Validierung von computergestütztem Equipment

Beachtung der Datenintegrität im GMP-Bereich – Teil 2*)

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

Technische und organisatorische Umsetzungen

Prinzipiell können die Maßnahmen zum Schutz der Datenintegrität auf 2 Ebenen umgesetzt werden:

- Technische Ebene: Hierzu gehören technische Umsetzungen zur Automatisierung und technische Kontrollen durch das computerisierte System. Der technische Maßnahmenkatalog sollte zusätzlich IT-Lösungen beinhalten.
  - Das effektivste Mittel, um v. a. unbeabsichtigte und unkontrollierte Änderungen an Daten zu verhindern, sind technische Maßnahmen. Dennoch sind organisatorische Maßnahmen notwendig, um das System konform zu betreiben und bestehende Risiken zu mindern.
- Prozedurale/organisatorische Ebene: Zu den organisatorischen Maßnahmen gehören z. B. Vorschriften und Anweisungen sowie die notwendigen Schulungen. Zusätzlich sollten Freigabe- und Genehmigungsprozesse sowie Review-Prozesse bzw. periodische Evaluierungen etabliert werden. Grundsätzlich sollten diese Prozesse regelmäßig überwacht werden, z. B. durch Selbstinspektionen.
  - Gerade dort, wo keine technische Lösung etabliert werden kann, um bestimmte Datenrisiken zu verringern, sollten organisatorische Maßnahmen zur Risikominderung ergriffen werden. Jedoch ist das Risiko bei diesen Maßnahmen deutlich höher als bei technischen Maßnahmen, sodass Systeme bevorzugt werden sollten, die die technischen Möglichkeiten bereitstellen (*Compliance by Design*).

Für eine effizientere Validierung ist es sinnvoll, übergeordnete Maßnahmen zu etablieren, um eine einheitliche Validierung der Systeme sicherzustellen. Diese sollten in einem generischen Ansatz im Zuge der Etablierung eines Validierungskonzeptes umgesetzt werden, z. B. in Form von Standard Operating Procedures (SOPs) und Prozessen sowie einer IT-Infrastruktur. Dieses Vorgehen kann v. a. in Projekten Anwendung finden, in denen Revalidierungen eines größeren Equipment-Bestands (z. B. aufgrund einer systematischen Gap-Analyse) erfolgen. Maßnahmen auf Systemebene lassen sich dann im Zuge der Validierung einführen. Dies kann z. B. durch gerätespezifische Dokumente erfolgen, die begleitend geschult werden.

Qualifizierte IT-Infrastruktur für PC-Systeme

Für die einheitliche Betrachtung einer Vielzahl an computerisierten Equipments im Unternehmen und zur Sicherstellung von effizienten Maßnahmen zur Erreichung der Datenintegrität ist es empfehlenswert, eine qualifizierte IT-Infrastruktur für diese Systeme zu etablieren. Die häufig vorkommende strukturelle Trennung der Zuständigkeiten zwischen einer übergeordneten IT-Einheit des Unternehmens und den Verantwortlichen für Equipmentqualifizierung erschwert die Validierung dieser Systeme. Ein IT-Support für die computerisierten Stand-Alone-Systeme im GMP-Bereich sollte demnach aufgebaut werden. Im Folgenden werden sinnvolle IT-Infrastrukturelemente für die Validierung der Systeme vorgeschlagen.

Netzwerkanbindung: Grundsätzlich sollten Stand-Alone-Systeme an ein Netzwerk angebunden werden. Es ist von Vorteil, diese Systeme in einem eigenen von anderen Unternehmensteilen getrennten Netzwerk-Segment ohne Internetanbindung mit einer Firewall zu betreiben, da so Eingriffe von außen minimiert werden können.

Standardrechner mit einheitlichen Sicherheitseinstellungen: Des Weiteren sollte die IT-Einheit des Unternehmens standardisierte PCs aufsetzen und dafür einheitliche technische Sicherheitsmaßnahmen festlegen. Das können z. B. automatisierte Sitzungssperrungen nach definierten Zeitintervallen, ein Ordnerzugriffsschutz oder die Nutzung von Redundant-Array-of-Independent-Disks (RAID)-Systemen sein. Durch solche Maßnahmen kann ein höherer Aufwand bei der Verteilung von Rechnern und der technischen Umsetzun-

*) Teil 1 dieses Beitrags ist erschienen in TechnoPharm 10, Nr. 3, 172–175 (2020).

