

Data Integrity and Compliance: What Every Lab Should Know



Lack of data integrity is a key reason for breaching compliance. Shweta Nair, Sr. Product Manager - Biotechnology at Advanced Instruments, sat down with Angela Bazigos, CEO of Touchstone Technologies Silicon Valley and a co-author of 21 CFR Part 11 FDA guidelines.

In 2017, data integrity issues were cited in 65% of all FDA warning letters. The main reason was incomplete data. In the pharmaceutical and biotechnology industries, this can be prevented by ensuring the trustworthiness and reliability of electronic records, a process that is also known as compliance with data integrity. The highest risks, when not working in a compliant manner, lie in import bans, product recalls, or even the closing of production plants.

The FDA defines the criteria under which electronic records and electronic signatures are considered trustworthy, reliable, and equivalent to paper records in Title 21 of the Code of Federal Regulations (21 CFR) Part 11.

By becoming FDA 21 CFR Part 11 compliant, organizations benefit from:

- Reduced costs by removing manual and paper processes while improving workflow processes
- Reduced costs of managing and documenting their entire record lifecycle, from routing and approval workflow, version control, and comparison to audit trails and reports
- Improved traceability – e-records are simpler for gathering, filtering, and presenting information for internal use or FDA audits
- Stronger controls over users' ability to design, amend, and approve forms
- Better management of global data, including product data, symbols, graphics, and languages
- Compliance with data integrity requirements

FDA 21 CFR Part 11 allows life science organizations to use e-records and e-signatures in place of paper. However, a piece of software by itself cannot be compliant. Any critical software

must be supported by a properly conceived and performed validation project, normally following current GMPs.

What is data integrity?

The completeness, consistency, and accuracy of data. Complete, consistent, and accurate data should be attributable, legible, contemporaneously recorded, original or a true copy, and accurate (ALCOA).

Is the FDA concerned with data integrity?

Per Edwin Rivera, of the Chief Investigations and Preapproval Compliance Branch at the FDA's Center for Drug Evaluation

ALCOA	Meaning	Meaning	Comments
A	Attribute	Who performed an action and when? If a record is changed, who did it and why?	Who did it? Source data
L	Legible	Data must be recorded in a permanent durable medium and be readable	Can you read it? Needs to be permanent
C	Contemporaneous	Data must be recorded when it was performed followed by date and time	Was it done real time?
O	Original	Is the information the original date or a certified true copy of the original data?	It is original or a true copy
A	Accurate	No errors or editing performed without documented amendments	Is it accurate?

Table 1: Ensuring data integrity through ALCOA

Research (CDER), one of FDA's biggest concerns is integrity of electronic data. Three of ten recent audits revealed data of highly questionable reliability that are currently under review at CDER. Additionally, the number of FDA warning letters pertaining to data integrity has grown exponentially, as FDA puts more focus on data integrity during inspections.

The FDA plans to continue to increase their focus on data integrity issues with:

1. Specialized training of investigational staff on uncovering data integrity, data manipulation, and fraud
2. Greater focus on data integrity and fraud
3. The agency's commitment to follow up on leads or information regarding data manipulation and fraud

Mr. Rivera also gave recommendations to the industry:

1. Train employees on proper handling and reporting of data
2. Assure the reliability of data reported in applications and manufacturing records

How do you achieve data integrity?

Data integrity issues are paramount to ensuring the validity of the data and their analyses. When data are altered in an electronic record system, the original data must remain visible within the system. The number of users who can alter the data must be limited. There must be an automatic audit trail that logs in the date, time, and source of every entry, decision, or change in the data that cannot be controlled by the user. Additionally, the system must be tested and validated.

The following are important record characteristics to achieve data integrity:

1. Retrievable and identifiable data
2. Data must be attributable to a specific subject
3. Audit trails identifying who altered the data, why it was altered, and when
4. Ability to reconstruct the trial

Could you define and provide examples of systems that are critical to data integrity?

For Part 11, data integrity is related to the trustworthiness of the e-records generated/managed by critical systems. The FDA is most concerned about systems that are involved with product distribution, product approval, manufacturing, and quality assurance because these systems pose the most risk in terms of product quality and/or public safety.

Shweta Nair: Which organizations does Part 11 apply to?

Angela Bazigos: Part 11 applies to drug organizations, biotech companies, medical device organizations, CROs, and several other FDA-regulated industries (such as food and beverage manufacturing). Additionally, some organizations that are not FDA-regulated may choose to use Part 11 as a guide to assure that they are utilizing good processes for managing their electronic training records and other documents.

