association for **clinical data management**

FDA 21 CFR Part 11 Subpart B Electronic Records Requirements & Annex 11 Computerised Systems – Suggested Implementation

Regulatory Considerations DMEG

May 2021

www.acdmglobal.org

FDA 21 CFR Part 11 Subpart B Electronic Records Requirements & Annex 11 Computerised Systems – Suggested Implementation

Disclaimer

The information presented in this paper is provided as an aid to understanding the environment for electronic clinical research. The opinions of the author(s), and the ACDM do not necessarily reflect the position of individual companies. Readers should assess the content and opinions in the light of their own knowledge, needs and experience as well as interpretation of relevant guidance and regulations.

Scope

The following paper provides a summary of the regulatory requirements from the FDA, 21 CFR Part 11 and the Eudralex Volume 4 Annex 11 (also commonly named Electronic Records & Electronic Signatures or ER/ES) and provides you with some recommendation and/or direction that you should take into account when implementing a Computerised System with the intent to comply with these regulations.

Overview

Code of Federal Regulation (CFR) 21 Part 11 represents the FDA's current position of the security and management of electronic records that are created, modified, maintained, archived, retrieved, or transmitted and the electronic signatures executed upon the electronic records for clinical and research purposes.

Eudralex The Rules Governing Medicinal Products in The European Union, Volume 4, Good Manufacturing Practice, Medicinal Products for Human and Veterinary Use, Annex 11: Computerised Systems represents the European Commission's current position on the same. When complying with CFR 21 Part 11 and Annex 11 it is suggested that one also follows GxP.

What is GxP?

GxP is a set of regulations and quality guidelines formulated to ensure the safety of life sciences products while maintaining the quality of processes throughout every stage of manufacturing, control, storage, and distribution. The GxP standards were established by the Food and Drug Administration for a range of compliance related activities and are recognized as:

G: Stands for good
x: Variable
P: Stands for practices

The variable "x" depends on the application of the standards. The value of x can be M for "Manufacturing", C for "Clinical", L for "Laboratory", S for "Storage", D for "Distribution", R for "Review", etc. The purpose of the guidelines is to ensure that the regulated organizations comply with the standard processes of various functions. GxPs are mostly similar across all the countries.

The guidelines mainly focus on the following areas:

- Traceability – ensuring that the development history of the product can be reverse engineered.
- Accountability – Identifying the contribution of every individual involved in the development process.
- Data Integrity – Ensuring the reliability of data.

Why is GxP important?

Since the regulations of GxP are global, every company manufacturing life sciences product is affected by it. Therefore, meeting the GxP requirements is highly important. Though there are several GxPs, few of them are highly important for the life cycle of any product.

- Good Manufacturing Practices (GMP) – GMP are the guidelines recommended by agencies for the authorization and control of manufacturing of products such as drugs, medical devices, active pharmaceutical ingredients (APIs) etc. Adhering to these guidelines assure the agencies about the quality of the products and that the manufacturers have taken every possible measure to ensure the safety of the product.

- Good Clinical Practices (GCP) – GCP are international quality standards defined by the International Conference on Harmonization (ICH) that state the clinical trial regulations for the products that require testing on human subjects. The standards outline the requirements of a clinical trial and the roles and responsibilities of the officials involved in it. It ensures that no human experiments are performed just for the sake of medical advancement.

- Good Laboratory Practices (GLP) – These are the standards set by the FDA for non-clinical laboratory tests and studies conducted for assessing the safety and efficacy of the product. GLPs are a set of standards which define the framework for a non-clinical study and states how they should be performed, evaluated, reported etc.

- To place a product in any market, it is necessary for a company comply with the GxP regulations as well as CFR 21 Part 11 and EU Annex 11.

Below are purely suggestions as to how one might proceed after looking at both regulations CFR 21. Part 11 and EU Annex 11.

