M. K. JUCHHEIM GmbH & Co

Bildschirmschreiber LOGOSCREEN *es*

Konformitätserklärung 21 CFR Part 11

White Paper

Inhalt

Inhalt

1 Allgemeines

1.1 Einleitung

In der pharmazeutischen, der Lebensmittelindustrie und in verwandten Industriezweigen besteht für die Herstellung von Produkten eine Protokollierungspflicht.

Für die Aufzeichnung von Prozessdaten setzte man in der Vergangenheit Registriergeräte auf Papierbasis ein. Zum Schutz des Verbrauchers wurden die auf Papier aufgezeichneten Parameterwerte über Jahrzehnte archiviert, um damit einen lückenlosen Nachweis der Produktion und Nachvollziehbarkeit bei Abweichungen sicher zu stellen.

Mit dem Einzug der papierlosen Prozessschreibertechnik hat sich die Registrierung von Papier auf Bildschirmschreiber verlagert.

Für die ordnungsgemäße und eindeutig nachvollziehbare Aufzeichnung der elektronischen Prozessdaten hat die amerikanische Gesundheitsbehörde

"Food & Drug Administration (FDA)"

1997 den **21 CFR Part 11** (Code of Federal Regulations) verabschiedet.

In diesem Gesetz werden die Anforderungen an **Electronic Records & Electronic Signature**, also die papierlose Protokollierung von Produktionsabläufen sowie die der elektronischen Unterschrift, welche der handgeschriebenen Unterschrift entspricht, definiert.

Die Einhaltung der Forderungen des 21 CFR Part 11 bildet mittlerweile die Grundlage für die weltweite Akzeptanz von Produkten der Pharma- und Lebensmittelindustrie.

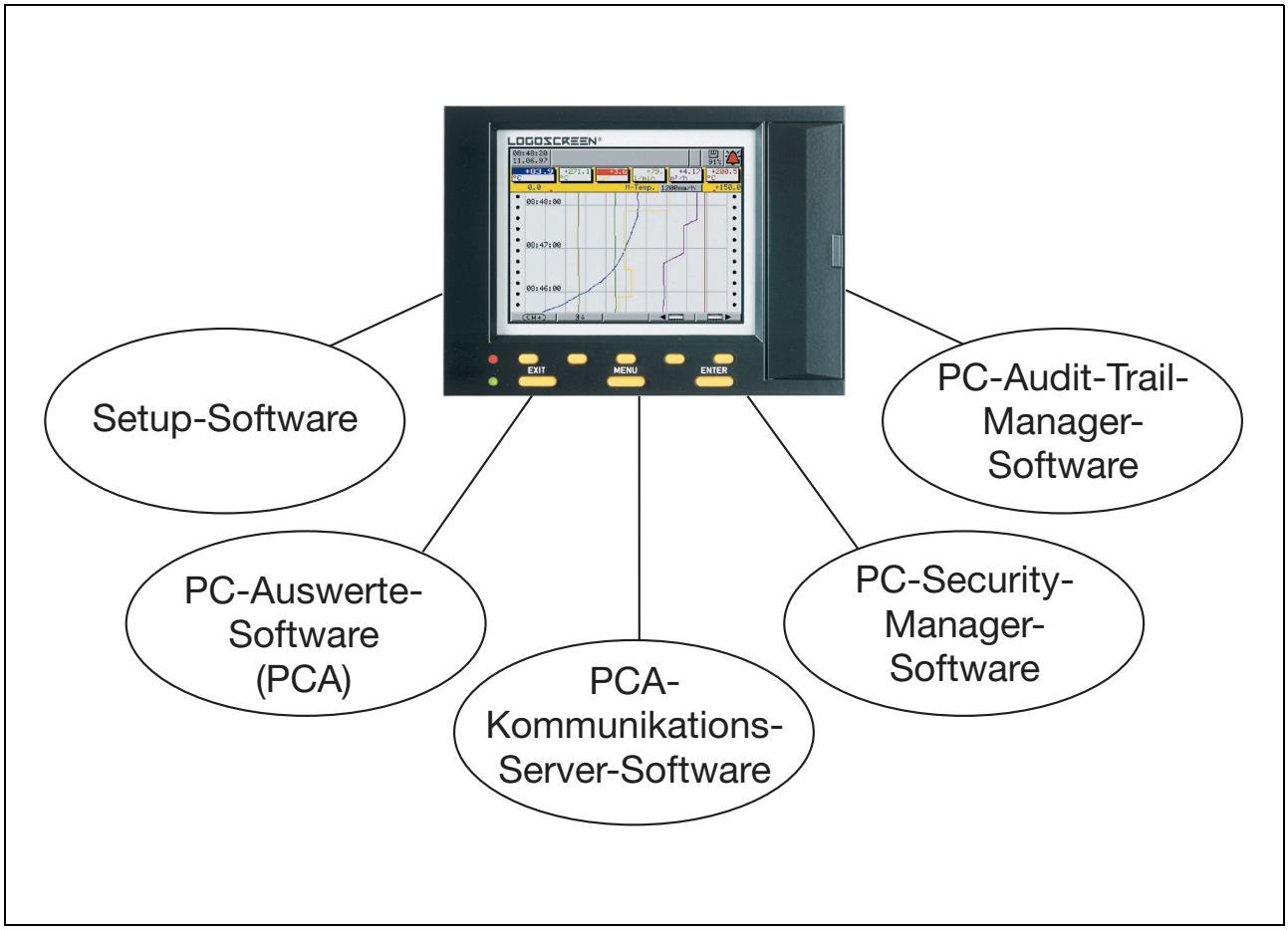
Dieses „White Paper“ liefert dem Anwender in Kapitel 3 zu jedem Abschnitt der Gesetzestexte eine Aussage zur getroffenen Sicherstellung der Forderung.

