www.qadata.co.za

QAData

Understanding FDA Title 21 CFR Part 11: Electronic guidance

Introduction

FDA Title 21 CFR Part 11:Electronic Records; Electronic Signatures; Final Rule (1997)

INITIAL REGULATION RELEASED

- High profile audit findings
- Industry complaints to wasting resources and non-value added specifications
- Confusion across other industries ie: device, biologicals

RESULTED IN A GUIDANCE DOCUMENT BEING RELEASED…….

Introduction

Guidance for Industry, Part 11, Electronic Records;Electronic Signatures — Scope and Application (2003)

BUT, THIS WAS NOT ENOUGH, BECAUSE:

- Guideline and not the law
- Intended to convey FDA's "current thinking"
- Many within the industry, while pleased with the more limited scope defined in the guidance, complained that, in some areas, the 2003 guidance contradicted requirements in the 1997 Final Rule.

Introduction

Guidance for Industry Computerized Systems Used in Clinical Investigations (2007)

FURTHER GUIDANCE RELEASED:

- Supplements the previous guidelines
- Defines the scope of CFR Part 11 and when it applies

Background

- 21 CFR Part 11 includes 36 pages out of which only 3 pages constitute the rule itself, the other 33 pages are a preamble with comments from the FDA on feedback from the industry.
- Part 11 has a total of 19 requirements. Some of them are specific to Part 11, others are more generic requirements of some or all FDA regulations.
- In this presentation we list the most important requirements and give some interpretations for implementation.

When does it apply ? new, narrow scope

The new narrow scope of the guidance states that Part 11 applies when:

- The record is required by a predicate rule, e.g., electronic batch records for 21 CFR Part 211 and electronic training records in 21 CFR Part 58.
- The electronic records are used to demonstrate compliance with a predicate rule, e.g., electronic training records for compliance with 21 CFR Part 211.

(predicate rule=all other 21 CFR Part regulations)

When does it apply ?

1. When electronic records are used instead of paper.
2. When persons make printouts but still rely on the electronic records in the computerized system to perform regulated activities.
3. Records submitted to the FDA, under predicate rules (even if such records are not specifically identified in agency regulations) in electronic format.
4. Electronic signatures intended to be the equivalent of handwritten signatures, initials and other general signings required by predicate rules

When does it apply ?

While point 1,3 and 4 are obvious, point 3 requires some interpretation……

"When persons make printouts but still rely on the electronic records in the computerized system to perform regulated activities."

A "regulated activity" is any activity that is required by a FDA regulation

Step-by-step guide

1. Check if the record is required by a predicate rule or used to demonstrate compliance with a predicate rule.
2. Next, we determine if the record fits in the new, narrow scope

The main criterion is whether the record is maintained in electronic format in place of paper format, or if the record is maintained in electronic format in addition to paper records and if persons rely on the electronic record to perform regulated activities.

Step-by-step guide

Remember it applies to all steps from data acquisition and evaluation

3. Finally, we make a risk assessment of the criticality of the Part 11 records and document the result.
4. Based on the outcome appropriate Part 11 controls are implemented.

CFR Part 11 requirements 1-19

System Validation - 11.10(a)

Validation should include application specific functions as well as functions related to Part 11, electronic audit trail and electronic signatures. Recommended test procedures include:

- Limited and authorized system access. This can be achieved by entering correct and incorrect password combinations and verifying if the system behaves as intended.
- Limited access to selected tasks and permissions. This can be achieved by trying to get access to tasks as permitted by the administrator and verifying if the system behaves as specified.
- Computer generated audit trail. Perform actions that should go into the e-audit trail according to specifications. Record the actions manually and compare and contrast the recordings with the computer generated audit trail.