FDA 21 CFR Part 11 section	Review of CFR 21.11	Review of EU Annex 11	Possible Documentation Implementation
11.10(a)	• Validate Closed System functionality and operations.	**4.1** – 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.	• Computer Software Validation (CSV) Policies/SOPs to define validation procedures and methodologies (system and project) • Documentation that records validation throughout system and project life-cycle • Includes Supplier's audit for making sure software layer is covered • It might also include "infrastructure" layer as well if separate layer/contracted or handled by someone else.
	Not present in CFR 21 Part 11 N/A **N.B. Even though EU Annex 11 refers to GMP in the guidance documents, the scope of Annex 11 applies to GMP and GxP (GMP/GxP).**	4.2 – Validation documentation should include change control records (if applicable) and reports on any deviations observed during the validation process. 4.3 – An up to date listing of all relevant systems and their GMP/GxP functionality (inventory) should be available. 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. **4.4** – User Requirements Specifications should describe the required functions of the system, be based on documented risk assessment and GMP/GxP impact, and	

FDA 21 CFR Part 11 section	Review of CFR 21.11	Review of EU Annex 11	Possible Documentation Implementation
		be traceable throughout the life cycle. **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. **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. **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. **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	

FDA 21 CFR Part 11 section	Review of CFR 21.11	Review of EU Annex 11	Possible Documentation Implementation
		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. 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. 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.	
11.10(b)	• Validate system functionality to create and export record copies in human and machine readability formats	• 8.1 – It should be possible to obtain clear printed copies of electronically stored data.	Documentation to support validation of Report/Export functionality and output (CSV, SAS, PDF) ***N.B.*** *In specific cases Policies/SOP might be needed as well, e.g. for eCRF or eTMF when export process is being used at project end for "certified copy" aspect.*

FDA 21 CFR Part 11 section	Review of CFR 21.11	Review of EU Annex 11	Possible Documentation Implementation
11.10(c)	• Record "locking" procedures • *Control of user access (see 1d)* • Defined retention periods • Back-up/Recovery processes • Long-term safe storage of records • Record integrity after system upgrades • Record integrity in lieu of system security	**7.1** – Data should be secured by both physical and electronic means against damage. Access to data should be ensured throughout the retention period. **7.2** – Regular back-ups of all relevant data should be done. **8.1** – It should be possible to obtain clear printed copies of electronically stored data. **12.1** – Physical and/or logical controls should be in place to restrict access to computerized systems to authorized persons.	• CSV Policies/SOPs to define all listed procedures • Documentation showing validation history of: ○ user access/management ○ record locking ○ retention periods ○ back-up documentation ○ recovery documentation ○ long-term security testing ***N.B.*** *Caution, backup and archive might be different. As per ITIL and other standards it must be different. https://en.wikipedia.org/wiki/ITIL*
11.10(d)	• Validate system user access functionality • Management of users (access granted, maintained, reviewed, revoked) at sponsor and project level, including sponsor administrators • Institution level training and use of security and authentication procedures ***N.B.*** *"periodic review" of user accesses is extremely important as well from a data integrity perspective* ***N.B.*** *See 11.10 1g for functional level*	**2** – All personnel should have appropriate qualifications, level of access and defined responsibilities to carry out their assigned duties. **12.1** – Physical and/or logical controls should be in place to restrict access to computerized systems to authorized persons. Suitable methods of preventing unauthorized 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.	• CSV Policies/SOPs to define: ○ user management and controls (sponsor and project) ○ password/authentication processes & management • Documentation showing validation history of: ○ User Access Validation including general user access ○ User access requests and management ○ Reviews of User Access

FDA 21 CFR Part 11 section	Review of CFR 21.11	Review of EU Annex 11	Possible Documentation Implementation
		12.3 – Creation, change, and cancellation of access authorizations should be recorded.	

