

III DATENSICHERHEIT

Sichere Datenräume – nur etwas für Spezialisten?

Ludger Wess, Akampion GmbH, Hamburg

Forschungs- und Entwicklungsdaten sind in der Biotechnologie-Branche das wichtigste Kapital eines Unternehmens, aber bislang nutzen nur wenige Firmen Sicherheitsstandards, die über eine Firewall oder E-Mail-Verschlüsselungen hinausgehen.

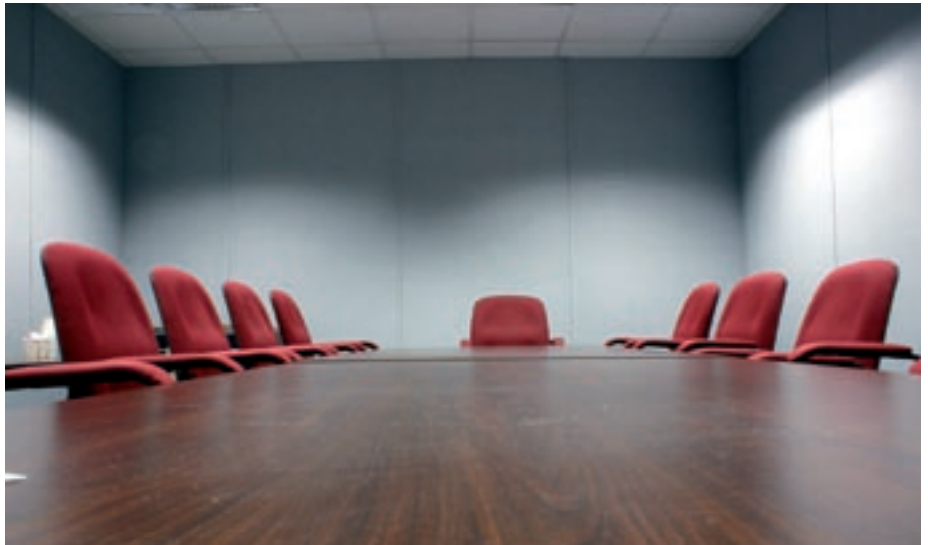
Die Vorbereitung und Durchführung klinischer Studien zählt zu den anspruchsvollsten logistischen Aufgaben eines Biotech-Unternehmens. Dabei ist es wichtig, sämtliche Dokumente und Vorgänge – Schriftwechsel, Protokolle, Patientendaten usw. – vollständig zu dokumentieren und sicher aufzubewahren und gleichzeitig berechtigten Personen Zugang dazu zu gewähren. Klinische Daten müssen nicht nur von Rechts wegen geschützt werden. Sie zählen wie Patente und anderes geistiges Eigentum zum wichtigsten Kapital des Unternehmens – für die Zulassung von Produkten ebenso wie für erfolgreiche Lizenz- oder Kaufverhandlungen.

Traditionell gibt es für die Aufbewahrung hoch vertraulicher Daten und den Zugriff darauf den so genannten sicheren Datenraum – einen zugangskontrollierten Raum im Gebäude des Unternehmens, in dem die Daten in Papierform aufbewahrt werden. Solche Räume können effizient verhindern, dass vertrauliche Dokumente unberechtigt eingesehen oder gar kopiert werden.

Doch für eine globalisierte Industrie mit klinischen Zentren und Partnern auf der ganzen Welt ist diese klassische Vorgehensweise nicht mehr adäquat. Ablage und Management der Daten sind ebenso wie die Suche nach darin enthaltenen Einzelinformationen extrem zeitaufwendig. Zudem können dabei hohe Reisekosten entstehen, und es ist so gut wie unmöglich, mehreren interessierten Parteien parallel Einblick in die Unterlagen zu geben.

Riskante Datenweitergabe

Viele Unternehmen setzen daher auf die Weitergabe ihrer Daten in elektronischer Form. Doch das ist extrem riskant, selbst wenn es in verschlüsselter Form geschieht.



Verwaist: der real existierende „sichere Datenraum“. Neue, virtuelle Lösungen?

An erster Stelle ist die Leichtigkeit zu nennen, mit der Dateien kopiert und verbreitet werden können. Als Konsequenz kann das Unternehmen nicht mehr kontrollieren, wer seine Daten liest und an wen sie weitergegeben werden. Hinzu kommt – wie zahlreiche Beispiele zeigen – dass damit das Risiko extrem ansteigt, dass die Datenträger (CDs, DVDs, Laptops usw.) gestohlen werden oder verlorengehen. Zudem ist es schwierig, die Daten zu aktualisieren oder Dokumente nachzureichen.

