Computersystemvalidierung in Qualitätsmanagementsystemen von Medizinprodukteherstellern

Die Validierung von Computersystemen ist keine neue Anforderung. Bereits seit 1996 fordert die FDA im 21CFR820.70(i) die Validierung von automatisierten System und Software, welche in der Produktion und/oder im Qualitätsmanagementsystem eingesetzt wird. Spätestens mit der Umstellung auf die neue ISO 13485:2016 wurde das auch in Europa klargestellt. Dennoch hadern viele Unternehmen noch immer mit einer pragmatischen Umsetzung dieser Anforderung. Diese Checkliste soll realistische Umsetzungsmöglichkeiten aufzeigen.

Anzuwendende Normen

Für die Validierung der Computersysteme gibt es zahlreiche Richtlinien und auch Normen. Für die Vorgehensweise in dieser Checkliste wurden vor allem folgende Dokumente angewandt:

- FDA Guidance general principles of software validation, January 2002
- ISO/TR 80002-2:2017 Medical device software – Part 2: Validation of software for medical device quality systems

Weitere Dokumente können je nach Bedarf verwendet werden (wie beispielsweise PIC/S GUIDANCE GOOD PRACTICES FOR COMPUTERISED SYSTEMS IN REGULATED “GXP” ENVIRONMENTS, Good Automated Manufacturing Practice Supplier Guide for Validation of Automated Systems in Pharmaceutical Manufacture (“GAMP V”).

Checkliste zur Dokumentationsauswahl

Diese Checkliste gibt eine Auswahl an möglichen Inhalten einer Computersystemvalidierung. Die Inhalte der Checkliste eignen sich im Grundsatz für einfache und auch komplexe Validierungsvorhaben.

Dabei sind drei Schritte vorgesehen:

- Schritt 1: Erfassen der Hardware und Software
- Schritt 2: Ermitteln des Anwendungszwecks der Software
- Schritt 3: Durchführen von Tests

Michael Schaefer –Quality Management and Regulatory Affairs in Medical Devices
Heiligkreuzstrasse 59, 72379 Hechingen, Germany, +49 (0) 171 585 1234, +49 (0) 7471 930 1237
For more information visit www.quality-on-site.com or contact michael@quality-on-site.com

Schritt 1: Erfassen der Hardware und Software

Die folgende Tabelle zeigt typische Bestandteile eines Computersystems in der Produktion, sowie Beispiele der erwarteten Dokumentation und Überprüfung:

Beispiele für Bestandteile	Erwartete Dokumentation und Überprüfung
Hardware	Type und Bezeichnung der speicherprogrammierbaren Steuerung
	Type und Bezeichnung des verwendeten PC‘s
	Angaben zu eingebauten Controllern, Eproms, ...
	Schnittstellen (LAN, WLAN, RS232, USB, ...)
	Leistungsdaten (Prozessor, Speichervolumina, ...)
	Notwendiges Zubehör (Scanner, Verbindungskabel, Festplatten, Hardware-Keys, ...)
	Zugehörige Server (Bezeichnung, Standort, Schnittstellen, ...)
	Zugehörige Workstations oder Drucker
Software	Angaben zum Betriebssystem (Windows 7, Windows 10, Linux, ...)
	Angaben zu fertig gekaufter Software (Excel, Minitab, t-xpert, ...) mit der jeweiligen Versionsnummer
	Angaben zu speziell erstellter oder angepasster Software (ERP-Systeme.....) mit der jeweiligen Versionsnummer
	Selbst erstellte Software (Excel-Arbeitsblätter, Makros, ...) mit den jeweiligen Programmen als Ausdruck

Schritt 2: Ermitteln des Anwendungszwecks der Software

Die folgende Tabelle zeigt Beispiele für typische Anwendungszwecke der Software:

Beispiele qualitätsrelevanter Anwendungszwecke	Beispiele nicht qualitätsrelevanter Anwendungszwecke
Die Software steuert die Anfahrtsposition von Messpunkten bei einer Bauteilprüfung.	Die Software erfasst die Maschinenstillstände zur Berechnung der Produktivität.
Die Software errechnet die Mittelwerte von drei Messwerten zur Inprozesskontrolle.	Die Software berechnet die Herstellkosten eines Medizinproduktes.
Die Software regelt die Prozessparameter eines validierten Produktionsprozesses.	Die Software steuert eine Arbeitsplatz-absaugung, die der Arbeitssicherheit dient.
Die Software archiviert Qualitätsaufzeichnungen.	Die Software archiviert Finanzdaten.

