21 CFR Part 11 Electronic Records; Electronic Signatures

Frequently Asked Questions

What is 21 CFR Part 11?

21 CFR Part 11 establishes requirements to ensure that electronic records and electronic signatures are trustworthy, reliable and generally equivalent substitutes for paper records and traditional handwritten signatures. Electronic records and electronic signatures may be used to meet record and signature requirements of 21 CFR Parts 210 and 211 when part 11 requirements are met.

What is an Electronic Record?

As defined by the FDA, “Electronic record means any combination of text, graphics, data, audio, pictorial, or other information representation in digital form that is created, modified, maintained, archived, retrieved, or distributed by a computer system.”

For many systems, this is either a relational database entry or a document (word-processing file (such as Microsoft® Word), bitmap image, PDF, AutoCAD drawing, etc.). Additionally, the concept of an electronic record includes output from instrumentation (digital signals combined with defined parameters for manipulating signals), software code, etc. E-mail is also considered an electronic record, if it is used for reviewing or approving documents or as part of a change control process.

It is important to consider to what types of records Part 11 applies. The regulations apply to records required by what the FDA refers to as a predicate rule. A predicate rule is a previously published regulation such as Good Laboratory Practice (GLP) and Current Good Manufacturing Practice (CGMP). The predicate rule mandates:

- What records must be maintained
- The content of records
- Whether signatures are required
- How long records must be maintained

If there is no FDA requirement that a particular record be created or retained, then 21 CFR Part 11 most likely does not apply to the record. For example, financial records are not required or reviewed by the

---

FDA and therefore a system that handles exclusively financial documents would not need to comply with Part 11.

**What is an Electronic Signature?**

According to the FDA, “Electronic signature means 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.”

Certain signatures are required by predicate rules. If these signatures are executed electronically, then Part 11 compliance is required. Part 11 also covers non-required signatures if they are executed against required electronic records.

**If you have Electronic Signatures, do you have to comply with Electronic Record Requirements?**

Use of Electronic Signatures implies that a system is an Electronic Record system, and must be in compliance with all provisions of 21 CFR Part 11.

**If you have Electronic Records, do you have to comply with Electronic Signature Requirements?**

First of all, the system may not require signatures, electronic or otherwise. The FDA states that “The agency stresses that part 11 does not require that any given electronic record be signed at all. The requirement that any record bear a signature is contained in the regulation that mandates the basic record [i.e., the predicate rule] itself. Where records are signed, however, by virtue of meeting a signature requirement or otherwise, part 11 addresses controls and procedures intended to help ensure the reliability and trustworthiness of those signatures.”

Secondly, the FDA states that “…persons may use electronic records in lieu of paper records or electronic signatures in lieu of traditional signatures, in whole or in part…”

Solutions other than electronic signature are possible even for electronic record systems. For example, documents may be printed, signed, and either the signature page or the entire document scanned and re-entered into the system.

**When does Part 11 apply to an electronic system?**

The FDA states “Part 11 is intended to apply to systems that create and maintain electronic records under FDA’s requirements in Chapter I of Title 21, even though some of those electronic records may be printed on paper at certain times. The key to determining part 11 applicability, under §

---

2 Ibid.
3 Ibid, p. 13438.
11.1(b), is the nature of the system used to create, modify, and maintain records, as well as the nature of the records themselves. Part 11 is not intended to apply to computer systems that are merely incidental to the creation of paper records that are subsequently maintained in traditional paper-based systems. In such cases, the computer systems would function essentially like manual typewriters or pens and any signatures would be traditional handwritten signatures. Record storage and retrieval would be of the traditional ‘‘file cabinet’’ variety. More importantly, overall reliability, trustworthiness, and FDA’s ability to access the records would derive primarily from well-established and generally accepted procedures and controls for paper records. For example, if a person were to use word processing software to generate a paper submission to FDA, part 11 would not apply to the computer system used to generate the submission, even though, technically speaking, an electronic record was initially created and then printed on paper.”

Part 11 applies to all electronic records required by an FDA predicate rule. The regulation does not apply, however, to paper records that are, or have been transmitted by electronic means, such as faxing (21 CFR 11.1 (b)).

