

MANAGEMENT SUMMARY: ELEKTRONISCHE SIGNATUREN IN PHARMAZEUTISCHEN UNTERNEHMEN ASPEKTE TECHNISCHER UND JURISTISCHER SICHERHEIT

Dr. Stefan Schmitz, CMC Pharma GmbH, Mannheim

Einführung

Bedenkt man die Masse an Papier, die in der Pharmaindustrie tagtäglich erstellt, verteilt, unterzeichnet, versendet, archiviert, gesucht und vernichtet wird, erscheint es geradezu unumgänglich sich mit dem Thema elektronische Dokumentation zu befassen. Betrachtet man dann näher die Computersysteme, mit denen das Papier erzeugt wird, stellt man fest, dass häufig nur Papier ausgedruckt wird, um einen selbst definierten de facto Standard zu erfüllen; nämlich die Vorgabe: Unterschriebene Papiere sind Rohdaten und werden archiviert.

Nicht zuletzt deswegen erlauben die Zulassungsbehörden - oder besser - fordern sie die Einreichung von pharmazeutischen Dossiers in elektronischer Form. Die Bestrebungen der ICH (International Conference on Harmonization) mündeten in einem international einheitlichen Standard zur elektronischen Einreichung von Zulassungsunterlagen. Der Ansatz wird als eCTD (electronic Common Technical Document) bezeichnet und gibt Architekturen, Namens- und Dateistrukturen, sowie Datenformate vor [1].

Bei der Verwendung elektronischer Dokumente anstelle von Papier treten allerdings wesentliche Forderungen auf, die sich in der Papierwelt nur unter Anwendung krimineller Energie stellten, nämlich nach der Echtheit des Unterzeichners, der Unversehrtheit des Dokuments nach Erstellung und Freigabe, der Untrennbarkeit

von Unterschrift und Dokument, sowie der Vertraulichkeit während des Versands.

Gesetzliche Regelungen in den USA

Diese Thematik wurde in dem bereits seit 1997 gültigen amerikanischen Gesetzestext 21 CFR Part 11 behandelt [2, 3, 4]. Hier werden die Randbedingungen beschrieben, unter denen die FDA (Food and Drug Administration) elektronische Dokumente als rechtlich äquivalent zu händisch unterschriebenen Papierdokumenten betrachtet.

Dieses Gesetz erlaubt ausdrücklich die Verwendung elektronischer und digitaler Signaturen, sowie biometrischer Merkmale zur Sicherstellung der Authentizität des Autors, der Datenintegrität, der Verbindung von Signatur und Dokument, sowie der Vertraulichkeit. Es muss hier darauf hingewiesen werden, dass die geforderte Verschlüsselung von Unterschriften im Falle digitaler Signaturen nichts mit dem Thema Vertraulichkeit zu tun hat, denn das Dokument ist nach der Anwendung einer verschlüsselten Signatur immer noch zu 100 % lesbar; die Vertraulichkeit lässt sich nur durch zusätzliche Verschlüsselung des gesamten Dokumenteninhalts oder Teilen davon herstellen. Dies geschieht fast immer nach dem Prinzip der asymmetrischen Verschlüsselung und der Anwendung eines PKI-Systems (Public Key Infrastructure).

Es sei hier erwähnt, dass die FDA den 21 CFR Part 11 auf alle Dokumente anwendet, die durch vorherrschende Guidelines

CMC Pharma GmbH

www.cmc-pharma.de
info@cmc-pharma.de

(„predicate rules“) zu den Themen Dokumentation und Archivierung reguliert sind, sofern der Unternehmer entscheidet diese Dokumente in elektronischer Form zu führen.

Im Gegensatz zur europäischen und insbesondere der deutschen Gesetzgebung ist die elektronische Signatur nach 21 CFR Part 11 nicht an eine spezifische Hardware (nämlich eine sichere Signaturerstellungseinheit) gebunden, sondern lediglich an die Verwendung wenigstens zweier Komponenten: Identifizierungscode (eindeutige Identifizierung) und Passwort (geheime Komponente) gekoppelt. Damit lassen sich zwar 21 CFR Part 11 – konforme Unterschriften realisieren, die juristische Beweiskraft ist in diesem Falle aber nicht gegeben. Im juristischen Streitfall sind diese Arten von Unterschriften zwar als Beweismittel zugelassen, die beschuldigte Person wird aber bestreiten die elektronische Unterschrift mittels Identifizierungscode und Passwort geleistet zu haben, eine immanente Problematik der Verwendung nicht-biometrischer Identifizierungsmethoden.