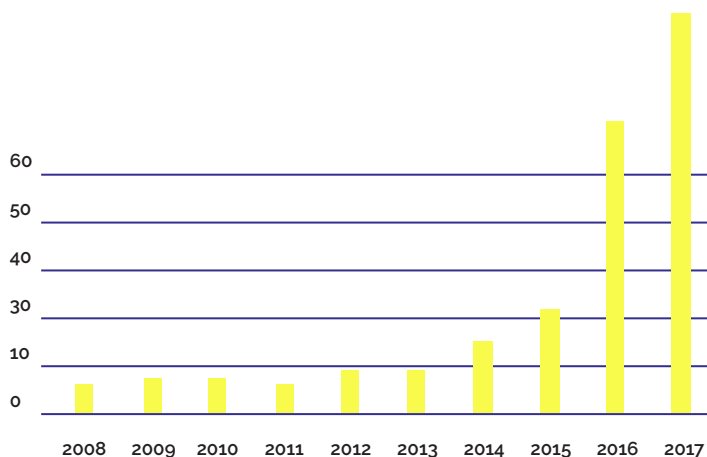


Figure 1: Data integrity associated warning letters, CY2008-CY2017

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

The ramifications include a number of areas:

1. Evaluation of the regulatory impact and the scope of the system. Is it an e-record, e-signature, etc.? The rule includes all records that are generated, stored, or reported, such as attendance records, test scores, and many others
2. Certification to the FDA that a company considers e-signatures to be the legally binding equivalent of traditional handwritten signatures
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. Costs and staffing for all items mentioned above

What is the difference between 21 CFR Part 11 and EU Annex 11?

The relationship between FDA's Part 11 (21 CFR Part 11) and the EU's Annex 11 (EudraLex rules governing medicinal products in the EU, Volume 4, GMP, medicinal products for human and veterinary use) diverges in philosophy. Both documents cover the same topic: the use of computerized systems in regulated activities. However, the approach of Part 11 is to make clear there are requirements to be met in order to conform to regulations. The emphasis is on activities and reporting.

In contrast, the approach of Annex 11 is to make clear how to conform to its rules. Annex 11 is a detailed guide to the areas of compliance that need documentation. A significant difference is the approach to risk management. Annex 11 points to risk assessment as the start of compliance activities. Part 11 differentiates security for open and closed systems, with extra security measures for open systems but without reference to risk or criticality. The aggregate of these differences is represented visually with the point-to-point comparison matrix shown in Table 2.

What records does Part 11 apply to?

The regulation applies to all aspects of the research, clinical study, maintenance, manufacturing, and distribution of medical products. It covers:

- Required records that are maintained in electronic format in place of paper format
- Required records that are maintained in electronic format in addition to paper format, and that are relied on to perform regulated activities
- Records submitted to FDA in electronic format
- E-signatures that are intended to be the equivalent of hand-written signatures

What is the difference between a closed and open system?

The agency agrees that the most important factor in classifying a system as closed or open is whether the persons responsible for the content of the e-records control the access to the system containing those records.

A closed system refers to an environment in which system access is controlled by those persons responsible for the content of e-records that are in the system (e.g., inside the company's firewall). An open system denotes an environment in which system access is not controlled by those persons who are responsible for the content of e-records that are in the system (e.g., outside the company's firewall). If those persons do not control such access, then the system is open because the records may be read, modified, or compromised by others to the possible detriment of the persons responsible for record content. Hence, those responsible for the records would need to take appropriate additional measures in an open system to protect records from being read, modified, destroyed, or otherwise compromised by unauthorized and potentially unknown parties.

What is an e-signature? If you have e-signatures, do you have to comply with e-record requirements?

According to the FDA, "Electronic signature means a computer data compilation of any symbol or series of symbols executed,

- FDA-483
- Warning letters
- Import alerts
- Withheld product approvals
- Cancellation of government contracts
- Product recalls
- Seizure
- Consent decree of permanent injunction
- Civil money penalties
- Suspension or revocation of licences



- Prosecution (including indictments and temporary or permanent debarment, if found guilty)
- Damage to a company's reputation
- Loss of sales
- Loss of jobs
- Loss of share value
- Closing or taking over company

Figure 2 What happens if an organization does not comply with data integrity?

adopted, or authorized by an individual to be the legally binding equivalent of the individual's handwritten signature". Certain signatures are required, and if they are executed electronically, then compliance is needed. Use of e-signatures implies that a system is an e-record system, and must be in compliance with all provisions of 21 CFR Part 11.

What is the definition of hybrid system? Could you give an example of one?

A 'hybrid system' is defined as an environment consisting of both electronic and paper-based records (frequently characterized by handwritten signatures executed on paper). A very common example of a hybrid system is one in which the system user generates an e-record using a computer-based system (e-batch records, analytical instruments, etc.) and is then required to sign that record as per the predicate rules (GLP, GMP, GCP). However, the system does not have an e-signature option, so the user has to print out the report and sign the paper copy. Now the user has an e-record and a paper/handwritten signature. The system has an electronic and a paper component, hence the term, hybrid.

If using a hybrid system approach to e-signatures, how do you link the handwritten signature to the e-record?

Since Part 11 does not require that e-records be signed using e-signatures, e-records may be signed with handwritten signatures. If the handwritten signature is applied to a piece of paper, it must link to the e-record. The FDA will publish guidance on how to achieve this link in the future, but for now it is suggested that you include in the paper as much information as possible to accurately identify the unique electronic record (e.g., at least file name, size in bytes, creation date, and a hash or checksum value). However, the master record is still the e-record. Thus, signing a printout of an e-record does not exempt the record from Part 11 compliance.

