22. Jahrgang · November · 3/2020

PM QM

Fachzeitschrift für pharmazeutische Medizin und Qualitätsmanagement

3

ZUR SACHE
Datenspende als Chance

BERICHTE + ANALYSEN + MEINUNGEN
Digital Health and Digital Treatments: The New Reality

QUALITÄTSMANAGEMENT
Kann die CLOUD eine GxP-konforme Lösung für die Pharmaindustrie sein?

DGPharMed
Deutsche Gesellschaft für Pharmazeutische Medizin e.V.

GQMA
GERMAN QUALITY MANAGEMENT ASSOCIATION E.V.

Cloud Computing: unterschiedliche Cloud-Modelle und ihre Vor- und Nachteile – Was die Experten sagen

Kann die CLOUD eine GxP-konforme Lösung für die Pharmaindustrie sein?

Um den Einbezug einer Cloud-basierten Lösung in das Pharmaumfeld ging es in der letzten Ausgabe dieses Journals [PM QM 2020, 22/2:104-107]. Es wurden gängige Cloud-Modelle kurz und übersichtlich präsentiert und besondere Anwendungsfälle vorgestellt. Gerade für das stark reglementierte Pharmaumfeld stellen sich viele Fragen, insbesondere: Wie geeignet und konform ist ein Cloud-basierter Ansatz bzw. kann dieser sein? Der folgende Beitrag und die darin enthaltenen Experteninterviews liefern Einblicke in die Sicht- und Denkweise eines XaaS Dienstleisters – „X as a Service", wobei X für eines der verschiedenen Cloud-Modelle stehen kann –, eines Pharmaunternehmens als Kunde, einem Cloud-Provider als Dienstleister, einem Vertreter einer deutschen Behörde und schlussendlich einem Anwendungsprovider.

| Dr. Arno Terhechte, Dr. Philipp Osl, Patrick Pichler, Björn Niggemann

Die Cloud im Server-Raum. © ELPRO

Vorbemerkungen

Zur kurzen Erklärung der Cloud-Modelle werden nachfolgend die drei Kernbegriffe nochmals genannt:

- **Cloud-Provider** • Das ist der Anbieter von Cloud-Lösungen, wie z.B. Amazon, Microsoft, Google etc., der die Cloud-Infrastruktur (Hardware bzw. Software) zur Verfügung stellt.
- **Anwendungsprovider** • Das ist diejenige Organisation (z. B. ein Unternehmen, eine Contract Research Organization – CRO), die dem Endkunden (Kunde bzw. Nutzer) eine Cloud-Lösung für eine Applikationsanwendung zur Verfügung stellt bzw. im Kundenauftrag betreibt. Der Anwendungsprovider nutzt dafür die Services eines Cloud-Providers. Ein Beispiel: Kunden, die eine Reise planen, nutzen dazu z. B. das Online-Reiseportal Expedia. Expedia ist dabei der Anwendungsprovider, der dem Reise-Kunden seine Services anbietet. Expedia selbst

nutzt für diese Kunden den Cloud-Provider Amazon Web Services.
- **Kunde** • Der Kunde ist der Nutzer, der schlussendlich die Cloud-Lösung für sich oder sein Unternehmen nutzt.

Das nachfolgende Interview mit Experten gibt Antworten auf allgemeine Fragen, die alle drei eben genannten Parteien gleichermaßen beschäftigen. Dabei können die Fragen niemals abschließend beantwortet werden. Auch beruhen die Antworten des jeweiligen Experten (Partei) auf eigenen Anschauungen und beruflicher Erfahrungen aus der eigenen Praxis und können somit nicht als generell gültiger Standard betrachtet werden. Dennoch soll der Beitrag eine Basis schaffen, auf der alle in einen Cloud-Implementierungsprozess eingebundenen Parteien aufbauen können. Die ausgewählten Fragen sind insofern ein Konsens zwischen den vier Autoren dieses Beitrags, als dass sie die wichtigsten und immer wiederkehrenden Fragen verkörpern.

Dieser Beitrag und die Interviews hinterfragen die Ablage von Daten auf Servern externer Supplier. Dazu sind grundsätzlich zwei Aspekte zu unterscheiden:

Einerseits ist es bereits Standard, Daten auf Servern diverser Provider selbst abzulegen. Nachfolgend wird jedoch nicht detailliert darauf eingegangen, um was für Daten es sich im Speziellen handelt; das wäre sehr komplex. Der Beitrag bleibt aufgrund der Komplexität eher generell. Bei der Verwendung des Begriffs „GMP Daten" (Good Manufacturing Practice) würde es sonst kompliziert, und ein solcher Beitrag würde den Rahmen dieses Journals überschreiten. In der Praxis werden vermutlich nur sehr wenige Unternehmen ihre Batch Reports extern ablegen. Mit beispielsweise Dokumenten wie Standard Operating Procedures (SOPs) oder Guidance Dokumenten ist man da heutigen Tags aber schon ein Stück weiter.

