Assessment of Clindox CRFweb Version 2.0

For Compliance with the Requirements of

FDA 21 CFR 11 (Electronic Records and Electronic Signatures, Final Rule) and EU GMP Annex 11

Report Prepared By: R.D.McDowall, BSc, PhD, CSci, CChem, FRSC Director R.D.McDowall Limited 73 Murray Avenue, Bromley, Kent, BR1 3DJ, UK	**Report Prepared For**: Tom Beaufoy Chief Information Officer Clindox Drinan Enterprise Centre, Feltrim Road, Swords, Co Dublin, Ireland
Signature RDMcDowall	Date: 17th July 2016

Document Information

General Information

Project Name	CRFweb Version 2.0
Document Identity (file name)	Clindox CRFWeb V2.0 Part 11 Assessment Report V2.0 20170717

Document Revision History

Version	Date	Reason for Change	Status
V 1.0	26 Nov 2015	Final Version	Approved
V 1.1	30 Mar 2017	First draft of CRFweb version 2.0	Draft
V 1.2	17 Apr 2017	Update of the document	Draft
V 1.3	22 Jun 2017	Update of the document following Release notes and screen shots	Draft
V 1.4	15 Jul 2017	Incorporation of Sections of Draft FDA Guidance on Part 11 and Clinical Investigations	Draft
V 2.0	17 Jul 2017	Final version	Approved

Distribution List of the Approved Paper Document

Copy No.	Name	Department
1	Original Signed Document	Clindox

Table of Contents

1. Executive Summary

1. Clindox CRFweb version 2.0 has been assessed for compliance with the technical requirements of FDA's 21 CFR 11 and EU GMP Annex 11 (Computerised Systems) by Dr R.D.McDowall, Director, R D McDowall Ltd, UK in March – June 2017.

   The assessment was conducted at two levels:
   - User of the system with typical access privileges for running the application
   - System administrator with all access privileges

   One problem about interpreting Part 11 for GCP is that the regulations are focussed on the process of clinical development rather than computerised systems. Therefore, the FDA Guidance for Industry on Computerised Systems in Clinical Investigations has been used to help interpret Part 11 for this assessment.

   The issue of this report was delayed following the publication in late June 2017 of the FDA's draft guidance on Use of Electronic Records and Electronic Signatures in Clinical Investigations Under 21 CFR Part 11 – Questions and Answers. The pertinent sections of this guidance have been copied into section 6 of this report and either cross referenced to Section 5 which deals with the interpretation of Part 11 or answered in Section 6. It should be noted that the FDA guidance is still draft but the intention of section 6 is to answer questions that may arise from its publication.

2. It is important to recognise that compliance with both 21 CFR 11 requires technical controls that are responsibility of the supplier (Clindox) as well as the procedural and administrative controls that are the responsibility of the customer. This assessment discusses all applicable controls and highlights the responsibilities of both the supplier and a customer for compliance with the regulations. This is especially important as Clindox is a SaaS application operated in a third party hosting site.

   To be compliant with the Part 11 and Annex 11 regulations all appropriate technical, administrative and procedural controls need to be in place for any system. Therefore both the supplier and the customer have roles and responsibilities in the regulatory compliance of any computerised system.

3. Clindox have a developing Quality Management System (QMS) covering the Agile-based software development process. – procedures are in place that cover the software development and will be expanded over time.

4. Clindox software is compliant with 21 CFR 11 technical controls.
   - Security and Access Controls are adequate with roles defined and unique user names
   - Operational System Checks (the software works in the correct sequence or workflow and cannot be overridden) is defined by the eCRF and the visit schedule for each clinical study
   - Integrity of data is maintained by the database and all actions in the system are attributable to individuals via their log-on credentials
   - Audit Trails exist in the software and they track the identity of who performs each task
   - Part 11 compliant electronic signatures have been implemented in the application for signing the completed eCRF.

5. As the system is Software as a Service (SaaS) within a hosted environment some additional requirements need to be considered outside of 21 CFR 11 technical compliance (these are specific EU GMP Annex 11 requirements):
    - The adequacy of the IT hosting environment needs to be assessed e.g. physical security, fire suppression, redundancy of power, internet access resilience and environmental controls
    - IT infrastructure must be qualified and controlled
    - IT staff operating the system must be given GXP awareness training with respect to how it impacts their jobs
    - Backup and recovery need to be validated and test restores performed regularly with evidence that restores work

2. Purpose

The purpose of this document is to document the 21 CFR 11 and EU GMP Annex 11 assessment of the Clindox CRFweb version 2.0 performed by Bob McDowall, Director, R D.McDowall Ltd, UK.

The assessment was carried out on 29th March 2017 at the offices of R.D.McDowall Ltd with follow up information added to this report as the software was finalised for release.

2.1 Software Version Assessed

Clindox CFRweb version 2.0 was assessed for compliance with the technical controls of 21 CFR 11.

2.2 Overview of the Clindox System

Clindox was originally a company that had a business in the Nordic region based on producing paper Case Report Forms (CRFs) for clinical trials. The application was developed as a request from customers for a simple to use web interface to record patient data and replace paper CRFs. The parent company is located in Dublin with software development taking place via Clindox India, a subsidiary located in Pune with 6 – 7 programming staff. Agile software development uses Jira (an Atlassian product) to manage the backlog and select user stories and epics for individual sprints. The front end web design, wireframes and programming in HTML and CSS, is managed through a third party that uses Axure RP. Testing of the system is currently manual although automation of the process is being explored..

The Clindox system is a SaaS (Software as a Service) application with the current system is hosted in the US but European hosting sites are also used to comply with EU data protection directives. The current hosting provider is Amazon Web Services (AWS).

An editor is responsible for translating the protocol requirements into an eCRF for investigators to fill-in. Before use the eCRF is circulated to a sponsor to review and update or publish. The published eCRF is completed by an investigator via the web. A monitor checks the entries as well as the system flagging up discrepancies and either asks questions to clarify answers or approves the completed eCRF. An administrator role is used for managing the system and user account management.

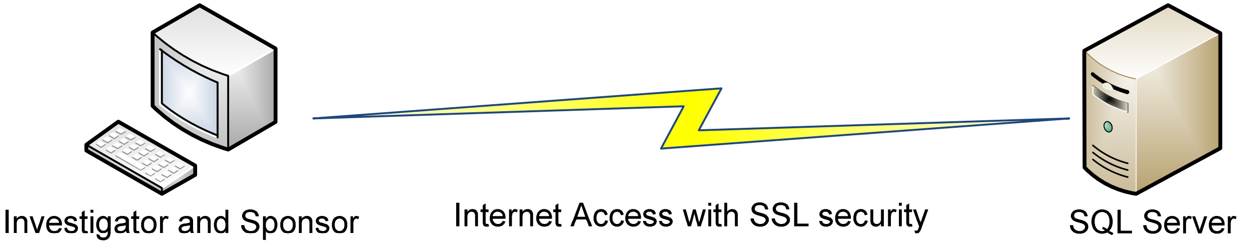
2.3 GAMP Software Category

Clindox software is classified as GAMP software category 3 (non-configurable commercial product) as defined in version 5 of the GAMP guide in Appendix M4.

The reason is that the business process cannot be changed as the software focuses on eCRF design and use in a clinical study. Although the eCRF can be configured for each clinical study this is the normal function of the software. In addition, user controls should be in place to verify and publish the finished eCRF before use in any specific study.

2.4 System Architecture

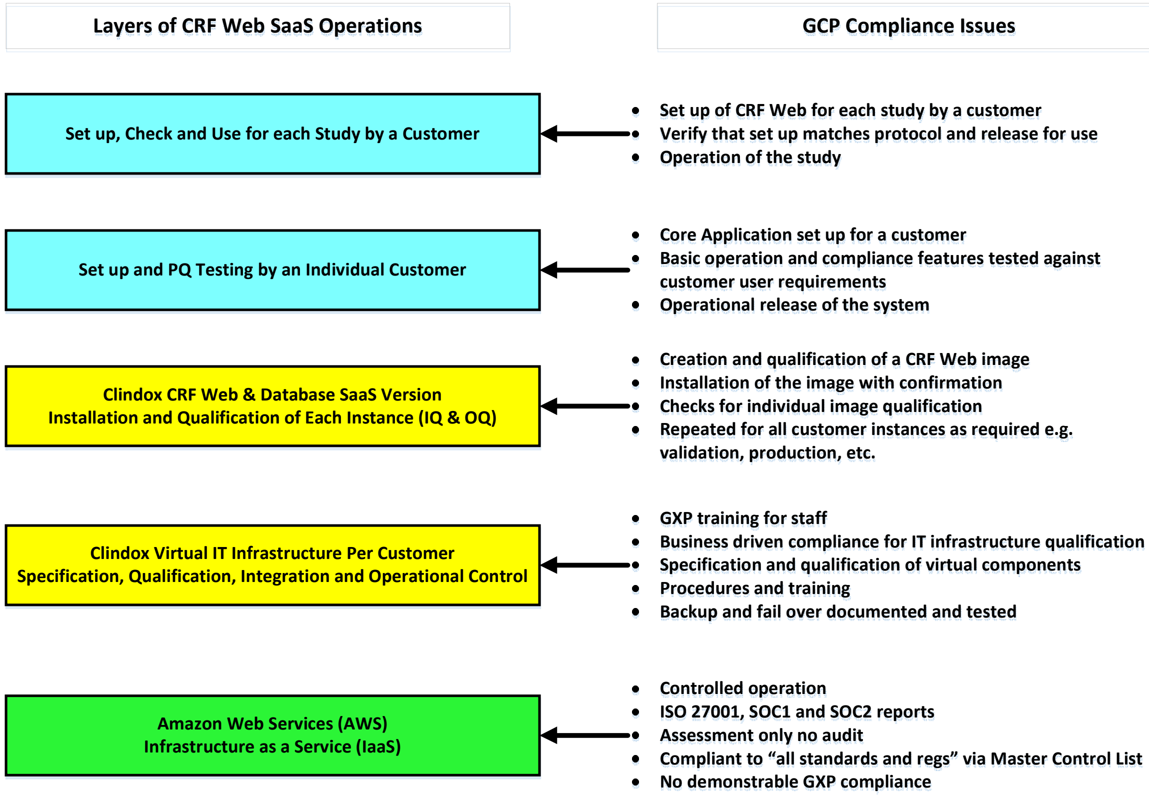
Clindox software is implemented as a SaaS application using a global hosting company offering Infrastructure as a Service (IaaS) on a country or region specific basis. The IaaS hosting provider is Amazon Wed Services.