1.2 Umsetzung der 21 CFR Part 11

JUMO erfüllt mit dem neuen Bildschirmschreiber **LOGOSCREEN *es*** und den zugehörigen PC-Softwarekomponenten Setup, PCA, PCA-Kommunikationsserver, Security-Manager-Software und Audit-Trail-Manager-Software und dessen Funktionseigenschaften die FDA-Forderungen der 21 CFR Part 11 in Bezug auf Electronic Records (elektronische Aufzeichnung) und Electronic Signature (elektronische Unterschrift).

1.3 Die Systemkomponenten des LOGOSCREEN *es*

Der Bildschirmschreiber **LOGOSCREEN *es*** stellt mit seinen Systemkomponenten im Sinne des 21 CFR Part 11 ein geschlossenes System dar.



1.4 Die PC-Software-Komponenten

1.4.1 Setup-Software (zum Konfigurieren des Recorders)

- dialoggesteuertes Programm zum Konfigurieren des Recorders,
- die Konfigurationsdaten können auf Datenträger archiviert und über einen Drucker ausgegeben werden.

1.4.2 PC-Auswerte-Software für die Prozessdaten (PCA)

- Visualisierung, Archivierung und Auswertung der gespeicherten Daten.

1.4.3 PCA-Kommunikations-Server-Software (ermöglicht das Auslesen von Daten)

- mit ihm können die Recorderdaten über die serielle Schnittstelle ausgelesen werden,
- das Auslesen ist manuell oder automatisiert möglich, z. B. jeden Tag um 23.00 Uhr,
- über Modem können die Daten auch ferngesteuert ausgelesen werden.

1.4.4 PC-Security-Manager-Software (kontrolliert den Zugang zum System)

- verwaltet die Benutzerliste von PC und Recorder,
- prüft den Zugang von Nutzern zu den PC-Programmen und erteilt oder verweigert die Freigabe zum System,
- stellt die Authentizität der elektronischen Unterschrift sicher.

1.4.5 Recorder-Security-Manager-Software (kontrolliert den Zugang zum Recorder)

- speichert die Benutzerliste im Recorder,
- prüft den Zugang zum Recorder und erteilt oder verweigert die Freigabe,
- stellt die Authentizität der elektronischen Unterschrift sicher.

1.4.6 PC-Audit-Trail-Manager-Software (erfasst und speichert alle Aktionen)

- erfasst Bedienereingriffe mit Zeitstempel, Bedienername, Details und Grund der Änderung,
- speichert und bestätigt alle Aktionen, die der Nutzer ausführt.

2 Bewertung der Forderung

Die folgenden Ausführungen basieren auf der Annahme, dass der Leser über Kenntnisse der grundlegenden Forderungen der 21 CFR Part 11 verfügt.

Absatz	**Anforderungen:** ***Subpart B: Electronic Records* (Teil B: Elektronische Dokumente)**
§ 11.10 *Controls for closed systems* (Kontrollen für geschlossene Systeme)	
(a)	*Validation of systems to ensure accuracy, reliability, consistend intended performance, and the ability to discern invalid or altered records.* Validierung von Systemen, um Genauigkeit, Zuverlässigkeit, kontinuierliche, planmäßig Leistung und die Fähigkeit, ungültige oder veränderte Dokumente zu entdecken, zu gewährleisten. Anforderung erfüllt! ✔ Das System, bestehend aus Bildschirmschreiber (nachfolgend Recorder genannt) und den dazugehörigen PC-Programmen, wird validiert, um Genauigkeit, Zuverlässigkeit und kontinuierliche, planmäßige Leistungen zu gewährleisten. ✔ Es ist sichergestellt, dass ungültige oder veränderte Dokumente (bzw. Manipulationsversuche) erkannt, im Audit-Trail dokumentiert werden und nicht zur Auswertung zur Verfügung stehen.
(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. Persons should contact the agency if there are any questions regarding the ability of the agency to perform such review and copying of the electronic records.* Die Möglichkeit, akkurate und vollständige Kopien der Dokumente sowohl in lesbarer als auch in elektronischer Form zum Zwecke von Inspektionen, Überprüfungen und dem Kopieren durch die Behörde zu erzeugen. Die Behörde soll kontaktiert werden, wenn Zweifel darüber bestehen, ob sie derartige Überprüfungen vornehmen und die elektronischen Dokumente kopieren kann. Anforderung erfüllt! ✔ Alle Daten werden in einem proprietären, nicht offen gelegten, über Prüfsummenalgorithmen abgesicherten Binärformat gespeichert. ✔ Die Prozessdaten sind am Recorder bzw. am PC lesbar dargestellt. ✔ Für die Darstellung der Daten am PC ist eine JUMO-PC-Auswertesoftware vorhanden, mit der alle gespeicherten Daten visualisiert, kopiert oder ausgedruckt werden können.

