Schlüsselwörter	Dokumentation, elektronisch, Aufbewahrung, § 20 AMWHV	
Querverweise, Bezug	42. Sitzung EFG 11 (TOP B5), 43. Sitzung EFG 11 (TOP B8), 44. Sitzung EFG 11 (TOP B6 und B7)	
erstellt	EFG 11	
fachlich geprüft	Dr. Arno Terhechte (EFG 11)	30.01.2020
formell geprüft	Dr. Katrin Reder-Christ (ZLG)	31.01.2020
Beschlussfassung durch:	☒ erstellende EFG ☐ Länderreferentengremien	
beschlossen	EFG 11	04.12.2019
	Humanarzneimittelbereich Dr. Birgit Jung, Vorsitzende AG AATB	- entfällt -
	Tierarzneimittelbereich Dr. Dagmar Duda-Spiegel, Vorsitzende AG TAM	- entfällt -
	Tierimpfstoffbereich Dr. Gabriela Wallner, Vorsitzende AG TT	- entfällt -
	gültig ab	03.02.2020

1 Fragestellung

Die AMWHV bestimmt in § 20, dass die Aufbewahrung von Dokumenten *„in einem geeigneten Bereich der von der Erlaubnis nach § 13, § 72 oder § 72c Absatz 4 des Arzneimittelgesetzes erfassten Räume erfolgen“* muss.

Wie ist diese Anforderung bei elektronischen Dokumenten umzusetzen?

2 Erläuterung

2.1 Hintergrund

Der Trend zur Digitalisierung und zum Ersatz der papierbasierten Dokumentation durch elektronische Aufzeichnungen (E-Records) nimmt im pharmazeutischen Umfeld stetig zu.

Gleichzeitig werden computergestützte Systeme von multinationalen Konzernen global als Client/Server-Lösungen eingeführt. Dieses betrifft Enterprise-Resource-Planning-Systeme (ERP), Manufacturing-Execution-Systeme (MES), Labor-Informations- und Management-Systeme (LIMS), aber auch Systeme zum Change-, CAPA- und Trainingsmanagement.

In den letzten Jahren hat sich der Trend massiv verstärkt, die IT und die computergestützten Systeme teilweise oder vollständig an Dritte zugunsten verschiedener Cloud Service Modelle auszulagern: Infrastructure as a Service (IAAS), Platform as a Service (PAAS) und Software as a Service (SAAS), wobei Letzteres als Servicemodel immer stärker in Anspruch genommen wird.

Die vorherige Version dieses Votums hatte die Konstellation im Fokus, dass ein global arbeitendes Pharmaunternehmen die GMP-kritischen Daten an einer oder mehreren Betriebsstätten vorhält, die nicht in der Herstellungserlaubnis (HE) gelistet sind, jedoch direkt der Organisation (PU oder HE-Inhaber) zuzuordnen sind und somit in der geschlossenen Betriebsumgebung unter dem etablierten und der Überwachung unterliegendem QM-System betrieben werden. Externe IT-Abteilungen werden grundsätzlich unter den genannten Prämissen gleichgestellt.

2.2 Rechtliche Aspekte

§ 10 Abs. 2 AMWHV formuliert zur Dokumentation: *„Werden die Aufzeichnungen mit elektronischen, fotographischen oder anderen Datenverarbeitungssystemen gemacht, ist das System ausreichend zu validieren. Es muss mindestens sichergestellt sein, dass die Daten während der Dauer der Aufbewahrungsfrist verfügbar sind und innerhalb einer angemessenen Frist lesbar gemacht werden können. Die gespeicherten Daten müssen gegen Verlust und Beschädigung geschützt werden.“*

Gem. Annex 11 sollte die IT Infrastruktur (IAAS, PAAS) qualifiziert und die Anwendung (SAAS) validiert werden. Explizit bezogen auf die Datenspeicherung muss gewährleistet sein, dass Daten durch physikalische und elektronische Maßnahmen vor Beschädigung geschützt werden sollen und dass die Verfügbarkeit, Lesbarkeit und Richtigkeit der gespeicherten Daten geprüft werden sollten. Der Zugriff auf Daten sollte während des gesamten Aufbewahrungszeitraums gewährleistet sein.

