JUMO LOGOSCREEN fd

Secure Data Management and FDA-Compliant Measured Data Recording

White Paper 706585
21 CFR Part 11

JUMO

2013-02-08/00597365

Contents

Contents

1.1 Introduction

The production of products in the pharmaceutical and food industry as well as related industrial sectors is subject to mandatory record keeping requirements.
In the past, people used paper-based recorders for recording process data. To protect consumers, the parameter values recorded onpaper were archived for decades to ensure complete proof of production and traceability in the event of deviations.
The introduction of paperless process recording technology triggered a shift from paper-based to paperless recorders.
The **Food & Drug Administration (FDA)** in the USA passed Title 21 CFR Part 11 (Code of Federal Regulations) in 1997 regulating the proper and clearly traceable recording of electronic process data.
This law defines the requirements for **Electronic Records and Electronic Signatures**, i.e. the paperless logging of production processes as well as electronic signatures that correspond to a handwritten signature.
Compliance with the requirements of Title 21 CFR Part 11 now forms the foundation for the global acceptance of products from the pharmaceutical and food industry.
Section 3 of this white paper provides the user with information on the measures taken to meet the requirements for each section of the legal text.

1.2 Implementation of Title 21 CFR Part 11

With the LOGOSCREEN fd paperless recorder and the corresponding PC software component setup program, PC Evaluation Software, PCA Communication Software, PC security manager software, and PC audit trail manager software and its functional features, JUMO meets the FDA requirements of Title 21 CFR Part 11 in terms of electronic records and electronic signatures.

1.3 LOGOSCREEN fd system components

The LOGOSCREEN fd paperless recorder, in conjunction with its system components, meets the definition of a closed system according to Title 21 CFR Part 11.

1 General information

1.4 PC software components

1.4.1 Setup program

- Configures the recorder via a dialog-controlled program
- Archives the configuration data on storage media and outputs it via a printer

1.4.2 PC Evaluation Software for the process data (PCA3000)

- Visualization, archiving, and evaluation of saved data

1.4.3 PCA Communication Software (PCC)

- Manually or automatically reads out the recorder data via the serial interface, e.g. every day at 11:00 p.m.
- Also extracts the data by remote control via a modem

1.4.4 PC security manager software (PCS)

- Manages the PC and recorder user list
- Checks user access to the PC programs and issues or rejects authorization to access the system
- Ensures the authenticity of the electronic signature

1.4.5 Recorder security manager software

- Saves the user list in the recorder
- Checks user access to the recorder and issues or rejects authorization
- Ensures the authenticity of the electronic signature

1.4.6 PC audit trail manager software (PCAT)

- Records user actions with a time stamp, user name, details, and the reason for the change
- Saves and confirms all actions performed by the user

2.1 Requirements

The following explanations are based on the assumption that the reader has knowledge of the basic requirements of Title 21 CFR Part 11.

Section	Requirements: Subpart B: Electronic Records
§ 11.10 Controls for closed systems	
Personnel who use closed systems to create, modify, maintain, or transmit electronic records shall 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. Such procedures and controls shall include the following:	
a)	Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records. **Requirement fulfilled!** ✔ The system, which comprises paperless recorders (hereinafter referred to as recorders) and the corresponding PC programs, is validated to ensure accuracy, reliability, and continuous scheduled services. ✔ It is ensured that invalid or unchanged documents (or manipulation attempts) are identified, documented in the audit trail, and not available for evaluation.
b)	The ability to generate accurate and complete copies of records in both human readable and electronic form suitable for inspection, review, and copying by the agency. Personnel should contact the agency if they have any questions regarding the ability of the agency to perform such a review and copy the electronic records. **Requirement fulfilled!** ✔ All data is stored in a proprietary, non-disclosed binary format secured via checksum algorithms. ✔ The process data is displayed in a readable format on the recorder or PC. ✔ PC Evaluation Software is available for displaying the data on the PC. This software allows you to visualize, copy, or print all saved data.