Weitere gesetzliche Vorgaben zum Umgang und zur Sicherheit elektronischer Signaturen gibt es zu anderen interessierenden Themengebieten pharmazeutischer Unternehmen, wie z.B. HIPAA (Health Information Protection and Accountability Act, 45 CFR Part 142) [5], sowie dem Sarbanes Oxley Act von 2002 [6], die sich mit der Datensicherheit von Patientendaten, respektive der Sicherheit und Nachvollziehbarkeit von Unternehmensdaten im Bereich Controlling und Bilanzierung beschäftigen.

Gesetzliche Regelungen in der EG und in Deutschland

In der Europäischen Gemeinschaft ist seit 1999 die EG Signaturrechtlinie (EGSIGRL) [7] gültig, während in Deutschland seit 2001 das Signaturgesetz (SigG) [8] gilt. Im Unterschied zur EG definiert das deutsche Gesetz den Unterzeichner (Signatory) mit Signaturschlüsselinhaber, welches prinzipiell voraussetzt, dass ein solcher Schlüssel existiert. Das deutsche Signaturgesetz unterscheidet drei Stufen elektronischer Signaturen:

Die einfache elektronische Signatur

- Daten, die in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verknüpft sind und die zur Authentifizierung dienen.

Die fortgeschrittene elektronische Signatur

- ausschließlich dem Signaturschlüssel-Inhaber zugeordnet.
- die Identifizierung des Signaturschlüssel-Inhabers ermöglicht.
- mit Mitteln erzeugt, die der Signaturschlüssel-Inhaber unter seiner alleinigen Kontrolle halten kann, und
- mit den Daten auf die sie sich bezieht so verknüpft, dass eine nachträgliche Veränderung der Daten erkannt werden kann.

Die qualifizierte elektronische Signatur (zusätzlich zu fortgeschrittenen elektronischen Signaturen)

- auf einem zum Zeitpunkt ihrer Erzeugung gültigen qualifizierten Zertifikat beruhen und
- mit einer sicheren Signaturerstellungseinheit erzeugt wird.

Der Begriff Signaturschlüssel-Inhaber bedeutet aber nicht gleichzeitig Eigentümer des Schlüssels, d.h. die Anwendung des Signaturschlüssels ist nicht notwendigerweise gebunden an die autorisierte Person, sondern lediglich an den jeweiligen Benutzer (Inhaber) des Schlüssels zum Zeitpunkt der Signatur. Damit ist auch hier grundsätzlich die juristische Problematik anzusprechen, die sich aus der Verwendung von Kombinationen aus Schlüsseln auf Signaturkarten und PIN (6-stellig) oder der Verwendung von Identifizierungscodes und Passwörtern (meist 8-stellig) ableitet, nämlich die fehlende Zuordnung von autorisierter Person und der fraglichen geleisteten elektronischen Signatur. Juristen fordern daher biometrische Komponenten zur Anwendung elektronischer Unterschriften, wenn es darum geht gerichtliche Beweisbarkeit herzustellen.

Hier ist das pharmazeutische Unternehmen in Zusammenarbeit mit Juristen aufgefordert die Unterschriften des Unternehmens pro Unternehmensbereich zu klassifizieren und verschiedene Risikostufen im Bezug auf Produktqualität und -haftung herzustellen.

Die zurzeit händisch ausgeführten Unterschriften der Mitarbeiter des Unternehmens werden bewertet und daraus abgeleitet die Art der elektronischen Signatur zugeordnet. Spätestens an der Stelle, wo es um die Freigabe einer Produktqualität

für den Markt geht, die ja letztlich eine Zusage der Wirksamkeit und Sicherheit des Arzneimittels für den Patienten ist, sollte neben der technischen Sicherheit auch die juristische Sicherheit der elektronischen Signatur bedacht werden, denn Produkthaftung in den USA kann im Extremfall die Existenz des Unternehmens gefährden.

In Deutschland können beim BfArM (Bundesamt für Arzneimittelsicherheit) laut AMG-EV (Arzneimittelgesetz – Einreichungsverordnung) [9] zwar elektronische Daten in PGP-verschlüsselter Form (Vertraulichkeit) eingereicht werden, allerdings gibt es noch keinen akzeptierten Standard für die Anwendung elektronischer Unterschriften.

Der Vollständigkeit halber sei erwähnt, dass die elektronische Archivierung von Dokumenten im kaufmännischen Bereich den Regelungen von HGB (Handelsgesetzbuch), AO (Abgabenordnung), GOB (Grundsätze ordnungsgemäßer Buchung) und GOBS (Grundsätze ordnungsgemäßer DV-gestützter Buchungssysteme) unterliegen.