**Does Part 11 Apply to Legacy Systems?**

Part 11 applies to all Electronic Record/Electronic Signature systems, even those developed before the ruling was issued. The FDA states:

“Certain older electronic systems may not have been in full compliance with Part 11 by August 20, 1997, and modification to those so called “legacy systems” may take more time. As explained in the preamble to the final rule, Part 11 does not grandfather legacy systems and FDA expects that firms using legacy systems will begin taking steps to achieve full compliance.”

**If I have electronic records, can I submit them electronically?**

Not necessarily. There are some documents that must be submitted as paper. These documents include FDA Forms 356H, 2253, 2567, and 3397, as well as certifications or declarations. The full list of documents that may be submitted electronically is contained in public docket No. 92S-0251, which can be found on the FDA Web site (www.fda.gov).

For documents that are signed with handwritten signatures, but for which the originals are not required to be submitted, some companies scan the signature page into an EDMS, and some merely provide a statement that the signature page is on file. In either case, the paper document would continue to be the official copy of the document.

For records that are maintained but not necessarily submitted to FDA, electronic records can substitute for

---

5 Ibid, p. 13437.
paper records as long as they meet the criteria set forth in the rule (62 FR:13435).

**Do all electronic documents that require a signature have to be signed electronically?**

No, documents that have been created and maintained electronically may be signed and submitted as paper documents.

**What are biometric and non-biometric signatures?**

FDA Definition: “Biometrics means a method of verifying an individual’s identity based on measurement of the individual’s physical feature(s) or repeatable action(s) where those features and/or actions are both unique to that individual and measurable.” 7 The results are used to verify an individual's identity. Non-biometric systems are those based on an identification code and password.

**What are the advantages and disadvantages of each approach?**

<table>
<thead>
<tr>
<th></th>
<th>Biometric</th>
<th>Non-Biometric</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advantages</td>
<td>• Considered less likely by the FDA to be compromised</td>
<td>• Minimal investment in tools and customizations</td>
</tr>
<tr>
<td></td>
<td>• Cannot be lost, stolen, or shared</td>
<td>• Minimal user training</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Deployable to new locations without managing acquisition and integration of hardware</td>
</tr>
<tr>
<td>Disadvantages</td>
<td>• Much higher capital investment, potentially higher operating costs</td>
<td>• Require additional password protection to be in place (password aging, recall, checks for patterns of unauthorized use, etc.)</td>
</tr>
<tr>
<td></td>
<td>• May not be well-accepted by users</td>
<td>• Difficult to overcome culture of sharing passwords at some companies</td>
</tr>
<tr>
<td></td>
<td>• Require measurement devices to be available at each desk, area or site in accordance with the business process</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Requires routine device checks/calibration</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Devices can be set to pass/fail at different levels – this requires up front evaluation</td>
<td></td>
</tr>
</tbody>
</table>

Does the FDA prefer biometric over non-biometric signatures?

The FDA currently shows no preference, although they do note “…that biometrics-based electronic signatures, by their nature, are less prone to be compromised than other methods such as identification codes and passwords.”

What types of biometric devices are available?

<table>
<thead>
<tr>
<th>Authentication Method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Finger-print</td>
<td>The fingerprint’s strength is its acceptance, convenience and reliability. It takes little time and effort for somebody using a fingerprint identification device to have their fingerprint scanned. Studies have also found that using fingerprints as an identification source is the least intrusive of all biometric techniques. Verification of fingerprints is also fast and very reliable. Users will not experience as many errors in matching when they use their fingerprints versus many other biometric methods. In addition, a fingerprint identification device can require very little space on a desktop or in a machine. One of the biggest fears of fingerprint technology is the theft of fingerprints. Skeptics point out that latent or residual prints left on the glass of a fingerprint scanner may be copied. However, a good fingerprint identification device only detects live fingers and will not acknowledge fingerprint copies.</td>
</tr>
<tr>
<td>Palm Print</td>
<td>The advantages of a palm print are similar to the benefits of a fingerprint in terms of reliability. However, palm print scanners can take up a lot of room. This may prevent users from integrating these scanners into their systems.</td>
</tr>
<tr>
<td>Retinal Scan</td>
<td>The retina has an advantage over the fingerprint because it has more characteristics to identify and match. This however, does not mean that a retinal scanner is more accurate or reliable than a fingerprint scanner. Eye and retinal scanners are ineffectual with the blind and those who have cataracts. The retinal scanner can also be very cumbersome for users, since it requires them to place their eyes into an identification unit.</td>
</tr>
<tr>
<td>Signature</td>
<td>Signature verification is another biometric area that has its plusses and minuses. Signatures can provide security, but forged signatures pose a problem. This will prevent signature verification from being integrated into high-level security applications.</td>
</tr>
<tr>
<td>Voice Patterns</td>
<td>While voice recognition is convenient, it is not as reliable as other biometric techniques. A person with a cold or laryngitis may have problems using a voice recognition system.</td>
</tr>
</tbody>
</table>

