Techno Pharm IT

Validierung von computergestütztem Equipment

Beachtung der Datenintegrität im GMP-Bereich – Teil 1

Dr. Susan Spiller • Testo Industrial Services, Kirchzarten

Korrespondenz: Dr. Susan Spiller, Testo Industrial Services GmbH, Gewerbestraße 3, 79199 Kirchzarten; **e-mail**: sspiller@testotis.de

PEER REVIEW

Zusammenfassung

Für die Validierung und Qualifizierung von standardisierten Stand-Alone-Systemen, die insbesondere in pharmazeutischen Good-Manufacturing-Practice(GMP)-Bereichen (z. B. in der Qualitätskontrolle) Anwendung finden, ist es sinnvoll, ein übergeordnetes Validierungskonzept zu etablieren. In diesem Beitrag werden praktikable Lösungsansätze aufgeführt, um eine Standardisierung des Validierungsansatzes, der technischen Maßnahmen und der Validierungs- bzw. Life-Cycle-Dokumente zu erreichen und darüber hinaus die Integrität der mit dem Equipment erzeugten Daten unter Berücksichtigung aller behördlichen Anforderungen sicherzustellen.

Key Words

- Equipmentqualifizierung
- Softwarevalidierung
- CSV-Konzept
- Datenintegrität
- Computerisiertes Equipment im GMP-Bereich

Einleitung

Die Thematik der Sicherstellung von Datenintegrität bei Equipment nimmt an Bedeutung zu. Computerisiertes Equipment lässt sich hierbei je nach Komplexität in Gruppen einteilen. Während es für groß angelegte Server-Client-Varianten (z. B. Chromatographie-Systeme) bereits etablierte Validierungskonzepte gibt (basierend auf anerkannten Guidelines), ergeben sich bei der Validierung von sog. Stand-Alone-Equipment zahlreiche Fragen, die es zu lösen gilt, um den Guidelines zu entsprechen.

Hierzu ist es sinnvoll, ein übergeordnetes risikobasiertes Validierungskonzept zu etablieren, das standardisiert auf eine Vielzahl an Stand-Alone-Systemen in Good-Manufacturing-Practice(GMP)-Bereichen der pharmazeutischen Industrie angewandt werden kann.

Dieses Konzept sollte ein Risikomanagement über den gesamten Lebenszyklus hinweg beinhalten[1]. Einerseits ergeben sich daraus prozedurale Regelungen, die im Rahmen der Validierung und Qualifizierung getroffen werden sollten, sowie diverse Möglichkeiten zur technischen Umsetzung.

Andererseits muss das Risikomanagement die Grundlage für die Aufrechterhaltung des validierten Zustands des Equipments bilden. Somit müssen bereits vor der Umsetzung organisatorische Strukturen etabliert werden, die den gesamten Lebenszyklus des Equipments und der erzeugten Daten abbilden.

Im Folgenden werden Lösungsansätze und Vorgehensweisen zur einheitlichen Validierung von Computersystemen dargestellt, bestehend aus einem PC mit einer Auswertungs-/Steuerungssoftware und dem dazugehörigen Equipment. Im Fokus der Betrachtung steht typisches analytisches Equipment, mit dem Daten (insbesondere Rohdaten) erzeugt werden (z. B. Spektrometer oder Partikelmessgeräte). Die hier vorgestellten Vorgehensweisen können insbesondere in Unternehmen mit einem größeren Equipment-Bestand Anwendung finden.

Data Governance

In der pharmazeutischen Industrie muss eine lückenlose Rückverfolgbarkeit aller Stufen der Arzneimittelherstellung, -prüfung und -freigabe gewährleistet sein. Dafür muss

Autor

Dr. Susan Spiller

Dr. Susan Spiller ist promovierte Chemikerin (Dipl.). Seit 2015 ist sie im technischen Außendienst der Testo Industrial Services GmbH als Qualifizierungsingenieurin in pharmazeutischen Unternehmen tätig. Sie verfügt über mehrjährige Erfahrung in der Durchführung, Konzeptionierung und Koordination von Validierungen/Qualifizierungen verschiedenster computerisierter Systeme mit dem Schwerpunkt auf Datenintegrität und betreut als CSV-Beauftragte unterschiedlichste Softwarevalidierungsprojekte.