Each user has a unique identity (which is typically their e-mail address) plus a password and Capcha log in to access the system via the Internet. Secure socket layer security is used to ensure that data entered is not hacked.

2.5 SaaS and IaaS Layers

Layers of the system are presented in the figure below which shows the responsibilities shared between Amazon Web Services (AWS), Clindox and the Customer:



Layers of CRF Web SaaS Operations

GCP Compliance Issues

Set up, Check and Use for each Study by a Customer

- Set up of CRF Web for each study by a customer
- Verify that set up matches protocol and release for use
- Operation of the study

Set up and PQ Testing by an Individual Customer

- Core Application set up for a customer
- Basic operation and compliance features tested against customer user requirements
- Operational release of the system

Clindox CRF Web & Database SaaS Version
Installation and Qualification of Each Instance (IQ & OQ)

- Creation and qualification of a CRF Web image
- Installation of the image with confirmation
- Checks for individual image qualification
- Repeated for all customer instances as required e.g. validation, production, etc.

Clindox Virtual IT Infrastructure Per Customer
Specification, Qualification, Integration and Operational Control

- GXP training for staff
- Business driven compliance for IT infrastructure qualification
- Specification and qualification of virtual components
- Procedures and training
- Backup and fail over documented and tested

Amazon Web Services (AWS)
Infrastructure as a Service (IaaS)

- Controlled operation
- ISO 27001, SOC1 and SOC2 reports
- Assessment only no audit
- Compliant to “all standards and regs” via Master Control List
- No demonstrable GXP compliance

The Responsibilities of the three parties involved SaaS

- AWS: provide the controlled physical infrastructure and hypervisor (Zen) within the latter are AWS templates for virtual infrastructure components by Clindox.
- Clindox: using the AWS templates create and qualify one or more virtual environments for a customer including the CRFweb instance. Staff monitoring and maintaining the SaaS instances are trained in GXP compliance
- Customer: validates their instance of CRFweb and operates it in a compliant manner

2.6 Referenced Documents

The following documents are referenced in this assessment report.

2.6.1 Regulations

- 21 CFR 11: Electronic Records; Electronic Signatures Final Rule, 1997
- ICH E6 Good Clinical Practice regulations, 1996
- EU GMP Annex 11 Computerised Systems, 2011

2.6.2 Regulatory Guidance

- FDA Guidance for Industry: Part 11 Scope and Application 2003
- PIC/S PI-011-3, Computerised Systems in GXP Environments, 2007
- FDA Guidance for Industry: Computerised Systems in Clinical Investigations, 2007

2.6.3 Industry Guidance

- Good Automated Manufacturing Practice (GAMP) guidelines, Version 5, ISPE, Tampa FL, 2008
- Good Automated Manufacturing Practice (GAMP) Good Practice Guide IT Infrastructure Control and Compliance, ISPE, Tampa FL, 2005
  Note that the second edition of this guidance is in preparation and should be published 2nd half of 2017
- E-TMF.org
- Critical Path Institute (www.c-path.org)
- Google Material Design templates

3. 21 CFR 11: Electronic Records and Electronic Signatures

Published in March 1997 and effective on 20th August 1997, the Electronic Records; Electronic Signature final rule (21 CFR 11) has had the greatest impact on computerized systems than any other regulation. The basic requirement is to ensure that computerized systems produce records that have the integrity and reliability and electronic signatures are trustworthy and equivalent to handwritten signatures executed on paper records.

3.1 21 CFR 11 Compliance Assessment Checklist

The following 21 CFR 11 compliance assessment has been developed and compiled from a number of compliance assessments performed for clients since 1999. The FDA's Guidance for Industry on Part 11 Scope and Application has narrowed the scope of Part 11 and has modified the compliance requirements for a number of Part 11 requirements notably validation, device and operational system checks, audit trail, copies of records and retention of records. However if working electronically the impact of this relaxation is limited.

3.2 Interpretation of 21 CFR 11

The interpretation of sections of 21 CFR 11 requirements is based on Bob McDowall's experience since 1998 in interpreting the regulations for a number of clients. This work has included the writing or review of Corporate Part 11 Policies and corporate procedures, training staff in 21 CFR 11 assessments and performing part 11 assessments on behalf of clients. In addition, Bob McDowall has published a book on validation for chromatography data systems, numerous book chapters, articles and given workshops and presentations on this subject that can be used to interpret the regulation and its 2003 revision (FDA Guidance for Industry; Part 11 Scope and Application).

3.3 Format of the Compliance Assessment Tables

The tables for the assessment of the Part 11 compliance of Clindox have the following structure:

- Column 1: 21 CFR 11 reference number
- Column 2: presents the specific section from the Part 11 regulation and is typically quoted verbatim – underneath are the questions for assessment derived from the requirement.
- Column 3: defines the type of control required. For ease of presentation, administrative and procedural controls are summarised under the topic "Proc" and technical controls are listed under "Tech"
- Column 4: this defines the responsibility for the control item – the customer for procedural controls and the supplier (Clindox-Toledo) for technical controls.
- Column 5: Assessment of the software and / or any supporting comments

Ref No.	21 CFR 11 Requirement and Reference	Control	Responsible	Assessment
	§ 11.10 Controls for Closed Systems			
	System Validation [11.10(a)] ***Validation of the systems to ensure accuracy, reliability, consistent intended performance and the ability to discern altered and invalid records.***			

3.4 Assessment Approach

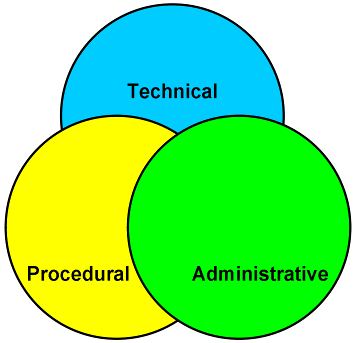
This compliance assessment was based on the following ways of using and accessing the system:

- Using the system as a normal user with simulated and real instruments
- Using the system as an administrator with all access privileges

3.5 Technical, Administrative and Procedural Controls

Part 11 requires a regulated healthcare organisation to have in place three levels of control:

- Administrative controls: e.g. policies for Part 11 and the use of electronic signatures
- Procedural controls: SOPs for using the system
- Technical controls: functions built into software that ensure the reliability and integrity of the function e.g. security, audit trails



Supplier:
Technical
Controls

Customer:
Procedural &
Administrative
Controls

Figure 2: A 21 CFR 11 compliant system requires 3 elements: one from the supplier and two from the user

Please note that you cannot purchase a 21 CFR 11 compliant application. There are applications that can be designed to be compliant with 21 CFR 11 technical controls, but it is the user that is responsible for providing policies and procedures to ensure the systems are fully compliant with the regulations and the predicate rule applicable. This is shown in Figure 2 below and illustrates the importance of an integrated approach to 21 CFR 11 compliance and why a there are no 21 CFR 11 compliant applications.

4. 21 CFR 11: Controls Required for Electronic Records

Abbreviations for 21 CFR 11 Control Type: Proc = Procedural & Administrative (Customer responsibility); Tech = Technical (Supplier responsibility)

Ref No.	21 CFR 11 Requirement and Reference	Control	Responsible	Assessment
	§ 11.10 Controls for Closed Systems			
	System Validation [11.10(a)] ***Validation of the systems to ensure accuracy, reliability, consistent intended performance and the ability to discern altered and invalid records.***			
11.10(a) / 1	Is the system validated to the Company standards?	Proc Proc	Customer Supplier	The end user is responsible for validation following established company policies and procedures. Clindox have evolved their procedures for controlling software development using their Agile process and the use of software tools such as Jira, Confluence and Bit Bucket. will help enforce working procedures. The QMS has procedures to define working practices and this is enforced by configuration of Jira.
11.10(a) / 2	Did validation include tests and checks that demonstrate compliance with all applicable parts of 21 CFR 11 (e.g. audit trail, backup/restore, archive, security controls, device/terminal checks, e-signatures)? If No, determine omissions as part of the Action Plan. This is based on these technical controls being designed, programmed and tested into the system by the supplier.	Proc Proc	Customer Customer	The end user is responsible for validation of these features following established company policies. Policies within the Clindox software enable a customer to fine tune some of the controls e.g. password length and expiry period. The settings of these application policies will need to be documented by each regulated customer following their computerised system validation policy and procedures.
	Record Inspection [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.***			
11.10(b) / 3	Can the system generate accurate and complete copies of records in both human readable and electronic form (ASCII, PDF) for inspection by the FDA?	Tech Proc	Supplier Customer	Output from the system should be either printed direct form the system or printing a secure PDF. SDTM, CDISC and XPT. ADM output is also provides a snap shot of the data inputs and transactions carried out on them. HTML output is only used for CRFs in development. An SOP for the handing over of electronic records during an inspection is recommended.