Der zweite Aspekt und vermutlich der interessantere ist die Ablage von Daten durch Dritte. Zweckdienlich und transparent ist es, die Thematik an einem Beispiel zu hinterfragen: Bereich Data Logger Leasing – was passiert mit diesen Daten?

Daran angelehnt sind die Fragen einfacher zu verstehen bzw. zu beantworten, lassen sich aber nicht auf alle anderen Bereiche ausdehnen.

Einleitung

Die Cloud kennen wir zwischenzeitlich alle – sie ist meistenorts aus unserem Alltag nicht mehr wegzudenken und macht vor allem unser Privatleben einfacher. Die Zeiten, in denen wir uns Sorgen machen mussten, wie wir Daten von A nach B bekommen, damit jemand anderes auch darauf zugreifen kann, sind im Grund vorbei. Aber, wie bereits im letzten Beitrag erläutert, zieht die Cloud mehr und mehr in die industrielle Nutzung ein. Was auch gut ist, denn in Zeiten von Klimawandel, Lean Management und Globalisierung braucht es auch hier ein Umdenken. „Schneller", „effizienter" und „klimafreundlicher" sind somit nur einige wenige aber wichtige Stichwörter im Cloud-Zusammenhang.

Aber die Einführung und Anwendung einer Cloud gestaltet sich in vielen Bereichen schwierig. Gründe dafür gibt es viele, vor allem aber sind es Bedenken hinsichtlich der Einhaltung der Vorgaben in Richtlinien, Gesetzen und Verordnungen, hinsichtlich der Wahrung der Datenintegrität, Datensicherheit, Rückverfolgbarkeit, Ausfallsicherheit etc. Aus diesem Grund haben sich alle Parteien der Lieferkette bis hin zur Behörde zusammengetan und liefern Antworten auf die wichtigsten Fragen als Grundbaustein für den Entscheid: Cloud – Ja oder Nein? Allenfalls muss man den Begriff Cloud hier an dieser Stelle „vermeiden" – technisch reden wir letztlich von einem Server und der dazugehörenden Kunden-Schnittstelle.

Wem gehören die Daten in der Cloud? Auf welche Regelungen muss ich als Kunde in den Verträgen mit dem Anwendungsprovider besonders achten?

Dr. Arno Terhechte: Ich möchte in diesem Zusammenhang den Begriff RU (Regulated User, welcher dem Erlaubnisinhaber – Herstellungserlaubnis gemäß § 13 AMG sowie Importerlaubnis gemäß § 72 AMG – entspricht) verwenden. Gemäß § 10 (2) Arzneimittel- und Wirkstoffherstellungsverordnung (AMWHV) ist der RU dafür verantwortlich, sicherzustellen, dass – wenn Aufzeichnungen mit elektronischen, fotografischen oder anderen Datenverarbeitungssystemen gemacht werden – das System ausreichend zu validieren ist. 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. Zudem muss der RU die Datenschutz-Grundverordnung (DGSVO) beachten. Kritisch sind im Besonderen Daten, die vertraulich sind und/oder persönliche Daten enthalten. Dieses ist z. B. relevant für klinische Plattformen oder Blutbanksoftware, die als Software-as-a-Service (SaaS) über ein Cloud-Model bereitgestellt werden. Aus technischer Sicht sind territoriale Grenzen im Cloud Computing natürlich unerheblich. Für das geltende Recht ist dagegen der Ort der Verarbeitung relevant.