2 Requirement assessment

Section	Requirements: Subpart B: Electronic Records
§ 11.10 Controls for closed systems	
c)	Protection of records to enable their accurate and ready retrieval throughout the record retention period. **Requirement fulfilled!** ✔ The data is stored in the internal recorder memory. ✔ The internal recorder memory does not serve to transport data. ✔ The data archived in the internal memory can be extracted via an interface (serial or Ethernet), a CompactFlash card, or a USB stick by authorized personnel and archived in the PC. ✔ Access to the interface is protected by a user ID and password, which electronically monitors access to the CompactFlash card or the USB stick. ✔ A proprietary, non-disclosed binary format secured via checksum algorithms ensures that the data cannot be tampered with. ✔ The data provided on the CompactFlash card or the USB stick is saved in a PC system for archiving and evaluation.
d)	Limiting system access to authorized individuals. **Requirement fulfilled!** ✔ System access is limited by assigning various rights to authorized people. ✔ Each user must log into the system using his user ID and password. ✔ The administrator assigns rights that are checked by the PC security manager software each time the system is accessed. ✔ Only the administrator can change user rights. ✔ Data that has already been recorded and archived also remains unmodified when rights are changed.

Section	Requirements: Subpart B: Electronic Records
§ 11.10 Controls for closed systems	
e)	Use of 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. **Requirement fulfilled!** ✔ The audit trail software is part of the device software and the corresponding PC programs (separate audit trails). The audit trail is automatically generated and cannot be configured or switched off. ✔ It is ensured that all actions triggered by the operating personnel are automatically recorded and archived with the date and time. ✔ Audit trail data cannot be changed or deleted in the device. ✔ Personnel authorized to do so can add text or comments after entering a user ID and password. ✔ All data saved in the recorder's audit trail is imported along with the process data into the PC Evaluation Software and is available there. ✔ Audit trail data can be made available for review at any time using the PC Evaluation Software.
f)	Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate. **Requirement fulfilled!** ✔ The order of steps, such as the batch reporting, is defined. This allows you to configure whether an electronic signature must be provided for batch reporting. If an electronic signature is to be required, for example, it is not authorized for ongoing batch reports (in contrast to the completed batch reports). ✔ Another case: the recorder can be configured so that when the user logs off, he is requested to provide an electronic signature for the authorized (logged on) time period.

2 Requirement assessment

Section	Requirements: Subpart B: Electronic Records
§ 11.10 Controls for closed systems	
g)	Use of 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. **Requirement fulfilled!** ✔ The access rights to the system are assigned by the administrator. ✔ These access rights are checked and managed by the security manager software in the recorder or by the PC security manager software. ✔ Only personnel with administrator rights can create or delete user lists. ✔ To access the system, a user must always log on using a unique user ID and password. ✔ The administrator can limit the time period in which a password can be used. After this time period expires, the user must enter a new password or he loses access authorization.
h)	Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction. **Requirement fulfilled!** ✔ The recorder can only be configured or operated by personnel authorized for this. This also applies to connecting sensor lines or interface cables to the secured rear panel of the recorder. ✔ Data saved in the recorder is automatically linked with a device ID number (production number) that is always unique and can therefore be uniquely assigned.

Section	Requirements: Subpart B: Electronic Records
§ 11.10 Controls for closed systems	
i)	Determination that personnel who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks. **Requirement fulfilled!** ✔ All personnel involved in the development of the LOGOSCREEN fd and the corresponding PC software have been trained in the content and requirements of Title 21 CFR Part 11. ✔ LOGOSCREEN fd users are also offered corresponding training courses.
j)	The establishment of, and adherence to, written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures in order to deter record and signature falsification. **Not applicable!** The user is responsible for this.
k)	Use of 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 system documentation. **Not applicable!** The user is responsible for this.

2 Requirement assessment

Section	Requirements: Subpart B: Electronic Records
§ 11.30 Controls for open systems	
	Personnel 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 in § 11.10, 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. **Not applicable!** The LOGOSCREEN fd and the corresponding PC programs represent a closed system.