11.10(e)	• Validate traceability trail functionality and ability to meet specific requirements for all record changes (e.g. automatic, cannot be changed, or soft or hard deleted)
	• Traceability trail can be viewed in human readable form and will remain operational throughout archive period
	
	N.B. *Hard deletion. Some systems do offer to perform a "soft delete" or "logical delete", which means, the data remains somehow to the database for ever, nevertheless not "front end" visible anymore by majority of users (other than administrator).*
		8.1 – It should be possible to obtain clear printed copies of electronically stored data.
		7.1 – Access to data should be ensured throughout the retention period.
		9 – Consideration should be given, based on a risk assessment, to building into the system the creation of a record of all GMP/GxP relevant changes and deletions (a system generated "audit trail"). For change or deletion of GMP/GxP relevant data the reason should be documented. Audit trails need to be available and convertible to a generally intelligible form and regularly reviewed.
		12.4 – Management systems for data and for documents should be designed to record the identity of operators entering, changing, confirming or deleted data including date and time.
			• CSV Policies to define traceability trail requirements (functional and long-term)
			• Documentation showing validation history of:
			  ○ traceability trail validation
			  ○ traceability trail security (long-term)
			  ○ traceability of user credentials

FDA 21 CFR Part 11 section	Review of CFR 21.11	Review of EU Annex 11	Possible Documentation Implementation
11.10(f)	• System requires users to log in before they can use system functionality	**N/A** (no direct Annex 11 counterpart).	• Documentation showing validation whereby users are forced to login before using system functionality

11.10(g)	• Validate system user access in terms of functionality restriction
	• Management of user access at functional level (e.g. use of Data Access Groups to restrict site access, and use of targeted functionality restrictions offered by system)
	• Users must be trained to use the functionality to which they have been granted access
		2 – All personnel should have appropriate qualifications, level of access and defined responsibilities to carry out their assigned duties.
		12.1 – Physical and/or logical controls should be in place to restrict access to computerized systems to authorized persons. Suitable methods of preventing unauthorized 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.
			• CSV Policies/SOPs to define:
			  ○ user management (at functional level)
			• Documentation showing validation history of:
			  ○ User Access Validation including general user access and functionality restrictions
			  ○ User access requests and management
			  ○ Reviews of User Access
			  ○ Training to use functionality

11.10(h)	• Validate equipment used to collect information for regulatory submission, ensure integrity of data source, and ensure adequate instructions and staff training	**6** – 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.	• CSV Policies/SOPs to define validation and use of equipment used to collect data for regulatory submission
			• Documentation showing validation history of:
			  ○ Validation of equipment (initial and ongoing)
			  ○ Instructions for use of equipment
			  ○ Training of equipment users
			  ○ Integrity of transfer of data from source (equipment) to system/final repository
			
			N.B. *Integrity of data transfer from source to system is very important and must be part of CSV from a "data life cycle perspective"*

FDA 21 CFR Part 11 section	Review of CFR 21.11	Review of EU Annex 11	Possible Documentation Implementation
			N.B. *Depends how you articulate your CSV SOP. Any equipment/device can be defined to a system's scope by it's nature. This also depends how you split layers: infrastructure/software/system layers to prevent redundancy*

11.10(i)	• Maintain records of CV/ experience/ training for all staff working at sponsor level and on individual projects (at sites) developing, maintaining, or using system	**2** – All personnel should have appropriate qualifications, level of access and defined responsibilities to carry out their assigned duties.	• CSV Policies/SOPs to define maintenance of "Employee Portfolio"
			• Documentation showing records (sponsor and project/site) of:
			  ○ CV
			  ○ Experience
			  ○ Training

11.10(j)	• Maintain system to record training in security good practice to ensure all staff are trained and aware of responsibilities relating to their conduct and accountability using systems with electronic records using electronic signatures (including falsification of records and signatures)	**N/A** (no direct Annex 11 counterpart).	• CSV Policies/SOPs to define requirements and training in responsibilities for staff using electronic signatures, including how they will be held accountable for the integrity of their actions
			• Documentation showing history of:
			  ○ Training
			  ○ Monitoring/traceability of user activities

11.10(k)	• Maintain system operations documentation which includes controls for distribution and use
	• Implement version and change control procedures to create a traceability trail
		N/A (no direct Annex 11 counterpart to 21 CFR 11.10(k)(1)).
		10 – Any changes to a computerized system including system configuration should only be made in a controlled manner in accordance with a defined procedure.
			• CSV Policies/SOPs to define how systems documentation will be managed, including change control procedures
			• Documentation showing history of:
			  ○ Version-controlled system documents
			  ○ Distribution/Use if applicable

