IT-Sicherheit bei Konfiguration und Betrieb eines Studiensoftwaresystems

Dr. Philippe Verplancke
CEO XClinical GmbH & CIO Kompetenznetz Vorhofflimmern
TMF Workshop Sicherheitskonzepte, 11.12.2006

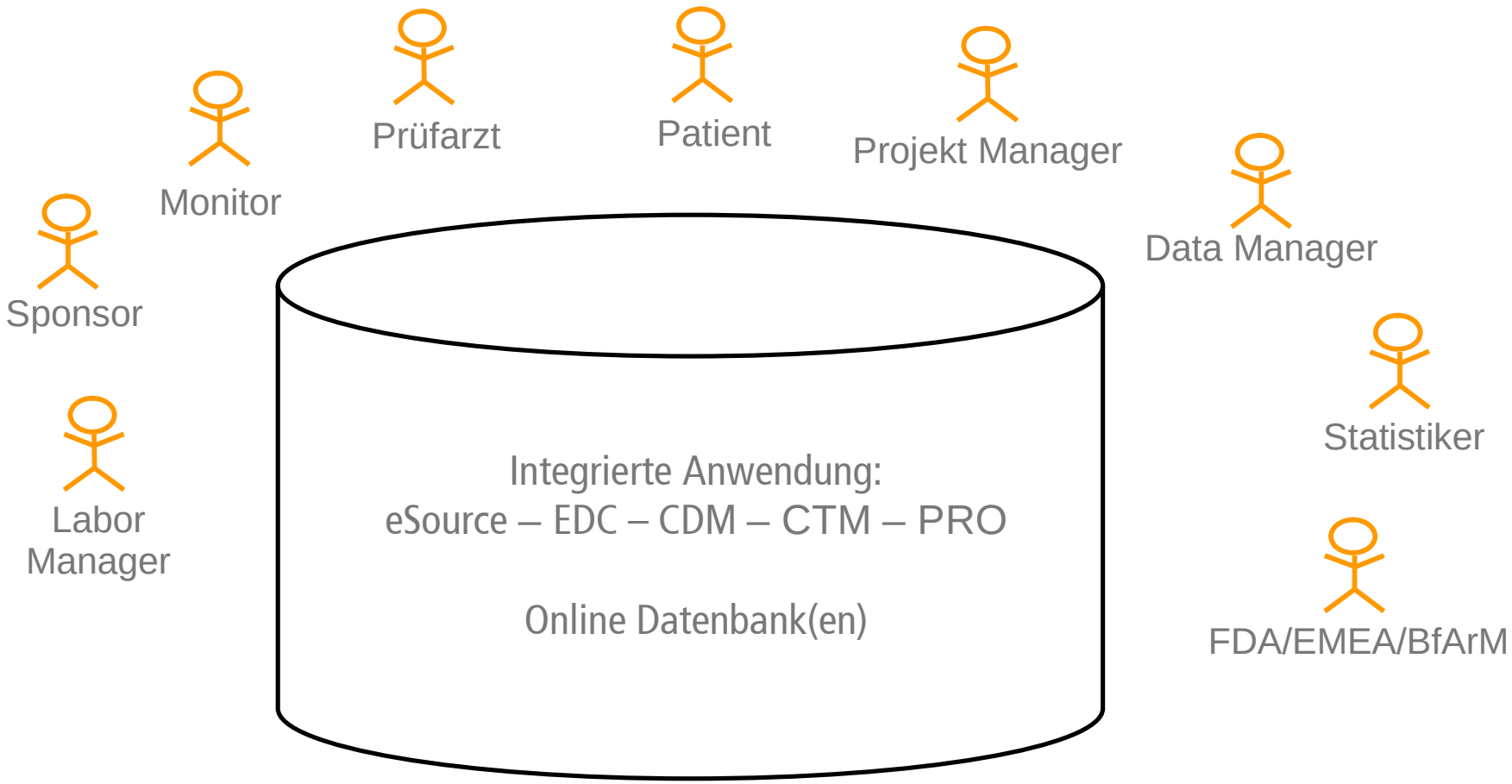
Agenda

- XClinical
- Anwendungsbereich
- Risiken
- Anforderungen
- Lösungen

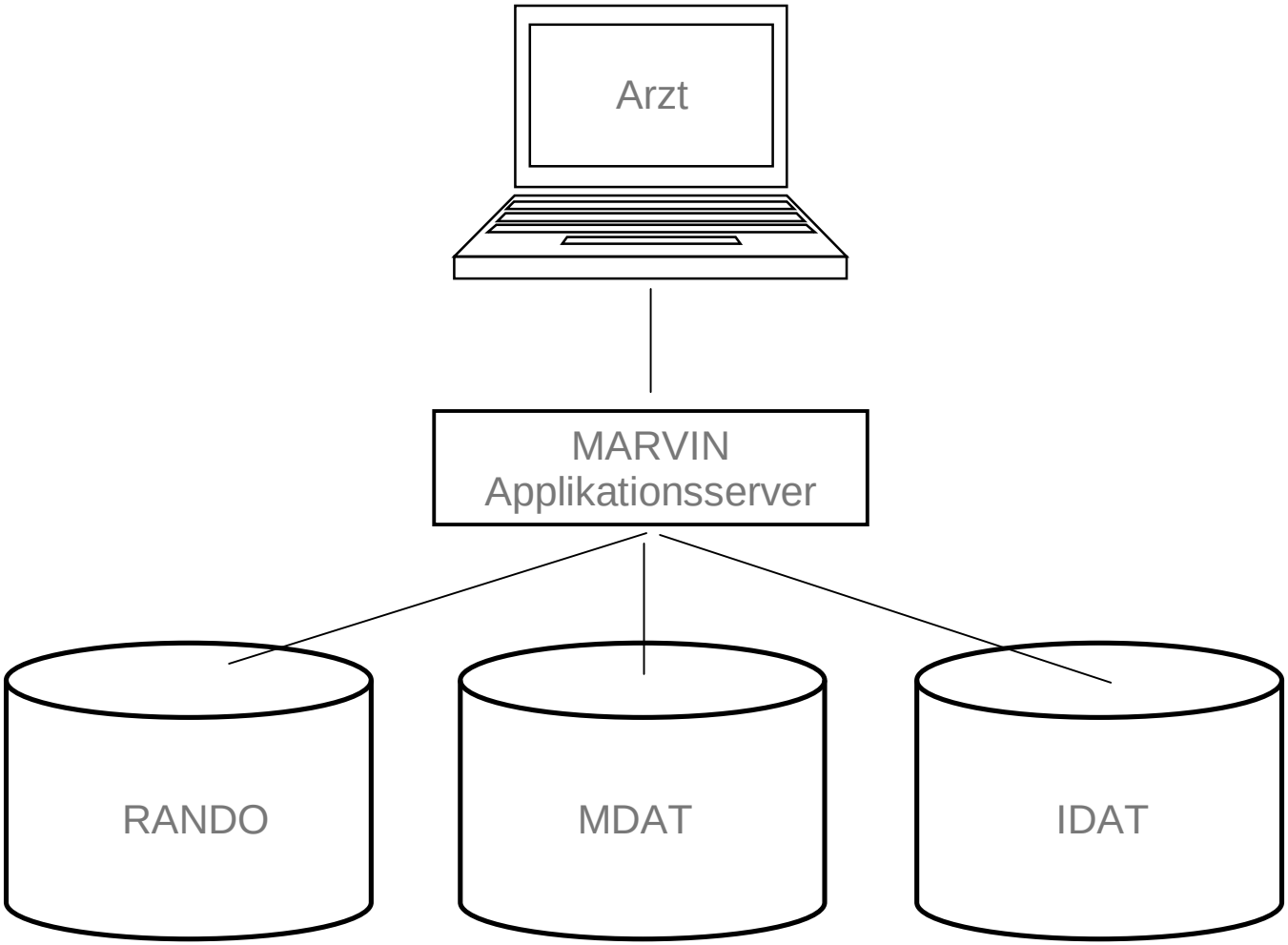
XClinical & MARVIN

- XClinical ist ein unabhängiger EDC/CDM-Anbieter mit Büros in München, Paris und Bethesda
- Das online EDC/CDM-System MARVIN ist vollständig auf CDISC aufgebaut
- XClinical ist aktives Mitglied der CDISC-Organisation
- MARVIN implementiert eine zentrale Speicherung von personenbezogenen Daten an einem von den medizinischen Daten getrennten Ort (zentrale Anforderung des Datenschutzes)
- Mehr als 26 Studien mit mehr als 43.000 dokumentierten Patienten

Unzählige Use Cases, unterschiedliche Usertypen



Eine Anwendung - Unterschiedliche Daten an unterschiedlichen Orten



Dimensionen der IT-Sicherheit

- **Scope (Anwendungsbereich)**
  - Ø Studiensystem = "Silo"-System: 1 Softwareinstanz pro Studie, kein Austausch mit anderen Studien nur mit anderen Systemen in derselben Studie
  - Ø Koppelung mit KIS wird hier noch nicht betrachtet (aufgrund GCP-Anforderungen ist eine solche Koppelung für klinische Studien noch weit von der Realisierung entfernt)

- **Sicherheitsniveau (akzeptabeles Restrisiko)**
  - Ø Festgelegt durch 21CFR11
  - Ø Gefordert durch Datenschutz (sofern die Daten nicht sofort beim Verlassen des Studienzentrums anonymisiert werden)
  - Ø Festgelegt durch das Unternehmen, das die Studien durchführt