TechnoPharm 10, Nr. 3, 172–175 (2020)

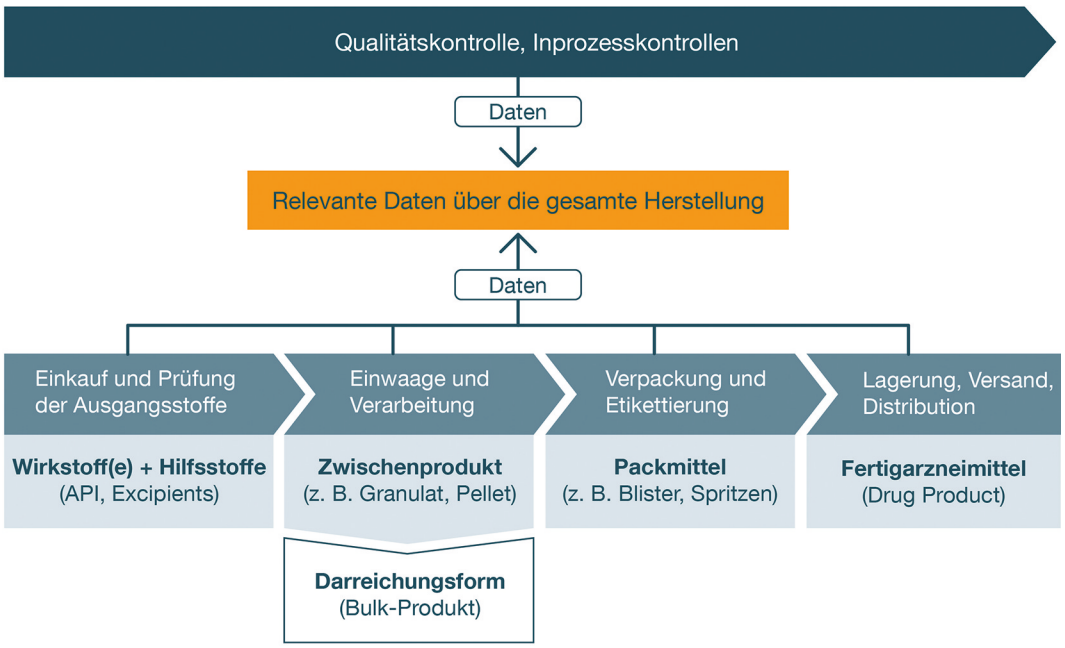

Abbildung 1: Data-Mapping auf Herstellungsprozessebene eines Arzneimittels zur Bewertung von GMP-relevanten Daten (Quelle aller Abbildungen: Testo Industrial Services GmbH).

die Vollständigkeit und Unversehrtheit von GMP-Daten über deren gesamten Lebenszyklus hinweg gesichert werden. Um diese Integrität der Daten herzustellen, werden verschiedene Prinzipien zugrunde gelegt. Die U.S. Food and Drug Administration (FDA) definiert dazu das ALCOA-Prinzip [2], das fordert, dass Daten zuordenbar (*Attributable*), lesbar (*Legible*), zeitgenau (*Contemporaneous*), original (*Original*) und richtig (*Accurate*) sind. Dieses Prinzip wurde erweitert um die Eigenschaften Vollständigkeit (*Complete*), Konsistenz (*Consistent*), Dauerhaftigkeit (*Enduring*) und Abrufbarkeit (*Available*) und ist als ALCOA plus oder ALCOA+[5] bekannt [3]. Die Anforderungen, die sich aus diesem Prinzip ergeben, werden durch die PIC/S Guidance PI 041-1 (Draft 3) [3] erläutert.