2 Bewertung der Forderung

Absatz	Anforderungen: *Subpart B: Electronic Records* (Teil B: Elektronische Dokumente)
§ 11.10 *Controls for closed systems* (Kontrollen für geschlossene Systeme)	
(c)	*Protection of records to enable their accurate and ready retrieval throughout the records retention period.* Schutz der Dokumente, um ein akkurates und jederzeitiges Abrufen während der Aufbewahrungszeit der Dokumente zu ermöglichen. Anforderung erfüllt! ✔ Die Daten werden im internen Speicher des Rechners gespeichert. ✔ Der interne Speicher des Recorders dient nicht zum Datentransport. ✔ Die im internen Speicher archivierten Daten können über eine serielle Schnittstelle oder über eine Compact-Flash-Card von dazu berechtigten Personen ausgelesen und im PC archiviert werden. ✔ Der Zugriff auf die serielle Schnittstelle ist über Benutzer-ID und Passwort geschützt, der Zugriff auf die Compact-Flash-Card ist mechanisch verriegelt und wird elektronisch überwacht. ✔ Die Manipulationssicherheit der Daten ist durch ein proprietäres, nicht offen gelegtes, über Prüfsummenalgorithmen abgesichertes Binärformat sichergestellt. ✔ Die auf der Compact-Flash-Card bereitgestellten Daten werden in einem PC-System zur Archivierung und Auswertung gespeichert.
(d)	*Limiting system access to authorized individuals.* Begrenzung des Systemzugriffs auf befugte Personen. Anforderung erfüllt! ✔ Der Systemzugriff ist durch die Vergabe unterschiedlicher Rechte auf befugte Personen begrenzt. ✔ Jeder Benutzer muss sich durch Benutzer-ID und Passwort im System anmelden. ✔ Durch den Administrator werden Rechte vergeben, die bei jedem Zugriff auf das System durch die Security-Manager-Software geprüft werden. ✔ Das Ändern von Benutzerrechten ist ausschließlich durch den Administrator möglich. ✔ Bereits erfasste und archivierte Daten bleiben auch bei der Änderung von Rechten unverändert.

2 Bewertung der Forderung

Absatz	Anforderungen: *Subpart B: Electronic Records* (Teil B: Elektronische Dokumente)
§ 11.10 *Controls for closed systems* (Kontrollen für geschlossene Systeme)	
(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.* Verwendung sicherer, computergenerierter, mit einem Zeitstempel versehener Audit-Trail, um Datum und Uhrzeit von durch Bedienpersonal vorgenommenen Einträgen und Aktionen, die elektronische Dokumente erstellen, ändern oder löschen, unabhängig aufzeichnen zu können. Änderungen an Dokumenten dürfen zuvor vorgenommene Einträge nicht verdecken. Der Audit-Trail muss über einen Zeitraum aufbewahrt werden, der mindestens dem für die entsprechenden elektronischen Dokumente geforderten entspricht, und soll der Behörde zu Überprüfungszwecken und zum Kopieren zugänglich gemacht werden. Anforderung erfüllt! ✔ Die Audit-Trail-Software ist Bestandteil der Gerätesoftware und der dazugehörenden PC-Programme (getrennte Audit-Trails). Der Audit-Trail wird automatisch generiert und kann nicht konfiguriert oder abgeschaltet werden. ✔ Es ist sichergestellt, dass alle vom Bedienpersonal ausgelösten Aktionen mit Datum und Uhrzeit automatisch erfasst und archiviert werden. ✔ Audit-Trail-Daten können im Gerät nicht geändert oder gelöscht werden. ✔ Das Hinzufügen von Texten / Kommentaren ist durch dafür autorisierte Personen nach Eingabe von Benutzer-ID und Passwort möglich. ✔ Alle im Audit-Trail des Recorders gespeicherten Daten werden zusammen mit den Prozessdaten in die JUMO-PC-Auswertesoftware übernommen und stehen dort zur Verfügung. ✔ Audit-Trail-Daten können über die PC-Auswertesoftware jederzeit zur Überprüfung zugänglich gemacht werden.
(f)	*Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.* Durchführung funktionaler Systemüberprüfungen, um, wo anwendbar, die erlaubte Abfolge von Schritten und Ereignissen umzusetzen. Anforderung erfüllt! ✔ Die Abfolge von Schritten wie z. B. der Chargenprotokollierung ist festgelegt. So kann konfiguriert werden, ob für eine Chargenprotokollierung überhaupt eine elektronische Unterschrift geleistet werden muss. Falls sie erforderlich sein sollte, wird sie beispielsweise für laufende Chargenprotokolle (im Gegensatz zu beendeten Chargenprotokollen) nicht zugelassen. ✔ Ein weiterer Fall: Der Recorder kann so konfiguriert werden, dass der Benutzer beim Ausloggen aufgefordert wird, eine elektronische Unterschrift für den verantwortlichen (eingeloggten) Zeitbereich zu leisten.

