EVADO
CLINICAL SOFTWARE

Compliance Statement

AUSTRALIA UNITED STATES SINGAPORE
Evado Pty Ltd
L 13, 114 William St Melbourne VIC 3000 Australia
t : +61 3 9600 3616 f : +61 3 9242 4779 w: www.evado.com e: info@evado.com
ACN: 138 226 927

FDA CRF21 Part 11 Compliance Statement

Published by the EVADO Pty. Ltd., Melbourne, Victoria

Document Information

Author:	Ross Anderson
Date:	20 Feb 2017
Version:	7
Approval:	
Approved	20 February 2017

Version History

Ver	Date	Description	Author
0.1	11 Sep 07	First Draft	Ross Anderson
1	12 Sep 07	First release	Jennie Anderson
2	16 Dec 07	Update document for release	Jennie Anderson
3	27 Sep 09	Change to Evado Pty Ltd	Ross Anderson
4	08/01/2010	Change Address	Ross Anderson
5	23/05/2011	Change of address	Ross Anderson
6	16 Jul 2012	Update the letter head	Ross Anderson
7	20/02/17	Update to match Evado version 4	Ross Anderson

Contents

1 Executive Summary

Pharmaceutical, biotechnology and other life sciences companies face the challenge of continuously improving the quality and productivity of their operations in accordance with Good Manufacturing Practice and other GMP standards, while satisfying the regulatory requirements of the U.S. Food and Drug Administration. A fundamental requirement of the FDA regulations is the delivery and management of training to employees and consultants that enables them to perform their assigned functions and assure quality results that satisfy these regulations and fulfill predicated rules.

EVADO has been designed to manage the capture clinical trial or study information. EVADO is a simple to use enterprise-wide Clinical Report Form (eCRF) management system that replaces the paper CRF. EVADO provides a web-based environment for the design, collection and storage of clinical trial records. EVADO is both cost effective and intuitive to use and it manages the eCRF life cycle from creation to completion. Developed in consultation with researchers, investigators and CRO's, EVADO has been designed to simplify the data capture and data management of clinical trials. Trial safety data is provided on line.

This white paper identifies the specific features and technical controls of EVADO that are required to meet the compliance requirements found in 21 CFR Part 11 regarding the management of electronic records and electronic signatures.

EVADO provides a comprehensive platform for managing clinical trials. Utilising the powerful advanced technology features of SQL2008/SQL2012, the core EVADO software provides clinical research organisations with a web-based environment for managing the collection of clinical information, in conformance with the 21 CFR Part 11 requirements.

2 Addressing the requirements of 21 CFR Part 11

The following sections of this document identify the technical controls provided by Evado in EVADO to address individual 21 CFR Part 11 section requirements.

2.1 Subpart B—Electronic Records

2.1.1 Section 11.10 Controls for Closed Systems

EVADO is designed to serve as a closed system. A closed system is defined in this Section as "an environment in which system access is controlled by persons who are responsible for the content of electronic records that are on the system". EVADO provides the necessary controls to ensure the authenticity, integrity and confidentiality of electronic records contained in the EVADO database and incorporates a secure audit trail functionality that supports training activity records documentation and retention requirements.

The following explains the compliance approach utilised in EVADO with respect to the technical controls for closed systems specified in Section 11.10.

2.1.1.1 Validation of systems

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

EVADO developed EVADO using a cyclic software development methodology and the appropriate IEEE software engineering standards combined with our internal Quality System that covers documentation, development, testing (including user testing) and customer support. (Evado procedures are available for clients to review upon request).

2.1.1.2 Generate accurate and complete copies in human readable form

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 such a review and copying of the electronic records.

EVADO gives users the ability to print records and/or generate reports in paper form, or export data in electronic form.

2.1.1.3 Read records throughout their retention period

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

EVADO is a database-driven application, supported by the following industry standard database engines: Microsoft SQL Server 2008/SQL2012. This SQL server is designed to be scalable and expandable to support large amounts of data and to grow with use. Completed records remain online indefinitely allowing users to read historical records.

EVADO does not restrict the number of records stored. However the systems record indexing capacity is limited to 2,000 million records. Scheduled database backups are also recommended throughout the established retention period to ensure record protection.