Zur Umsetzung einer Data Governance – also dem Management, der Kontrolle und dem Beherrschen von Daten und Datenflüssen – ist ein Risikomanagement über den gesamten Datenlebenszyklus (Erzeugung, Verwendung, Aufbewahrung, Vernichtung) und den Systemlebenszyklus [1] hinweg notwendig. Dieses Risikomanagement sollte die Produktqualität, die Patientensicherheit und die Datenintegrität abdecken.

Für eine Risikobetrachtung zum Schutz von Daten empfiehlt die PIC/S Guidance 2 Fragestellungen:

- Die Kritikalität der Daten: Manche Daten sind kritischer zu bewerten als andere. Welche Auswirkung haben die Daten auf Entscheidungen und auf die Produktqualität?
  - Je höher die Kritikalität ist, umso größerer Aufwand muss zum Schutz dieser Daten betrieben werden.
- Datenrisiko: Wie leicht können Daten geändert oder gelöscht werden, wie hoch ist die Entdeckungswahrscheinlichkeit einer solchen Manipulation?
  - Je leichter Datenmanipulation unbemerkt stattfinden kann, umso mehr Maßnahmen müssen ergriffen werden, um dies wirksam zu verhindern.
  - Beispiel: Statische Daten, die nicht durch Auswertungen oder weitere Verarbeitungen veränderbar sind oder durch den Anwender beeinflusst werden können, haben ein geringeres Manipulationsrisiko als dynamische Daten, deren Auswertung oder Bewertung variabel erfolgen kann (z. B. durch Integrationen/Prozessierungen).

Die Risikobetrachtung sollte sich nicht nur auf die Systemfunktionalität beziehen, sondern auch auf Prozesse, mit denen die Daten gewonnen werden oder für die die Daten relevant sind. Dabei muss bedacht werden, dass sich Produktionsprozesse von der Qualitätskontrolle unterscheiden und Methoden zur Datenerstellung verschiedene Risiken bei der Handhabung von Daten beinhalten.

Relevante Daten

Um zu identifizieren, welche Daten im GMP-Prozess relevant sind, sollten die Datenflüsse der im Prozess erhobenen Daten analysiert werden. Darüber hinaus ist zu spezifizieren, welche Daten davon eine Kritikalität aufweisen, um die Integrität dieser Daten über den gesamten Prozess sicherzustellen. Ein Data-Mapping kann über den gesamten Herstellungsprozess erfolgen. Das Mapping sollte die Herstellungs- und Qualitätskontrolldaten umfassen (Abb. 1).