FDA 21 CFR Part 11 section	Review of CFR 21.11	Review of EU Annex 11	Possible Documentation Implementation
11.30	• Validate Open System functionality and operations	**5** – Computerized 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. **7.1** – Data should be secured by both physical and electronic means against damage. **7.2** – Regular back-ups of all relevant data should be done. **12.1** – Physical and/or logical controls should be in place to restrict access to computerized systems to authorized persons.	• CSV Policies/SOPs to define how system will be used as an Open System (e.g. use of surveys) • Documentation showing records of how Open systems/surveys are managed ***N.B.*** *If "open" that only some CSV aspects will enforce security aspects e.g. robust encryption for data transfers, https for sure, perhaps penetration testing as well etc.*
11.50(a)	• The record associated with an electronic signature must show: ○ the printed name of the signer ○ the date/time the signature was executed ○ the meaning associated with the signature • System includes functionality to allow forms that will be signed should collect the printed name (as well as signature), use "Now"	**14** – Electronic records may be signed electronically. Electronic signatures are expected to have the same impact as hand-written signatures, be permanently linked to their respective record, and include the time and date that they were applied.	• CSV Policies/SOPs to define: ○ how to design a form that will collect an electronic signature (i.e. to meet the requirements of this clause) ○ management of cases where an electronic signature is invalidated by a subsequent amendment to the form (would require the form to be re-signed, while retaining a record of the original signature in the traceability trail) • Documentation showing validation of a project using electronic signatures

FDA 21 CFR Part 11 section	Review of CFR 21.11	Review of EU Annex 11	Possible Documentation Implementation
	functionality to record date/time the signature was executed, and there should be clear text designed into the form associated with the signature, explaining the meaning of the signature.		
11.50(b)	• The electronic signature (as defined in 11.50(a) above) should be presentable in human-readable form		• Documentation showing the electronic signature can be presented in human-readable form (e.g. may form specific part of project-specific validation documentation)
11.70	• The traceability trail should ensure that any signature applied to an electronic record will remain associated with the record. This may be incorporated into validation.	**14** – Electronic signatures are expected to be permanently linked to their respective record.	• Documentation from validation to show that the signature cannot be removed, copied or changed to falsify that or another record

FDA 21 CFR Part 11 section	Review of CFR 21.11	Review of Annex 11	Possible Documentation Implementation
11.100(a)	• System and procedural measures ensure that every electronic signature is unique and will never be used by anyone else. (e.g., all usernames are unique.	**N/A** (no direct Annex 11 counterpart).	• CSV Policies/SOPs to define how unique usernames will be maintained for all users, including preventing the deletion of information relating to the electronic signature once it has been used (i.e. usernames not deleted) • Documentation showing assignment and maintenance of all usernames within the system ***N.B.*** *User Access Management SOP should in general be robust enough regarding uniqueness of user id/password definition*
11.100(b)	• Assign unique credentials to each individual and Verify the identity of each and every individual prior to access/username being assigned	**N/A** (no direct Annex 11 counterpart).	• CSV Policies/SOPs to define the process for requesting and assigning a username for system access, including verification of identity prior to assignment. • Documentation showing log of access requests and completion of "due diligence" ***N.B.*** *Should be covered as part of the overall SOP framework about user access management handling.*
11.100(c)	• **A letter of Non-Repudiation Agreement for digital signatures must be submitted** to the FDA in accordance with the Part 11 instructions, where FDA submission is appropriate • The organisation must provide additional proof or testimony that a specific electronic signature is legally binding, if requested by the FDA	**14.a** –Electronic signatures are expected to have the same impact as hand-written signatures.	• Documentation would be the letter itself, with evidence both electronic and hard copies were sent (and additional information if applicable) ***N.B.*** *Ensure each individual understands the legal aspect of using their e-signature as a legally binding equivalent to their handwritten signature AND remind them of this fact. This can be done by using the following methods:-* *a) you can have a popup reminder embedded in the system that reminds users each time they sign something electronically or,*