Section	Requirements: Subpart B: Electronic Records
§ 11.50 Signature manifestations	
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.  ✔ The electronic signature assigned to the relevant records is displayed on the recorder or via the PC Evaluation Software in readable form. The electronic signature always includes the names of the signer in block letters, date and time down to the second when the signature was made and the meaning of the signature. Batches, time periods, or comments can be linked with electronic signatures. No data can be tampered with, since the recorder and the corresponding PC programs generate the time themselves. The user must have specific authorization to change the recorder time. Each change is documented in the audit trail in a manner that cannot be deleted.

2 Requirement assessment

Section	Requirements: Subpart B: Electronic Records
§ 11.50 Signature manifestations	
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). **Requirement fulfilled!** ✔ The electronic signature is part of the recorder raw data. ✔ The recorder raw data comprises the electronic record, electronic signature, audit trail data, and the checksum. The format is generated in the recorder and cannot be modified for transmitting the data to and saving it on the PC. ✔ The recorder raw data, including the electronic signature is recorded in a proprietary, non-disclosed binary format secured by checksum algorithms. The recorder raw data including the linked electronic signatures that cannot be deleted are tamper-proof. ✔ The electronic signature is added to the readable version of the electronic documents (display or printout) that is derived from the raw data. ✔ The printed copy or electronic copy (PDF format) includes a note indicating that the display format is derived from the recorder raw data.

Section	Requirements: Subpart B: Electronic Records
§ 11.70 Signature/record linking	
	Electronic signatures and handwritten signatures executed for 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. **Requirement fulfilled!** ✔ The recorder raw data, including the electronic signature is recorded in a proprietary, non-disclosed binary format secured by checksum algorithms. ✔ The recorder raw data including the linked electronic signatures that cannot be deleted are tamper-proof. ✔ Security manager software functions are set up on the recorder and the corresponding PC programs with the following tasks that cannot be changed: PC security manager software: • Generates and manages the PC and recorder user list • Checks user access to the PC programs and issues or rejects authorization • Ensures the authenticity of the electronic signature Security manager software (recorder): • Saves the user list in the recorder • Checks user access to the recorder and issues or rejects authorization • Ensures the authenticity of the electronic signature ✔ Access to the recorder or the corresponding PC programs defined by the security manager software ensures that an individual cannot falsify or copy an electronic signature. ✔ The recorder and the corresponding PC programs do not allow the electronic signature to be changed or deleted. The recorder and the corresponding PC programs detect attempts to change or delete an electronic signature and display them. ✔ The event is documented in the audit trail in a manner that cannot be deleted.

2 Requirement assessment

Section	Requirements: Subpart C: Electronic Signatures
§ 11.100 General requirements	
a)	Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else. **Requirement fulfilled!** ✔ The PC security manager software allows the administrator to set up the users on the recorder, their rights, their initial password, and their password restrictions and transmit them encrypted and summarized in a user list and to the recorder. ✔ The PC security manager software ensures the uniqueness of the combination consisting of the user name and his user ID for each user entered in the user list. ✔ Although user rights can be revoked (by the administrator), they cannot be removed from the user list. ✔ The recorder security manager software is based on the user list and ensures the authenticity of the electronic signature.
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. **Not applicable!** The system owner is responsible for this.
c)	Personnel 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. **Not applicable!** The system owner is responsible for this.
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. **Not applicable!** The system owner is responsible for this.
2)	Personnel 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. **Not applicable!** The system owner is responsible for this.

Section	Requirements: Subpart C: Electronic Signatures
§ 11.200 Electronic signature components and controls	
a) 1)	Electronic signatures that are not based on biometrics shall: employ at least two distinct identification components, such as an identification code and password.  ✔ The electronic signature can only be performed by a user who is authorized by the administrator and who has been authenticated by the access control (PC security manager software) using a user ID (user name) and the recorder password or the corresponding PC programs.
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.  ✔ In all cases, only one user at a time can be authorized by the recorder or PC security manager software using the rights assigned to him by the administrator. ✔ The electronic signature can only be executed by a user logged into the recorder or the corresponding PC programs and requires full authentication in the initial instance and each repeated instance by the security manager software using the user ID (user name) and password. ✔ Prior to executing the electronic signature, the user is shown the following text: "your signature is legally binding and is the equivalent of your handwritten signature."
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.  ✔ The electronic signature can only be executed by a user authenticated in the recorder or the corresponding PC programs and requires full authentication in the initial instance and each repeated instance by the security manager software using the user ID (user name) and password.