Hybridsysteme aus Papier und elektronischen Aufzeichnungen

Die zunehmende Vernetzung und Verzahnung von Prozessen erfordert in immer stärkerem Maß die Integration elektronischer Dokumente in den digitalen Workflow, denn nur so können die immanenten Vorteile der elektronischen Datenverarbeitung genutzt werden. Nach einer Analyse der Gartner Group entfallen auf jeden Dollar Papierdruckkosten ca. 30 bis 60 Dollar Folgekosten für:

- Vorhaltung
- Transport

CMC Pharma GmbH

www.cmc-pharma.de
info@cmc-pharma.de

- Nachbearbeitung (Austausch bei Änderung)
- Zwischenlagerung
- Archivierung
- Recherche

Die meisten Unternehmen betreiben zurzeit Hybridsysteme, d.h. Papier und elektronische Dokumente im Parallelbetrieb. Dies führt an einigen wesentlichen Stellen immer wieder zu zeit- und kostenintensiven Medienbrüchen, die darin bestehen, dass unnötigerweise Papiausdrucke erzeugt und per Hand unterzeichnet, abgelegt und als Rohdaten definiert werden. Oft werden aber die primär erzeugten elektronischen Rohdaten von der Datenquelle weitergegeben, bearbeitet und schließlich berichtet. Diese häufig mehrstufigen und über mehrere Softwaresysteme realisierten Datentransfers finden häufig unkontrolliert (oder zumindest auf unsicheren Wegen) statt und werden bestenfalls im Anschluss an den durchgeführten Transfer durch eine Qualitätssicherungsabteilung visuell mit den Daten der Datenquelle verglichen. Auf diese Weise soll die Datenintegrität zwischen Datenquelle und Datenziel sichergestellt werden.

Das Hauptproblem warum Papier und nicht die primären elektronischen Daten als Rohdaten definiert werden, liegt an der Tatsache, dass kein Softwarelieferant und erst recht nicht der pharmazeutische Unternehmer sicher stellen kann, dass ein verwendetes proprietäres Datenformat über den gesetzlich vorgeschriebenen Aufbewahrungszeitraum Datensicherheit, Datenintegrität und vor allem Lesbarkeit gewährleistet. Hier sollte überlegt werden, ob nicht durch Speichern der Ergebnisdaten in einem langzeitarchivierbaren Datenformat eine tragfähige Lösung gefunden werden kann.

Seit dem 01.10.2005 existiert die neue Guideline der International Standard Organisation ISO 19005:2005 [10], welche das Format PDF1.4 (oder auch als PDF/A-1 bezeichnet) als langzeitarchivierbares Datenformat für Zeichen, Raster- und Vektorgrafiken anerkennt. Damit ist es möglich die bisher auf Papier gedruckte Information, direkt in einem PDF-Format zu speichern, digital zu signieren und einem Verteilungs- und Archivierungsprozess zuzuführen. Damit werden erhebliche Einsparungen an Papier und dem damit verbundenen Workflow erzielbar. Allerdings sind die entsprechenden Maßnahmen zur Umsetzung wie im letzten Kapitel dieses Dokumentes beschrieben, einzuführen.

Es wird von behördlicher Seite gefordert systemspezifische Rohdatendefinitionen zu benennen, denn damit beginnen letztendlich die Strategie und die Konzeption der Sicherstellung von Datensicherheit und Datenintegrität über die geforderten Aufbewahrungszeiträume [4, 11, 12].

Konsequenzen für die Umsetzung elektronischer Signaturen

Aus dem bisher gesagten ergeben sich mindestens die folgenden konkreten Konsequenzen für die Anwendung behördenkonformer und rechtssicherer Dokumentation:

- Entscheidung ob elektronische Unterschriften im Unternehmen eingesetzt werden und wenn, auf welcher Ebene, in welchen Systemen?
- Klassifizierung der Unterschriften nach Rechtsbedeutung und Haftbarkeit; Zuordnung der Art elektronischer Signaturen zur entsprechenden traditionellen Unterschrift.
- Definition von Rohdaten für jedes spezifische System.