Bei der Gestaltung von Verträgen (Service Level Agreement – SLA) mit dem Cloud Solution Provider (CSP) sollten folgende Aspekte beachtet werden:
- Serviceumfang, Responsezeiten, Verfügbarkeit
- Server/Datenstandorte
- Subunternehmer, Dienstleister der CSP
- Zertifizierung, Nachweis der Erfüllung von Sicherheitsstandards
- Kommunikation und Ansprechpartner

- Möglichkeit und Tools, um den Service zu monitoren
- Umgang mit Sicherheitsereignissen
- Regelungen zum Vorgehen bei Änderungen
- Escape Strategien, Business Continuity
- Vertragsstrafen für die Nichteinhaltung der Vereinbarungen

Dr. Philipp Osl: Die Data Ownership, also die Frage, wem die Daten gehören, gilt es jedenfalls vertraglich zu klären. Für Monitoring-Daten ist es aus meiner Sicht unstrittig, dass diese dem Kunden gehören. Für die Zukunft werden allerdings zusätzliche Fragestellungen interessant werden, wie z. B. ob der Kunde als Dateneigner dem Anwendungsprovider ein anonymisiertes Nutzungsrecht einräumen möchte, damit dieser auf Basis der Daten vieler Kunden eine Heat Map der Problempunkte im globalen Transportnetzwerk aggregieren kann – ein Service, von dem der Kunde zur besseren Planung seiner Transportwege wiederum profitieren würde. Wichtig ist, wie gesagt, eine klare vertragliche Regelung.

Welche Bedeutung hat der geografische Speicherort, d. h. der Standort der Server?

Dr. Arno Terhechte: Die Wahl des geografischen Speicherortes ist relevant, wenn man sicherstellen möchte, dass Dritte aufgrund bestehender nationaler Gesetze nicht auf Daten des RU zugreifen können sollen (Beispiel USA) und der RU dadurch vermeiden kann, gegen die DGSVO zu verstoßen. Eine andere Motivation besteht darin, dass der RU sein geistiges Eigentum schützt, indem er den Speicherort spezifiziert.

Dass der geografische Speicherort der einzige Ort ist, an dem die Daten gespeichert sind und nicht z. B. Subunternehmen in anderen geografischen Regionen als Back-up oder Infrastructure as a Service (IAAS) installiert sind, sollte im SLA fixiert und im Rahmen der CSP-Qualifizierung verifiziert werden.

Dr. Philipp Osl: Der geografische Speicherort ist aus Datenschutz- und sonstigen rechtlichen Gründen entscheidend, um den Zugriff durch unerwünschte „Autoritäten" zu verhindern. Demgegenüber sollte angesichts der zunehmenden Verwendung von Datenbank-Clustern auch für On-Premise-Lösungen die Frage nach dem genauen Server bzw. der exakten Festplatte keine Rolle mehr spielen.

Macht es aus regulatorischer Sicht einen Unterschied, ob ich eine private Instanz der in der Cloud betriebenen Anwendung nutze oder eine geteilte Instanz?

Dr. Arno Terhechte: Basierend auf den Ergebnissen des Data Assessments, des Assessments der Kritikalität der Applikation und des Assessments zur Business Continuity 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 entsteht. Wird ein Outsourcing bejaht, sollte das Bereitstellungsmodell in Abhängigkeit der Kritikalität gewählt werden. Private und Community Cloud Modelle sind für vertrauliche Daten der Public Cloud vorzuziehen. Die Art und Weise, wie unterschiedliche Tenanten (Mieter oder Pächter) voneinander abgegrenzt und getrennt sind, ist abhängig vom Bereitstellungsmodell und in einer „Private Cloud" besser als in einer „Public Cloud".

Dr. Philipp Osl: Derartige Entscheidungen sind selbstverständlich immer risikobasiert zu fällen. Von einem technischen Standpunkt aus ließe sich argumentieren, dass für GxP-Anwendungen eine sichere Steuerung der Zugriffe auf Benutzerebene gewährleistet sein muss, also auf einer granulareren Ebene als zwischen unterschiedlichen Organisationen, die sich eine Instanz einer Cloud-Anwendung teilen. So gesehen dürfte aus einer Datensicherheits- und -integritätsperspektive die Frage nach Public oder Private Cloud keine Rolle spielen. Allerdings wird es i.d.R. Unterschiede bei anderen wichtigen Aspekten geben, beispielsweise bei der Bestimmung von Zeitpunkten für das Einspielen von Updates. Hier bieten private Instanzen zweifelsohne Vorteile.

Welche Dokumentation seitens des Cloud-Providers muss mindestens vorliegen? Genügt ein aktueller SOC II-Bericht (System and Organization Control)?

Dr. Arno Terhechte: Gemäß Annex 11 [Computerised Systems – EudraLex Volume 4 GMP] sind Kompetenz und Zuverlässigkeit des Lieferanten Schlüsselfaktoren bei der Auswahl eines Produktes oder eines Dienstleisters. Die Notwendigkeit eines Audits sollte auf einer Risikobewertung basieren.