Ref No.	21 CFR 11 Requirement and Reference	Control	Responsible	Assessment
11.10(b) / 4	Does the Computer System generate copies to which a user has access to e.g. configuration settings, protocols, CRFs, etc?	Tech	Supplier	This function is to be developed by Clindox.
	Records Protection [11.10(c)] ***Protection of records to enable their accurate and ready retrieval throughout the records retention period.***			
11.10(c) / 5	Are all electronic records saved to a secure area, preferably on the site Network?	Tech	Supplier	Clindox can establish an AWS location or region to meet a customer's specific requirements.
11.10(c) / 6	Do SOPs cover who is responsible for backup and recovery and how this shall be done?	Tech	Supplier	Backup is via the hosting site and a full backup is scheduled overnight. Secondary failover locations can also be established for system resilience and security of backup.
11.10(c) / 7	Do SOPs cover who is responsible for long term archiving and retrieval and how this shall be done?	Proc	Customer	The users should comply with their corporate standards or guidelines for archival and retrieval of electronic records.
11.10(c) / 8	Are all electronic records included in system backups?	Proc	Supplier	The supplier is responsible for backup and recovery of e-records contained within the system according to the service agreement between Clindox and a customer. AWS backup the system and Clindox also backup customer data and hold this off site
11.10(c) / 9	Can data generated from earlier software versions be retrieved from archive and viewed in its entirety?	Tech	Supplier	Yes, data can be migrated from existing versions of the application as the C-DISC ODM Model is used.
11.10(c) / 10	If records can be copied outside the application, is user access to the copy read-only? • If no, does the software prohibit the overwriting of the original record by the copy?	Tech Proc	Supplier Customer	Secure PDF is the main output for this. The application can also output data as CSV, XML and XPT but these are not secure and can be edited. The audit trail will record the time and date of exported data. When available, the customer needs to have procedures for handling the data copied or exported from the system.
11.10(c) / 11	Are Critical Records stored in one location only? • If No, do validated automatic functions exist to maintain data integrity?	Tech	Supplier	Records entered into the CRF are stored in a central database. As noted above, resilience using a failover site can be used
11.10(c) / 12	Is concurrent write access by multiple users prohibited?	Tech	Supplier	Not applicable as the investigator completes a CRF and then a monitor reviews the data.
11.10(c) / 13	Can data be recreated after Computer System failures?	Proc	Customer	Providing that the system has been backed up, the system and data can be recreated after a failure.
11.10(c) / 14	Are the records protected from hazards such as fire, heat and water by environmental controls (e.g. ventilation, fire suppression systems, etc.)?	Proc	Supplier	Not investigated directly as part of this assessment. However, AWS are ISO 27001 certified. As part of this standard there are redundant fire suppression controls and the hosting site will not be subject to water ingress

Ref No.	21 CFR 11 Requirement and Reference	Control	Responsible	Assessment
11.10(c) / 15	Have retention periods for the electronic records retained in the system been specified?	Proc	Customer	This is dependent on the contract between the customer and Clindox.
	Security [11.10(d)]: ***Limiting system access to authorized individuals.***			
11.10(d) / 16	Are devices for storage of electronic records (e.g. PC, file/database servers and backup and archive durable media) located in a controlled area or physically secured?	Proc	Supplier	The backup from AWS is disk to disk. The hosting site is secure and only AWS staff have access to the site and is secure as the company is ISO 27001 certified. Clindox staff have remote access to the IaaS area only.
11.10(d) / 17	Does the system limit system access to authorised individuals?	Tech Proc	Supplier Customer	Yes, the system enforces that each individual user must have a unique user identity. The user types and access privileges for each are user configurable. A single user identity can have more than one user type and the activities of a user are logged against their user type. There is a capability matrix for user type versus access privileges that can be printed out for each study on paper or secure PDF. Define and maintain a list of current and historical users of the system. Ensure that user identities are not shared.
11.10(d) / 18	Does the system prevent deletion of users from the system, to ensure uniqueness of user identities? The user identity should be “deactivated” but retained.	Tech	Supplier	If a user identity is suspended or deactivated, the record remains within the database and a new user with an existing identity cannot be created within the database.
11.10(d) / 19	Does the system have a password-protected inactivity lock enabled?	Proc Tech	Customer Supplier	The customer must enable the inactivity locks by configuring this option: enabling it and setting the inactivity period. There is a user configurable inactivity time-out function available in the software.
11.10(d) / 20	Is user access to the Operating System restricted to the System Administrator, or equivalent authorised user?	Proc	Customer	The SOP for logical security should include the definition of who can access the operating system, coupled with training to implement the SOP.
11.10(d) / 21	If the computer system can be accessed remotely, are additional security measures, such as “call back” or SecurID included?	Proc	Customer	Not applicable.
11.10(d) / 22	Do remote access sessions automatically log-off when a disconnect is detected?	Tech	Supplier	Not applicable as the is no remote access, the application is direct access via the web.

Ref No.	21 CFR 11 Requirement and Reference	Control	Responsible	Assessment
11.10(d) / 23	Are safeguards in place to detect attempts at unauthorised use, and to lock the account after several consecutive unsuccessful attempts to enter a password?	Tech Proc	Supplier Customer	The system has a default of 3 attempts at access and then the account will lock See also 11.300(d) answers Part of the system administration SOP should include how to unlock disabled accounts.
11.10(d) / 24	Is there an approved procedure that describes the administration of user and administrator security and access control (system security)?	Proc	Customer	The customer must write an SOP to control system access and the establishment and maintenance of logical security.
	Audit Trail [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.***			
11.10(e) / 25	Are there computer-generated (automatic audit trails) of all user actions?	Tech	Supplier	There are two audit trails in the Clindox system which are activated at installation and cannot be turned off. The first is a transactional log that records every activity within the system. The second is a simple right click when a field is indicated as changed and information about the reason for change can be revealed. The audit trail starts from when an eCFR has been published. This is acceptable as the earlier versions are draft and unapproved.
11.10(e) / 26	Are audit trail entries date stamped DD-MMM-YYYY?	Tech	Supplier	Time stamps are configurable in the format of DD/MM/YYYY or MM/DD/YYYY, DD/MMM/YYYY, YYYYY/MM/DD or MMM/DD/YYYY. .

Ref No.	21 CFR 11 Requirement and Reference	Control	Responsible	Assessment
11.10(e) / 27	Are audit trails time stamped HH-MM-SS in local time?	Tech	Supplier	Server time is the time stamp within the system. The time stamp in the audit trail uses a 24 hour clock together with the time zone of the server. Local time is shown only on a user's workstation location.
11.10(e) / 28	Are there controls to ensure that the system clock date and time stamps are accurate and secure from tampering?	Proc	Supplier	As the system is hosted by AWS and no individual from either Clindox or the customer can change the time settings. It is assumed that the clock is synchronised with a trusted time source e.g. internet time source linked to a national laboratory or a network time protocol (NTP) server.
11.10(e) / 29	Do all audit trail entries include operator identity, using full name or the Customer-defined user ID of an individual?	Tech	Supplier	The full name of the user (not user identity is entered into the audit trail) along with the old and new values, the user action, modified by plus the date and time
11.10(e) / 30	Is there an audit trail entry for system activity, including all user logon and failed access attempts?	Tech	Supplier	Yes, see 11.10(e)/29
11.10(e) / 31	Is an audit trail entry generated during creation of all data?	Tech	Supplier	Yes, for published eCRFs and system events.
11.10(e) / 32	Is an audit trail entry generated during modification of all data by a user?	Tech	Supplier	The audit trail for a study is only operational after the eCRF has been published.
11.10(e) / 33	Is an audit trail generated during "deletion" or "inactivation" of all data?	Tech	Supplier	Yes
11.10(e) / 34	If the record is changed does the system retain/display the old and new values?	Tech	Supplier	Yes
11.10(e) / 35	Does each audit trail entry describe the action performed?	Tech	Supplier	Yes
11.10(e) / 36	Does the audit trail contain sufficient information to allow a reviewer to trace all changes to a record from its current state back to the original values?	Tech Proc	Supplier Customer	The audit trail contains a configurable field for a user to enter a reason for change. Develop the reasons for change for the system
11.10(e) / 37	Is the audit trail directly associated with the record, but located separately?	Tech	Supplier	The audit trail is a separate record in the database
11.10(e) / 38	Are audit trail records being maintained for at least as long as the retention of the underlying records? (Are they backed up with the records and can they be retrieved?)	Tech Proc	Supplier Customer	The audit trail is part of the records contained in the database. Backing up the database means that all records are backed up in a single operation and can be maintained by the user.

Ref No.	21 CFR 11 Requirement and Reference	Control	Responsible	Assessment
11.10(e) / 39	Is a read-only display or report available for viewing the audit history?	Tech	Supplier	A read only display of the audit trail is available..
11.10(e) / 40	Are audit trails available for review and copying by regulatory authority?	Tech Proc	Supplier Customer	There is the ability to search and print either hardcopy or output XLS or secure PDFfile of the audit trail entries A procedure for review of audit trail entries is required.
11.10(e) / 41	Are all users, (including the Administrator) unable to modify audit trail details?	Tech	Supplier	The audit trail is encrypted in the database
11.10(e) / 42	Are changes to user authority levels and permissions audit trailed?	Tech	Supplier	Yes
	Operational Checks [11.10(f)] ***Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.***			
11.10(f) / 43	If the sequence of system steps or events is important in a process, is this enforced by the system? (as appropriate)?	Tech	Supplier	The published eCRF for an individual study contains the visits scheduled, data entered and questions raised by the monitor. The progress of individual data items is also colour coded to identify the status of each visit and where in the process the work is and who is responsible.
	Authority Checks [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.***			
11.10(g) / 44	Does the software require entry of a separate user ID and password, in addition to that required by the operating system?	Tech	Supplier	Yes, plus a captcha function to avoid webbot hacking of the system due to weak user passwords
11.10(g) / 45	Does each user have an individual account?	Tech Proc	Supplier Customer	Yes Customers need to have a user management SOP to ensure segregation of duties and avoid conflicts of interest.