Es wird empfohlen eine Liste aller Software im Qualitätsmanagementsystem und der Produktion anzulegen. Dies erfolgt meist im Rahmen des Validierungsmasterplans (VMP). Darin sollte der Anwendungszweck jeder Software kurz beschrieben sein. Nicht-qualitätsrelevante Software wird meist nicht validiert.

Schritt 3: Durchführen von Tests

Die folgende Tabelle zeigt typische Schritte eines Computersystems, sowie Beispiele möglicher Tests. Welche Tests erforderlich und sinnvoll sind, wird vom Anwendungszweck abhängen und ist üblicherweise auch ein Ergebnis einer risikobasierten Betrachtung. Die Anwendung der EN 14971:2012 wird dazu empfohlen.

Beispiele einzelner Schritte	Beispiele zugehöriger Tests
Passworteingabe zum Starten des Systems	Falscheingabe von Passwörtern
	Unberechtigter Zugriff auf Benutzerebenen
Auswahl eines Fertigungsprogramms	Hochladen eines Fertigungsprogrammes bei Normalauslastung des Datennetzes
	Hochladen eines Fertigungsprogrammes mit maximaler Datenmenge bei hoher Ausnutzung des Datennetzes
	Hochladen eines Fertigungsprogrammes bei Unterbrechung des Datennetzes
Eingabe von Produktionsdaten und/oder Prozessparametern	Eingabe nicht zugelassener Werte (zu kleine Werte, zu große Werte)
	Unterlassen von Dateneingaben
	Eingabe korrekter Werte, auch an den zugelassenen Grenzen
	Eingabe mit unterschiedlichem Syntax (zB Groß-Kleinschreibung, Punkte versus Komma, Sonderzeichen, maximale Nachkommastellen, ...)
Steuern des Produktionsablaufs	Kontrolle ob der Produktionsablauf korrekt ausgeführt wird, auch bei komplizierten Abläufen.
Anzeigen der Produktionsparameter	Kontrolle ob alle Parameter richtig angezeigt werden
Ausgabe von Produktionsdaten und/oder Prozessparametern	Kontrolle, ob die Ausgabe korrekt erfolgt
Bewerten und/oder Berechnung von Ergebnissen	Kontrolle, ob die Ergebnisse richtig bewertet / berechnet werden

	Prüfe ob hinterlegte Berechnungsformeln unberechtigt manipuliert werden können.
Abspeichern von Fertigungsprogrammen, Produktionsdaten, Prozessparametern und/oder Ergebnissen	Abspeichern bei Normalauslastung des Datennetzes
	Abspeichern einer maximalen Datenmenge bei hoher Ausnutzung des Datennetzes
	Abspeichern bei Unterbrechung des Datennetzes
	Kontrolle ob von anderen Nutzern oder von außen ein Zugriff und/oder eine Manipulation der Daten erfolgen kann.
Einscannen von Dokumenten / Aufzeichnungen	Kontrolle, ob Dokumente vollständig und leserlich eingescannt werden.
	Kontrolle, ob beidseitig bedruckte Dokumente als solches eingescannt werden.
Zugriff auf Anlagen / Daten von außen (Fernwartung, Ferndiagnose)	Überprüfen ob Fernwartung, Ferndiagnose möglich ist
	Kontrolle ob ein unberechtigter Zugriff erfolgen (Hacker-Angriff) kann.