8 Ibid, p. 13440.
If non-biometric (i.e., username/password) systems are used, must a “double-password” system be in place?

The same user name and password can be used for entering the system and signing records. However, to use them as an electronic signature, they must be entered as a distinct event, including the meaning of the signature, demonstrating that the signer is aware of its implications.

In the Documentum world, this means that the Documentum user name and password (generally the same as the operating system username and password) can be used to sign records. Non-biometric electronic signature components must consist of one identification component and one password.

In a June 3, 1999, videoteleconference on Electronic Records and Electronic Signatures, Paul Motise of the FDA stated, “As long as the signing password complies with Part 11 provisions, it may be the same as the login password. Having a separate signature password may be more secure, however”.

He also stated that it is acceptable for a system administrator to have the ability to reset a user’s password, as there will always be a number of employees in an organization that will need a higher level of privileges, but suggests limiting this group as much as possible.

He also stated that passwords can be shared if used exclusively for read-only functions.

What is the difference between an open and a closed system?

The FDA defines a closed system as “an environment in which system access is controlled by persons who are responsible for the content of electronic records that are on the system.” The FDA does allow systems with dial-in access to be considered closed “where access is authorized by, and under the control of, the organization that operates the system”. The FDA does recommend that controls beyond those employed for system access from within its facility be implemented for dial-in systems.

What are the main technical ramifications of 21 CFR Part 11 on my system?

Some important technical implications of complying with 21 CFR Part 11 include:

1. Determination of whether the system is “open” or “closed”

2. Integration of signature via biometrics or password

3. Generation of audit trails - audit trails must be electronic, and meet a number of additional FDA

---

9 FDA Electronic Workshop: Electronic Records and Electronic Signatures Title 21 CFR Part 11, January 1999
11 Ibid, p. 13441.
requirements (see questions below)

4. Controls on user name and password, including password aging for non-biometric signature systems

5. Detection of unauthorized entry

6. User authority checks (i.e., checks within the code to determine if a user should be able to perform an action based on their privileges)

7. Security of RDBMS

8. How records are displayed (this involves examining all potential output mechanisms.)

What are the main business ramifications of 21 CFR Part 11 on my system?

1. Evaluation of the regulatory impact and the scope of the system. Is it electronic record, electronic signature, etc.?

2. Certification to the FDA that a company considers Electronic Signature to be the legally binding equivalent of traditional handwritten signatures (one certification from corporate headquarters is sufficient to cover all sites that are part of that corporation 12)

3. Various SOPs to document establishment of user identity, user accountability, procedures, etc.

4. Audit trail monitoring

5. Validation of commercial and custom software

6. Qualification of personnel developing, administering, maintaining or using the system

7. Archiving and retrieval

8. Cost and staffing for all of the above

Does Out-of-the--box Documentum workflow with sign-off meet the FDA requirements?

No, for a couple of reasons:

- The FDA requires, in addition to the printed name of the signer and the date and time of the signature, “The meaning (such as review, approval, responsibility, or authorship) associated with the signature.” You are unlikely to establish this from a workflow without customizations.

12 FDA Electronic Workshop: Electronic Records and Electronic Signatures Title 21 CFR Part 11, January 1999
The FDA states that "The items identified in paragraphs (a)(1), (a)(2), and (a)(3) [i.e., name, date/time, and meaning] 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)." Without a customization such as publishing, the signature will not appear with a viewed or printed copy of the record.