CFR Part 11 requirements 1-19

System Validation - 11.10(a)…continued

- Accurate and complete copies. Calculate results from raw data using a defined set of evaluation parameters (e.g., chromatographic integrator events, calibration tables etc.). Save raw data, final results and evaluation parameters on a storage device. Switch off the computer. Switch it on again and perform the same tasks as before using data stored on the storage device. Results should be the same as for the original evaluation.
- Binding signatures with records. Sign a data file electronically. Check the system design and verify that there is a clear link between the electronic signature and the data file. For example, the link should include the printed name or a clear reference to the person who signed, the date and time and the meaning of the signature

CFR Part 11 requirements 1-19

Accurate and Complete Copies - 11.10(b) and 11.10(c)

"Procedures should be in place to generate accurate and complete copies of records in both human readable and electronic form suitable for inspection, review, and copying by the agency. Persons should contact the agency if there are any questions regarding the ability of the agency to perform such review and copying of the electronic records"

CFR Part 11 requirements 1-19

Accurate and Ready Retrieval - 11.10(c)

"Records must be protected to enable their accurate and ready retrieval throughout the records retention period".

- The agency wants to be able to trace final results back to the raw data using the same tools as the user had when this data was generated.

Knowing that in some instances the records must be kept for ten or more years, and as computer hardware and software have a much shorter lifetime, one can anticipate problems with this paragraph.

CFR Part 11 requirements 1-19

Limited Access - 11.10(d)

"Procedures should be in place to limit system access to authorized users".

- Limited access can be ensured through physical and/or logical security mechanisms.
- Most companies already have procedures in place. For logical security users typically log on to a system with a user I.D. and password. Physical security through key locks or pass cards in addition to logical security is recommended for high-risk areas, for example, for data centres with network severs and back-data. These procedures should be very well documented and validated.

CFR Part 11 requirements 1-19

User-Independent Computer Generated Time-Stamped Audit Trails - 11.10(e)

"Procedures should be available to use 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."

This paragraph has been the subject of many questions and discussions.

The problem lies mainly in how it is implemented, especially which details are recorded.

CFR Part 11 requirements 1-19

User-Independent Computer Generated Time-Stamped Audit Trails - 11.10(e) ....continued

- Most important is the word “independently”, which means independently from the operator. The main purpose is to ensure and prove data integrity.
- If the data has been changed the computer should record what has been changed and who made the change. The audit trail functionality should be built into the software and is especially important for critical computer related processes with manual operator interaction.

CFR Part 11 requirements 1-19

Operational System Checks - 11.10(f)

"Procedures should be available to use operational system checks to enforce permitted sequencing of steps and events, as appropriate."

CFR Part 11 requirements 1-19

Use of Authority Checks - 11.10(g)

"Procedures should be available to use 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".

- Authority checks must be in place to ensure "authenticity, integrity and confidentiality" of electronic records, and to ensure that the signer cannot "readily repudiate the signed record as not genuine."

CFR Part 11 requirements 1-19

Use of Authority Checks - 11.10(g) …….continued

- This requires procedural and technical controls. Procedures should be in place to assign access to systems and permitted tasks to individuals and the system should be able to verify that an individual is permitted or authorized to perform the requested function.
- Authority checks should be used when an individual attempts to:
  - Access a system.
  - Perform selected permitted tasks.
  - Change a record.
  - Electronically sign a record.

CFR Part 11 requirements 1-19

Use of Device Checks - 11.10(h)

"Procedures should be available to use device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction".

- This requirement refers to automatically determining the identification and location of a piece of equipment hardware or another computer system. An example would be that a computer system controlling an instrument should automatically recognize the equipment as a valid input device through its serial number. If the serial number is not set up in the computer's database the instrument cannot be used as an input device.

Device checks are not required in all cases but only "where appropriate".

CFR Part 11 requirements 1-19

People Qualification - 11.10(i)

"Procedures should be available to determine that persons who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks".

- People qualification is a GxP requirement and not specific to Part 11. Procedures should be in place to document tasks and qualifications, to develop a gap analysis and to develop an implementation plan on the gaps that can be filled. This paragraph applies to users as well as developers of systems and also to people supporting all kinds of computer systems including network infrastructure.