Ref No.	21 CFR 11 Requirement and Reference	Control	Responsible	Assessment
11.10(g) / 46	Has the system various user-defined access control levels?	Tech Proc	Supplier Customer	Yes, there are three predefined roles with access levels that are provided as default by the supplier, these are: Administrator, Data Input and Monitor A user account management SOP is required for managing user access to the system.
11.10(g) / 47	If the system has various user levels, are there SOP(s) in place to describe how a user's access shall be defined?	Proc	Customer	The customer should have an SOP that defines the user types with the associated access privileges associated with each type. Users and their access privileges need to be reviewed on a regular basis – see the EU GMP section on Annex 11.
11.10(g) / 48	Are modifications/deletions to data always performed through the application control? (E.g. data are not changed through SQL or other data access tools).	Tech	Supplier	Only Clindox have the database password, therefore modification of data by customers via the backdoor is not possible.
	Device and Terminal Checks [11.10(h)] ***Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction***			
11.10(h) / 49	Are device checks to determine validity of the source of input or operation designed and implemented in the system (as appropriate)*? [E.g. an application indicating that data input is derived from a particular device, such as a balance, should identify the device or only allow data entry from that device, and not from a terminal].*	Tech	Supplier	Not applicable to Clindox
11.10(h) / 50	Are terminal checks to determine validity of the source of input implemented?	Tech	Supplier	Not applicable to Clindox

Ref No.	21 CFR 11 Requirement and Reference	Control	Responsible	Assessment
	Personnel Qualifications [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***			
11.10(i) / 51	Has it been documented that the following persons have the education, training, and experience to perform their assigned tasks: Developers of the computerised system? *Note: Following the preamble, this requirement only goes as far as internal developers. (Comment 87). In order to answer Yes to this question, the vendor must maintain training records, and be aware of the 21 CFR 11 implications. Documentation should be available for review during audits.*	Proc	Supplier	Key Clindox staff have read and interpreted Part 11 regulations to enable the technical requirements to be incorporated in the software.. AWS staff have a list of controls to which they operate across all customer areas that include GXP regulations. Training in these controls is recorded in the ISO 27001 QMS of AWS.
11.10(i) / 52	External maintainers of the computerised system?	Proc	Supplier	AWS staff have a list of controls to which they operate across all customer areas that include GXP regulations. Training in these controls is recorded in the ISO 27001 QMS of AWS
11.10(i) / 53	Internal maintainers of computerised system?	Proc	Customer	Training of the maintainers of the system needs to be documented by the customer.
11.10(i) / 54	Users of the computerised system?	Proc	Customer	Training of user's needs to be documented by the customer.
	Accountability and Responsibility for Actions [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***			
11.10(j) / 55	Have policies and/or procedures holding individuals accountable and responsible for actions initiated under their electronic signatures been established and followed?	Proc	Customer	The customer needs to have an SOP coupled with effective training for the use and accountability for the user of electronic signatures.

Ref No.	21 CFR 11 Requirement and Reference	Control	Responsible	Assessment
	Systems Documentation Controls [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.*** *Note: This covers vendor supplied manuals/documentation as well as logs for the system (backup, errors etc.)*			
11.10(k) / 56	Are there adequate controls over the distribution of documentation for system operation and maintenance?	Proc	Customer	Controlled copies of SOPs should be issued by the Quality Assurance Department.
11.10(k) / 57	Are there adequate controls over access to documentation for system operation and maintenance?	Proc	Customer	The procedures and other documentation for system operation and maintenance must be controlled.
11.10(k) / 58	Are there adequate controls over the use of documentation for system operation and maintenance?	Proc	Customer	The procedures and other documentation for system operation and maintenance must be controlled.
11.10(k) / 59	Are revision and change control procedures in place to maintain an audit trail that documents the time-sequenced development and modification of the systems documentation? *(Only applies to documentation that can be changed by individuals within Customer).*	Proc Proc	Supplier Customer	Yes, manuals for each version of Clindox software are controlled and available as PDF files. The customer is responsible for ensuring only the correct version of the manual is available for use. When the software is updated, the old versions of the manual will need to be withdrawn and archived.

Ref No.	21 CFR 11 Requirement and Reference	Control	Responsible	Assessment
	§11.50 Signature Manifestations.			
	Signing Requirements [11.50(a)] ***(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.***			
11.50(a) / 1	Do electronically signed electronic records contain information associated with the signing that clearly indicates: The full printed name of the signer? [11.50 (a)(1)]	Tech	Supplier	Electronic signature includes the full name of the signer
11.50(a) / 2	The date and time when the signature was executed? [11.50(a)(2)] *N.B. Handwritten signatures on paper records require date only.*	Tech	Supplier	The date and time of the signing is captured by the application
11.50(a) / 3	The meaning of the signature? [11.50(a)(3)]	Tech	Supplier	The reason for signature is defined in the set up for the eCFR e.g. submit for review or signoff.
	Controls for Electronic Signatures [11.50(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).***			
11.50(b) / 4	Are all items in the signature manifestation subject to the same controls as for electronic records? [11.50(b)].	Tech	Supplier	Yes
11.50(b) / 5	Are all items in the signature manifestation included as part of any human readable form of the electronic record (such as electronic display and/or printout or report)? [11.50 (b)]	Tech	Supplier	The signature manifestation is on a secure PDF of the eCRF and includes the meaning of the signature, date and time..
11.50 (b) / 6	Is there the ability to revoke an electronic signature?	Tech	Supplier	Not yet, this may be required in a later revision of the application

Ref No.	21 CFR 11 Requirement and Reference	Control	Responsible	Assessment
	§11.70 Signature/Record Linking.			
	Linking Signatures to Electronic Records [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.***			
11.70 / 1	Are all *electronic* signatures on electronic records 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? [11.70]	Tech	Supplier	Yes via a secure PDF.
11.70 / 2	Are *hand written* signatures on electronic records linked to their respective electronic records? *Note: Minimum requirement is initials of signer, print date/time unique sample identifier, and, if appropriate, file name and location / file size.*	Proc	Customer	This is not applicable as the system is designed to work electronically
11.70 / 3	Does the system identify whether a record has been modified after application of the electronic signature, and require a new signature?	Tech	Supplier	The secure PDF containing the electronic signature is tamper evident
11.70 / 4	When changes are made to previously approved electronic records, are electronic or hand-written signatures applied to updated records, and linked to the original signed record?	Tech	Supplier	If a revision is made to a record the electronic signature reason is amended.

5. 21 CFR 11: Controls Required for Electronic Signatures

Abbreviations for 21 CFR 11 Control Type: Proc = Procedural & Administrative (Customer responsibility); Tech = Technical (Supplier responsibility)

Ref No.	21 CFR Requirement and Reference	Control	Responsible	Assessment
	§11.100 General Requirements.			
	Uniqueness of Signature [11.100(a)] ***(a) Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.***			
11.100 (a) / 1	Are electronic signatures unique to an individual? [11.100 (a)]	Proc	Customer	An SOP is required to ensure that user identities are unique to an individual and not reused
11.100 (a) / 2	Does the system prohibit use of shared/group accounts as components of electronic signatures?	Tech	Supplier	Yes, user identities must be unique and not shared – see 11.100(a)/1
	Verification of Identities [11.100(b)] ***(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 (b) / 3	Electronic signatures cannot be reused by, or reassigned to, anyone else [11.100 (b)]	Proc	Customer	See 11.100(a)/1
	Certification to the FDA [11.100(c)] **(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.***			
11.100 (c) / 4	Is the identity of an individual verified before an electronic signature is allocated? [11.100 (c)]	Proc	Customer	The customer needs to ensure via a procedure that user identities are verified
11.100 (c) / 5	Has the customer organisation sent a letter to the FDA, stating their intent to use electronic signatures?	Proc	Customer	Before using a system with electronic signatures, the organisation must send a letter to the FDA stating that electronic signatures are legally equivalent to handwritten signatures.

Ref No.	21 CFR Requirement and Reference	Control	Responsible	Comments
	§11.200 Electronic Signature Components and Controls.			
	Components and Sessions [11.200(a)] ***(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.*** (1) Be used only by their genuine owners; and (2) 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 (a) / 1	Is the signature made up of at least two components, such as an identification code and password or an ID card and a password? [11.200 (a)(1)]	Tech	Supplier	Yes, two components (user identity and password) are used for an electronic signature
11.200 (a) / 2	When several signings are made during a continuous session, is the secret part of the signature executed at each signing? Both components must be executed at the first signing of a session. [11.200 (a)(1)(i)]	Tech	Supplier	Both components are used throughout the application when signing any record
11.200 (a) / 3	If signings are not done in a continuous session, are both components of the electronic signature executed with each signing? [11.200 (a)(1)(ii)]	Tech	Supplier	See 11.200(a)/2
11.200 (a) / 4	Are signatures designed to ensure that they can only be used by their genuine owners? [11.200 (a)(2)]	Proc	Customer	Procedural controls are required to ensure that passwords are not used by persons other than the correct owner of the password.

Ref No.	21 CFR Requirement and Reference	Control	Responsible	Comments
11.200 (a) / 5	Would an attempt to falsify an electronic signature require the collaboration of at least two individuals? [11.200 (a)(3)]	Proc	Customer	Yes: sharing the user identity and password
	Biometric Electronic Signatures [11.200(b)] ***(b) Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.***			
11.200 (b) / 6	Have biometric electronic signatures been validated including attempted use by other users? [11.200(b)]	N/A	N/A	Not applicable, biometrics are not used by the application
	§11.300 Controls for Identification Codes/Passwords.			
	Uniqueness of Electronic Signature [11.300(a)] ***(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 (a) / 1	Does the system keep all password details confidential, so that they are not available to any system user, including the Administrator?	Tech	Supplier	Password are encrypted within the system using an MD5 algorithm and passwords are obscured when entering. Passwords are 10 characters long and must have at least 1 upper case letter and 1 symbol. There is automatic password expiry with notification to the user.
11.300 (a) / 2	Are controls in place to maintain the uniqueness of each combined identification code and password, such that no two individuals can have the same combination of identification code and password? [11.300 (b)]	Proc Tech	Customer Supplier	The customer needs to ensure that identities are allocated to a single individual and never reused and passwords must never be divulged. There is a technical control to ensure that user identities cannot be duplicated.
	Checking of IDs and Passwords [11.300(b)] ***(b) Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password ageing).***			
11.300 (b) / 3	Are procedures in place to ensure that the validity of identification codes is periodically checked? [11.300 (b)]	Proc	Customer	The customer needs to have a procedure in place for a regular check of the users defined in the system and making any corrective actions.

Ref No.	21 CFR Requirement and Reference	Control	Responsible	Comments
11.300 (b) / 4	Do passwords periodically expire and need to be revised? [11.300(b)]	Tech Proc	Supplier Customer	Yes, there is an option for the system administrator to define the time before the password must be changed. There is also an option to notify users that their password is about to expire. The customer needs to implement the password aging time that is consistent with their organisation's corporate policies.
11.300 (b) / 5	Are passwords obscured when entered?	Tech	Supplier	Yes, the characters used in the password are obscured. There is also a configuration possible that defines the minimum number of characters that must be used.
	Loss of Passwords and Tokens [11.300(c)] ***(c)Following loss management procedures to electronically deauthorize 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 (c) / 6	Is there a procedure for recalling identification codes and passwords if a person leaves or is transferred? [11.300(c)]	Proc	Customer	The customer needs a procedure for a system administrator to suspend an account when a user moves, changes position or leaves the company.
11.300 (c) / 7	Is there a procedure for temporary or permanent replacements using suitable rigorous controls? [11.300(c)]	Tech	Supplier	Clindox require a procedure needs to ensure that resetting of account passwords is secure and that only the appropriate account is reset. Clindox have developed a function where by a user can input personal data so that if their current password is forgotten a new one can be e-mailed to them.
	Unauthorised Use [11.300(d)] ***(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 (d) / 9	Is there a technical feature to detect attempts at unauthorised use and for informing security? [11.300(d)]	Tech	Supplier	When a user enters their password incorrectly three times the account is locked.