TechnoPharm 10, Nr. 4, 230–234 (2020)

gen der Standards (z. B. Einschränkung der Änderungsrechte auf Betriebssystemebene) entstehen. Zu beachten ist dabei, dass nicht jedes System mit dem gleichen Rechner funktioniert – es empfiehlt sich daher, die jeweilige Ausstattung bzw. Konfiguration in enger Abstimmung mit dem Lieferanten festzulegen.

Active Directory: Bei vielen Softwares kann die Benutzerverwaltung an das Active Directory angebunden werden, wodurch ein einheitlicher Zugriffschutz, Passworteinstellungen und eine Benutzer-Administration über eine zentrale IT-Einheit möglich sind. Allerdings bietet nicht jede Software diese Möglichkeit, daher sollte bei der Anschaffung neuer Software speziell auf dieses Feature geachtet werden.

Patch Management: Betriebssystem-Patches sollten kontrolliert im Rahmen eines Change-Control-Verfahrens in die Systeme eingespielt werden, damit sichergestellt werden kann, dass die Patches keinen funktionalen Einfluss auf die Systeme haben.

Datensicherung: Bei der Datensicherung ist es ratsam, auf standardisierte Systeme zurückzugreifen, damit ein automatisches Backup erfolgen kann. Manuelle Backup-Funktionen sind sowohl durch die manuelle Handhabung an sich als auch technisch fehleranfällig. Als doppelte Absicherung sollte auch das Datensicherungssystem selbst durch ein Backup gesichert werden.

Denkbar sind Daten-Capture-Systeme, die die Daten vom System automatisiert abholen. Diese werden schließlich auf Servern gesichert, die nicht am Equipment lokalisiert sind. Sollten Skripte verwendete werden, mit denen Daten migriert oder verschoben werden, ist eine Validierung dieser Skripte notwendig.

Da sich die Datenablage und -struktur bei jeder Software unterscheidet (Flat-File-basiert in Ordnerstrukturen oder Datenbanken), sollte bei der Wahl des Datensicherungssystems darauf geachtet werden, dass die Sicherung dieser Datenstrukturen technisch möglich ist, z. B. kann es Probleme bei zu großen Systemdatenbanken geben. Auch sollten die gesicherten Daten nicht überschrieben werden können, sondern es sollte eine Versionierung erfolgen.

Das Intervall der Datensicherung muss so gewählt werden, dass das Risiko eines Datenverlusts minimal gehalten wird, z. B. messtäglich.

Zu beachten ist, dass für das Datensicherungssystem eine Validierung notwendig ist, SOPs zum Betrieb vorliegen und die Aufrechterhaltung des validierten Zustands durch regelmäßige Evaluierung und Instandhaltung geregelt ist. Ergänzend muss die Funktionalität zwischen dem computerisierten Equipment und dem Datensicherungssystem nicht nur in der Validierung, sondern regelmäßig getestet werden.

Das Änderungsmanagement am Datensicherungssystem muss eine Risikobetrachtung enthalten, die die Auswirkung der Änderung für alle angeschlossenen Systeme bewertet.

Datenaufbewahrung und -wiederherstellung: Das größte Problem, das sich für die Langzeitaufbewahrung stellt, ist, dass verschiedene proprietäre Datenformate oder Datenbanken nur mit der herstellereigenen Software lesbar sind und nicht in offene Formate umgewandelt werden können. Hier müssen technische Lösungen eingesetzt werden, die gewährleisten, dass die Daten abrufbar und lesbar bleiben bzw. eine Recovery-Möglichkeit besteht. Dies gilt ebenso bei Softwareupdates, denn dabei besteht die Gefahr, dass die Daten mit einer neueren Softwareversion nicht mehr lesbar sind. Aus diesem Grund ist die Archivierung der Daten meist schwierig realisierbar, insbesondere bei Bestandssystemen. Daher sollte bereits bei der Anschaffung eines Systems darauf geachtet werden, dass der Hersteller ein Archivierungskonzept anbietet und dass es bei Softwareupdates eine Abwärtskompatibilität oder die Möglichkeit zur Datenmigration der Bestandsdaten gibt.