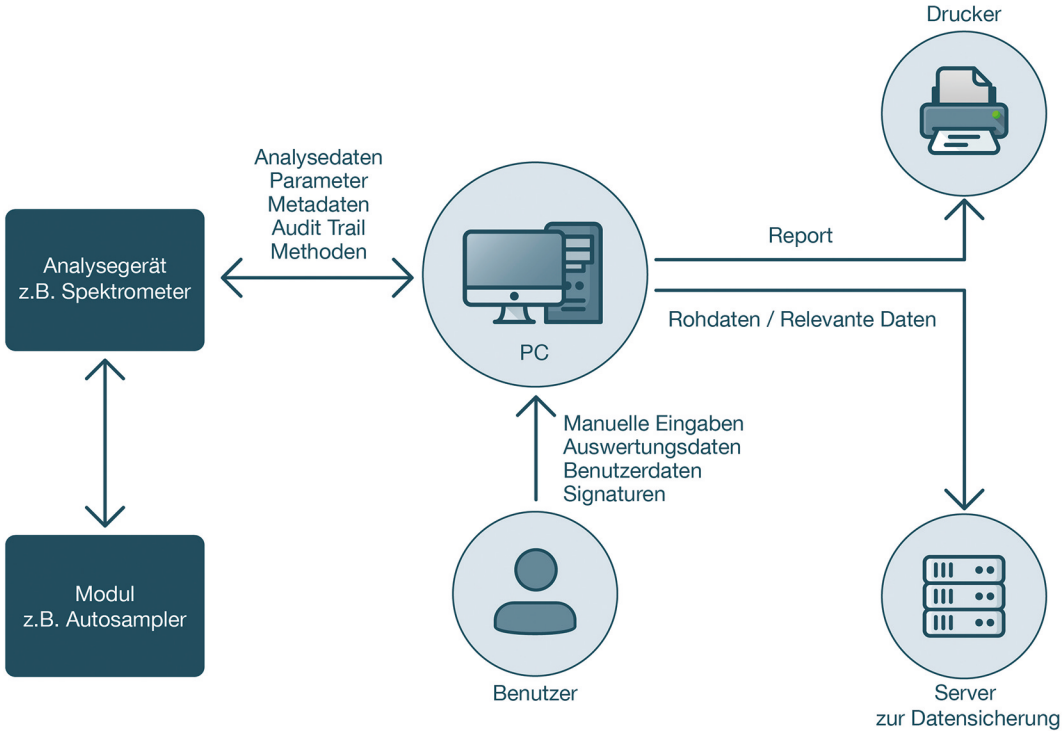

Abbildung 2: Data Mapping auf Systemebene am Beispiel eines computerisierten Laborequipments in der Qualitätskontrolle.

Dieser Gesamtprozess kann dann in Teilprozesse zerlegt und die Datenflüsse können in den Teilprozessen erfasst und bis auf Systemebene nachvollzogen werden. So kann aufgezeigt werden, welche mit dem Equipment erzeugten Daten in einen finalen Bericht einfließen und über welche Systeme dies erfolgt, z. B. über ein Laboratory Information and Management System (LIMS) oder ein Manufacturing Execution System (MES).

Für das Data-Mapping auf Systemebene empfiehlt es sich, den Analyseprozess mit dem Equipment zu betrachten. Das Mapping umfasst die Daten, die für die Erstellung, Rückverfolgbarkeit, Nachvollziehbarkeit und Auswertung der Daten relevant sind.

Beispiele hierfür sind: Rohdaten, Metadaten, Audit Trails, Parameter, Ergebnisse, verarbeitete Daten.

Sind die relevanten Daten und deren Erzeugung identifiziert, so sind auf diese Daten die Datenintegritäts-Anforderungen anzuwenden. Die Bewertung des Datenrisikos bestimmt die Maßnahmen, die getroffen werden müssen.

Für die Validierung des computergestützten Systems muss dann die Systemgrenze definiert werden, d. h., es ist festzulegen, welche Schnittstellen in der Validierung mitbetrachtet werden sollen. Wenn die Daten elektronisch direkt in ein LIMS übertragen werden, sollte dieses Interface in die Validierung risikobasiert als Schnittstellenbetrachtung einbezogen werden. Bei Hybridsystemen, bei denen die elektronischen Daten im System selbst und auf einem Papierbericht als Rohdaten vorliegen, umfasst der Validierungsumfang den Ausdruck und die Schnittstellenbetrachtung bzgl. der Datensicherung (Abb. 2).

Datenlebenszyklus innerhalb des Systemlebenszyklus

Bei der Validierung eines computergestützten Equipments muss beachtet werden, dass sich der Datenlebenszyklus vom Systemlebenszyklus unterscheidet, da die mit dem Equipment erzeugten Daten über den Equipmentlebenszyklus hinaus aufbewahrt und lesbar gehalten werden müssen. Bei Hybridsystemen ist zudem zu beachten, dass sowohl die elektronischen als auch die Papieraufzeichnungen zu betrachten sind.