	N.B. *You must submit to FDA the fact you going use electronic signatures. This evidence is often asked during inspection.*		*b) at the time you grant a user access to an application and where you do verify the identity of user, you capture this legal aspect again in a form or, c) for internal employees, you have HR capture the same information as part of hiring process. This last (c) option works well if you have several systems offering the e-signature feature and where you do capture such information only once*
11.200(a)(1)	• Non-biometric electronic signatures should employ at least two distinct components (e.g. username and password). • The user should use both elements to log in and only one element (e.g. password) to implement a series of signatures within a single session. • The user should use both elements to apply an electronic signature in separate sessions (i.e. not continuous access)	**12.1** – Physical and/or logical controls should be in place to restrict access to computerized systems to authorized persons. Suitable methods of preventing unauthorized 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.	• CSV Policies/SOPs to define the process for implementing the use of electronic signatures, including the use of multiple signatures in a continuous session vs. separate, non-continuous sessions. • Documentation would be shown by validation of the electronic signature process.
11.200(a)(2)	• Non-biometric signatures should only be used by their genuine owners. This should be embedded in policies/SOPs and training	**12.1** – Physical and/or logical controls should be in place to restrict access to computerized systems to authorized persons. Suitable methods of preventing unauthorized 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.	• CSV Policies/SOPs to specify that an individual should use only their electronic signature and no-one else's. • Documentation would be covered by training in the relevant Policies/SOPs and by audit

11.200(3)(a)	• Processes should ensure that it should not be possible for one person alone to use another individual's electronic signature. Training should stress that passwords should not be written down or shared, and passwords should be stored in an encrypted fashion within the system. Passwords should not be printed/visible when typed in. ***N.B.*** *This is also about password policy itself: length, usage of special characters, history of password, renewal of password etc.*	**12.1** – Physical and/or logical controls should be in place to restrict access to computerized systems to authorized persons. Suitable methods of preventing unauthorized 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.	• CSV Policies/SOPs should define the behaviours and processes which should be followed by individuals with respect to their passwords. • Documentation of training in the content/use of the Policies/SOPs as well as additional cyber-security training should be used as evidence individuals have been adequately training. Audit may be employed to show that individuals are following the requirements of Policies/SOPs. Validation should show that passwords are not visible when typed and not even visible to administrators from the back end.
11.200(3)(b)	• This covers electronic signatures using Biometrics. System does not support this functionality at the present time.	**12.1** – Physical and/or logical controls should be in place to restrict access to computerized systems to authorized persons. Suitable methods of preventing unauthorized 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.	• N/A
11.300	• Controls must be in place to ensure security and integrity of electronic signatures based on identification codes. ○ Username/password must be unique (manage through	**12.1** – Physical and/or logical controls should be in place to restrict access to computerized systems to authorized persons. Suitable methods of preventing unauthorized entry to the system	• CSV Policies/SOPs should define: ○ Maintenance of unique usernames ○ Review of usernames and password security ○ Management of situations where the loss of a device or token could compromise password integrity

	unique username management) and never reused ○ Usernames should be reviewed for "currency" from time to time. ○ Password change should be enforced periodically or otherwise managed to ensure they remain strong ○ Deauthorisation procedures to be implemented where loss of devices or tokens could compromise password integrity ○ Safeguards to detect unauthorised use of usernames or passwords, and notify appropriate individuals within the organisation who are responsible for investigating possible breach. ○ Testing of devices such as (API) tokens before and during use to ensure correct functioning	may include the use of keys, pass cards, personal codes with passwords, biometrics, restricted access to computer equipment and data storage areas. **11** – Computerized systems should be periodically evaluated to confirm that they remain in a validated state and are compliant with GMP/GxP. Such evaluations should include, where appropriate security. **12.3** – Creation, change, and cancellation of access authorizations should be recorded.	○ Processes to be implemented to check behaviours such that unauthorised use of a username or password will be detected. Relevant IT staff will be notified of the situation and they should implement appropriate action (link to company's CAPA SOPs). ○ how devices such as API tokens will be tested before and during use (link to CSV SOPs). • Documentation will cover: ○ Training in use of Policies and SOPs ○ Administration of usernames and password management ○ Device loss/deauthorisation management ○ Logs of unauthorised access detection, plus logs of actions taken (where appropriate) ○ Logs of device testing (where appropriate)