3 Ergebnis

Im Falle einer elektronischen Dokumentation ist die Anforderung der Aufbewahrung von E-Records/Dokumenten in von der Erlaubnis nach § 13, § 72 oder § 72c Absatz 4 des Arzneimittelgesetzes erfassten Räumen erfüllt, wenn in den von der Erlaubnis erfassten Räumen mindestens ein Endgerät (z. B. Terminal oder PC nebst Drucker) zur Verfügung steht, so dass ein Zugriff auf die Gesamtheit der Daten und Metadaten möglich ist, lesbare Ausdrucke und Kopien auf Datenträgern erzeugt werden können.

Ebenso müssen die Vorgaben zur Qualifizierung der IT-Infrastruktur (IAAS, PAAS), der Validierung der Applikation (SAAS) und die Sicherstellung der Verfügbarkeit, Lesbarkeit und Integrität von einem (internen oder externen) Dienstleister erfüllt werden.

Bei dieser Betrachtung werden die Spezifika und besonderen Risiken, die sich aus dem Bereitstellungsmodell für den jeweiligen Service ergeben, nicht ausreichend berücksichtigt. Die speziellen Risiken, die sich aus einem Shared Service (Private Cloud, Community Cloud, Public Cloud) – also einem Service, den sich der Erlaubnisinhaber mit einer unbestimmten Anzahl weiterer u.U. auch nicht regulierter Nutzer teilt - gegenüber einer konzerninternen Struktur ergeben, müssen Einfluss haben u. a. auf die Entscheidung,

- ob eine externe Lösung akzeptabel ist,
- welche spezifischen Anforderungen sich hinsichtlich Verfügbarkeit und Vertraulichkeit ergeben,
- welches Bereitstellungsmodel (Private Cloud, Community Cloud) geeignet ist,
- welche Nachweise der Serviceprovider erbringen muss, um zu belegen, dass er die o. g. spezifischen Anforderungen erfüllt,
- welche sicherheitsrelevanten Anforderungen an den Zugriff zu stellen sind.

Aus diesem Grund sind auch Anforderungen an den Erlaubnisinhaber zu stellen, die die Voraussetzung für die Nutzung eines Cloud Services (CS) sein sollten:

- Data Assessment

  Das Data Assessment sollte analysieren, welche Anforderungen an Vertraulichkeit, Integrität und Verfügbarkeit der Daten bestehen.

- Assessment der Kritikalität der Applikation

  Sofern SAAS Lösungen genutzt werden, ist die Kritikalität der Anwendung zu beurteilen. Dabei ist der Einfluss auf die Produktqualität und Patientensicherheit entscheidend. D. h. „Produktnahe Systeme“ wie ein MES oder LIMS sind kritischer als Systeme, die qualitätssichernde Prozesse wie „Training, Änderungskontrolle“ unterstützen.

- Assessment zur Business Continuity

  Welche Risiken bestehen für die Patientenversorgung, wenn der Service nicht zur Verfügung steht.

Basierend auf diesen Ergebnissen, sollte die Entscheidung getroffen werden, ob ein Outsourcing und im Besonderen die Nutzung eines CSP möglich ist, ohne dass daraus eine Gefährdung für Patientinnen/Patienten und/oder die Qualität des Arzneimittels besteht.

Falls ein Outsourcing bejaht wird, sollten nachvollziehbare und verifizierbare Anforderungen als Ergebnis des Assessments resultieren, die

- die Grundlage für die Auswahl des CSP bilden.
- im Service Level Agreement verankert sind.
- im Rahmen der Qualifizierung und Validierung verifiziert wurden.
- im Rahmen eines kontinuierlichen Assessments des CSP im Sinne von Quality Attributs überprüft werden können.
- die Löschung der Daten nach Beendigung des Geschäftsverhältnisses sicherstellen.
- die Verlagerung der Daten oder der Anwendung zurück oder zu einem anderen CSP ermöglichen.