Ref No.	21 CFR Requirement and Reference	Control	Responsible	Comments
11.300 (d) / 10	Is there a procedure for immediate and urgent reporting to security/management any attempt at unauthorised use of identification codes and passwords? [11.300(d)]	Proc	Customer	The local administrator needs a procedure for responding to security breaches on the hosted system.
	Checking Devices [11.300(e)] ***(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.***			
11.300 (e) / 11	Are tokens or devices regularly checked or replaced?	N/A	N/A	Tokens and devices are not supported by the software.

6. FDA Guidance Use of Electronic Records and Electronic Signatures in Clinical Investigations

Note: The FDA draft Guidance for Industry entitled Use of Electronic Records and Electronic Signatures in Clinical Investigations Under 21 CFR Part 11 – Questions and Answers was issued in June 2017. This section is based on Section IVB for outsourced clinical services but integrates some the questions from other parts of the guidance referenced in this specific section of the draft guidance. The material in this section is only a portion of the draft FDA guidance. FDA questions are complete but the FDA answers in the next two sections have been edited and therefore, it is recommended that the whole document is read to obtain a complete picture of the guidance.

6.1 Section IV B. Outsourced Electronic Services

FDA recognizes that sponsors and other regulated entities may choose to outsource electronic services. Examples of these types of electronic services are data management services, including cloud computing services. According to the National Institute of Standards and Technology, cloud computing is defined as “a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.” [NIST SP 800-145].

When these electronic services are used to process data for FDA-regulated clinical investigations, sponsors and other regulated entities should consider whether there are adequate controls in place to ensure the reliability and confidentiality of the data. Sponsors and other regulated entities should consider the factors in the following bulleted list when determining the suitability of the outsourced electronic services. If the outsourced electronic service does not provide the data security safeguards described in the following bulleted list, sponsors and other regulated entities should consider the risks of using such service (e.g., infringement of patient privacy rights, lack of reliability of the data in the clinical investigation and its regulatory implications).

Validation documentation (see sections IV.A.Q1 – and IV.B.Q15)

- *Ability to generate accurate and complete copies of records*
- *Availability and retention of records for FDA inspection for as long as the records are required by applicable regulations*

Question	FDA Answer	Answers or Cross Reference to Section 5
Q1. What should sponsors and other regulated entities consider when using a risk-based approach for validation of electronic systems used in clinical investigations?	• Sponsors and other regulated entities should use a risk-based approach for validating electronic systems owned or managed by sponsors and other regulated entities. • Validation may include, but is not limited to, demonstrating correct installation of the electronic system and testing of the system to ensure that it functions in the manner intended • When using a risk-based approach for validating electronic systems, sponsors and other regulated entities should consider (1) the purpose and significance of the record, including the extent of error that can be tolerated without compromising the reliability and utility of the record for its regulatory purpose and (2) the attributes and intended use of the electronic system used to produce the record.	• The responsibility for validation rests with the customer • See §11.10(a) Q&A

Question	FDA Answer	Answers or Cross Reference to Section 5
Archiving capabilities	• Access controls (see section IV.A.Q4) and authorization checks for users' actions • Secure, computer-generated, time-stamped audit trails of users' actions and changes to data • Encryption of data at rest and in transit • Performance record of the electronic service vendor and the electronic service provided • Ability to monitor the electronic service vendor's compliance with electronic service security and the data integrity controls	• See the answer in 11.10(b), 11.10(e), 11.50, 11.70 and Sub-Part C (11.100 to 11.300) • Data are encrypted in transit from the investigator site and also when stored within CRFWeb • Assessment of the service provider and AWS
Q11. If sponsors and other regulated entities outsource electronic services, who is responsible for meeting the regulatory requirements?	• Sponsors and other regulated entities are responsible for meeting the regulatory requirements. • Moreover, sponsors are responsible for assessing the authenticity and reliability of any data used to support a marketing application for a medical product. • Thus, the sponsor is ultimately responsible for the clinical investigation and for ensuring that all records and data required to adequately perform and document the clinical investigation are obtained and available to FDA upon request and in a timely and reasonable manner	• This is a customer responsibility
Q12. Should sponsors or other regulated entities establish service agreements with the electronic service vendor?	• Yes, sponsors and other regulated entities should obtain service agreements with the electronic service vendor. • Before entering into an agreement, the sponsor or other regulated entity should evaluate and select electronic services based on the electronic service vendor's ability to meet the part 11 requirements and data security safeguards described in the previous bulleted list (see section IV.B). • Service agreements should include a clear description of these specified requirements and the roles and responsibilities of the electronic service vendor	• An agreement between the customer and Clindox is essential for a SaaS service that defines the roles and responsibilities of the two parties. • There is also a structured implementation process to define the client and study set up of CRFWeb including user set-up, study design, workflow definition, reporting requirements and user training.
Q13. Does FDA consider it acceptable for data to be distributed across a cloud computing service's hardware at several different geographic locations at the same time without being able to identify the exact location of the data at any given time?	• If appropriate controls are in place, there are no limitations regarding the geographic location of cloud computing services. • However, it is critical for sponsors and other regulated entities to understand the data flow and know the location of the cloud computing service's hardware in order to conduct a meaningful risk assessment regarding data access, integrity, and security. • Data privacy laws may differ from country to country. Therefore, sponsors and other regulated entities should perform appropriate risk assessments to ensure that data residing on storage devices outside their country can be retrieved and accessed during FDA inspections.	• As noted in 11.10, the location of the service is customer driven. • The client database can be configured to their requirements to ensure that local geographical requirements are met.

Question	FDA Answer	Answers or Cross Reference to Section 5
Q14. What should sponsors and other regulated entities have available on site to demonstrate that their electronic service vendor is providing services in accordance with FDA's regulatory requirements?	• Sponsors and other regulated entities should have the following information available to FDA upon request at each of their regulated facilities that use the outsourced electronic services: o Specified requirements of the outsourced electronic service o A service agreement defining what is expected from the electronic service vendor (see section IV.B.Q12) o Procedures for the electronic service vendor to notify the sponsor or other regulated entity of changes and incidents with the service	• As noted in the adjacent column, there three requirements that customers need to address in conjunction with Clindox.
Q15. What should sponsors and other regulated entities consider when deciding to validate outsourced electronic services that are used in clinical investigations?	• A risk-based approach to validation similar to that described in section IV.A.Q1 should be taken for outsourced electronic services. • It is ultimately the responsibility of the sponsor or other regulated entity to ensure that the outsourced electronic service is validated as appropriate. • Sponsors and other regulated entities should obtain documentation from the electronic service vendor that includes, but is not limited to, a description of standard operating procedures and results of testing and validation to establish that the outsourced electronic service functions in the manner intended.	• As noted in 11.10(a), validation is the responsibility of the customer. • A supplier assessment may be way to leverage the work performed by Clindox to reduce initial validation • Each study is created first in a test environment and then tested to ensure that edit checks, formulae, configurable data, sets, roles and reports work as specified. Then the study is made live.
Q16. Under what circumstances would FDA choose to inspect the electronic service vendor?	• Under certain circumstances, FDA may choose to inspect the electronic service vendors, such as when they are or were engaged in providing services and functions that fall under areas regulated by FDA. • For example, if the criticality of the investigation requires inspection and the required records are not available from the sponsor or the clinical investigation site, FDA may choose to inspect records specific to the clinical investigation at the vendor's facilities to ensure that FDA requirements are met. • The sponsor or other regulated entity is ultimately responsible for ensuring that regulated records and data are available to FDA during an investigation or an inspection.	• Access can be grated either via the site administrator or via the CRFWeb super administrator

6.2 V. Electronic Signatures

An electronic signature is 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 (§ 11.3(b)(7)). In general, a signature may not be denied legal effect or validity solely because it is in electronic format, and a contract or other record relating to a transaction may not be denied legal effect, validity, or enforceability solely because an electronic signature or electronic record was used in its formation.

FDA regulations found in part 11 set forth the criteria under which FDA considers electronic records, electronic signatures, and handwritten signatures executed to electronic records to be trustworthy, reliable, and generally equivalent to a handwritten signature executed on paper (see 21 CFR 11.1(a)). To be considered equivalent to full handwritten signatures, electronic signatures must comply with all applicable requirements under part 11. Electronic records that are electronically signed must contain information associated with the signing that clearly indicates the printed name of the signer, the date and time when the signature was executed, and the meaning associated with the signature (see § 11.50). The name, date and time, and meaning are subject to the same controls as electronic records and must be included as part of any human readable form of the electronic record (see § 11.50(b)). In addition, electronic signatures and handwritten signatures executed to electronic records must be linked to the respective electronic records to ensure that the signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means (§ 11.70).

Question	FDA Answer	Answers or Cross Reference to Section 5
Q24. What methods may be used to create valid electronic signatures?	• FDA does not mandate or specify any particular methods for electronic signatures, including any particular biometric method upon which an electronic signature may be based. • Part 11 regulations permit a wide variety of methods to create electronic signatures, including the use of computer-readable ID cards, biometrics, digital signatures, and username and password combinations • When a document is electronically signed, the electronic signature must be accompanied by a computer-generated, time-stamped audit trail (see §§ 11.10(e) and 11.50(b)). When study participants provide an electronic signature, clinical investigators should ensure that the participants understand the legal significance of the signature.	• Only user identity and password are used in CFRWeb for electronic signatures.