Grundsätzlich wird die Aufgabe auch dadurch erleichtert, dass anhand gesetzlicher Vorgaben Regelungen zu Aufbewahrungsfristen der Daten getroffen werden. Nicht alle Daten müssen 20 oder mehr Jahre lang aufbewahrt werden. Eine Kategorisierung solcher Daten mit kontrollierter Löschung verringert den Aufwand für die Infrastruktur.

Die aufbewahrten Daten müssen jederzeit abrufbar und wiederherstellbar sein. Dies muss regelmäßig überprüft werden. Zur Wiederherstellungstestung bietet es sich an, dies nicht im validierten Produktivsystem durchzuführen, sondern z. B. in einem qualifizierten Testsystem oder aber in einer virtuellen Testumgebung. Auch hierfür sollten entsprechende IT-Ressourcen zur Verfügung stehen.

Geregelter operativer Betrieb von computerisiertem Equipment

Bei einem größeren Equipment-Bestand ist es angebracht, ein übergeordnetes einheitliches Konzept zu entwickeln, das die Prozesse zum Betrieb der Stand-Alone-Systeme (unter Einbindung der IT-Infrastruktur) und zum Datenmanagement regelt. So können der Validierungsumfang definiert (z. B. durch Definitionen von Systemgrenzen) und darauf basierend gleiche Standards für die Equipmentsysteme festgelegt werden. Ohne übergeordnetes Konzept basiert das Vorgehen auf einer Einzelbetrachtung der Equipmentsysteme mit festgelegten Maßnahmen pro System. Dies birgt allerdings die Gefahr, dass eine nachträgliche Harmonisierung innerhalb des Equipment-Bestands nur unter deutlichem Mehraufwand realisierbar ist, z. B. indem umgesetzte Maßnahmen bei bereits validierten Systemen korrigiert werden müssen und dies im Rahmen eines Change-Control-Verfahrens erfolgen muss. Eine Konzeptentwicklung innerhalb oder nach der Umsetzungsphase bei den Einzelsystemen ist daher erfahrungsgemäß schwieriger und erfor-

dert mehr Aufwand, Zeit und Ressourcen als die Etablierung eines übergeordneten Konzepts mit anschließender standardisierter Validierung/Qualifizierung der Systeme. Auch werden Redundanzen, Neustrukturierungen und die mehrfache Durchführung bzw. Korrekturen von festgelegten Maßnahmen vermieden.

Das Vorgehen und die Betrachtungsweise sollten einheitlich sein, auch bzgl. einer Mangelbehebung. Die Grundausrichtung sollte zum Ziel haben, nicht nur einen validierten Zustand herzustellen, sondern auch das Equipment im Geschäftsprozess weiter betreiben zu können.

Im Folgenden werden Maßnahmen zur Umsetzung eines konformen Betriebs des computerisierten Equipments genannt [1][3][5]:

- Regelungen zum Audit Trail und Audit Trail Review
- Verbindliche Benutzerkonzepte: Darunter fallen z. B. die Trennung von Administrator und User mit ergänzenden Berechtigungsgruppen z. B. für die Methodenerstellung. Die Administration sollte von einer unabhängigen Unternehmenseinheit übernommen werden, um die Segregation of Duties (übersetzt: Funktionstrennung) sicherzustellen.
- Regelungen zum Zugriffschutz, z. B. Passwortregeln und elektronische Signaturen
- Ein auf computerisierte Systeme zugeschnittenes Änderungsmanagement, das z. B. festlegt, welche Änderungen am System Change-Control-pflichtig sind. Ein solches Änderungsmanagement beträfe insbesondere die Konfiguration von Systemen.
- Periodische Evaluierungen und Review-Prozesse (darunter fallen u. a. Logbücher, Audit Trails, Benutzerberechtigungen, Datensicherungs- und Wiederherstellungstests)
- Abweichungsmanagement: Erarbeitung von Definitionen, welche Vorkommnisse Abweichungen im Betrieb des Equipments darstellen
- Lieferantenmanagement
- Schulungskonzepte
- Investigation/Corrective-Action-and-Preventive-Action(CAPA)-Konzepte

Bei all diesen Prozessen ist es förderlich, wenn eine übergeordnete IT-Einheit des Unternehmens nicht losgelöst von GMP-Prozessen mit computerisiertem Equipment agiert, sondern z. B. in das Änderungsmanagement miteinbezogen und darin geschult wird. Dies gilt insbesondere dann, wenn diese Einheit nicht der Systemeigner für das computergestützte Equipment ist. Verantwortlichkeiten im Unternehmen sollten hier klar geregelt werden.