**From what system should the date and time for Electronic Signature time stamps come?**

The FDA originally advised that the signer’s local date and time be recorded as the date and time stamp for electronic signatures. However, the agency has reconsidered its position on this matter.

The new draft position states “You should implement time stamps with a clear understanding of what time zone reference you use. Systems documentation should explain time zone references as well as zone acronyms or other naming conventions. For example the time zone reference might be a central point like Greenwich Mean Time, a point local to the computer where the activity linked to the time stamp occurs, or a point where the time stamp clock (e.g., a time stamp server) is located”.

**When should the audit trail for a record begin?**

While the FDA has not provided a Guidance document concerning audit trails, the general rule is to being the audit trail from the point a document (record) becomes effective.

The Industry Coalition on 21 CFR Part 11 has provided guidance for its members. The following recommendations come from a memo from a Coalition meeting. Several staff members from the FDA were present at the meeting, including Paul Motise and John Taylor.

For records where predicate rules require contemporaneous recording of information with the actions that produced the information, the audit trail must begin with the first human readable form of the information.

For records where predicate rules allow preliminary versions of a record, the audit trail should begin when changes to and deletions of the record and time when these occurred have an impact on the integrity of the record. This type of record has three subtypes that were addressed.

1. Single signature records – it is not necessary to audit trail preliminary drafts of this type of record. The audit trail can begin at the point the individual signing the record considers it to be complete by signing the record. The audit trail should include the event of signing the record.

2. Multiple signature records – if a single record consists of content authored and signed by multiple people, the audit trail should begin with the first signature applied to the record so that “Once a signature has been affixed, the words attributed to that should not be changed so as to alter the attributed statements”.

---

3. Unsigned records – the audit trail for unsigned documents should begin when, according to Standard Operating procedures, the document is complete and recorded in a retrieval form.

**Are there rules for how to maintain records through their retention period?**

The FDA has no rule regarding how to maintain electronic records until their expiration. However, they do describe two methods, “The Time Capsule Approach” and “The Electronic Records Migration Approach”. In the first approach, the electronic records are maintained on the original system used to create the electronic record. This system must remain intact with no upgrades. A disadvantage to this approach is that system documentation must be kept updated and personnel to work with the system trained.

The second approach entails moving the electronic records from the system where they were originally created to another system. The result of the migration must be an electronic record that continues to adhere to 21 CFR Part 11.

The FDA has issued a Draft Guidance on maintaining electronic records titled “Guidance for Industry, 21 CFR Part 11; Electronic Records; Electronic Signatures, Maintenance of Electronic Records (July 2002)”

**Does the FDA require validation of commercial software?**

The FDA in many cases does require the validation of commercial software for its intended use. They state “The agency believes that commercial availability is no guarantee that software has undergone ‘‘thorough validation’’ and is unaware of any regulatory entity that has jurisdiction over general purpose software producers. The agency notes that, in general, commercial software packages are accompanied not by statements of suitability or compliance with established standards, but rather by disclaimers as to their fitness for use. The agency is aware of the complex and sometimes controversial issues in validating commercial software. However, the need to validate such software is not diminished by the fact that it was not written by those who will use the software.”

In a June 3, 1999, videoteleconference on Electronic Records and Electronic Signatures, Paul Motise of the FDA provided the following common sense guidelines to using and validating commercial software:

- Don’t use version 1.0 (that is, an initial release) of software if possible
- Research known problems with the software and potential fixes
- Maintain change control of the software
- Plan and execute function testing for intended uses of the software
- Obtain specifications that can be used for testing

---

• Audit the software company to determine their standards, practices, etc.

What are the implications of using Optical Character Recognition (OCR) within an Electronic Records system?

Use of OCR raises a number of issues. OCR is not 100% accurate. In addition, it may be necessary to establish a uniform policy for use of OCR so that it is not performed on an irregular or ad hoc basis, which makes it difficult to use the results in a systematic manner.

For regulatory submission systems, the determination of whether OCR is required should be a topic for the pre-meeting with the FDA, and deciding which documents/reports will be provided in imaged format, vs. searchable PDF. A plan and procedure for ensuring the accuracy of OCR should be part of the project