2 Bewertung der Forderung

Absatz	Anforderungen: *Subpart B: Electronic Records* (Teil B: Elektronische Dokumente)
§ 11.10 *Controls for closed systems* (Kontrollen für geschlossene Systeme)	
(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.* Durchführung von Befugnisprüfungen, um zu gewährleisten, dass nur befugte Personen das System benutzen, Dokumente elektronisch signieren, Zugriff auf die Eingabe- oder Ausgabegeräte des Betriebs- oder des Computersystems haben, Dokumente ändern oder den entsprechenden Vorgang manuell durchführen können. Anforderung erfüllt! ✔ Die Zugriffsrechte auf das System werden durch den Administrator vorgegeben. ✔ Diese Zugriffsrechte werden durch die Security-Manager-Software im Recorder geprüft bzw. durch die PC-Security-Manager-Software geprüft und verwaltet. ✔ Nur Personen mit „Administrator-Rechten“ können Benutzerlisten anlegen oder löschen. ✔ Vorraussetzung für den Systemzugang eines Benutzers ist immer eine Anmeldung über eine eindeutige Benutzerkennung (Benutzer-ID und Passwort). ✔ Die Nutzung eines Passwortes kann durch den Administrator zeitlich begrenzt werden. Nach Ablauf dieser Zeit muss der Benutzer ein neues Passwort eingeben oder er verliert die Zugriffsberechtigung.
(h)	*Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.* Durchführung von Geräte- (z. B. Terminal-) überprüfungen, um, wo anwendbar, die Gültigkeit der Dateneingabe- oder der Funktionsbefehlsquelle bestimmen zu können. Anforderung erfüllt! ✔ Der Recorder kann nur durch dazu berechtigte Personen konfiguriert oder bedient werden. Das gilt auch für den Anschluss von Sensorleitungen oder Schnittstellenkabeln auf der gesicherten Rückwand des Recorders. ✔ Daten, die im Recorder gespeichert werden, werden automatisch mit einer für alle Zeit einmaligen, eindeutigen Geräte-Identifikationsnummer (Produktionsnummer) verbunden und können so eindeutig zugeordnet werden.

2 Bewertung der Forderung

Absatz	Anforderungen: *Subpart B: Electronic Records* (Teil B: Elektronische Dokumente)
§ 11.10 *Controls for closed systems* (Kontrollen für geschlossene Systeme)	
(i)	*Determination that persons who develop, maintain, or use electronic record / electronic signature systems have the education, training, and experience to perform their assigned tasks.* Feststellung, ob diejenigen, die Systeme für elektronische Dokumente oder Unterschriften entwickeln, pflegen oder verwenden, die für die Aufgaben notwendige Ausbildung und Schulung durchlaufen haben und über die entsprechende Erfahrung verfügen. Anforderung erfüllt! ✔ Alle an der Entwicklung des LOGOSCREEN *es* und der dazugehörigen PC-Software beteiligten Personen wurden bezüglich der Inhalte und Anforderungen der 21 CFR Part 11 geschult. ✔ Entsprechende Schulungen werden auch den Nutzern des LOGOSCREEN *es* angeboten.
(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.* Festlegen und Einhalten von schriftlichen Verfahrensanweisungen, dass einzelne für unter ihrer elektronischen Unterschriften vorgenommene Handlungen verantwortlich gemacht werden, um so Abschreckungsmechanismen für das Fälschen von Dokumenten und Unterschriften zu schaffen. Nicht zutreffend! Liegt in der Verantwortung des Anwenders.
(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 systems documentation.* Einsatz geeigneter Kontrollen über Systemdokumentation, inklusive: (1) Adäquate Kontrollen bei der Verteilung von, dem Zugriff auf und der Verwendung von Dokumentation zur Systembedienung und -wartung. (2) Revisions- und Änderungskontrollverfahren, um so einen Audit-Trail zu erhalten, der die zeitliche Reihenfolge der Entwicklung und Veränderung der Systemdokumentation dokumentiert. Nicht zutreffend! Liegt in der Verantwortung des Anwenders.

2 Bewertung der Forderung

Absatz	Anforderung: *Subpart B: Electronic Records* (Teil B: Elektronische Dokumente)
§ 11.30 *Controls for open systems* (Kontrollen für offene Systeme)	
	Persons 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. Werden offene Systeme zum Erstellen, Ändern, Pflegen oder Übertragen elektronischer Dokumente verwendet, sollen Verfahren und Kontrollen eingerichtet weren, die dafür bestimmt sind, die Authentizität, die Integrität und, falls erforderlich, die Vertraulichkeit der elektronischen Dokumente von der Erstellung bis zum Erhalt sicherzustellen. Derartige Verfahren und Kontrollen müssen, wo anwendbar, die in § 11.10 dargelegten Anforderungen berücksichtigen und weitere Maßnahmen umfassen, so z. B. die Dokumentenverschlüsselung und den Einsatz geeigneter Standards für digitale Unterschriften, um soweit unter den gegebenen Umständen notwendig die Authentizität, Integrität und Vertraulichkeit der Dokumente zu gewährleisten. **Nicht zutreffend!** Der LOGOSCREEN *es* und die zugehörigen PC-Programme repräsentieren ein geschlossenes System.

