Version 3
Issue date
Jan 25

APIC
ACTIVE PHARMACEUTICAL INGREDIENTS COMMITTEE

Data Integrity

Frequently Asked Questions (FAQ)

Data Integrity

Frequently asked questions (FAQ)

1. Introduction

This document contains a collection of frequently asked questions that have been submitted by the industry to the DI taskforce. The intention of this documents is that this is a living document that will be updated as new questions are opposed to the group.

Questions to the taskforce can be submitted by using this link: Contact - APIC (cefic.org)

Revision History		
Version	**Changes**	**Date**
1.0	New Document	April 2023
2.0	Added additional questions (highlighted in red); added chapters and questions numbering	January 2025
3.0	Added question and answer on blank forms (highlighted in red)	October 2025

Contents

2. Digital and electronic signatures:

Q1: What is the difference between a digital and an e-signature?

A: A digital signature is attached to an electronic file and not maintained within an electronic system and stays with the data and moves with the data. The signature can be verified by the recipient.
An e-signature is executed and maintained within a validated electronic system and stays in the electronic system. The e-signature can only be verified in the source system.

Q2: What is the best practice to handle hybrid signature?
(Hybrid signature is mixing handwritten or 'wet' signatures and digital signatures/e-signature on the same document)

A: It is the preference to sign off documents fully wet or fully digital. Hybrid signature should be more exceptional if there are no other options.
In that case the handwritten signature(s) must be applied first and afterwards the document can be prepared for digital signature(s). In that way the metadata for the digital signature(s)/e-signature(s) can be maintained. The fully signed electronic document is the official GXP document. (a printout doesn't contain the metadata and verification of digital signatures/e-signatures can't be done)
The wet or a true copy of the wet signature and e-signed copy must be kept as a linked document in a secure, validated for intended use, environment, in line with the company's record management policy.

Q3: Is it acceptable to use a scanned image of a wet signed document as GXP? (internal use)

A: It is only acceptable if the scanned image is a verified true copy of the original wet signed record and allowed by your local, legal and regulatory requirements. The wet or a true copy of the wet signature must be retrievable, reproducible and unaltered for the retention period of the record.

Q4: How do I need to handle a document with a scanned image of a wet signed document that I also need to sign? (external use, e.g. with third parties, working on different locations)

A: This document can be used if the party who's sending this scanned document has an established true copy process in place and the scanned document is already verified and attested as a true copy. The sender should have and an established document retention policy in line with your expectations.

Q5: How do we handle digitally signed documents in an electronic document management system? (e.g. loading an Adobe digitally signed document into your document management systems without loosing the digital signature certificate)

A: The document management system should be validated for this intended use, verifying that the digital signature is maintained in the system and that it is possible to retrieve it when necessary. This process should be defined and documented.

If it is not possible to maintain this digital signature in the system, the digitally signed document should be stored in a secure validated environment.

3. Password management:

Q1: When I logged into a system, do I need to re-authenticate myself for every data entry?

A: No, it depends upon the criticality of the data/action. This criticality should be based upon process mapping and a risk assessment as explained in the guide. Criticality of the data and/or responsibility associated with the action should be taken into account when evaluating electronic signature requirements.

Q2: What are the requirements for e-signature components?

A: This practice is described in 21CFR11, chapter 11.200 'e-signature and components':

(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 (= user ID and password or biometrics); 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.

(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

Q3: Is the storage of passwords in the internet browser allowed for GXP applications?

A: No, ideally this feature should be deactivated in all browsers used for GXP applications.

4. Access management:

Q1: Can I use generic accounts for 3rd party support employees? (e.g. lab technicians, on-line support SAP)

A: No. The account should be attributable to the person executing the actions and there should be processes and systems in place to manage this.

Q2: Can we extend the time of a user session before this is automatically locked for inactivity because of a HSE (health-safety-environment) concern? (e.g people need to interact in case of emergency in a DCS-distributed control system in production)

A: The inactive time of a user session should be managed by the user locking their computer station when they move away for an extend period of time to prevent unauthorised actions been taken by other persons. The automatic lock is a security measure. A reasonable amount of time should be supported by a risk assessment.