It also applies to 3rd parties, eg: external service providers supporting an IT infrastructure.

CFR Part 11 requirements 1-19

Individual Accountability - 11.10(j)

"Procedures should be available to establish, and adhere to, written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification".

- Procedures should make employees aware that electronic signatures have the same meaning as handwritten signatures. The content of the procedures should be communicated in trainings and enforced.
- It is recommended that employees should sign a statement like: "I understand that electronic signatures are legally binding and have the same meaning as handwritten signatures".

CFR Part 11 requirements 1-19

Controls Over System Documentation - 11.10(k)

"Procedures should be in place for 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".

CFR Part 11 requirements 1-19

Controls Over System Documentation - 11.10(k)
.......continued

- System documentation includes all lifecycle documents from validation planning, vendor assessment, development documentation and specifications, to installation records, operation and test procedures and protocols, change control and procedures to ensure system security and the operator's authenticity. All documentation should follow approved change control processes and should be under revision control. Controls should be in place to ensure that the most recent version of the document is always used.

CFR Part 11 requirements 1-19

Use of Digital Signatures for Open Systems - 11.30

"Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified for closed systems, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality“.

CFR Part 11 requirements 1-19

Use of Digital Signatures for Open Systems - 11.30

……..continued

- This requires software for document encryption and may also require hardware and software for generating digital signatures. Typically computer systems used in pharmaceutical operations are closed systems without a need for digital signatures. An example for an open system would be if analytical data generated by a contract laboratory is transmitted to the sponsor through the public Internet.

EG's on how open systems can be used are described in presentation 5.

CFR Part 11 requirements 1-19

Requirements for Signed Electronic Records - 11.50

"(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.

(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)."

CFR Part 11 requirements 1-19

Linking records to Signatures - 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."

- The main purpose of this requirement is to link electronic signatures to relevant electronic records and also to the signer of the records.
- The signer should be recognized by the system through user I.D./password and procedures and technical controls should ensure that the signer is uniquely identified.

CFR Part 11 requirements 1-19

Linking records to Signatures - 11.70 …….continued

- This definitely requires not only the development of procedures but even more importantly behavioural changes on using I.D. codes and passwords.
- The taboo against sharing a password with a colleague is usually much lower than teaching somebody how to abuse a handwritten signature. But under Part 11 both have the same consequence.
- Software should also recognize any change to a signed record. Typically this is done through linking the electronic signature to the electronic audit trail.

CFR Part 11 requirements 1-19

General requirements for electronic signatures - 11.100

"(a) Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.

(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.

(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.

CFR Part 11 requirements 1-19

General requirements for electronic signatures - 11.100

……..continued

(1) The certification shall be submitted in paper form and signed with a traditional handwritten signature, to the Office of Regional Operations (HFC-100), 5600 Fishers Lane, Rockville, MD 20857.

(2) Persons using electronic signatures shall, upon agency request, provide additional certification or testimony that a specific electronic signature is the legally binding equivalent of the signer's handwritten signature."

CFR Part 11 requirements 1-19

Electronic signature components and controls - 11.200

"(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.

CFR Part 11 requirements 1-19

Electronic signature components and controls - 11.200

……..continued

"…(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.

(2) Be used only by their genuine owners; and

(3) 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.

(b) Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.

CFR Part 11 requirements 1-19

Controls for identification codes/passwords - 11.300

Persons who use electronic signatures based upon use of identification codes in combination with passwords shall employ controls to ensure their security and integrity. Such controls shall include:

(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.

(b) Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).

CFR Part 11 requirements 1-19

Controls for identification codes/passwords - 11.300

……..continued

(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.

(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.

CFR Part 11 requirements 1-19

Controls for identification codes/passwords - 11.300

……..continued

(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."

21 CFR Part 11-summary

- Implementing the regulation on electronic signatures and records will have major consequences.
- It is recommended to follow a step-by-step approach, see:

CFR PART 11_stepbystep.pdf