2 Requirement assessment

Section	Requirements: Subpart C: Electronic Signatures
§ 11.200 Electronic signature components and controls	
a) 2) 3)	Electronic signatures that are not based on biometrics shall: 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 it's genuine owner requires collaboration of two or more individuals. **Requirement fulfilled!** ✔ This is ensured by the specified method for creating and managing the user list, which provides the basis for authorizing and authenticating a user. ✔ A user cannot by himself use an electronic signature other than his own. ✔ Each attempt is detected and documented in the audit trail in a manner that cannot be deleted. ✔ Each user uses a password defined according to the preset restrictions. Only the user knows this password. No one can read passwords out of the recorder or using the PC programs, for example.
b)	Electronic signatures based on biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners. **Not applicable!** There are no plans for an electronic signature based on biometrics.

Section	Requirements: Subpart C: Electronic Signatures
§ 11.300 Controls for identification codes/passwords	
Personnel who use electronic signatures based on the 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.  ✔ The PC security manager software allows the administrator to set up the users on the recorder, their rights, and their password restrictions and transmit them encrypted and summarized into a user list and to the recorder. ✔ A device ID number (production number) that is always unique ensures that all data is assigned to a recorder. ✔ The PC and recorder security manager software ensures the uniqueness of each combination consisting of a user ID 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).  ✔ The same high security criteria, which also apply to the electronic records, are used for the user list as a basis for the recorder and PC access controls. ✔ Actions that tamper with the user list are detected. In this case, the user list is disabled and this event is documented in the audit trail in a manner that cannot be deleted. ✔ The recorder and PC security manager software ensures that the restrictions set up by the administrator are checked each time the user list is changed and each time the access controls are checked. This includes the obsolescence of passwords. ✔ The user whose password is outdated is blocked and the event is documented in the audit trail in a manner that cannot be deleted. Only the administrator can reauthorize these users.
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.  ✔ The recorder and the corresponding PC programs do not use any markers, tokens, etc. The security is achieved using the user rights and password restrictions configured by the administrator. This means, for example, an initial password must be configured by the administrator, which the user must immediately change upon initial access so that only he knows the password. In addition, a validity period can be preset for the password. ✔ If the restrictions are not observed, the user's authorization is revoked. ✔ This event is documented in the audit trail in a manner that cannot be deleted.

Section	Requirements: Subpart C: Electronic Signatures
§ 11.300 Controls for identification codes/passwords	
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. **Requirement fulfilled!** ✔ The PC and recorder security manager software prevent unauthorized access. Each attempt is detected and documented in the recorder or PC audit trail in a manner that cannot be deleted.
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. **Not applicable!** The recorder and the corresponding PC software do not use or generate any markers, tokens, etc., which contain user ID or password information.

3 Reference list

[1] Mass & Peither AG
GMP publishing house
Title 21 CFR 210/211 cGMP FOR FINISHED PHARMACEUTICALS
incl. Title 21 CFR 11 electr. records/electr. signatures
with German translation and index

3 Reference list

JUMO GmbH & Co. KG

Street address:
Moritz-Juchheim-Straße 1
36039 Fulda, Germany
Delivery address:
Mackenrodtstraße 14
36039 Fulda, Germany
Postal address:
36035 Fulda, Germany
Phone: +49 661 6003-0
Fax: +49 661 6003-607
E-mail: mail@jumo.net
Internet: www.jumo.net

JUMO Instrument Co. Ltd.

JUMO House
Temple Bank, Riverway
Harlow - Essex CM20 2DY, UK
Phone: +44 1279 63 55 33
Fax: +44 1279 63 52 62
E-mail: sales@jumo.co.uk
Internet: www.jumo.co.uk

JUMO Process Control, Inc.

6733 Myers Road
East Syracuse, NY 13057, USA
Phone: 315-437-5866
1-800-554-5866
Fax: 315-437-5860
E-mail: info.us@jumo.net
Internet: www.jumousa.com