C&A

Improving Your Security

21 CFR Part 11
Electronic Records
Electronic Signatures Validation

Guide

Index

Glossary of Terms (Definitions)

Term	Definition
Biometrics	A method of verifying an individual's identity based on measurement of the individual's physical feature(s) or repeatable actions where those features and/or actions are both unique to that individual and measurable.[1]
Closed System	An environment in which system access is controlled by persons who are responsible for the content of electronic records that are on the system.[1]
Open System	An environment in which system access is not controlled by persons who are responsible for the content of electronic records that are on the system.[1]
Computer Systems Validation	Confirmation by examination and provision of objective evidence that computer system specifications conform to user needs and intended uses, and that all requirements can be consistently fulfilled.
Digital Signature	An electronic signature based upon cryptographic methods of originator authentication, computed by using a set of rules and a set of parameters such that the identity of the signer and the integrity of the data can be verified.[1]
Electronic Signature	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.[1]
Handwritten Signature	The scripted name or legal mark of an individual handwritten by that individual and executed or adopted with the present intention to authenticate a writing in a permanent form. The act of signing with a writing or marking instrument such as a pen or stylus is preserved. The scripted name or legal mark, while conventionally applied to paper, may also be applied to other devices that capture the name or mark.[1]
Off-the-Shelf Software (OTS/COTS software)	A generally available software component for which the user can not claim complete software life cycle control.[3]

Person	Includes an individual, partnership, corporation, and association. [4]
Predicate Rule	Requirements set forth in the Act, the PHS Act, or any FDA regulation, with the exception of part 11.
Regression Analysis And Testing	A software verification and validation task to determine the extent of verification and validation analysis and testing that must be repeated when changes are made to any previously examined software products.[5]
Regression	Testing Rerunning test cases which a program has previously executed correctly in order to detect errors spawned by changes or corrections made during software development and maintenance.[5]
Reliability	The ability of a system or component to perform its required functions under stated conditions for a specified period of time.[2]

Scope

We intend to provide information with respect to FDA's current thinking on acceptable ways of meeting part 11 requirements to ensure that electronic records and electronic signatures are trustworthy, reliable, and compatible with FDA's public health responsibilities.

Unless otherwise specified below, all terms used in this draft guidance are defined in FDA's draft guidance document "*Guidance For Industry, 21 CFR Part 11; Electronic Records; Electronic Signatures, Glossary of Terms*" a document common to the series of guidances on part 11.

The document 21 CFR Part 11 [Docket No. 92N–0251] RIN 0910–AA29 Of the DEPARTMENT OF HEALTH AND HUMAN SERVICES (Food and Drug Administration) emitted Thursday March 20, 1997 state : "*The final rule provides criteria under which FDA will consider electronic records to be equivalent to paper records, and electronic signatures equivalent to traditional handwritten signatures. Part 11 (21 CFR part 11)*"

This guidance applies to electronic records and electronic signatures that persons create, modify, maintain, archive, retrieve, or transmit under any records or signature requirement set forth in the Federal Food, Drug, and Cosmetic Act (the Act), the Public Health Service Act (PHS Act), or any FDA regulation.

We intend to provide with this draft guidance useful information and recommendations to:

- Persons subject to part 11;
- Persons responsible for validation of systems used in electronic recordkeeping;
- Persons who develop products or services to enable implementation of part 11 requirements;

Part 11 Regulatory Requirements

Section 11.10 requires persons to :
"*employ procedures and controls* designed to *ensure* the *authenticity, integrity*, and, when appropriate, the *confidentiality of electronic records*, and to ensure that the *signer cannot readily repudiate* the signed record as not genuine."

To satisfy this requirement persons must, among other things, employ procedures and controls that include :
"*validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.*"

Key Principles

Here are some key principles you should consider when validating electronic recordkeeping computer systems.

System Requirements Specifications

Regardless of whether the computer system is developed in-house, developed by a contractor, or purchased off-the-shelf, establishing documented end user (i.e., a person regulated by FDA) requirements is extremely important for computer systems validation.

Without first establishing end user needs and intended uses, we believe it is virtually impossible to confirm that the system can consistently meet them.

Once you have established the end user's needs and intended uses, you should obtain evidence that the computer system implements those needs correctly and that they are traceable to system design requirements and specifications.

It is important that your end user requirements specifications take into account predicate rules, part 11, and other needs unique to your system that relate to ensuring :

- record authenticity,
- integrity,
- signer non-repudiation,
- when appropriate, confidentiality.