Web-basierter Secure Dataroom

Das Münchener Unternehmen Brainloop AG (www.brainloop.com), führender Anbieter von Software-Lösungen für das hoch sichere, unternehmensübergreifende Bearbeiten und Verteilen von vertraulichen Dokumenten, hat daher einen web-basierten Secure Dataroom entwickelt, der intuitiv und ohne Training genutzt werden kann. Er lässt sich sehr schnell einrichten, aber auch im Datenzentrum des Kunden installieren. Alle Aktionen werden protokolliert, und die unberechtigte Verteilung von Dokumenten durch

Download, Druck oder Weiterleitung wird wirksam unterbunden – bis auf den Desktop des Informationsempfängers. Selbst der IT-Betreiber hat keinen Zugriff.

„Damit bietet der Secure Dataroom Biotech-Firmen die Möglichkeit, ohne großen Aufwand vertrauliche Informationen wie klinische Studien oder geistiges Eigentum unter vollständiger Wahrung der Besitzrechte dem externen Betrachter zugänglich zu machen“, so Peter Weger, CEO der Brainloop AG.

Beispiel Lizenzverhandlungen: Hierbei geht es um höchst widersprüchliche Ziele – einerseits sollen streng vertrauliche, wertvolle Informationen potentiellen Lizenznehmern zugänglich gemacht, andererseits aber gleichzeitig geschützt werden. Zudem kann es im frühen Stadium solcher Verhandlungen mehrere Wettbewerber geben, die die Unterlagen bewerten müssen, während am Ende nur einer von ihnen den Zuschlag erhalten wird. Daher ist es von zentraler Bedeutung, dass der Zugang zu den hochsensiblen Informationen so gewährt und wieder entzogen werden kann, dass beim Transfer und bei der Evaluierung keine Dokumente zurückbleiben. Zudem muss verhindert

werden, dass diese Daten hinter dem Rücken des Unternehmens kopiert und weitergegeben werden. Midas Pharma GmbH, Dr. Marcus Stumpf, Managing Director: „Der Brainloop Secure Dataroom hilft uns, sicher, einfach und anwenderfreundlich hochsichere Informationen an unsere Partner zu verteilen. Wir können durch das intelligente Berechtigungskonzept und die Nachvollziehbarkeit genau regeln und kontrollieren, wer wann was an den Dokumenten vorgenommen hat.“

„Unser Secure Dataroom“ so Weger, „kann vertrauliche Informationen wie zum Beispiel den Datenbestand klinischer Studien oder geistiges Eigentum externen Benutzern zugänglich machen, ohne dass dabei die Besitzrechte des Unternehmens beeinträchtigt und sensible Patientendaten preisgegeben werden. Das Unternehmen behält dabei zu jeder Zeit die volle Kontrolle darüber, wer Zugang zu den Daten hat.“

Geringe Investitionen

Die Vorteile: Die Investitionen sind vergleichsweise gering, denn sie betragen weniger als die Kosten für die Einrichtung eines physikalischen Datenraums, und um den Secure Dataroom einzurichten und zu managen, sind keinerlei Spezialkenntnisse oder aufwendige Software-Installationen erforderlich. Die Anwendung, die auf Wunsch innerhalb weniger Stunden zur Verfügung steht, ist Web-basiert und lässt sich mit nur wenigen Befehlen einrichten. Genauso einfach ist es, Nutzer hinzuzufügen oder zu entfernen, Dokumente hochzuladen und Rechte zuzuteilen. Auf Wunsch steht per Hotline ein

Kundenberater zur Verfügung. Brainloops Secure Dataroom arbeitet mit hoch sicherer Authentifizierung und 256-BIT-Verschlüsselung. Alle Dokumente sind sowohl im Ruhezustand als auch beim Versand verschlüsselt.

Für jeden Zugriff wird ein nur einmal gültiger PIN-Code benötigt, der jeweils per SMS versandt wird. Eine besondere technische Lösung, das Operator Shielding, verhindert dabei, dass Administratoren des Servers der Firmen, die die Daten z. B. für ihre Due Diligence evaluieren, Zugriff erhalten. Und da die Dokumente nicht auf dem Server des Partners verbleiben, können sie nach Abschluss einer Sitzung auch nicht rekonstruiert werden.

Zudem hat das Unternehmen die Möglichkeit, den Zugriff auf die zur Verfügung gestellten Dokumente zu beschränken, also je nach Nutzer bestimmte Daten gar nicht, andere nur zum Lesen und wieder andere zum Download, Druck oder sogar zur Bearbeitung freizugeben. Diese Rechte können individuell zugeteilt und entzogen werden. Für zusätzliche Sicherheit lassen sich Wasserzeichen in die Dokumente integrieren, die zum Beispiel im Ausdruck den Namen des jeweiligen Nutzers in den Hintergrund einfügen. Alle Zugriffe und Vorgänge werden automatisch und unveränderbar protokolliert.