2 Bewertung der Forderung

Absatz	Anforderungen: *Subpart B: Electronic Records* (Teil B: Elektronische Dokumente)
§ 11.50 *Signature manifestations* (Form der Unterschrift)	
(a)	*Signed electronic records shall contain information associated with the signing that clearly indicates 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.* Unterschriebene elektronische Dokumente müssen mit der Unterschrift verbundene Informationen beinhalten, die deutlich alle folgenden Punkte aufzeigen: (1) Name des Unterzeichnenden in Druckbuchstaben; (2) Datum und Zeitpunkt, zu dem die Unterschrift angefertigt wurde; und (3) die mit der Unterschrift verbundene Bedeutung (z. B. Überprüfung, Genehmigung, Verantwortlichkeit oder Urheberschaft). Anforderung erfüllt! ✔ Die den relevanten Aufzeichnungen zugeordnete elektronische Unterschrift wird am Recorder oder über die PC-Auswertesoftware in lesbarer Form dargestellt. Die elektronische Unterschrift beinhaltet in allen Fällen den Namen des Unterzeichnenden in Druckbuchstaben, Datum und sekundengenaue Uhrzeit, zu der die Unterschrift angefertigt wurde, sowie die Bedeutung der Unterschrift. Chargen, Zeiträume oder Kommentare können mit elektronischen Unterschriften verknüpft werden. Manipulationen sind nicht möglich, da Recorder und die dazugehörigen PC-Programme die Uhrzeit selbst generieren. Eine Änderung der Uhrzeit des Recorders setzt die Berechtigung des Benutzers dazu voraus. Jede Änderung wird nicht löschbar im Audit-Trail dokumentiert.

2 Bewertung der Forderung

Absatz	Anforderungen: *Subpart B: Electronic Records* (Teil B: Elektronische Dokumente)
§ 11.50 *Signature manifestations* (Form der Unterschrift)	
(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).* Die in den Absätzen (a)(1), (a)(2), und (a)(3) dieses Paragraphen aufgelisteten Punkte sollen den gleichen Kontrollen wie elektronische Dokumente unterworfen werden und in für Menschen lesbarer Version der elektronischen Dokumente (so z.B. elektronische Anzeige oder Ausdruck) beigefügt werden. **Anforderung erfüllt!** ✔ Die elektronische Unterschrift ist Bestandteil der Recorder-Rohdaten. ✔ Die Recorder-Rohdaten setzen sich zusammen aus dem Electronic Record, der elektronischen Unterschrift, Audit-Trail-Daten und der Prüfsumme. Das Format wird im Recorder erzeugt und unveränderbar für die Übertragung und Speicherung der Daten auf dem PC benutzt. ✔ Die Recorder-Rohdaten einschließlich der elektronischen Unterschrift sind in einem proprietären, nicht offen gelegten, über Prüfsummenalgorithmen abgesicherten Binärformat aufgezeichnet. Die Recorder-Rohdaten einschließlich der damit unlösbar verknüpften elektronischen Unterschriften sind manipulationssicher. ✔ Die elektronische Unterschrift ist der lesbaren - von den Rohdaten abgeleiteten - Version der elektronischen Dokumente (Display oder Ausdruck) hinzugefügt. ✔ Auf dem Drucker-Ausdruck oder auf dem elektronischen Ausdruck (PDF-Format) befindet sich der Hinweis, dass es sich um eine von den Recorder-Rohdaten abgeleitete Darstellungsform handelt.

2 Bewertung der Forderung

Absatz	**Anforderung:** ***Subpart B: Electronic Records* (Teil B: Elektronische Dokumente)**
§ 11.70 *Signature/record linking* (Verknüpfung Unterschrift/Dokument)	
	Electronic signatures and handwritten signatures executed to 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. Elektronische Unterschriften und handschriftliche Unterschriften auf elektronischen Dokumenten sollen mit den entsprechenden Dokumenten verknüpft werden, um zu gewährleisten, dass die Unterschrift nicht entfernt, kopiert oder anderweitig zum Zwecke der Fälschung eines elektronischen Dokuments durch übliche Methoden übertragen werden können. Anforderung erfüllt! ✔ Die Recorder-Rohdaten einschließlich der elektronischen Unterschrift sind in einem proprietären, nicht offen gelegten, über Prüfsummenalgorithmen abgesicherten Binärformat aufgezeichnet. ✔ Die Recorder-Rohdaten einschließlich der unlösbar verknüpften elektronischen Unterschriften sind manipulationssicher. ✔ Am Recorder und den dazugehörigen PC-Programmen sind sogenannte Security-Manager-Softwarefunktionen mit folgenden Aufgaben nicht veränderbar eingerichtet: PC-Security-Manager-Software: - erzeugt und verwaltet die Benutzerliste von PC und Recorder - prüft den Zugang zu den PC-Programmen und erteilt die Freigabe - stellt die Authentizität der elektronischen Unterschrift sicher Security-Manager-Software (Recorder): - speichert die Benutzerliste im Recorder - prüft den Zugang zum Recorder und erteilt die Freigabe - stellt die Authentizität der elektronischen Unterschrift sicher ✔ Der definierte Zugang zum Recorder oder zu den dazugehörigen PC-Programmen über die Security-Manager-Software schließt die Fälschung oder das Kopieren einer elektronischen Unterschrift durch eine Einzelperson aus. ✔ Der Recorder und die dazugehörigen PC-Programme lassen das Verändern bzw. Entfernen der elektronischen Unterschrift nicht zu. Der Recorder und die dazugehörigen PC-Programme erkennen den Versuch des Veränderns bzw. Entfernens einer elektronischen Unterschrift und zeigen dies an. ✔ Das Ereignis wird nicht löschbar im Audit-Trail dokumentiert.

