Statement of Compliance with 21 CFR Part 11

Vestigo is an application to manage the Investigational Drug Service. As such, it performs record-keeping functions subject to 21 CFR Part 11. The regulations require electronic features and controls as well as user policies and practices.

Vestigo undergoes rigorous internal testing for all development activities in order to ensure compliance with the regulation. Full compliance with 21 CFR Part 11 requires that the application be used in an environment with internal controls, local policies and procedures to ensure the application is used correctly.

Specifically, Vestigo employs the following capabilities to meet the requirements of the regulation:

Section	Requirement	Vestigo Capability
11.10 (b)	The system shall generate accurate and complete copies of records in human readable and electronic form suitable for inspection, review and copying	Vestigo presents standardized reports on the screen and in downloaded formats. Downloaded reports are available as PDF or in Excel.
11.10 (d)	The system shall limit system access to authorized individuals.	All parts of the Vestigo application are access controlled by username and password. Each account is given roles and permissions that limit the functions and data the account is able to access. Vestigo specifically supports elements of the 21 CFR Part 11 environment including encrypted passwords, enforcement of strong password selection and automatic password expiry. This enhanced security will also allow for automatic account locking for multiple failed attempts and recording of IP address for all accesses.
11.10 (e)	The system shall employ secure, computer-generated date/time stamped audit trails to independently record operator entries and actions that create, modify, or delete electronic records, without obscuring previously recorded information.	Every action performed by Vestigo is written to the log which records each action, when it occurred and who made the user was. These records are fully timestamped and cannot be edited.
11.10 (f)	The system shall enforce required steps and events sequencing, as appropriate (e.g., key steps cannot be bypassed or similarly compromised).	The application is specifically engineered to follow established workflows when building protocols, performing inventory transactions and dispensing. Users are unable to create or modify records outside of these workflows.

11.10 (g)	The system shall ensure that only authorized individuals can use the system, electronically sign a record, access the operations or computer system input or output device, alter a record, or perform the operation at hand.	All functions within Vestigo are tied to the security system and users can only perform the functions based on their roles within the application.
11.10 (h) (1)	The system shall determine, as appropriate, the validity of the source of data input or operational instruction.	The system will not accept unauthenticated sources. Vestigo is always run over HTTPS thereby removing the possibility for a third party to modify data being transmitted.
11.50 (a) (1), (2), (3)	The system shall ensure all signed electronic records contain the printed name of the signer, date/time signature was executed, and the meaning associated with the signature (e.g. approval, responsibility, authorship).	The records record the user name of the logged in user and a date/time the signature was executed. The date/time are set on the server and the user has no ability to modify. The meaning of the signature is based on the role of the user.
11.50 (b)	The system shall ensure the three signature elements (described in the previous requirement) of a signed electronic record are a part of any human readable form of the electronic record (e.g. electronic display or printout).	The signature items are included in all audit trail reports.
11.70 (a)	The system shall ensure electronic signatures are linked to their respective electronic records and that these electronic signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means.	The records are stamped with each transaction and cannot be modified by the user in any way.
11.100 (a)	The system shall ensure that each electronic signature is unique to one individual and shall not be reused by, or reassigned to, anyone else.	Uniqueness of Username and Password is enforced by the system. This uniqueness survives even the expiry of an account. Inactive accounts and their records are never removed from the system.
11.200 (a) (1)	The system shall employee at least two distinct identification components such as an identification code and a password.	Vestigo employs username and password protection for all functions.
11.200 (a) (1) (i)	The system requires the use of all electronic signature components for the first signing during a single continuous period of controlled system access.	All Vestigo actions require an active session where the authentication is valid. Upon expiration of the authentication, users are redirected to the login screen.

11.200 (a) (1) (i)	The system shall allow all subsequent signing during the same continuous period of controlled system access to use at least one electronic signature component.	The system will continue to use the originating session of each request after the first to maintain security of the session.
11.200 (a) (1) (i)	The system shall ensure users are timed out during periods of specified inactivity.	Time out in a 21 CFR Part 11 environment is enforced after 29 minutes of inactivity by default and cannot be changed.
11.200 (a) (1) (ii)	The system shall require the use of all electronic signature components for the signings not executed during a single continuous period of controlled system access.	All actions must be executed during a continuous period of controlled system access.
11.200 (a) (3)	The system shall require all attempted uses of an individual's electronic signature by anyone other than its genuine owner to require collaboration of two or more individuals.	No sharing of electronic signatures is permitted.
11.300 (a)	The system shall require that each combination of identification code and password is unique, such that no two individuals have the same combination of identification code and password.	The system will not allow duplication. Hashing is used to maintain integrity without storing actual information unencrypted.
11.300 (b)	The system shall require that passwords be periodically revised.	In hardened mode for use in 21 CFR Part 11 environments the system requires password changes every 90 days. This duration may be modified by the client.
11.300 (d)	The system shall employ transaction safeguards preventing the unauthorized use of password and/or identification codes.	Vestigo uses intrusion detection to identify fraudulent transactions. This includes automatic lockout after multiple failed attempts at log in.
11.300 (d)	The system shall detect and report unauthorized use of password and/or identification codes to specified units.	All failed attempts to log in are recorded in logs and available for viewing for administrators.

Questions regarding Vestigo can be sent to support@mccreadiegroup.com.