Für den Secure Dataroom gibt es in der Biotech-Industrie zahlreiche Anwendungsmöglichkeiten. Neben Lizenzverhandlungen zählen dazu auch Daten aus Forschung und Entwicklung, denn F&E wird heute zu meist in umfangreichen Netzwerken mit verschiedenen Dienstleistern durchgeführt. Diese Partner müssen nicht nur Zugang zu bestimmten vertraulichen Informationen erhalten, sondern auch in der Lage sein, auf

sichere Weise Konzepte, Daten und Analysen bereitzustellen, zu verändern und auf den jeweils neuesten Stand zu bringen. MediGene AG, Dr. Markus Hörer, Director Research&Analytics: „Der Brainloop Secure Dataroom gibt uns die Möglichkeit, temporär und schnell hochvertrauliche Informationen, zum Beispiel aktuelle Forschungsergebnisse, Berichte und Patentanmeldungen mit Kollaborationspartnern auszutauschen. Gleichzeitig können wir in einer kontrollierten und überwachten Umgebung die Besitzrechte der Dokumente sichern.“

Als drittes Anwendungsgebiet nennt Brainloop das Management von Partnerschaften: Hier müssen beinahe täglich Aktivitäten koordiniert und Fortschritte dokumentiert werden. Dazu ist es nicht nur notwendig, bestimmte IP miteinander zu teilen, sondern auch genau verfolgen zu können, wer wann was an den Informationen verändert hat. Und natürlich müssen die Weitergabe von Dokumenten, Online-Diskussionen und so weiter sicher stattfinden und ebenfalls dokumentiert werden.

Datensicherheit ist Vorstandssache

Besonderen Wert legt Brainloop auf die einfache Einrichtung und Bedienung, denn Datensicherheit ist Vorstandssache und sollte nicht an die IT-Abteilung delegiert werden, die Datensicherheit in der Regel als Problem der Infrastruktur betrachtet und sie nicht aus der Perspektive der Nutzer und der zu erreichenden Ziele sieht. ▼

Brigitte Ehret, Brainloop AG, München
BEhret@brainloop.com



Mitglied im Bundesverband
Medizinischer Auftragsinstitute
BVMA e.V.



GLP-Bescheinigung
herausgegeben durch das
Umweltministerium
Baden-Württemberg, Deutschland



Akkreditiert durch
Zentralstelle der Länder
für Gesundheitsschutz
bei Arzneimitteln
und Medizinprodukten
ZLG-P-974.98.05

Akkreditierung nach
DIN EN ISO/IEC 17025



mdt medical
device testing GmbH

Grenzenstrasse 13
D-88416 Ochsenhausen

Tel.: 07352 - 9114 - 0
Fax: 07352 - 9114 - 70

CRO-Dienstleistungen für die klinische Prüfung von Medizinprodukten

- Projektmanagement für klinische Studien
- Erstellung des klinischen Prüfplanes
- Entwicklung der Prüfbögen (CRF)
- Erstellung der Patienteninformation und Einwilligungserklärung
- Selektion von Prüfzentren
- On-Site Monitoring und Auditing
- Kommunikation mit Ethikkommissionen und zuständigen Behörden
- Datenmanagement auf Basis von Clintrial™
- Zweifache Dateneingabe und computergestütztes Data Cleaning
- Biometrische Planung, Auswertung und Erstellung integrierter Prüfberichte
- Erfüllung der EN ISO 14155 und der internationalen Guten Klinischen Praxis
- Erfüllung spezieller Anforderungen der amerikanischen FDA

Nicht-klinische Prüfdienstleistungen für Medizinprodukte

- Risikomanagement
- Erarbeitung von Prüfstrategien
- Biokompatibilitäts- und Toxizitätsprüfungen
- Mikrobiologische und virologische Prüfungen, Prozessvalidierungen
- Validierung der Reinigung, Aufbereitung und Sterilisation
- Physikalische und chemische Prüfungen zur Materialcharakterisierung
- Oberflächen-Analytik, Reinigungsvalidierung
- Mechanische und optische Prüfungen
- Verpackungs- und Haltbarkeitsprüfungen
- Sonderprüfungen für z.B. Kontaktlinsen, Intraokularlinsen, Kathetersysteme, etc.
- Unterstützung von Zulassungsverfahren in Europa (CE-Kennzeichnung) und weltweit
- Training für Risikomanagement nach EN ISO 14971