Question	FDA Answer	Answers or Cross Reference to Section 5
Q25.How should sponsors and regulated entities verify the identity of the individual who will be electronically signing records as required in 21 CFR 11.100(b)?	• Electronic signatures should be instituted in a manner that is reasonably likely to prevent fraudulent use. Therefore, the part 11 regulations require that an organization verify the identity of an individual before the organization establishes, assigns, or otherwise sanctions an individual's electronic signature or any element of such electronic signature (see § 11.100(b)). The electronic signature should also be implemented in a manner that prevents repudiation by the signatory and includes safeguards to confirm the identity of the individual and safeguards to prevent alteration of the electronic signature. • FDA does not specify any particular method for verifying the identity of an individual and accepts many different methods. For example, verifying someone's identity can be done by using information from some form of official identification, such as a birth certificate, a government-issued passport, or a driver's license. In addition, use of security questions to confirm an individual's identity may also be considered.	• This is a customer responsibility
Q26. When an individual executes a series of signings during a single, continuous period of controlled system access, could the initial logging into an electronic system using a unique username and password be used to perform the first signing and satisfy the requirements found in 21 CFR 11.200(a)?	• When an individual logs into an electronic system using a username and password, it is not necessary to re-enter the username when an individual executes a series of signings during a single, continuous period of controlled system access. After a user has logged into a system using a unique username and password, all signatures during the period of controlled system access can be performed using the password alone (§ 11.200(a)). • The signed document must contain information that clearly indicates the printed name of the signer, the date and time the signature was executed, and the meaning associated with the signature (see § 11.50). • In addition, in such cases, the signing should be done under controlled conditions that prevent another person from impersonating the legitimate signer. Such controlled conditions may include (1) requiring an individual to remain in close proximity to the workstation throughout the signing session (2) using measures for automatic inactivity disconnect that would de-log the first individual if no entries or actions were taken within a fixed, short time frame and (3) requiring that the single component needed for subsequent signings be known to and usable only by the authorized individual. • To make it impractical to falsify records, the electronic signature component executed for initial signing must be used only by its genuine owner (§ 11.200(a)(2)). The electronic signatures must be administered and executed to ensure that attempted use by anyone other than the genuine owners requires collaboration of two or more individuals (§ 11.200(a)(3)).	• See the answers to 11.200(a) • Two components are used throughout the system for electronically signing electronic records • The author notes that it has only taken the FDA 20 years to clarify this part of the regulation.

Question	FDA Answer	Answers or Cross Reference to Section 5
Q27. What requirements must electronic signatures based on biometrics meet to be considered an accepted biometric method?	• Biometrics means “a method of verifying an individual’s identity based on measurements of the individual’s physical features or repeatable actions where those features and/or actions are both unique to that individual and measurable.”34 Examples of biometric methods may include fingerprints, hand geometry (i.e., finger lengths and palm size), iris patterns, retinal patterns, or voice prints.	• Not applicable to CRFWeb as the system does not have biometric signature capability
Q28. Does FDA certify electronic systems and methods used to obtain electronic signatures?	• No. FDA does not certify individual electronic systems and methods used to obtain electronic signatures. Compliance with the provisions of part 11 is the basis for FDA’s acceptance of any electronic signature system, regardless of the particular technology or brand used. This approach is consistent with FDA’s policy in a variety of program areas. • For example, FDA does not certify manufacturing equipment used to make drugs or medical devices.	• The customer needs to evaluate the e-signature capability of CRF Web to determine if it complies with 21 CFR 11

.

7. EU GMP Annex 11, 2011

7.1 European Union GMP Annex 11 Update

In April 2008, the EU issued a proposed update of Annex 11 on computerised systems used in GMP environments, the update was approximately four times the size of the current version that had been in force since 1992. In the draft there was the ability to use electronic signatures for the first time in EU GMP regulations. There were approximately 1400 comments received by the EU and these were used to revise the draft regulation. The new version of Annex 11 was issued in January 2011 and became effective on 30th June 2011. There are some significant changes in the regulations for computerised systems including the requirement to qualify IT infrastructure.

7.2 Annex 11 and Chapter 4 are Equivalent to Part 11

Taken in combination, the regulations for computerised systems in Annex 11 and the new sections in Chapter 4 on the need to define raw data and new records retention requirements are equivalent to the 21 CFR 11 regulations. However, in this report only Annex 11 will be considered as CRF Web is a GCP application.

7.3 EU GMP Annex 11 Regulations for Computerised Systems

Many of the controls required by the new Annex 11 regulations are the same as those for 21 CFR 11. Therefore, in this section, where there is direct correlation between the Annex 11 and Part 11 controls the assessment will refer to the Part 11 assessment in the previous section of this document.

Ref No.	Annex 11 Requirement and Reference	Control	Responsible	Assessment
	Principle **This annex applies to all forms of computerised systems used as part of a GMP regulated activities. A computerised system is a set of software and hardware components which together fulfil certain functionalities.** • **The application should be validated;** • **IT infrastructure should be qualified.** **Where a computerised system replaces a manual operation, there should be no resultant decrease in product quality, process control or quality assurance.** **There should be no increase in the overall risk of the process.**			
A11/ P/ 01	Has the customer SOPs for computerised system validation?	Proc	Customer	The customer needs to have a procedure for the risk based validation of computer applications.
A11/ P/ 02	Is the customer's IT infrastructure qualified?	Proc	Supplier	AWS infrastructure installation and operation is undertaken through the Master Control list i.e. there is control of physical and virtual components

Ref No.	**Annex 11 Requirement and Reference**	Control	Responsible	Assessment
	1. Risk Management **Risk management should be applied throughout the lifecycle of the computerised system taking into account patient safety, data integrity and product quality. As part of a risk management system, decisions on the extent of validation and data integrity controls should be based on a justified and documented risk assessment of the computerised system.**			
A11/ 1/ 01	Has the supplier used risk management during the software development process for the application?	Proc	Supplier	Studies are first created as tests; where all edit checks, formulas and configurations are checked by us and the customer, they then sign off before it is copied to the live environment.
A11/ 1/ 02	Is risk management incorporated in the computer validation SOP and associated procedures?	Proc	Customer	Customers should also incorporate risk management throughout their computer validation procedures: e.g. system level risk assessment to determine if validation is required, risk assessment at the requirements level, risk assessment during change control, etc.
A11/ 1/ 03	Risk can also be managed by selecting commercial products rather than developing custom or bespoke software to automate a process.	Proc	Customer	Customers should select software that is in GAMP Categories 3 and 4 rather than develop custom solutions to minimise the impact of the system on data integrity, patient safety or product quality.

Ref No.	Annex 11 Requirement and Reference	Control	Responsible	Assessment
	2. Personnel **There should be close cooperation between all relevant personnel such as Process Owner, System Owner, Qualified Persons and IT. All personnel should have appropriate qualifications, level of access and defined responsibilities to carry out their assigned duties**			
A11/ 2/ 01	Have the supplier's development staff been trained in GXP awareness?	Proc	Supplier	Key staff involved in the development of software intended for GCP use have the appropriate combination of education, training and experience.
A11/ 2/ 02	Has the customer established processes for co-operation?	Proc	Customer	Co-operation needs to be established by senior management expectation and procedures within each customer.
A11/ 2/ 03	Are training records available to demonstrate the appropriate levels of education training and experience to perform assigned tasks?	Proc	Customer	Training records should demonstrate the appropriate level of education, training and experience to perform assigned tasks versus a position description.
	3. Suppliers and Service Providers **3.1 When third parties (e.g. suppliers, service providers) are used e.g. to provide, install, configure, integrate, validate, maintain (e.g. via remote access), modify or retain a computerised system or related service or for data processing, formal agreements must exist between the manufacturer and any third parties, and these agreements should include clear statements of the responsibilities of the third party.** **IT-departments should be considered analogous**.			
A11 / 3 / 01	Has the customer established an agreement with their IT supplier for services and support?	Proc	Customer	A customer needs to establish through a contract or service level agreement for the computing services from a supplier
A11 / 3 / 02	Are agreements in place to cover services supplied by Clindox to the customer?	Proc	Customer & Supplier	Agreements between Clindox and a customer need to outline the services provided and the responsibilities of both parties.
	3.2 The competence and reliability of a supplier are key factors when selecting a product or service provider. The need for an audit should be based on a risk assessment			
A11/ 3/ 04	Each customer needs a risk-based procedure for determining if a supplier audit is required or not	Proc	Customer	The customer's system risk assessment of Clindox should determine the need for an audit or not.

Ref No.	Annex 11 Requirement and Reference	Control	Responsible	Assessment
A11/ 3/ 05	Does the supplier have a quality management system?	Proc	Supplier	Clindox has a QMS for software development.
	3.3 Documentation supplied with commercial off-the-shelf products should be reviewed by regulated users to check that user requirements are fulfilled			
A11/ 3 / 06	Does the customer have a procedure to review supplier documentation?	Proc	Customer	Documentation provided by Clindox should to be reviewed to assess if any requirements have been fulfilled, this needs to be documented e.g. traceability (using Jira) or release report.
	3.4 Quality system and audit information relating to suppliers or developers of software and implemented systems should be made available to inspectors on request.			
A11/ 3 / 07	In the customer's regulatory inspection SOP is there facility to allow inspectors to read supplier audit reports?	Proc	Customer	Customers need to ensure that Clindox knows that audit /assessment reports can be read by inspectors and that any non-disclosure agreements signed need to include this contingency.
	4. Validation **4.1 The validation documentation and reports should cover the relevant steps of the life cycle. Manufacturers should be able to justify their standards, protocols, acceptance criteria, procedures and records based on their risk assessment**			
A11/ 4/ 01	Is there a risk-based computerised system validation SOP available?	Proc	Customer	Each customer needs to have a risk-based computer validation procedure that is flexible and fits the work done to the overall risk posed by the system and the data it contains.