2 Bewertung der Forderung

Absatz	Anforderungen: *Subpart B: Electronic Records* (Teil B: Elektronische Dokumente)
§ 11.100 *General requirements* (Allgemeine Anforderungen)	
(a)	*Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.* Jede elektronische Unterschrift soll eindeutig für eine Person sein und soll von keiner anderen Person wiederverwendet oder jemand anderem neu zugeordnet werden. Anforderung erfüllt! ✔ Mit der PC-Security-Manager-Software werden durch den Administrator die Benutzer am Recorder, deren Rechte, deren erstes Passwort und deren Passwort-Restriktionen eingestellt und in einer Benutzerliste verschlüsselt, zusammengefasst und an den Recorder übertragen. ✔ Die PC-Security-Manager-Software gewährleistet die Einmaligkeit und Eindeutigkeit der Kombination aus dem Benutzernamen und seiner Benutzer-ID für jeden in der Benutzerliste eingetragenden Benutzer. ✔ Benutzern können (durch den Administrator) zwar Rechte entzogen werden, aus der Benutzerliste entfernt werden können sie nicht. ✔ Die Security-Manager-Software des Recorders stützt sich auf die Benutzerliste und sorgt damit für die Authentizität der elektronischen Unterschrift.
(b)	*Before an organization establishes, assigns, certifies, or otherwise sanctions an in individual's electronic signature or any element of such signature, the organization shall verify the identify of the individual.* Bevor ein Unternehmen die elektronische Unterschrift einer Person oder Elemente dieser elektronischen Unterschrift festlegt, zuordnet, zertifiziert oder anderweitig billigt, soll es die Identität der entsprechenden Person überprüfen. Nicht zutreffend! Liegt in der Verantwortung des System-Owners.
(c)	*Persons 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.* Werden elektronische Unterschriften verwendet, soll die Behörde vor oder zum Zeitpunkt der Verwendung eine Bescheinigung erhalten, dass die elektronischen Unterschriften im System, die seit dem 20. August 1997 verwendet werden, das rechtlich verbindliche Äquivalent der traditionellen handschriftlichen Unterschrift darstellen. Nicht zutreffend! Liegt in der Verantwortung des System-Owners.

2 Bewertung der Forderung

Absatz	Anforderungen: *Subpart B: Electronic Records* (Teil B: Elektronische Dokumente)
§ 11.100 *General requirements* (Allgemeine Anforderungen)	
(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.* Die Bescheinigung muss in Papierform und mit einer traditionellen handschriftlichen Unterschrift beim Office of Regional Operations (HFC-100), 5600 Fishers Lane, Rockville, MD 20857 eingereicht werden. Nicht zutreffend! Liegt in der Verantwortung des System-Owners.
(2)	*Persons 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.* Werden elektronische Unterschriften verwendet, muss auf Ersuchen der Behörde eine zusätzliche Bescheinigung oder Bestätigung vorgelegt werden, aus der hervorgeht, dass eine bestimmte elektronische Unterschrift das rechtlich verbindliche Äquivalent zur handschriftlichen Unterschrift des Unterschreibenden darstellt. Nicht zutreffend! Liegt in der Verantwortung des System-Owners.

2 Bewertung der Forderung

Absatz	Anforderungen: *Subpart B: Electronic Records* (Teil B: Elektronische Dokumente)
§ 11.200 *Electronic signature components and controls* **(Bestandteile elektronischer Unterschriften, Kontrollen)**	
(a) (1)	*Electronic signatures that are not based upon biometrics shall:* *Employ at least two distinct identification components such as an identification code and password.* Elektronische Unterschriften, die nicht auf Biometrik basieren, sollen mindestens zwei verschiedene Identifikationskomponenten enthalten, so z.B. eine Benutzerkennung und ein Passwort. Anforderung erfüllt! ✔ Die elektronische Unterschrift kann nur durch einen (vom Administrator) autorisierten Benutzer geleistet werden, der über die Zugangskontrolle (Security-Manager-Software) mittels Benutzer-ID (Benutzernamen) und dem Passwort vom Recorder oder den dazugehörigen PC-Programmen authentisiert wurde.
(i)	*When an individual executes a series of signings during a single, continuous period of controlled system access, the first signing shall be excecuted using all electronic components; subsequent signings shall be excecuted using at least one electronic signature component that is only excecutable by, and designed to be used only by, the individual.* Unterschreibt eine Person während einer ununterbrochenen Sitzung mit kontrolliertem Systemzugriff mehrfach, soll die erste Unterschrift unter Verwendung aller Bestandteile der elektronischen Unterschrift vorgenommen werden. Anschließende Unterschriften sollen unter Verwendung mindestens einer Komponente, die nur von dieser Person ausführbar und auch nur dieser Person zur Verwendung zugeordnet ist, vorgenommen werden. Anforderung erfüllt! ✔ Immer nur ein Benutzer kann zu einer Zeit durch die Security-Manager am Recorder bzw. am PC-Security-Manager entsprechend der ihm (durch den Administrator) zugewiesenen Rechte autorisiert sein. ✔ Das Anfertigen der elektronischen Unterschrift ist nur durch den im Recorder oder den dazugehörigen PC-Programmen eingeloggten Benutzer möglich und erzwingt im erstmaligen als auch in jedem Wiederholungsfall die vollständige Authentisierung durch die Security-Manager-Software mit Benutzer-ID (Benutzernamen) und Passwort. ✔ Vor dem Anfertigen der elektronischen Unterschrift wird der Benutzer per Text auf folgenden Sachverhalt hingewiesen: „Ihre Unterschrift ist rechtlich verbindlich und ist das Äquivalent zu Ihrer handschriftlichen Unterschrift!“