Im Folgenden sind Anforderungen an die Qualität des CSP und die Datenintegrität (für Daten in Bewegung und in Ruhe) formuliert, die sich so explizit nicht im EU-GMP-Leitfaden wiederfinden, jedoch aus Sicht der EFG 11 als sinnvoll erachtet werden:

- Übertragung von Daten nur in verschlüsselter Form und in einer Art und Weise, die sicherstellt, dass die Daten vollständig und unverändert übertragen wurden.
- CSP, die vertrauliche Daten oder Daten mit hohen Anforderungen an die Verfügbarkeit in der Verantwortung bearbeiten, müssen über ein zertifiziertes ISMS verfügen (z. B. gemäß DIN 27001).
- CSP, die vertrauliche Daten und Daten mit hoher Kritikalität bearbeiten, müssen sich im Rahmen Ihrer Qualifizierung einem Penetrationstest unterziehen.
- Die Art der Speicherung kritischer Daten ist risikobasiert festzulegen (z. B. Nutzung geeigneter kryptographischer Verfahren).
- Das Bereitstellungsmodell sollte in Abhängigkeit der Kritikalität gewählt werden. Private und Community Cloud Modelle sind für vertrauliche Daten der Public Cloud vorzuziehen.

Die Qualifizierung und das fortlaufende Monitoring eines CSP sind umso wichtiger, je höher die Anforderungen an den Service und das Bereitstellungsmodell zu stellen sind. Eine mangelhafte Konfiguration der Infrastruktur kann zum Ausfall des Service oder zum Verlust oder Kompromittierung der Daten führen. Auf Basis einer Risikobewertung ist zu entscheiden, ob ein vor-Ort-Audit erforderlich ist. Beim Audit sind Personen zu beteiligen, die über ausreichende Erfahrungen in dieser speziellen Technologie verfügen. Je nach bereitgestelltem Service und Bereitstellungsmodell sollten mindestens folgende Aspekte im Audit adressiert werden:

- Sicherheit des Rechenzentrums
- Serversicherheit
- Netzsicherheit
- Anwendungs- und Plattformsicherheit
- Datensicherheit
- Verschlüsselungs- und Schlüsselmanagement
- ID- und Rechtemanagement
- Auswahl und Training der Mitarbeitenden
- Validierung und Qualifizierung

- externe Services und Subunternehmer
- Erhaltung des validierten Zustandes (Changemanagement, Konfigurationsmanagement, Patchmanagement, Monitoring und Reporting, Incident Management)

Es gelten grundsätzlich die gleichen Anforderungen an einen CSP wie an einen regulierten Nutzer. In der Praxis ergeben sich häufig folgende Unterschiede:

- Die Infrastruktur ist nicht dokumentiert qualifiziert.
- Änderungen an der Hard- und Middleware sowie den sicherheitsrelevanten Komponenten erfolgen ohne Zustimmung des Erlaubnisinhabers. Eine Benachrichtigung über Änderungen erfolgt kurzfristig oder gar nicht.
- Das QM-System des Cloud Service Providers entspricht nicht den EU-GMP-Standards.
- Ohne vorherige Zustimmung des Erlaubnisinhabers werden vom CSP Subunternehmer/Dienstleister eingesetzt, um die Infrastruktur (Rechenleistung, Storage) zu erweitern.

Datenschutzrechtliche Bestimmungen bleiben unberührt.

