures.	☐
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.	Not applicable for the software. The Verigo Software System does not utilize electronic signatures.	☐
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.	Not applicable for the software. The Verigo Software System does not utilize electronic signatures.	☐
d	The certification shall be submitted in paper form and signed with a traditional handwritten signature, to	Not applicable for the software. The Verigo Software System does not utilize electronic	☐

	the Office of Regional Operations, 12420 Parklawn Drive, RM 3007 Rockville, MD 20857.	signatures.	

Sec. 11.200 - Electronic signature components and controls

Ref	FDA Requirement	Verigo Implementation	☑
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.	Not applicable for the software. The Verigo Software System does not utilize electronic signatures.	□

b	Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.	N Not applicable for the software. The Verigo Software System does not utilize electronic signatures.	☐

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:

Ref	FDA Requirement	Verigo Implementation	☑
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	Not applicable for the software. The Verigo Software System does not utilize electronic signatures.	☐
b	Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).	Not applicable for the software. The Verigo Software System does not utilize electronic signatures.	☐
c	Following loss management procedures to electronically reauthorize 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.	Not applicable for the software. The Verigo Software System does not utilize electronic signatures.	☐

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.	Not applicable for the software. The Verigo Software System does not utilize electronic signatures.	□
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.	Not applicable for the software. The Verigo Software System does not utilize electronic signatures.	□