Ref No.	Annex 11 Requirement and Reference	Control	Responsible	Assessment
	4.2 Validation documentation should include change control records (if applicable) and reports on any deviations observed during the validation process			
A11/ 4/ 02	Is there a means of recording changes to validation documents?	Proc	Customer	This should be part of a customer’s validation and document control procedures.
A11/ 4/ 03	Is there a means of documenting deviations observed during the validation?	Proc	Customer	This should be part of a customer’s validation procedures.
	4.3 An up to date listing of all relevant systems and their GMP functionality (inventory) should be available.			
A11/ 4/ 04	Is there an inventory of all GMP and Non-GMP systems (including spreadsheets) for the laboratory?	Proc	Customer	The system level risk assessment should be linked with the computerised system inventory to list all systems including System as well as spreadsheets. The inventory can either be a separate document or part of a Validation Master Plan for computerised systems. It is important to keep the inventory current and include all new systems added, upgraded or retired. An electronic system is probably the most effective way of achieving this.
	4.3 For critical systems an up to date system description detailing the physical and logical arrangements, data flows and interfaces with other systems or processes, any hardware and software pre-requisites, and security measures should be available.			
A11/ 4/ 05	Does the customer have a risk assessment process that categorises systems according to risk?	Proc	Customer	Risk management must be applied throughout the computer life cycle as per Annex 11 clause 1. Categories of system risk are important as they define the amount of validation that needs to be performed on each type and extent of the controls that need to be applied to each system.

Ref No.	Annex 11 Requirement and Reference	Control	Responsible	Assessment
A11/ 4/ 06	Is there a procedure for writing a system description for critical systems only?	Proc	Customer	Only critical systems need a system description that needs to be kept current. The customer's risk assessment methodology should determine if System is a critical system or, if interfaced to another system, a component of a critical system. Some required information for a system description listed in Annex 11 may be found in other documents so the system description should cross-reference these documents rather than repeat the same information.
	4.4 User Requirements Specifications should describe the required functions of the computerised system and be based on documented risk assessment and GMP impact			
A11/ 4/ 07	Does a URS exist that covers the functions that the system must perform (intended use)?	Proc	Customer	A user requirements specification is essential to define the intended use of the computerised system. A computerised system cannot be validated without a current URS (see FDA Guidance for Industry entitled General Principles of Software Validation, section 5.2).
A11/ 4/ 08	Are user requirements traceable throughout the life-cycle?	Proc	Customer	Requirements need to be traceable to the place in the life cycle where they are verified or tested. Therefore, they should be uniquely numbered to enable effective traceability.
	4.5 The regulated user should take all reasonable steps, to ensure that the system has been developed in accordance with an appropriate quality management system. The supplier should be assessed appropriately.			
A11/ 4/ 09	Does the computer validation SOP have provision for risk based assessment to determine if a supplier should be audited or not?	Proc	Customer	This links with clause 3.3. The need to audit a supplier and obtain information about the quality system and product development should be based on a risk assessment.
A11/ 4/ 10	There should be a specific assessment to determine if Clindox should be audited, a remote questionnaire sent or no action required	Proc	Customer	This requirement links with clause 3.3. The need to audit a supplier and how to obtain quality system and application development information should be based on a risk assessment. This should be documented in the validation of System.

Ref No.	Annex 11 Requirement and Reference	Control	Responsible	Assessment
	4.6 For the validation of bespoke or customised computerised systems there should be a process in place that ensures the formal assessment and reporting of quality and performance measures for all the life-cycle stages of the system			
A11/ 4/ 11	Is there any bespoke software in the application?	N/A	N/A	This clause is not applicable to system as it is a commercial product and there is no bespoke software supplied for the application.
A11/ 4/ 12	How is bespoke software managed?	N/A	N/A	CRF Web is a commercially available configurable product and there is no bespoke or custom software in the application.
	4.7 Evidence of appropriate test methods and test scenarios should be demonstrated. Particularly, system (process) parameter limits, data limits and error handling should be considered. **Automated testing tools and test environments should have documented assessments for their adequacy.**			
A11/ 4/ 13	How are test methods and test scenarios managed?	Proc	Customer	There needs to be a test plan for the user acceptance testing (UAT) or performance qualification (PQ) phase of the system life cycle that manages the overall test scenarios for System validation.
A11/ 4/ 14	How are validation test scenarios linked to the user requirements?	Proc	Customer	Testing scenarios need to be based on the user requirements specification and linked via a traceability matrix. The testing needs to be based on the way the system is used as defined in the URS.
A11/ 4/ 15	How are test cases designed?	Proc	Customer	Test cases should be designed to include testing to pass as well as testing to fail. In addition, testing should include stress testing of limits and error handling especially at critical points of an analysis e.g. where a result is in specification or out of specification.
A11/ 4/ 16	How is testing evidenced?	Proc	Customer	Test evidence can be based on a combination of paper printouts, screen shots, and electronic records within the application such as test reports and audit trail entries.
A11/ 4/ 17	How will automated test tools be assessed for their adequacy?	Proc	Customer	If automated test tools are used in a validation they need to be qualified to demonstrate that they are fit for purpose. Note that it is unlikely that automated testing will be used by a customer to validate System software.

Ref No.	Annex 11 Requirement and Reference	Control	Responsible	Assessment
	4.8 If data are transferred to another data format or system, validation should include checks that data are not altered in value and/or meaning during this migration process			
A11/ 4/ 18	Is this a new installation of the application?	N/A	N/A	This clause would not apply for a new installation of System.
A11/ 4/ 19	What happens if this is a new version of System is being implemented?	Tech	Supplier	If the installation is an upgrade to a new version of System, Clindox will provide software utilities for the migration of data.
A11/ 4/ 20	How will the migration be validated?	Proc	Customer	The customer needs to ensure that the original database is backed up and then migrate the data to the new data base using the software utilities provided. Checks to ensure the completeness and accuracy of the data migration need to be carried out.
	5. Data **Computerised systems exchanging data electronically with other systems should include appropriate built-in checks for the correct and secure entry and processing of data, in order to minimize the risks**			
A11/ 5/ 01	What controls and checks are there for data acquired from instruments connected to System?	Tech	Supplier	System identifies that the individual instrument selected for an analysis is the correct one for the method.
A11/ 5/ 02	How are data acquired from instruments checked for accuracy?	Tech Proc Proc	Supplier Supplier Customer	Development of the system ensures that data are generated at the instrument and then transferred correctly to the System system. Qualification by Clindox-Toledo ensures that the instrument and System software are correctly installed and communicate together at a system level in a customer’s laboratory. Validation of the installation to demonstrate that the instrument and System work under actual conditions of use is required including capacity testing, if appropriate.

Ref No.	Annex 11 Requirement and Reference	Control	Responsible	Assessment
A11/ 5/ 03	If System is interfaced to another software package, what controls are there to ensure that data are correctly transferred?	Tech Proc Proc	Supplier Supplier Customer	A similar approach to that in assessment A11/ 5/ 02 above is required for application to application communication.. Testing of the interface capacity (i.e. stress test) and error handling between the two applications may be appropriate.
	6. Accuracy Checks **For critical data entered manually, there should be an additional check on the accuracy of the data. This check may be done by a second operator or by validated electronic means. The criticality and the potential consequences of erroneous or incorrectly entered data to a system should be covered by risk management**			
A11/ 6/ 01	What checks are there on the accuracy of data entered manually into the system?	Proc	Customer	Risk assessment should be carried out by the customer to determine the extent of accuracy checks needed for System.

Ref No.	Annex 11 Requirement and Reference	Control	Responsible	Assessment
	7. Data Storage **7.1 Data should be secured by both physical and electronic means against damage. Stored data should be checked for accessibility, readability and accuracy. Access to data should be ensured throughout the retention period**			
A11/ 7/ 01	How is physical access to the computer room and communication cabinets controlled?	Proc	Supplier	AWS do not allow access by non-AWS personnel to their hosting sites.
A11/ 7/ 02	How is access controlled to data stored on the System server?	Proc	Customer	User account management needs to be implemented so that only authorised individuals can access the system.
A11/ 7/ 03	How are stored data checked for accessibility, readability and accuracy?	Proc	Customer	A risk based determination needs to be made to determine the frequency of and extent of checks to be made to ensure that data are readable and have not changed.
	7.2 Regular back-ups of all relevant data should be done. Integrity and accuracy of backup data and the ability to restore the data should be checked during validation and monitored periodically.			
A11/ 7/ 04	Has the backup software application been qualified as part of the infrastructure qualification?	Proc	Supplier	AWS have controlled process for installation and integration of equipment and software into environment.
A11/ 7/ 05	Is there a backup SOP?	Proc	Supplier	There is a backup and recovery SOP that defines the backup and records that show backup has been done.
A11/ 7/ 06	Has the backup and restore of the System data base been validated?	Proc	Supplier / Customer	Backup and restore needs to be validated before System is released for use in an operational environment.
A11/ 7/ 07	Is there a procedure for checking that backups can be periodically restored?	Proc	Customer	Periodic checks that data can be restored from backup media need to take place and be documented.

Ref No.	Annex 11 Requirement and Reference	Control	Responsible	Assessment
	8. Printouts 8.1 It should be possible to obtain clear printed copies of electronically stored data.			
A11/ 8/ 01	Can electronic records within the system be printed out?	Proc	Customer	See the answer under 21 CFR 11.10(b).
	8.2 For records supporting batch release it should be possible to generate printouts indicating if any of the data has been changed since the original entry			
A11/ 8/ 02	Are printouts available to demonstrate if data used for batch release in System have been changed since the original entry?	Tech	Supplier	The audit trail will indicate those records that are changed.
A11/ 8/ 03	If System is involved in generating data for batch release, has this feature been validated?	N/A	N/A	Not applicable as CFRweb is a GCP application.

Ref No.	Annex 11 Requirement and Reference	Control	Responsible	Assessment
	9. Audit Trails **Consideration should be given, based on a risk assessment, to building into the system the creation of a record of all GMP-relevant changes and deletions (a system generated "audit trail").** **For change or deletion of GMP-relevant data the reason should be documented.** **Audit trails need to be available and convertible to a generally intelligible form** **and regularly reviewed**			
A11/ 9/ 01	Is an audit trail needed with System?	Tech	Supplier	Audit trails are an integral part of the system
A11/ 9/ 02	Is there an audit trail in System?	Tech	Supplier	Yes, System has an effective and secure audit trail to meet GXP requirements. See also the detailed comments in the Part 11 section under §11.10(e).
A11/ 9/ 03	Is there a field for a user to add a reason when data are changed?	Tech	Supplier	Yes, there is a field for a user to add the reason for change.
A11/ 9/ 04	Is the audit trail searchable and can the searches be printed?	Tech	Supplier	System has the ability for users to search the audit trail and the output can be printed or converted to a PDF file if required.
A11/ 9/ 05	Is there a means of showing that the audit trail has been reviewed?	Tech Proc	Supplier Customer	Currently the audit trail does not have a report function indicating that a supervisor has reviewed the audit trail that is stored within the system. A procedure is needed for reviewing the System audit trail, the frequency of this review and how to document the review is required.