2 Bewertung der Forderung

Absatz	Anforderungen: *Subpart B: Electronic Records* (Teil B: Elektronische Dokumente)
§ 11.200 *Electronic signature components and controls* **(Bestandteile elektronischer Unterschriften, Kontrollen)**	
(ii)	*When an individual excecutes one or more signings not performed during a single, continuous period of controlled system access, each signing shall be excecuted using all of the electronic signature components.* Unterschreibt eine Person mehrfach, allerdings nicht während einer einzigen ununterbrochenen Sitzung mit kontrolliertem Systemzugriff, soll jede Unterschrift unter Verwendung aller Komponenten der elektronischen Unterschrift vorgenommen werden. Anforderung erfüllt! ✔ Das Anfertigen der elektronischen Unterschrift ist nur durch den im Recorder oder den dazugehörigen PC-Programmen authentifizierten Benutzer möglich und erzwingt im erstmaligen als auch in jedem Wiederholungsfall die vollständige Authentisierung durch die Security-Manager-Software mittels Benutzer-ID (Benutzernamen) und dem Passwort.
(2) (3)	*Be used only by their genuine owners; and be adminstered and excecuted 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.* ..nur von den eigentlichen Benutzern verwendet werden dürfen; und so verwaltet und ausgeführt werden dürfen, dass gewährleistet ist, dass der Versuch einer Person, eine ihr nicht eigene elektronische Unterschrift zu verwenden, die Zusammenarbeit von zwei oder mehr Personen erforderlich macht. Anforderung erfüllt! ✔ Dies ist sichergestellt durch den vorgegebenen Weg der Erstellung und Verwaltung der Benutzerliste, die die Basis für die Autorisierung und Authentisierung eines Benutzers ermöglicht. ✔ Ein Benutzer alleine ist nicht in der Lage, eine andere elektronische Unterschrift als seine eigene zu verwenden. ✔ Jeder Versuch wird erkannt und nicht löschbar im Audit-Trail dokumentiert. ✔ Jeder Benutzer verwendet ein entsprechend den voreingestellten Restriktionen festgelegtes Passwort. Dieses Passwort ist alleine dem Benutzer bekannt. Niemand kann Passworte aus dem Recorder oder etwa mit Hilfe der PC-Programme auslesen.
(b)	*Electronic signatures based upon biometrics shall be designed to ensure that the cannot be used by anyone other than their genuine owners.* Auf Biometrie basierende elektronische Unterschriften müssen so angelegt sein, dass sie außer von den eigentlichen Benutzern von niemand anderem verwendet werden können. Nicht zutreffend! Die auf Biometrie basierende elektronische Unterschrift ist nicht vorgesehen.

2 Bewertung der Forderung

Absatz	Anforderungen: *Subpart B: Electronic Records* (Teil B: Elektronische Dokumente)
§ 11.300 *Controls for identification codes/passwords* (Kontrollen für Benutzerkennungen/Passwörter)	
(a)	*Persons who use electronic signatures based upon use of identification codes in combination with passwords shall employ controls to ensure their security and integrity. Such controls shall include:* *Maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password.* Werden elektronische Unterschriften verwendet, die auf dem Einsatz von Benutzerkennungen in Kombination mit Passwörtern beruhen, sind Kontrollen zu schaffen, die die Sicherheit und Integrität der Unterschriften gewährleisten. Derartige Kontrollen sollen folgende Punkte beinhalten: Erhalt der Einzigartigkeit jeder Kombination aus Benutzerkennung und Passwort, so dass eine Kombination nur einmal vergeben ist. Anforderung erfüllt! ✔ Mit der PC-Security-Manager-Software werden durch den Administrator die Benutzer am Recorder, deren Rechte und deren Passwort-Restriktionen eingestellt und in einer Benutzerliste verschlüsselt, zusammengefasst und an den Recorder übertragen. ✔ Die Zuordnung aller Daten zu einem Recorder wird durch eine für alle Zeit einmalige, eindeutige Geräte-Identifikationsnummer (Produktionsnummer) gewährleistet. ✔ Die PC-Security-Manager-Software und die Security-Manager-Software des Recorders gewährleisten die Einzigartigkeit jeder Kombination aus Benutzerkennung und Passwort.
(b)	*Ensuring that identification code and password issurances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).* Gewährleistung, dass die Ausgabe von Benutzerkennungen und Passwörtern regelmäßig überprüft oder die Kennungen und Passwörter zurückgenommen oder überprüft werden (um z.B. das Veralten von Passwörtern zu verhindern). Anforderung erfüllt! ✔ Für die Benutzerliste als Basis der Zugangskontrolle von Recorder und PC werden die gleichen hohen Sicherheitskriterien angewendet, die auch für die Electronic Records gelten. ✔ Eine Manipulation an der Benutzerliste wird erkannt. In diesem Falle wird die Verwendung der Benutzerliste gesperrt und dieses Ereignis nicht löschbar im Audit-Trail dokumentiert. ✔ Die Security-Manager-Software des Recorders und die PC-Security-Manager-Software gewährleisten bei jeder Änderung der Benutzerliste als auch bei jeder Überprüfung der Zugangskontrolle eine Überprüfung der vom Administrator eingestellten Restriktionen, darin enthalten: das Veralten von Passworten. ✔ Der Benutzer, dessen Passwort veraltet ist, wird gesperrt und das Ereignis nicht löschbar im Audit-Trail dokumentiert. Nur der Administrator kann diesen Benutzer wieder freigeben.