4 Definitionen, Abkürzungen und grundlegende Dokumente

4.1 Definitionen und Abkürzungen

Cloud Computing: Cloud Computing ist ein Modell, das es erlaubt, bei Bedarf jederzeit und überall bequem über ein Netz auf einen geteilten Pool von konfigurierbaren Rechnerressourcen (z. B. Netze, Server, Speichersysteme, Anwendungen und Dienste) zuzugreifen, die schnell und mit minimalem Managementaufwand oder geringer Serviceprovider-Interaktion zur Verfügung gestellt werden können

Community Cloud: In diesem Model wird die Infrastruktur von mehreren Institutionen geteilt, die ähnliche Interessen haben. Eine solche Cloud kann von einer dieser Institutionen oder einem Dritten betrieben werden.

CSP (Cloud Service Provider): Ein **Cloud Service Provider** ist ein Drittanbieter, der eine **Cloud**-basierte Infrastruktur oder Plattform oder einen Dienst/Applikation anbietet.

ERP (Enterprise-Resource-Planning): ERP bezeichnet die unternehmerische Aufgabe, Ressourcen wie Kapital, Personal, Betriebsmittel, Material und Informations- und Kommunikationstechnik im Sinne des Unternehmenszwecks rechtzeitig und bedarfsgerecht zu planen, steuern und verwalten. Eine Kernfunktion von ERP ist in produzierenden Unternehmen die Materialbedarfsplanung.

IAAS (Infrastructure as a Service): Bereitstellung von IT-Ressourcen wie z. B. Rechenleistung, Datenspeicher oder Netzen als Dienst

LIMS (Labor-Informations- und Management-System): Diese Kategorie von Softwaresystemen befasst sich mit der Datenverarbeitung im analytischen Labor. Es handelt sich um Software-basierte Labor- und Informations-Managementsysteme, die den Betrieb eines modernen Labors unterstützen, indem sie für die Auftragserfassung, Methoden-, Proben- Standard- und Messwertverwaltung eingesetzt werden.

MES (Manufacturing Execution System): Als Manufacturing Execution System wird eine prozessnah operierende Ebene eines mehrschichtigen Fertigungsmanagementsystems be-

zeichnet. Es zeichnet sich durch die direkte Anbindung an die verteilten Systeme der Prozessautomatisierung aus und ermöglicht die Führung, Lenkung, Steuerung oder Kontrolle der Produktion in Echtzeit.

PAAS (Platform as a Service): Bereitstellung einer kompletten Laufzeit- bzw. Entwicklungsumgebung als Dienstleistung

SAAS (Software as a Service): Bereitstellung von IT-Anwendungen als Dienstleistung

Private Cloud: Hier wird die Cloud-Infrastruktur nur für eine Institution betrieben. Sie kann von der Institution selbst oder einem Dritten organisiert und geführt werden und kann dabei im Rechenzentrum der eigenen Institution oder einer fremden Institution stehen.

Public Cloud: Von ihr wird gesprochen, wenn die Services von der Allgemeinheit oder einer großen Gruppe, wie beispielsweise einer ganzen Industriebranche, genutzt werden können und von einem Anbieter zur Verfügung gestellt werden.

Regulierter Nutzer: z. B. der Inhaber der Herstellungs- oder Importerlaubnis oder der Pharmazeutische Unternehmer

4.2 Grundlegende Dokumente

- Gesetz über den Verkehr mit Arzneimitteln (Arzneimittelgesetz, AMG)[1]
- Verordnung über die Anwendung der Guten Herstellungspraxis bei der Herstellung von Arzneimitteln und Wirkstoffen und über die Anwendung der Guten Fachlichen Praxis bei der Herstellung von Produkten menschlicher Herkunft (Arzneimittel- und Wirkstoffherstellungsverordnung, AMWHV)[1]
- EU-GMP-Leitfaden, Teil I und Annex 11[1]
- BSI Eckpunktepapier „Sicherheitsempfehlungen für Cloud Computing Anbieter“ (Stand: Februar 2012)
- ENISA „Cloud Computing: Benefits, Risks and Recommendations for Information Security“ (Stand: November 2009)

[1] In der zum Zeitpunkt der Publikation des Votums geltenden Fassung.