Das heißt, 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 zur Kompromittierung der Daten führen. Auf Basis einer Risikobewertung ist zu entscheiden, ob ein Vor-Ort-Audit erforderlich ist. Eine Zertifizierung kann die Compliance mit Sicherheitsstandards bescheinigen. Vorzuziehen sind internationale Normen, die die spezielle Thematik des Services adressieren: ISO/IEC 27001 Information Technology – Security Techniques – Information Security Management Systems – Requirements, ISO/IEC 27017: Cloud Computing Security and Privacy Management System-Security Controls, ISO/IEC 27036-4: Guidelines for security of cloud services. In jedem Fall sollte der Scope des Zertifikates bewertet werden.

Wie auditiere ich einen Cloud-Anbieter, wenn dieser keine Audits zulässt?

Dr. Arno Terhechte: Wenn die Assessments zu dem Ergebnis kommen, dass ein Vor-Ort-Audit erforderlich ist, ist in der Konsequenz ein CSP, der dieses nicht zulässt, nicht

geeignet. Hingewiesen sei an dieser Stelle auf die Möglichkeit der Joint Audits oder Shared Audits.

Björn Niggemann: Es besteht auch immer die Möglichkeit, bei einem Cloud-Anbieter ein Joint-Audit anzufragen. Das bedeutet, dass sich mehrere Unternehmen bzw. Kunden zusammenschließen, um gemeinsam ein für alle gültiges und anwendbares Audit durchzuführen. Das reduziert den Aufwand auf allen Seiten, liefert aber gleichzeitig einen guten Nachweis der Einhaltung rechtlicher Vorgaben und Kundenvorgaben. Ein solches wird beispielsweise gerade bei Amazon Cloud Services in München geplant.

Wie kann eine Cloud validiert werden? Welche Ansätze sind ein Muss?

Dr. Arno Terhechte: Die Applikation muss validiert und die Infrastruktur qualifiziert werden. Die Validierung der Applikation entspricht im Wesentlichen der einer Applikation on premise. Annex 11 und GAMP 5 (Good Automated Manufacturing Practice) liefern hier entsprechende Hinweise. Die Herausforderung ist die Trias aus CSP, RU und Softwareanbieter. Hier sind eine gute Kommunikation und ein gutes Projektmanagement erforderlich.

Die Qualifizierung einer dynamischen Infrastruktur, die zudem einem sehr dynamischen Weiterentwicklungsprozess unterliegt, ist die tatsächliche Herausforderung. Hier bestehen häufig Schwächen der CSP, dem RU gegenüber die sogenannte „documented evidence" zur Verfügung zu stellen, die es dem RU ermöglicht, von einer qualifizierten Infrastruktur auszugehen.

Dr. Philipp Osl: Bei der Validierung von GxP-relevanten Anwendungen, wie sie ELPRO bereitstellt, gibt es keine Unterschiede zwischen Cloud- und On-Premise-Lösungen.

Wie können die Eigentümerrechte von Daten geschützt werden?

Dr. Philipp Osl: Da die Eigentümerrechte von Daten mit denen

Cloud Computing und Regularien. © ELPRO

von anderen Sachgegenständen identisch sind, können aus Sicht des Unternehmens ELPRO auch analog dieselben Schutzmechanismen genutzt werden:

- Datenzugriff auf die Kundendaten durch den Cloud-Provider sehr klar definieren und vertraglich festhalten.
- Strikte Begrenzung des Datenzugriffs vom Anwendungsprovider auf die Kundendaten (Zugriff auf den Root-Server haben nur sehr wenige, ausgewählte Mitarbeiter des Anwendungsproviders).
- Zugriffe auf Kundendaten durch den Anwendungsprovider über den Root-Server werden in einem Audit-Trail mitprotokolliert und erfasst.
- Zugriffe von Dritten werden durch klar definierte Sicherheitsmechanismen so gut wie möglich unterbunden. Die Infrastruktur wird kontinuierlich auf Hackerangriffe überwacht. Erfolgreiche Hacking-Angriffe werden analysiert und dokumentiert. Gehackte Zugriffsdaten (Passwörter etc.) müssen umgehend vom Cloud-Provider oder Anwendungsprovider durch neue ersetzt werden. Der Kunde wird über den Datenangriff informiert und ihm werden die neuen Zugriffsdaten übermittelt. Die Sicherheitslücke wird schnellstmöglich durch geeignete Maßnahmen abgestellt und geschlossen. Falls möglich, wird der Hackerangriff zurückverfolgt.
- Auf Wunsch des Kunden müssen die Daten durch den Anwendungsprovider sicher und unwiderruflich vernichtet werden, z. B. wenn das Vertragsverhältnis endet.
- Sämtliche oben genannten Punkte – und sicherlich noch viele weitere – sollten im SLA klar benannt und definiert sein. Der Anwendungsprovider sollte entsprechende Klauseln in dem SLA mit dem Cloud-Provider haben und der Kunde sollte entsprechende SLA-Vereinbarung mit dem Anwendungsprovider abschließen.