For example, as noted above, section 11.10 has a general requirement that persons who use *closed systems* to create, modify, maintain, or transmit electronic records must employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that signers cannot readily repudiate signed records as not genuine.

In addition, section 11.30 requires persons who use *open systems* to employ procedures and controls identified in section 11.10, as appropriate; persons who use open systems must also implement special procedures and controls, such as document encryption and use of digital signature standards, as necessary under the circumstances, to ensure record authenticity, integrity, and confidentiality.

Other factors not specifically addressed in part 11 may also impact on electronic record trustworthiness, integrity and system performance.

You should consider these factors and establish appropriate requirements specifications for them, as well.

Here are some examples:

- Scanning processes: where a paper record is scanned to create an electronic record, scanner resolution, scanning rates, color fidelity, and the type of hardware interface may impact the accuracy and reliability of the electronic record as well as system performance.
- Scalability: in a networked environment, system performance may be affected by the number of workstations and bandwidth demands of file size and types.
- Operating environment: sources of electromagnetic interference, radio frequency interference, temperature/humidity, and electrical power fluctuations may affect system performance.

Documentation of Validation Activity

We consider thorough documentation to be extremely important to the success of your validation efforts.

Validation documentation should include a :

- validation plan
- validation procedures
- validation report,

and should identify who in management is responsible for approval of the plan, the procedures and the report.

Validation Plan

The validation plan is a strategic document that should state what is to be done, the scope of approach, the schedule of validation activities, and tasks to be performed. The plan should also state who is responsible for performing each validation activity. The plan should be reviewed and approved by designated management.

Validation Procedures

The validation procedures should include detailed steps for how to conduct the validation.

It should describe the computer system configuration, as well as test methods and objective acceptance criteria, including expected outcomes. The procedures should be reviewed and approved by designated management.

Validation Report

The validation report should document detailed results of the validation effort, including test results. Whenever possible, test results should be expressed in quantified terms rather than stated as “pass/fail.” The report should be reviewed and approved by designated management.

Equipment Installation

Prior to testing, you should confirm that all hardware and software are properly installed and, where necessary, adjusted and calibrated to meet specifications. User manuals, standard operating procedures, equipment lists, specification sheets, and other documentation should be readily accessible for reference.

Dynamic Testing

Key Testing Considerations

- Test conditions: test conditions should include not only "normal" or "expected" values, but also stress conditions (such as a high number of users accessing a network at the same time). Test conditions should extend to boundary values, unexpected data entries, error conditions, reasonableness challenges (e.g. empty fields, and date outliers), branches, data flow, and combinations of inputs.
- Simulation tests: some testing may be performed using simulators, usually conducted off-line outside of the actual user's computing environment.
- Live, user-site tests: these tests are performed in the end user's computing environment under actual operating conditions. Testing should cover continuous operations for a sufficient time to allow the system to encounter a wide spectrum of conditions and events in an effort to detect any latent faults that are not apparent during normal activities.

Software testing should include:

- Structural testing: this testing takes into account the internal mechanism (structure) of a system or component. It is sometimes referred to as "white box" testing. Structural testing should show that the software creator followed contemporary quality standards. This testing usually includes inspection (or walk-throughs) of the program code and development documents.
- Functional testing: this testing involves running the program under known conditions with defined inputs, and documented outcomes that can be compared to pre-defined expectations. Functional testing is sometimes called "black box" testing.
- Program build testing: this testing is performed on units of code (modules), integrated units of code, and the program as a whole.

How test results should be expressed.

Quantifiable test results should be recorded in quantified rather than qualified (e.g. pass/fail) terms. Quantified results allow for subsequent review and independent evaluation of the test results.

Static Verification Techniques
While dynamic testing is an important part of validation, we believe that by using dynamic testing alone it would be virtually impossible to fully demonstrate complete and correct system performance.

A conclusion that a system is validated is also supported by numerous verification steps undertaken throughout the system development.

These include static analyses such as document and code inspections, walk-throughs, and technical reviews. Where available, knowledge of these activities and their outcomes can help to focus testing efforts, and help to reduce the amount of system level functional testing needed at the user site in order to validate that the software meets the user's needs and intended uses.

Extent of Validation
When you determine the appropriate extent of system validation, the factors you should consider include (but are not limited to) the following:

- The risk that the system poses to product safety, efficacy, and quality; note that product means the FDA regulated article (food, human or veterinary drug, biological product, medical device, or radiological product);
- The risk that the system poses to data integrity, authenticity, and confidentiality;
- The system's complexity; a more complex system might warrant a more comprehensive validation effort.