Am Beispiel einer Probenanalyse in einem Qualitätskontrolllabor kann der Datenlebenszyklus innerhalb des Systemlebenszyklus nachvollzogen werden (Abb. 3; siehe auch das Lebenszyklus-Modell für analytische Daten von R D McDowall [4]). Bei einer Probennahme und anschließender Probenvorbereitung entstehen bereits Daten, die in das System eingegeben werden, z. B. Chargen- und Proben-IDs. Es erfolgt eine Analyse mit dem Equipment – damit werden Rohdaten und daraus berechnete Daten erzeugt. Dazu gehören auch die jeweiligen Daten, die für die Erzeugung der Rohdaten relevant sind, wie Metadaten, Parameter, Audit Trails. Diese Daten werden

TechnoPharm 10, Nr. 3, 172–175 (2020)

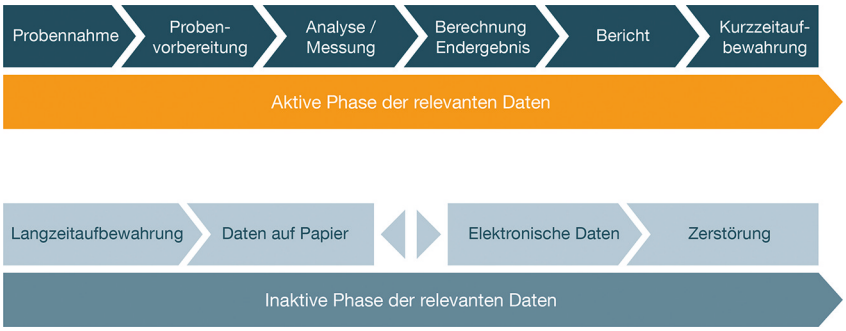

Abbildung 3: Datenlebenszyklus einer Probenanalyse im Quality-Control(QC)-Labor mit einem computerisierten Equipment, das als Hybridsystem betrieben wird.

in einem Review überprüft und anschließend berichtet. Die identifizierten relevanten Daten müssen aufbewahrt und lesbar gehalten werden sowie wiederherstellbar sein. Die Kurzzeitaufbewahrung erfolgt im computerisierten System; zudem existiert ein Backup in einem Datensicherungssystem. In dieser aktiven Phase ist ein Zugriff auf die Daten direkt über das computerisierte Equipment möglich. Die Datenintegrität wird durch die Validierung des Systems und die entsprechenden Maßnahmen im Systemlebenszyklus sichergestellt.

Wenn das computerisierte Equipment stillgelegt wird, erfolgt eine Langzeitaufbewahrung (je nach Aufbewahrungszeitraum) z. B. in einem Archivierungssystem. Hier muss sichergestellt werden, dass es eine Verknüpfung zwischen elektronischen und den dazugehörigen Daten auf Papier gibt. Die Daten werden innerhalb des Aufbewahrungszeitraums bis zur Zerstörung (z. B. durch kontrolliertes Löschen) vorgehalten. Auch in dieser inaktiven Phase müssen Datenintegrität und -sicherheit gewährleistet sein. Es sollte daher bereits bei der Validierung des computerisierten Equipments betrachtet werden, dass eine Langzeitaufbewahrung der relevanten Daten unter diesen Voraussetzungen möglich ist.

Diese Betrachtung beinhaltet nicht den gesamten Datenfluss über die Grenzen computerisierten Equipments hinweg, z. B., dass erzeugte Daten in den Endbericht zur Chargenfreigabe über andere Systeme (etwa ein LIMS) einfließen. Die Abgrenzung zur Validierung des computerisierten Equipments besteht in der Schnittstellenbetrachtung zu einem anderen validierten System, in das die Daten direkt übertragen werden (LIMS, Archivierungssystem, Datensicherungssystem), und ggf. zu Eingabegeräten. Die Validierung eines LIMS oder Datensicherungssystems ist jedoch nicht im Umfang der Equipmentvalidierung zu sehen, sondern muss gesondert durchgeführt werden.

Teil 2 dieses Beitrags wird in Ausgabe 4/2020 erscheinen.

Chefredakteur: Claudius Arndt, Leitender Redakteur: Jens Renke. Verlag: ECV · Editio Cantor Verlag für Medizin und Naturwissenschaften GmbH, Baendelstockweg 20, 88326 Aulendorf (Germany). Tel.: +49 (0) 7525-940 120, Fax: +49 (0) 7525-940 127. e-mail: redaktion-tp@ecv.de. www.ecv.de. Herstellung: rdz GmbH / Holzmann Druck GmbH & Co. KG.