This type of HSE concern should be managed independently of the GXP system with an emergency stop button as an example. If this is approach is not feasible, the computerized system should be designed as such that a fast intervention is possible. It is best practice for a system like a DCS to be configured in such a way that the screen does not completely goes into operating system lock and actions can be taken by clicking on the valve or object and entering a password to confirm the action.

5. Record life cycle management:

Q1: How to protect critical paper records? Is it necessary to scan all records or is physical protection (fire protected cabinets, location of the paper record archive(s)) sufficient?

A: Records should be protected and retrievable for the appropriate retention period. There is no need to scan under the condition that the documents are stored in a safe and secure environment.

Q2: Is it allowed to replace a physical paper archive if your scan your records? Can the paper records be destroyed afterwards?

A: In practice this is possible if the digital copy is a true copy, however you need to comply with local legal and regulatory requirements to decide if you can destroy the paper records or not.

Q3: If hardware and/or software packages are not supported anymore (Windows updates, application software), is it possible to print out the electronic data or do you need to keep the 'old' systems up and running? (with the risk that you're not able to see the electronic data anymore in case of soft and hardware errors)

A: A print-out is only allowed if it is a true copy with all raw data and meta-data. In practice this is very difficult. The first option is to migrate those data to an appropriate system. Another option is to create a virtual environment where you can run the legacy system in a validated state and where all data can be retrieved.

Q4: If approved forms and templates that are part of a procedure are printed out of an electronic system just before use (e.g. training attendees sheets, checklists, housekeeping checklists, …), is it necessary to have controlled issuance of those templates and forms, and to have a systematic audit trail review of those printing activities?

A: The term "FORM" should be used to refer to the controlled copies (blank forms) obtained from approved TEMPLATES stored as paper or through and electronic system.

If the form is printed and data is collected on paper, various provisions are to be taken to assure proper adherence to ALCOA+ principles; paper may not fully effective to prevent falsification. When the data are collected with electronic means, the controls has to be provided by the electronic system itself.

The criticality of forms should be defined, and controls should be based on criticality

A. Different levels of controls can be put in place to discourage falsification. For critical forms means to increase data integrity assurance include control the issuance of those documents, including controlled access for printing, reasoning for reprint, authentication of the original copy (e.g with stamps or signatures), control of distribution, binding in logbooks, second person review, reconciliation also through the audit trail review.

   Not all the above controls have to be put in place for all forms, in order to put the highest effort on most critical forms.

B. The criticality of forms can be defined based on the criticality of data they will record (i.e if they are used for production and release activities or for supporting processes), but also base on the probability that a falsification takes place (e.g. a printed form that is shared between different departments and personnel or printed by an independent department is less prone

to falsification than a form that is printed and used by the same department and by a limited number of people); the level of redundancy of the data that the form will capture (i.e. if it captures primary raw data or it summarizes or refer to data recorded also elsewhere) can also be considered in the form criticality assessment.

As per the example in the question, for the lower criticality blank forms (e.g. training attendees sheets), controlled printing only can be applied; for checklists, the control strategy should be designed based on the criticality of the data being collected.

Finally, forms should carefully designed to avoid potentials for data integrity issue including:

- Clearly defined fields to record data that allows the operator to understand how the data should be entered including specification limits and/or exempla
- Instructions on what to do if data do not fit the expectations
- Logic time sequencing
- Company Recognizable and standardized pattern/frame
- Archiving rules

6. Various:

Q1: How to deal with analytical testing where data is a visual check? (appearance, insoluble matter testing, TLC, …)

A: See table 1 ‘Minimum system requirements based on categories’ in the guide.

Q2: Is it allowed to use a personal notes in a lab or production environment? (personal notes: containing training info/attention points you documented during training or during discussions with colleagues, …)

A: No. All information needed to perform activities in a GXP environment should be described in controlled procedures and work instructions. Any data supporting a GXP batch must be controlled, maintained and reviewed.