Erst wenn diese Strukturen vorhanden sind, kann das computergestützte Equipment in der Weise aufgesetzt werden, dass die technischen Umsetzungen für die Validierung gewährleistet sind und auch nach der produktiven Freigabe der validierte Zustand aufrechterhalten werden kann.

Die spätere Korrektur einzelner Regelungen wird dennoch notwendig sein, da sich in der praktischen Umsetzung erfahrungsgemäß neue Problemstellungen ergeben, die zuvor nicht absehbar waren. Sie kann über CAPA-Prozesse oder ein Änderungsmanagement abgebildet werden.

Softwarevalidierung und Equipmentqualifizierung

Ein Vorgehen, das sich insbesondere lohnt, wenn gleiche Equipments mehrmals vorhanden sind, wird im Folgenden vorgestellt. Hierfür würde im ersten Schritt die Software eines Herstellers risikobasiert einmalig anhand der Anforderungen betrachtet werden – dies kann nach GAMP 5 [6] erfolgen. Die Equipments werden anschließend gemäß des unternehmensinternen Qualifizierungskonzepts qualifiziert.

Der Validierungsumfang ergibt sich aus der Risikoanalyse für das Equipment, den PC mit der Software, Schnittstellen zu anderen validierten Systemen und den Ergebnissen aus dem Data-Mapping. Hierfür können auch einzelne Equipmentkategorien/-klassen im Unternehmen etabliert werden, um die Detailtiefe der Validierung festzulegen. Zu beachten ist, dass ein einheitlicher Dokumentensatz erstellt und in das Qualifizierungskonzept des Unternehmens integriert wird.

Bewertung der Software

Das Grundprinzip für die hier betrachteten computerisierten Equipments basiert auf der Annahme, dass es sich bei der eingesetzten Software um eine Standardsoftware handelt, die nicht speziell für den Betreiber (also das Pharmaunternehmen) programmiert wurde. Der Lieferant bietet für Standardsoftware oftmals eine eigene Dokumentation der Installation Qualification (IQ)/Operation Qualification (OQ) an. Sollte diese Dokumentation die Benutzeranforderungen des Betreibers jedoch nicht vollständig abbilden, muss der Betreiber eigene Anwendertests durchführen – dies ist bei der Planung zu berücksichtigen. Nach entsprechenden Lieferantenbewertungen (z. B. durch Audits) kann das Pharmaunternehmen die Dokumentation akzeptieren und in die Risikobewertung für die Validierung integrieren.

Die Betrachtung vieler unterschiedlicher Equipments hat gezeigt, dass die Hersteller das Equipment mit einer Konformitätsaussage zu Datenintegrität anbieten, die jedoch nicht mit den unternehmenseigenen Anforderungen übereinstimmen. Oder die funktionale Umsetzung in der Software kann erst durch spezielle Einstellungen (Konfigurationen) sichergestellt werden. Deshalb ist diese Konformitätsaussage zu bewerten und ggf. durch weitere Maßnahmen gemäß den eigenen Anforderungen zu ergänzen. Zudem sollte der Betreiber einheitliche Datenintegritäts-Anforderungen an Software formulieren, diese dem Lieferanten zur Verfügung stellen und – wenn notwendig

TechnoPharm 10, Nr. 4, 230–234 (2020)

– die angebotene Software vor Anschaffung in einem vom Lieferanten zur Verfügung gestellten Testsystem überprüfen. Dieses Vorgehen vermeidet auch Fehlanschaffungen, sollten kritische Datenintegritäts-Anforderungen durch die Software nicht erfüllt sein.

