



Software Element

Usable solutions for regulated environments



fda 21 CFR part 11 checklist



Version: 1

Author: Sigfrid Dusci

Date: 04/14/09

fda 21CFR part 11 - checklist

Procedures and controls for closed systems

Requirement	Does the application comply with the requirement?	Is QA action required?	Comments
Is the application validated?			
Is it possible to discern invalid or altered records?			
Is the application capable of producing accurate and complete copies of electronic records on paper?			
Is the application capable of producing accurate and complete copies of records in electronic form for inspection, review, and copying by the FDA?			
Are the records readily retrievable throughout their retention period?			
Is application access limited to authorized individuals?			
Is there a secure, computer generated, time stamped audit trail that records the date and time of operator entries and actions that create, modify or delete electronic records?			
Upon making a change to an electronic record, is previously recorded information still available (i.e., not obscured by the change)?			

fda 21CFR part 11 - checklist

Requirement	Does the application comply with the requirement?	Is QA action required?	Comments
Is an electronic record's audit trail retrievable throughout the record's retention period?			
Is the audit trail available for review and copying by the FDA?			
If the sequence of application steps or events is important, is this enforced by the application (e.g., as would be the case in a process control application)?			
Does the application ensure that only authorized individuals can use the application, electronically sign records, access the operation, or computer application input or output device, alter a record, or perform other operations?			
If it is a requirement of the application that input data or instructions can only come from certain input devices (e.g., terminals), does the application check the validity of the source of any data or instructions received? (Note: This applies where data or instructions can come from more than one device, and therefore the application must verify the integrity of its source, such as a network of weigh scales, or remote, radio controlled terminals.)			

fda 21CFR part 11 - checklist

Requirement	Does the application comply with the requirement?	Is QA action required?	Comments
Is there documented training, including on the job training for application users, developers, IT support staff?			
Is there a written policy that makes individuals fully accountable and responsible for actions initiated under their electronic signatures?			
Are the distribution of, access to, and use of applications operation and maintenance documentation controlled?			
Is there a formal change control procedure for application documentation that maintains a time sequenced audit trail for those changes made by the pharmaceutical organization?			

fda 21CFR part 11 - checklist

Additional Procedures and Controls for Open System

Requirement	Does the application comply with the requirement?	Is QA action required?	Comments
Is data encrypted?			
Are digital signatures used?			

fda 21CFR part 11 - checklist

Signed Electronic Records

Requirement	Does the application comply with the requirement?	Is QA action required?	Comments
Do signed electronic records contain the following related information? <ul style="list-style-type: none">- The printed name of the signer- The date and time of signing- The meaning of the signing (such as approval, review, responsibility)			
Is the above information shown on displayed and printed copies of the electronic record?			
Are signatures linked to their respective electronic records to ensure that they cannot be cut, copied, or otherwise transferred by ordinary means for the purpose of falsification?			
Are electronic signatures unique to an individual?			
Are electronic signatures ever reused by, or reassigned to, anyone else?			
Is the identity of an individual verified before an electronic signature is allocated?			

fda 21CFR part 11 - checklist

Electronic Signatures (Non-biometrics)

Requirement	Does the application comply with the requirement?	Is QA action required?	Comments
Is the signature made up of at least two components, such as an identification code and password, or an id card and password?			
When several signings are made during a continuous session, is the password executed at each signing? (Note: both components must be executed at the first signing of a session.)			
If signings are not done in a continuous session, are both components of the electronic signature executed with each signing?			
Are non-biometrics signatures only used by their genuine owners?			
Would an attempt to falsify an electronic signature require the collaboration of at least two individuals?			
Has it been shown that biometrics electronic signatures can be used only by their genuine owner?			

fda 21CFR part 11 - checklist

Controls for Identification Codes and Passwords

Requirement	Does the application comply with the requirement?	Is QA action required?	Comments
Are controls in place to maintain the uniqueness of each combined identification code and password, such that no individual can have the same combination of identification code and password?			
Are procedures in place to ensure that the validity of identification codes is periodically checked?			
Do passwords periodically expire and need to be revised?			
Is there a procedure for recalling identification codes and passwords if a person leaves or is transferred?			
Is there a procedure for electronically disabling an identification code or password if it is potentially compromised or lost?			
Is there a procedure for detecting attempts at unauthorized use and for informing security?			
Is there a procedure for reporting repeated or serious attempts at unauthorized use to management?			
Is there a loss management procedure to be followed if a device is lost or stolen?			

fda 21CFR part 11 - checklist

Requirement	Does the application comply with the requirement?	Is QA action required?	Comments
Is there a procedure for electronically disabling a device if it is lost, stolen, or potentially compromised?			
Are there controls over the issuance of temporary and permanent replacements? (signing of a session.)			
Is there initial and periodic testing of tokens and cards?			
Does this testing check that there have been no unauthorized alterations?			