Wie kann ich Datenintegrität in der Cloud gewährleisten, wenn ich nicht selbst Eigner der Cloud bin?

Dr. Arno Terhechte: Annex 11 führt hierzu aus, dass Daten durch

Audit eines Cloud-Anbieters. © ELPRO

physikalische und elektronische Maßnahmen vor Beschädigung geschützt werden sollten. Die Verfügbarkeit, Lesbarkeit und Richtigkeit gespeicherter Daten sollten geprüft werden. Der Zugriff auf Daten sollte während des gesamten Aufbewahrungszeitraums gewährleistet sein. Nach Ansicht des Bundesamts für Sicherheit in der Informationstechnik (BSI) kann dieses nur durch kryptografische Verfahren gewährleistet werden. Diese Ansicht teile ich.

Dr. Philipp Osl: Verschlüsselungen bilden den logischen Ersatzpunkt. Um Manipulationen wirksam auszuschließen, bieten sich darüber hinaus auch Blockchain-basierte Lösungen an. Der zusätzlichen Sicherheit stehen aber hohe Rechenaufwände und letztlich auch die verteilte Datenhaltung in Blockchains entgegen. Dennoch werden wir zukünftig neue Lösungen in diesem Bereich sehen.

Kenne ich immer die Speicherorte meiner Daten? Und kann ich darauf Einfluss nehmen?

Dr. Arno Terhechte: Siehe dazu weiter oben. Sofern der Speicherort kritisch ist, muss dieser im Rahmen des SLA festgelegt und im Rahmen der Qualifizierung verifiziert werden. Dieses ist nicht nur GxP, sondern auch Business kritisch.

Wie werden Cloud-Server vor externen Zugriffen gesichert? Wer ist für diese Sicherung verantwortlich? Wer ist letztendlich haftbar? Werden sensibel Daten (Patientendaten, Studienergebnisse …) anders behandelt als nicht sensible Daten? Kann man Cloud-Daten löschen?

Dr. Arno Terhechte: Es muss für den RU gewährleistet sein, dass seine Daten auf allen Speichermedien und Speicherorten sowie in allen Versionen (z. B. verschiedene Back-up-Versionen) gelöscht werden, wenn die Geschäftsbeziehung beendet wird oder wenn der RU dieses wünscht. Dieses sollte Bestandteil des SLA und der Qualifizierung sein.

Gibt es so etwas wie einen Audit-Trail in der Cloud, also die Nachvollziehbarkeit, wer wann welche Änderungen in der Cloud gemacht hat?

Dr. Arno Terhechte: Ja, zumindest sollte eine Log-Datei verfügbar sein.

Wie kann ich während des Audits eines Cloud-Providers sicherstellen, dass es sich um genau diese Server handelt, die meine Daten hosten? Wie trainiert sind Cloud-Anbieter auf die regulatorischen Vorgaben wie GAMP 5 und 21 CFR part 11?

Dr. Arno Terhechte: Ein CSP muss nicht nach GAMP 5 oder 21 CFR (Code of Federal Regulations) Part 11 arbeiten, aber er muss über ein geeignetes Framework verfügen, welches äquivalenten Prinzipien folgt. Wenn dieses Framework sich an den Grundsätzen des EU-GMP-Leitfadens und/oder GAMP 5 orientiert, hilft es der Pharmaindustrie.

Besteht die Notwendigkeit sowie die technische Möglichkeit, über einen regelmäßigen Report die Ablage der Daten sowie deren Attribute zu verifizieren?

Dr. Arno Terhechte: Gemäß Annex 11 sollte die IT-Infrastruktur (IAAS, Platform as a Service – 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 und dass die Verfügbarkeit, Lesbarkeit und Richtigkeit der gespeicherten Daten geprüft werden sollen (s. o.). Der Zugriff auf Daten sollte während des gesamten Aufbewahrungszeitraums gewährleistet sein.