Independence of Review
It is a quality assurance tenet that objective self-evaluation is difficult. Therefore, where possible, and especially for higher risk applications, computer system validation should be performed by persons other than those responsible for building the system. Two approaches to ensuring an objective review are:
(1) Engaging a third party;
(2) dividing the work within an organization such that people who review the system (or a portion of the system) are not the same people who built it.

Change Control (Configuration Management)

Systems should be in place to control changes and evaluate the extent of revalidation that the changes would necessitate. The extent of revalidation will depend upon the change's nature, scope, and potential impact on a validated system and established operating conditions. Changes that cause the system to operate outside of previously validated operating limits would be particularly significant.

Contractor or vendor upgrades or maintenance activities, especially when performed remotely (i.e., over a network), should be carefully monitored because they can introduce changes that might otherwise go unnoticed and have an adverse effect on a validated system. Examples of such activities include installation of circuit boards that might hold new versions of "firmware" software, addition of new network elements, and software "upgrades", "fixes" or "service packs."

It is important that system users be aware of such changes to their system. You should arrange for service providers to advise you regarding the nature of such revisions so you can assess the changes and perform appropriate revalidation.

We consider regression analysis to be an extremely important tool that should be used to assess portions of a system that were themselves unchanged but are nonetheless vulnerable to performance/reliability losses that the changes can cause. For instance, new software might alter performance of other software on a system (e.g., by putting into place new device drivers or other code that programs share.) Regression testing should be performed based on the results of the regression analysis.

Special Considerations

Commercial, Off-The-Shelf Software

Commercial software used in electronic recordkeeping systems subject to part 11 needs to be validated, just as programs written by end users need to be validated. See 62 Federal Register 13430 at 13444-13445 (March 20, 1997.)

We do not consider commercial marketing alone to be sufficient proof of a program's performance suitability.

The end user is responsible for a program's suitability as used in the regulatory environment. However, the end user's validation approach for off-the-shelf software is somewhat different from what the developer does because the source code and development documentation are not usually available to the end user.

End users should validate any program macros and other customizations that they prepare.

End users should also be able to validate off-the-shelf software by performing all of the following:

End User Requirements Specifications

End users should document their requirement specifications relative to part 11 requirements and other factors, as discussed above. The end user's requirement specifications may be different from the developer's specifications. If possible, the end user should obtain a copy of the developer's requirements specifications for comparison.

Software Structural Integrity

Where source code is not available for examination, end users should infer the adequacy of software structural integrity by doing all of the following:

- Conducting research into the program's use history. This research should include: (1) Identifying known program limitations; (2) evaluating other end user experiences; and, (3) identifying known software problems and their resolution;
- Evaluating the supplier's software development activities to determine its conformance to contemporary standards. The evaluation should preferably be derived from a reliable audit of the software developer, performed by the end user's organization or a trusted and competent third party.

Functional Testing of Software

End users should conduct functional testing of software that covers all functions of the program that the end user will use. Testing considerations discussed above should be applied. When the end user cannot directly review the program source code or development documentation (e.g., for most commercial off-the-shelf software, and for some contracted software,) more extensive functional testing might be warranted than when such documentation is available to the user. More extensive functional testing might also be warranted where general experience with a program is limited, or the software performance is highly significant to data/record integrity and authenticity. Note, however, we do not believe that functional testing alone is sufficient to establish software adequacy.

The Internet

We recognize the expanding role of the Internet in electronic recordkeeping in the context of part 11. Vital records, such as clinical data reports or batch release approvals, can be transmitted from source to destination computing systems by way of the Internet.

Internet Validation

We recognize that the Internet, as computer system, cannot be validated because its configuration is dynamic. For example, when a record is transmitted from source to destination computers, various portions (or packets) of the record may travel along different paths, a route that neither sender nor recipient can define or know ahead of time. In addition, entirely different paths might be used for subsequent transfers.

The Internet can nonetheless be a trustworthy and reliable communications pipeline for electronic records when there are measures in place to ensure the accurate, complete and timely transfer of data and records from source to destination computing systems.

Validation of both the source and destination computing systems (i.e., both ends of the Internet communications pipeline) should extend to those measures. We therefore consider it extremely important that those measures are fully documented as part of the system requirements specifications, so they can be validated. Examples of such measures include:

- Use of digital signature technology to verify that electronic records have not been altered and that the sender's authenticity is affirmed.
- Delivery acknowledgements such as receipts or separate confirmations executed apart from the Internet (e.g., via fax or voice telephone lines.)