2 Bewertung der Forderung

Absatz	Anforderungen: *Subpart B: Electronic Records* (Teil B: Elektronische Dokumente)
§ 11.300 *Controls for identification codes/passwords* (Kontrollen für Benutzerkennungen/Passwörter)	
(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.* Befolgen von Verlustverfahren, um auf elektronischem Weg verlorenen, gestohlenen, fehlenden oder anderweitig möglicherweise unsicheren Marken (Tokens), Karten und anderen Vorrichtungen, die mit Benutzerkennungs- und Passwortinformationen versehen sind oder solche erzeugen, die Berechtigung zu entziehen und um unter geeigneter und strenger Kontrolle vorübergehenden oder ständigen Ersatz herauszugeben. Anforderung erfüllt! ✔ Recorder und die dazugehörigen PC-Programme verwenden keine Marken, Tokens o.ä. Die Sicherheit wird durch die vom Administrator eingestellten Benutzerrechte und Passwort-Restriktionen erreicht. So muss beispielsweise ein erstes Passwort vom Administrator eingestellt werden, welches der Benutzer sofort beim ersten Zugriff ändern muss, so dass sein Passwort nur ihm selbst bekannt ist. Weiterhin kann ein Gültigkeitszeitraum für das Passwort vorgegeben werden. ✔ Ein Nichtbeachten der Restriktionen führt zum Entzug der Berechtigung des Benutzers. ✔ Dieses Ereignis wird im Audit-Trail nicht löschbar dokumentiert.
(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.* Verwendung von Sicherheitsvorkehrungen für Transaktionen, die den unbefugten Einsatz von Passwörtern und/oder Benutzerkennungen verhindern und sofort und unter Hinweis auf die Dringlichkeit des Vorfalls jeden Versuch der unbefugten Benutzung entdecken und diesen an die Sicherheitseinheit des Systems und im Bedarfsfall an die Unternehmensführung weiterleiten. Anforderung erfüllt! ✔ Die PC-Security-Manager-Software und die Security-Manager-Software des Recorders verhindern den unautorisierten Zugriff. Jeder Versuch wird erkannt und nicht löschbar im Audit-Trail des Recorders oder im Audit-Trail des PC nicht löschbar dokumentiert.

2 Bewertung der Forderung

Absatz	Anforderungen: *Subpart B: Electronic Records* (Teil B: Elektronische Dokumente)
§ 11.300 *Controls for identification codes/passwords* (Kontrollen für Benutzerkennungen/Passwörter)	
(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.* Anfängliches und im Anschluss daran regelmäßiges Testen der Geräte, wie etwa Marken (Tokens) oder Karten, die mit Benutzerkennungs- oder Passwortinformationen versehen sind oder solche erzeugen, um zu gewährleisten, dass sie ordnungsgemäß funktionieren und nicht unbefugt verändert wurden. Nicht zutreffend! Recorder und die dazugehörige PC-Software verwenden oder erzeugen keine Marken, Tokens o.ä., die mit Benutzerkennungs- oder Passwortinformation versehen sind.

3 Literaturverzeichnis

[1] Mass & Peither GMP Verlag
21 CFR 210/211 cGMP FOR FINISHED PHARMACEUTICALS
(Aktuelle Gute Herstellungspraxis für Fertigarzneimittel)
inkl. 21 CFR 11 electr. Records/electr. Signature
(Elektr. Dokumente/elektr. Unterschrift)
mit deutscher Übersetzung und Stichwortverzeichnis

M. K. JUCHHEIM GmbH & Co

Hausadresse:
Moltkestraße 13 - 31
36039 Fulda, Germany
Lieferadresse:
Mackenrodtstraße 14
36039 Fulda, Germany
Postadresse:
36035 Fulda, Germany
Telefon: 0661 6003-725
Telefax: 0661 6003-681
E-Mail: mail@jumo.net
Internet: www.jumo.net

09.02/00408254