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 (Expertenfachgruppe computergestützte Systeme – Zentralstelle der Länder für Gesundheitsschutz bei Arzneimitteln und Medizinprodukten) 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.
- Die Art der Speicherung kritischer Daten ist risikobasiert festzulegen (z. B. Nutzung geeigneter kryptografischer Verfahren).

Welche Dokumentation seitens des Providers muss mindestens zur Verfügung stehen? Welchen Umfang muss die Qualifizierung des Systems beinhalten? Wie ist die Tiefe der Validierung der Schnittstellen und Funktionen?

Dr. Arno Terhechte: Es gelten grundsätzlich die gleichen Anforderungen an einen CSP wie an einen regulierten Nutzer. In der Praxis werden häufig folgende Defizite beobachtet:
- 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.

Fazit

Fragen, Sorgen und Bedenken gibt es viele. Wahrscheinlich nahezu unendlich viele. Nichtsdestotrotz haben wir die in unseren Augen wichtigsten Fragen mit den passenden Antworten aus verschiedener Perspektive zusammengefasst. Schlussendlich liegt die Verantwortung am Ende des Tages aber beim Kunden und damit beim Anwender der Cloud. Der Kunde allein entscheidet, ob, wie und welchen Weg man gehen möchte, um sich diesem Thema gewappnet zu stellten.

Am Ende des Tages ist und bleibt im Pharmabereich die Patientensicherheit das schützenswerteste Gut. Software muss funktionieren, Daten müssen verfügbar, manipulationsgeschützt, rückverfolgbar und integer sein. Unterschriften und Authentizität sind hierbei ebenso wichtig.

Daten sind, was unser digitales tägliches Leben heute ausmacht: unser virtuelles Lebenselixier. Wem wir das anvertrauen wollen und können, muss jeder für sich entscheiden. Die gelieferten Antworten sollen und können hoffentlich bei einer solchen Entscheidung helfen, wohlwissend, dass diese nicht abschließend sind oder jemals sein können. |

AUTOREN

Dr. Arno Terhechte, Regierungspharmaziedirektor, Bezirksregierung Münster, war nach dem Studium der Pharmazie und anschließender Promotion fünf Jahre in der Pharmazeutischen Industrie in den Geschäftsbereichen nationale Zulassung, internationale Zulassung und Qualitätskontrolle, zuletzt in der Funktion als stellv. Kontrollleiter, tätig. Seit 1998 war er bei der Bezirksregierung Düsseldorf in der Überwachung von Arzneimittelherstellern, seit 2003 ist er bei der Bezirksregierung in Münster im Pharmaziereferat tätig. Hier führt er neben der Überwachung von Arzneimittelherstellern Begehungen von Medizinprodukteherstellern und -betreibern durch. Er ist Leiter der Expertenfachgruppe 11 Computergestützte Systeme und Mitglied der Arbeitsgemeinschaft für Pharmazeutische Verfahrenstechnik e.V. (APV) Fachgruppe „Informationstechnologie“.

Dr. Philipp Osl ist CEO der ELPRO Gruppe. Neben seinem Studium in Wirtschaftsinformatik und einem Doktorat in „Business Innovation“ blickt er auf Erfahrungen als Projektleiter, Produktmanager und Gründer eines Technologie-Start-ups mit Niederlassungen in der Schweiz und Polen zurück.

Patrick Pichler ist studierter Biotechnologe und hat acht Jahre für die Österreichische Agentur für Gesundheit und Ernährungssicherheit (AGES) als Inspektor gearbeitet. Vorher war er elf Jahre unter anderem als Leiter Qualitätskontrolllabor in mehreren Firmen tätig. Seit 2019 ist er bei Merck beschäftigt und seit 2014 in der Rolle Head of Distribution Quality im Bereich Good Distribution Practice (GDP) zuständig.

Björn Niggemann ist seit April 2016 bei der ELPRO-BUCHS AG als Chief Quality Officer tätig. 2004 war er zunächst mit dem Aufbau und der Implementierung von GMP parallel zur bestehenden DIN ISO 17025-Zertifizierung beauftragt. 2007 hat er als Compliance Manager zu einem bestehenden Good Laboratory Practice (GLP) System ein GMP-System aufgebaut. Von 2009 bis 2010 arbeitete er bei einem Pharmadienstleister als GLP/cGMP Compliance Manager. 2010 bis 2016 war er in einem Schweizer Biotech-Unternehmen in der Rolle des Head of Operations and Quality tätig. Er ist zudem Präsident der GQMA – Germany Quality Management Association e.V.

Kontakt:
bjoern.niggemann@elpro.com