Benutzeranforderungen/User Requirement Specifications (URS)
Die Spezifikationen, die sich aus den Datenintegritätsanforderungen ergeben, sollten Anforderungen an die Funktionalität der Software enthalten. Beispiele hierfür sind Anforderungen an die Audit-Trail-Funktionalität, an die Benutzerverwaltung mit definierten Berechtigungen oder die Möglichkeit, die Benutzerverwaltung an das Active Directory anzubinden. URS zu Datenintegrität für Equipmentsoftware müssen nur 1 Mal für alle eingesetzten computerisierten Equipments formuliert werden und können dem Lieferanten als Lastenheft zur Verfügung gestellt werden.

Konfigurationen
Möglicherweise stehen bestimmte Funktionalitäten erst durch spezielle Konfigurationen in der Software zur Verfügung (z. B., dass zunächst ein Häkchen gesetzt werden muss, um den Audit Trail anzuschalten). Die Informationen zu den erforderlichen Konfigurationen kann der Lieferant in Form eines Pflichtenheftes bereitstellen. Daher müssen die Konfigurationen softwarespezifisch implementiert und getestet werden. Die Konfigurationen werden dann in einer Configuration Specification für das System festgehalten.

Verifizierung und Mängel
Insbesondere sollte an den Stellen getestet werden, an denen bei der Risikobewertung ein Risiko identifiziert wurde. Dafür können auch die Validierungsdokumente des Softwareherstellers miteinbezogen werden, sodass eine Testung nicht anhand eines Quellcodes erfolgen muss, sondern als Testung der spezifischen Funktionalität erfolgen kann: So wird etwa überprüft, ob der Audit Trail alle in den URS definierten Ereignisse aufzeichnet.

Es wird vorkommen, dass nicht alle Akzeptanzkriterien der Software erfüllt werden. Diese Mängel müssen bewertet werden. Aus dieser Bewertung können prozedurale oder IT-technische Maßnahmen abgeleitet werden, die im nächsten Schritt der Projektphase umgesetzt werden.

Prozedurale Lösungen sind systemspezifisch zu finden, je nach beabsichtigter Nutzung. Dennoch können für Mängel, die wiederkehrend bei unterschiedlicher Software auftreten, Standardmaßnahmen festgelegt werden. So kann z. B. in einer Anweisung definiert werden, dass Administratoren keine Messungen durchführen dürfen, falls das Berechtigungskonzept in der Software dies nicht verhindert. Darüber hinaus werden Review-Prozesse festgelegt, in deren Verlauf Abweichungen von Standardmaßnahmen auffallen würden, z. B., wenn ein Administrator eine Messung gestartet hätte.

IT-seitige Konfigurationen auf Betriebssystemebene können in die Configuration Specification mit aufgenommen werden. Dokumentiert z. B. der Audit Trail keine fehlgeschlagenen Login-Versuche, kann das Security Event Log des Betriebssystems entsprechend konfiguriert werden, oder es wird eine Softwarelösung etabliert, die eine Audit-Trail-Funktion beinhaltet.

Der Aufwand für die Softwarebewertung ist einmalig, sodass in Projekten, in denen mehrere gleiche computergestützte Systeme validiert werden, nur noch geprüft werden muss, ob für das jeweilige Equip-

ment die in der Configuration Specification definierten Konfigurationen in der Software vorgenommen und die definierten prozeduralen Maßnahmen umgesetzt wurden. Die Software wird in ihrer Grundfunktionalität nicht erneut betrachtet. Dies wird entsprechend referenziert. Einzuplanen ist, dass die Softwaretestung aus funktionalen Gründen evtl. nur in Kombination mit dem zugehörigen Equipment erfolgen kann.

Qualifizierung des Equipments

Wurde die Software hinsichtlich Datenintegritätsanforderungen verifiziert und bewertet, sind die funktionalen URS für das Equipment zu formulieren. Diese können generisch für alle Equipments des gleichen Typs mit der gleichen Software aufgesetzt werden. Die Anforderungen an die Installation der Software inklusive der Konfiguration sind einzubeziehen.

Für die Funktionalität des Equipments kann bei bestehendem Lieferantenmanagement die IQ/OQ-Dokumentation des Herstellers einbezogen werden.

Die Testungen erfolgen nach dem betreiberüblichen Qualifizierungskonzept für Standardequipment. Zusätzlich werden die korrekte Installation der Software und die Umsetzung der Konfiguration auf Betriebssystemebene/in der Software während der IQ getestet. Die Umsetzung der prozeduralen Maßnahmen kann z. B. in der OQ bzw. Process Qualification (PQ) abgeprüft werden.