2.1.1.4 Limiting access to the system

11.10 (d) Limiting systems access to authorized individuals

Each user of EVADO requires a unique Active Directory user account. A user's access to EVADO is controlled at two levels. The static role defines the menu and modules the user is able to access. The trial role delegation controls the user's role and actions with specific trials. The user's static role is defined by the application administrator and the trial roles are managed by the trial manager or principal investigator.

The user's password complexity and expiration period is defined by the Windows security policies that are defined by the Windows security policies.

2.1.1.5 Record audit trails

11.10 (e) Use of secure, computer generated, time-stamped audit trails to independently record the date and time 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's electronic records and shall be available for agency review and copying

A major component of Part 11 Compliance involves a system's audit trail capability.

EVADO audit trail operates at a number of levels to ensure compliance. Database journaling is deployed to ensure that a full audit trail is available for all records in the database. The audit interface allows auditors to view all recorded instances of a record and track all changes to that record. Soft deletion is used to cancel or delete records leaving an audit trail of all changes up until the withdrawal, cancellation or deletion of that record.

Each time a record is update, the user identity and a time date stamp is automatically added to the record. Critical user actions are independently logged, allowing management to view the activity in the system and provide a secondary audit trail of user actions.

A records audit trail is integral to the record, and is maintained for the life of the record.

Once a clinical trial record has been signed off by the orginal author, all subsequent changes to the record's values must annotated.

Trial management are able to access EVADO's audit trail at any time. The web audit interface allows management to view the audit trail of any record in the system.

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

EVADO has been designed to ensure records can only be updated when the pre-requisite steps have be undertaken and successfully completed.

2.1.1.6 User authorisation

11.10 (g) Use authority checks to ensure that only authorised 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.

The Windows Active Directory authentication is used to authenticate and identify all users using EVADO.

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

All external device inputs to the system are independently verified and validated prior to those data sources being used within an Evado clinical project.

The upload of configuration files in CSV or XML data formats are validated by the import process prior to saving these data objects to the Evado database.

The upload of binary or text data files by site users is considered a site document, and has been appropriately validated by the site user prior to uploading the Evado system.

At present EVADO does not provide any direct device inputs to the sytem.

2.1.1.7 Personal training and competency

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

Evado personnel involved in EVADO solution development and implementation have been trained by Evado in the product. Their CVs are available for review upon request. Training in EVADO is provided with each installation and additional training can be provided on request.

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

This is a client managed requirement

11.10 (k)(1) Use of the appropriate controls over systems documentation including: Adequate controls over distribution of, access to, and use of documentation for system operation and maintenance.

Evado has developed version controlled validation documentation as part of system implementation. Documentation is formally reviewed and approved. User manuals are provided to the client for each module of EVADO that is implemented.

2.1.1.8 Document control

11.10 (k)(2) Use of the appropriate controls over systems documentation including: Revision and change control procedures to maintain an audit trail that documents timesequenced development and modification of systems documentation.

Evado provides updated user manuals for all releases of EVADO. Evado has established procedures to control the revision and change of all system documentation for EVADO. A version history page is included in all controlled documents.

2.1.2 Open Systems

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, when appropriate, the confidentiality of the electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified is section.

11.10 As appropriate, and additional measures such as document encryption and the use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality.

Systems implemented by Evado are typically closed systems. That is, the client who has responsibility for the data is the one who controls access to that data. If this is not the case, Evado will work with the Client to develop suitable security and access procedures.

Evado's cloud based platform operates as an Open System, to fulfil the open system requirements Evado:

- Limits the direct access to the customer application server to Network Administrator and Application Administrator.
- The encryption management processes are performed by the Evado application prior to saving any data in the database and Evado automatically manages the encryption keys ensuring that multiple keys are used for various data object. This has been designed to combat brute force key generation.
- All database audit trails are DES3 encrypted, and record boh the old and new values of each change. Thereby providing a continuous audit trail of all changes.
- All patient personal data that is stored by a site, is DES 3 encrypted and only the users at that site have access to that data.
- Under normal circumstances all database updates are performed by the Evado application and include relevant record signoffs and audit trail logging.

- All user access is logged in the server's application event log and in a database table.
- All database scripts used to update the database schema, log when the script was performed along with the table that was updated and what changes have been made to the table.