Ref No.	Annex 11 Requirement and Reference	Control	Responsible	Assessment
	10. Change and Configuration Management **Any changes to a computerised system including system configurations should only be made in a controlled manner in accordance with a defined procedure**			
A11/ 10/ 01	Is there a change control SOP for computerised systems?	Proc	Customer	Change control is a customer procedure that needs to incorporate risk assessment to determine the level of revalidation required.
A11/ 10/ 02	Does the change control SOP cover configuration management?	Proc	Customer	The configuration of a computerised system is an input to the change process to help determine the extent and impact of a change. At the end of a change, the system configuration should be updated to reflect the change.
A11/ 10/ 03	How can the release notes from Clindox help with the change control process for system?	Proc	Supplier	Release notes from a supplier are an input into the change management process to help determine the impact and risk of a change and how much revalidation is required.
	11. Periodic Evaluation **Computerised systems should be periodically evaluated to confirm that they remain in a valid state and are compliant with GMP. Such evaluations should include, where appropriate, the current range of functionality, deviation records, incidents, problems, upgrade history, performance, reliability, security and validation status reports.**			
A11/ 11/ 01	Is there a process for identifying high, medium and low risk systems?	Proc	Customer	The risk posed by a computerised system determines the frequency of periodic review.
A11/ 11/ 02	Is there a formal schedule for periodic review of all computerised systems	Proc	Customer	There should be a time table for periodic review of computerised systems within a laboratory where each system is identified with the date of next review.
A11/ 11/ 03	Is there a procedure for periodic reviews?	Proc	Customer	This is an independent and formal audit of all regulated computerised systems on a defined schedule.

Ref No.	Annex 11 Requirement and Reference	Control	Responsible	Assessment
	12. Security **12.1 Physical and/or logical controls should be in place to restrict access to computerised system to authorised persons. Suitable methods of preventing unauthorised entry to the system may include the use of keys, pass cards, personal codes with passwords, biometrics, restricted access to computer equipment and data storage areas.**			
A11/ 12/ 01	How is access to the system controlled?	Tech	Supplier	Initial access is via user identity, password and captcha. The user identity is linked to further access control mechanisms that define user groups and user types each with configurable access privileges.
A11/ 12/ 02	How is access to System controlled?	Proc	Customer	User account management is required to only allow access to a computerised system to authorised individuals.
	12.2 The extent of security controls depends on the criticality of the computerised system.			
A11/ 12/ 03	How is the criticality of security controls determined?	Proc	Customer	A risk assessment will determine the extent of the controls to be deployed: physical, logical or procedural. The controls available in System are technical but need to be configured and implemented by the customer; see also the answers to questions A11/ 12/ 01 and A11/ 12/ 02 above.
	12.3 Creation, change, and cancellation of access authorisations should be recorded			
A11/ 12/ 04	How are user accounts created, changed and disabled?	Tech Proc Proc	Supplier Customer Customer	The software creates unique user identities within the database. A second account with the same name cannot be created. User account management should be authorised by the process owner and executed by an administrator. Records of current and historical users will need to be maintained similar to Part 11 earlier in this document.

Ref No.	Annex 11 Requirement and Reference	Control	Responsible	Assessment
	12.4 Management systems for data and for documents should be designed to record the identity of operators entering, changing, confirming or deleting data including date and time			
A11/ 12/ 05	How are the identities of users working on the system captured by the system?	Tech Tech Proc	Supplier Supplier Customer	All actions of individual users are identified in the audit trail and in the records of each analysis. Please see further comments under 21 CFR 11 and clause 9 of Annex 11. Time and date stamps in the system are linked to the server time. Customers should ensure that user identities or accounts are not shared between two or more users.
	13. Incident Management **All incidents, not only system failures and data errors, should be reported and assessed. The root cause of a critical incident should be identified and should form the basis of corrective and preventive actions**			
A11/ 13/ 01	How are incidents with computerised systems handled?	Proc	Customer	A procedure is required to record all incidents that have occurred with a computerised system, then to classify and analyse each one. A CAPA is required to for critical incidents to resolve the issue and prevent it occurring again.

Ref No.	Annex 11 Requirement and Reference	Control	Responsible	Assessment
	14. Electronic Signature **Electronic records may be signed electronically. Electronic signatures are expected to:** **a. have the same impact as hand-written signatures within the boundaries of the company,** **b. be permanently linked to their respective record,** **c. include the time and date that they were applied**			
A11/ 14/ 01	How are electronic signatures implemented in System?	Tech	Supplier	System has the technical controls to apply electronic signatures (via user identity and password) to electronic records as discussed in the sections on 21 CFR 11 earlier in this document. Reasons for signing are configurable and should be documented in the validation documentation.
A11/ 14/ 02	How are users trained to use electronic signatures?	Proc	Customer	Customers need procedural controls and training to use electronic signatures correctly and effectively as discussed in the section on 21 CFR 11.
	15. Batch Release **When a computerised system is used for recording certification and batch release, the system should allow only Qualified Persons to certify the release of the batches and it should clearly identify and record the person**			
A11/ 15/ 01	If a computerised system is used for batch release, how does it restrict the process to Qualified Persons only?	N/A	N/A	This requirement is not applicable as System does not provide the functionality for certification and release of batches by a Qualified Person.

Ref No.	Annex 11 Requirement and Reference	Control	Responsible	Assessment
	16. Business Continuity **For the availability of computerised systems supporting critical processes, provisions should be made to ensure continuity of support for those processes in the event of a system breakdown (e.g. a manual or alternative system). The time required to bring the alternative arrangements into use should be based on risk and appropriate for a particular system and the business process it supports. These arrangements should be adequately documented and tested**.			
A11/ 16/ 01	Is there a business continuity plan that has been tested	Proc Proc	Supplier Customer	AWS can provide failover locations to run a duplicate copy of the system if required. Recovery is dependent on an effective system of backup, therefore the latest backup needs to be available and accessible.
A11/ 16/ 02	Is the business continuity plan kept up to date?	Proc	Customer	This plan needs to be revised regularly to keep pace with technical developments and the revision tested to demonstrate that it works.
	17. Archiving **Data may be archived. This data should be checked for accessibility, readability and integrity. If relevant changes are to be made to the system (e.g. computer equipment or programs), then the ability to retrieve the data should be ensured and tested.**			
A11/ 17/ 01	Is there an archiving procedure in place?	Proc	Customer	Archiving is a customer driven process that is performed periodically that needs to be controlled by a procedure.
A11/ 17/ 02	Does the system provide the ability to archive data?	Tech	Supplier	Data from a completed study data can be extracted in .xls, Cdisc ODM .xml, Cdisc SDTP or SAS.xpt Studies data can be retrieved by the customer and a read only access provided.

8. Outline Biography of R.D.McDowall

- 15 years in the pharmaceutical industry with Smith Kline and French and Wellcome Research Laboratories plus six years in forensic toxicology

- Principal of McDowall Consulting (1993 – 2014) specialising in LIMS, chromatography data systems, computer validation, corporate validation and Part 11 policies, electronic signatures and electronic records, process redesign, laboratory automation strategies and projects. Twenty four years consulting experience and thirty years computer validation experience.

- Director of R.D.McDowall Limited (1998 – date) specialising in corporate computer validation and Part 11 policies, analytical equipment qualification and validation of GMP, GLP and GCP computerised systems

- Advisor to the Pharmaceutical Industry Group of PricewaterhouseCoopers and Coopers&Lybrand 1993 – 2015

- PhD degree from University of London, Chartered Scientist, Chartered Chemist and Fellow of the Royal Society of Chemistry

- Co-chair of a session the FDA and AAPS meeting on Validation of Bioanalytical Methods held in Crystal City, December 1990 and co-author of the published proceedings in 1992

- ISO 17025 (UKAS) assessor for chromatography and computer validation 1994 - 2000.

- Visiting Senior Fellow, Department of Chemistry, University of Surrey 1991-2001.

- Internationally recognised expert in validation of analytical methods, LIMS, laboratory automation, validation of computerised systems and 21 CFR 11

- Member of the Editorial Boards of LC-GC North America, LC-GC Europe, Spectroscopy, Quality Assurance Journal (2001 – 2011) and Journal of the Association of Laboratory Automation (2004 – 2009)

- Editor of Laboratory Information Management and Laboratory Automation and Information Management 1991-1998,

- Editor of the Pharma IT Journal 2006 – 2008.

- Published over 340 papers and book chapters, given over 900 presentations and workshops at symposia and meetings.

- Writer of the Questions of Quality column in LC-GC International and LC-GC magazines since 1993 and the Focus on Quality column in Spectroscopy since 1999

- Writer of the Validation and Verification Column and member of the Editorial Board of Scientific Data Management 1997 – 1999

- Author of Validation of Chromatography Data Systems published by the Royal Society of Chemistry, February 2005 and the second edition published in 2017

- Presenter at many training courses on regulatory compliance including the new EU GMP Annex 11 and Chapter 4

- Presented with the 1997 LIMS Award for contributions and advancement to the subject and teaching
- Long service teaching awards from the Association of Laboratory Automation and the Society for Laboratory Automation and Screening
- Co-author of a stimulus to the revision process for USP <1058> on Analytical Instrument Qualification published in Pharmacopoeial Forum January – February 2012 Co-author of the redrafted version of USP <1058> submitted to the USP Council of Experts in August 2013. The new version of <1058> is effective from 1st August 2017.
- Contributor to the GAMP Good Practice Guide on IT Infrastructure Compliance and Control, 2005
- Contributor to second edition of the GAMP Good Practice Guide for Risk-Based Approach to GXP Compliant Laboratory Computerized Systems published October 2012.
- Core member of the GAMP Special Interest Group on Data Integrity 2014 – date
- Subject Matter Expert Input and Review of the GAMP Guide on Records and Data Integrity, ISPE, April 2017.