What is FDA's view on date and time? Is it not mandatory that it is local?

The agency has reconsidered their position on local date and time stamp requirements. The FDA guidance states, "You should implement time stamps with a clear understanding of what time zone reference you use. Systems documentation

	Annex 11	Part 11
Scope/ Principle	Computerized systems as part of GMP regulated activities. Application should be validated. IT infrastructure should be qualified	E-records and e-signatures as used for all FDA regulated activities
Focus	Risk-based quality management of computerized systems	Using e-records and signatures in open and closed computer systems
Objective	Using a computerized system should ensure the same product quality and quality assurance as manual systems with no increase in overall risk	E-records and e-signatures should be as trustworthy and reliable as paper records and handwritten signatures

Table 2: High level mapping of EU Annex: 11 vs 21 CFR 11

should explain time zone references as well as zone acronyms or other naming conventions".

When does an audit trail begin? Should execution of a signature be audit trailed?

Audit trail initiation requirements differ for data vs textual materials. For data, if you are generating, retaining, importing, or exporting any electronic data, the audit trail begins from the instant the data hit the durable media. For textual documents, if the document is subject to approval and review, the audit trail begins upon approval and release of the document. Additionally, execution of a signature must be audit trailed.

What type of reporting capability on audit trail data should be supported?

According to Part 11 §11.10 (e), audit trails must be secure, computer-generated, and time stamped to independently record the date and time of operator entries and actions that create, modify, or delete e-records. Such audit trail documentation shall be retained for a period at least as long as that required for the subject e-records and shall be available for agency review and copying. Audit trails should say who did what to your records and when – why for GLP. Part 11 does not specify the format for audit trails. This should be discussed in a forthcoming FDA guidance document for Part 11 audit trails.

What must a vendor do to claim that their hardware and software are 'compliant' with 21 CFR Part 11?

No vendor can claim that their software products are certified Part 11 compliant. A vendor, instead, can say that they have all of the technical controls for 21 CFR Part 11 compliance built into their product, but remember, it is the responsibility of the user to implement the procedural and administrative controls (both correctly and consistently) along with using products with the correct technical controls for overall Part 11 compliance.

References

1. Visit: www.fda.gov/regulatory-information/search-fda-guidance-documents/part-11-electronic-records-electronic-signatures-scope-and-application
2. Visit: www.eduquest.net/Advisories/Comparison%20of%20FDA%20Part%2011%20and%20EU%20Annex%2011.pdf
3. Visit: www.mastercontrol.com/gxp-lifeline/annex-11-21-cfr-part-11-comparison
4. Visit: www.pragmatyxs.com/solutions/compliance/cfr-part-11-title-21-fda
5. Visit: www.labcompliance.com/solutions/expert_advice/part11/fda_inspections_2004-2007.aspx#G-330
6. Visit: www.socra.org/assets/SoCRA-Source/200302ERES-Compliance.pdf
7. Visit: www.elearninglearning.com/taurus/media/elearning/whitepapers/NetDimensionsbrief-21-cfr-part-11-faq-ltr.pdf
8. Visit: www.pharmaceuticalonline.com/doc/an-analysis-of-fda-warning-letters-on-data-integrity-0003
9. Visit: www.pda.org/docs/default-source/website-document-library/chapters/presentations/brazil/pharma-trends-day-1/data-integrity-case-studies.pdf?sfvrsn=6

About the authors



Angela Bazigos is the CEO of Touchstone Technologies Silicon Valley, a firm dedicated to providing expert compliance consulting and support services to pharma, biotech, medical devices, CMOs, and CROs. Angela is a co-author and prototype contributor of 21 CFR Part 11 guidance with the FDA. She continues to collaborate with the FDA on new guidance documents.



Shweta Nair is the Senior Product Manager, Biotechnology portfolio, at Advanced Instruments, a manufacturer of scientific analyzers that serves the biotech and pharma industries. The company recently launched a portfolio of osmometers that include data integrity features in support of 21 CFR Part 11 and EU Annex 11 compliance.



Two Technology Way / 781-320-9000
Norwood, Massachusetts 02062, USA
800-225-4034 Fax: 781-320-8181
aicompanies.com

For more information on osmometers that support 21 CFR Part 11, please visit
<https://www.aicompanies.com/biotech-solutions/>

Advanced Instruments certifies that the technical features needed for 21 CFR Part 11 and EU Annex 11 compliance are built into OsmoTECH® and OsmoTECH PRO osmometers. It is your responsibility to implement the necessary controls in your laboratory to comply with 21 CFR Part 11 and EU Annex 11 requirements.

© 2019 Advanced Instruments. OsmoTECH is a trademark of Advanced Instruments. All other trademarks are the property of their respective companies.

MP00088 Revo PCN01207