Revalidierung/ Requalifizierung

Bei computerisierten Equipments wird es in regelmäßigen Abständen zu Softwareupdates kommen – sei es, um das System auf dem neuesten Stand zu halten, Funktionalitäten zu verbessern, oder weil der Lieferant das System mit veralteter Software nicht mehr unterstützt.

Empfehlenswert ist, dass das Änderungsmanagement auf einen einheitlichen Maßnahmenkatalog zugreift, der häufig vorkommende Änderungen wie Softwareupdates oder Rechnertausch beinhaltet. Es ist nicht in jedem Fall notwendig, eine komplette Revalidierung des Systems vorzunehmen, wenn das Softwareupdate nur kleine Änderungen beinhaltet. Die vorgenommenen Änderungen werden vom Softwarelieferanten üblicherweise in Form von Release Notes zur Verfügung gestellt. Darauf basierend kann die Risikobewertung kritische Änderungen an Funktionalitäten identifizieren, die dann getestet werden sollten.

Standardisierung zur effizienten Umsetzung

Um bei vielen verschiedenen Equipments im Rahmen der Validierung ein einheitliches Vorgehen zu sichern, sollte – wie bereits beschrieben – eine Standardisierung erfolgen. Dadurch wird zusätzlich eine effiziente Qualifizierung der Equipments ermöglicht, die den Anforderungen aus 21 CFR Part 11 [7] und Annex 11 [1] gerecht wird. Dies beinhaltet Anweisungen, die das Qualifizierungskonzept und standardisierte technische Umsetzungen am computerisierten System beschreiben.

Zusätzlich sollte eine Anweisung den Betrieb und die Administration der Software regeln. Darin können u. a. das Berechtigungskonzept, die Rolle des Systemadministrators, die Häufigkeit der Audit Trail Reviews und der Benutzereinwahlen, die Systemwiederherstellung, die Datensicherung, die Datenarchivierung mit Verantwortlichkeiten, Schulungskonzepte und die Segregation of Duties für das System geregelt werden.

Für die Validierung sind einheitliche Dokumente und Templates erforderlich. Darunter fallen die Benutzeranforderungen (URS) zur Datenintegrität für Equipmentsoftware (vor dem Kauf als Lastenheft für den Lieferanten) und die Configuration Specification (basierend auf dem Pflichtenheft des Herstellers und IT-Maßnahmen auf Betriebssystemebene).

Auch für Mangelbehebungen sind einheitliche Prozeduren und technische Lösungen grundlegend.

Zusammengefasst sorgt ein Validierungskonzept, das standardisierte IT- und prozesstechnische Maßnahmen sowie einheitliche Anweisungs- und Qualifizierungsdokumente beinhaltet, für eine effiziente und harmonisierte Qualifizierung von computergestütztem Stand-Alone-Equipment. Durch die Wahl eines durchdachten risikobasierten Ansatzes unter Einbeziehung eines Data-Mappings und der Lieferanten kann das Equipment anschließend so betrieben werden, dass die Datenintegrität über den gesamten Datenlebenszyklus hinweg sichergestellt werden kann.

Literatur

[1] EGU-GMP-Leitfaden, Annex 11 - Computergestützte Systeme, 2011
[2] U.S. Department of Health and Human Services, Food and Drug Administration – Data Integrity and Compliance with cGMP. Guidance for Industry, 2016
[3] PI 041-1 (Draft 3) – Good Practices for Data Management and Integrity in regulated GMP/GDP Environments, 2018
[4] R D McDowall – Data Integrity and Data Governance: Practical Implementation in Regulated Laboratories – Royal Society of Chemistry, 2018
[5] Weiser et al. – Allgemeiner Datenintegritäts-Standard für Laborgerätesoftware – Pharm. Ind. 80, Nr. 11, 1564–1572 (2018)
[6] ISPE – GAMP® 5: Ein risikobasierter Ansatz für konforme GxP-computergestützte Systeme, 2008
[7] FDA 21 CFR Part 11 – Electronic Records, Electronic Signatures, 1997

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. Alle Rechte vorbehalten.