CMC Pharma GmbH

www.cmc-pharma.de
info@cmc-pharma.de

- Festlegung von Datenformaten für elektronische Aufzeichnungen.
- Umgang mit Systemen, die Daten in Datenbankformaten speichern vs. Systemen, die auf proprietären Filesystemen und –formaten beruhen.
- Validierung aller Systeme, die elektronische Aufzeichnungen inklusive elektronischer Unterschriften speichern.
- Realisierung von Audit Trails auf allen Part 11 relevanten Systemen.
- Speicherung der elektronischen Daten in revisionssicheren Archiven (Alternative dazu: Umschlüsselung von Dateien wegen Verfallsdatum von Schlüsseln).
- Benachrichtigung der FDA, dass elektronische Unterschriften gleichbedeutend mit händisch unterschriebenen Dokumenten ab einem bestimmten Datum verwendet werden.
- Belehrung der Mitarbeiter über die rechtlichen, insbesondere haftungsrechtlichen Konsequenzen ihrer elektronischen Unterschrift.
- Schulung aller Mitarbeiter, die solche Systeme erstellen, pflegen, betreiben oder benutzen.
- Etablierung eines Qualitätssicherungssystems, welches per SOP mindestens die folgenden Aktivitäten regelt:
 - Erstellung und Verwaltung digitaler Schlüssel zur Anwendung digitaler Signaturen.
 - Im Falle biometrischer Unterschriften: Realisierung der Verifikation

- biometrischer Merkmale und Verwaltung der biometrischen Daten der unterschriftsberechtigten Mitarbeiter
- Identifizierung der Mitarbeiter mit elektronischer Unterschriftsberechtigung.
- Erstellung und Verwaltung von Schlüsseln zur Herstellung vertraulicher Dokumente nach dem PKI-Verfahren (z.B. PGP).
- Systemspezifische Definition von Rohdaten (elektronische Aufzeichnungen) und Umgang mit diesen Rohdaten über den gesetzlichen Aufbewahrungszeitraum.
- Migrationskonzept zur Berücksichtigung der Alterung von Datenträgern.
- Backup – und Archivierung elektronischer Aufzeichnungen.
- Wiederherstellbarkeit archivierter elektronischer Aufzeichnungen über den gesetzlichen Aufbewahrungszeitraum.
- Regelmäßige Auditierung und Überprüfung der elektronischen Archive durch die QS zur Prüfung von Ordnungsmäßigkeit, Vollständigkeit, Datensicherheit und der Datenintegrität archivierter elektronischer Aufzeichnungen.
- Umschlüsselung verschlüsselter Dateien nach Ablauf des Haltbarkeitsdatums elektronischer Schlüssel.

Referenzen

- [1.] ICH eCTD Specification V 3.0 Oct 08 2002
- [2.] 21 CFR Part 11 Final rule, dated Aug 20 1997
- [3.] 21 CFR Part 11 Guideline „Scope and Application“ Final Guidance Aug 2003
- [4.] Deutsche Übersetzung des 21 CFR Part 11 Final Rule, S. Schmitz, 2001
- [5.] HIPAA (45 CFR Part 142), 1996
- [6.] Sarbanes Oxley Act 2003, USA
- [7.] Richtlinie 1999/39/EG EGSIGRL vom 13. Dez. 1999
- [8.] Deutsches Signaturgesetz vom 16.05.2001
- [9.] AMG-Einreichungsverordnung vom 21. Dezember 2000
- [10.] ISO 19005:2005 vom 01.10.2005
- [11.] OECD – Konsensdokument Nr. 10, 1995
- [12.] GLP Inspektorenhandbuch, 9. Auflage, Anhang 6 „Inspektion EDV-gestützter Systeme“ vom Dez. 2004

Glossar

Abkürzung	Erläuterung
AMG-EV	Arzneimittelgesetz - Einreichungsverordnung
AO	Abgabenordnung
CFR	Code of Federal Regulations
DV	Datenverarbeitung
eCTD	Electronic Common Technical Document
EGSIGRL	Europäische Gemeinschaft Signaturrechtlinie
FDA	Food and Drug Administration
GOB	Grundsätze ordnungsgemäßer Buchführung
GOBS	Grundsätze ordnungsgemäßer Buchführung mittels DV gestützten Systemen
HIPAA	Health Information Privacy and Accountability Act
HGB	Handelsgesetzbuch
ICH	International Conference on Harmonization
PDF	Portable Data Format
PGP	Pretty Good Privacy
PKI	Public Key Infrastructure
SigG	Signaturgesetz Deutschland
SOP	Standard Operating Procedure
SOX	Sarbanes Oxley Act

Dr. Stefan Schmitz, 20.11.2005

CMC Pharma GmbH

www.cmc-pharma.de
info@cmc-pharma.de