IT Sicherheitsrisiken

- **In Bezug auf 21CFR11**
  - Unbefugte Manipulation der Daten (Betrug seitens Arzt oder Pharma-Firma)

- **In Bezug auf Datenschutz**
  - Verletzung der Privatsphäre des Patienten

- **In Bezug auf die Unternehmensinteressen**
  - Verlust von Firmeneigentum (geistiges Eigentum über Medikamentenentwicklung)
  - Imageverlust

Ø **Ein einzelner "Einbruch" verursacht selten großer realer Schaden, wahrscheinlich vor allem Imageverlust.**

Sicherheitsanforderungen aus 21CFR11

- **Amerikanisches Gesetz; durch andere Nationen nicht weiter vertieft**

- **Studiensystem = geschlossenes System**
  - Zugangskontrolle (mindestens Username-Passwort)
  - Passwortmanagement
  - Nachvollziehbarkeit von Datenänderungen (Audit Trail)
  - Verschlüsselung von Datenübertragungen (keine Angabe von Schlüssellänge)

- **Datenintegrität: "elektronische" oder "digitale" Signatur, i.e. Kryptographie (PKI , Smart Cards, etc.) wird hier nicht gefordert!**

- **Jeder Anwender, insbesondere Administratoren, ist vertraglich an strenge Vorschriften gebunden**

Weitere Sicherheitsanforderungen

- **Aus der Datenschutzgesetzgebung**
  - Im Wesentlichen nur eine zusätzliche Anforderung ggb. 21 CFR 11: dass Zugriffsberechtigungen auf IDAT und MDAT streng getrennt gehandhabt werden können.

- **Aus Unternehmensvorgaben**
  - können beliebig hochgeschraubt werden, über gesetzliche Anforderungen hinaus
  - oft sehr vernünftig aufgrund einer Kosten-Riskenanalyse

Bandbreite der möglichen Lösungen

Von	Bis
• Smartcard / Biometrie	• Username - Passwort
• Kryptographische Signatur mit offizieller PKI	• Keine kryptographischen Signaturen
• Dedizierte Laptops, onsite Validierung	• Keine dedizierte Client-HW, keine Site-Validierung
• Hardware VPN-Zugang	• Normaler Internetzugang
• Point-top-Point Applikations-verschlüsselung mit Client-Zertifikat	• Nur normale SSL Verschlüsselung
• Doppelte Hardware Firewall mit Trennung zwischen Appl. Server und Datenbankserver	• Einfache Firewall
• Fail-over Schaltung	• Hot oder Cold Standby
• Nur neueste Betriebssyteme mit einer einzigen Browser-version	• Alle möglichen Betriebssyteme und Browserversionen
• Keine automatischen Updates	• Automatische Updates

Gängige Lösung liegt in der Mitte

- Teilweise dedizierte Laptops, nur eine Betriebssystem- und Browserversion erlaubt
- Username – Passwort, keine kryptographischen Signaturen
- Normaler Internetzugang
- SSL-Verschlüsselung
- Doppelte Firewall und Trennung zwischen Applikations- und Datenbankserver
- Fail-over Schaltung der Server

Kostengünstige Lösung ist akzeptabel und vernünftig

- Hinweis: Im Bereich IT gibt es keine Verpflichtung, eine höhere Sicherheit als die auf Papier basierenden Prozesse zu schaffen!

  Denkanstoß: Wer kontrolliert/garantiert, dass der Kurierdienst keine Daten im CRF ändert?

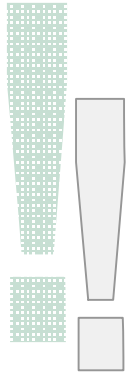
- Keine dedizierte Client-Hardware, alle Betriebssystem- und Browserversionen erlaubt
- Username – Passwort, keine kryptographischen Signaturen
- Normaler Internetzugang
- SSL-Verschlüsselung
- Eine Firewall, Applikations- und Datenbankserver auf gemeinsamer Hardware
- Hot Standby Schaltung der Server
- Juristische und geografische Trennung der IDAT- und MDAT-Server

Schlussfolgerung

- Keine eindeutigen gesetzlichen Vorgaben für IT-Sicherheit bei der Durchführung von klinischen Studien
- Beurteilung des ausreichenden Sicherheitsniveaus wird letztlich von den GCP Auditoren und den Unternehmen vorgenommen
- GCP und 21 CFR 11 erlauben eine kostengünstige, vernünftige Lösung wenn dies sauber dokumentiert ist und auch schriftlich eine Risikoanalyse niedergelegt ist.

Vielen Dank für Ihre Aufmerksamkeit!

Fragen und Antworten



EDC made easy

XClinical GmbH
Siegfriedstrasse 8
80803 Munich

Germany

Tel: +49 (0)89 / 45 22 77 – 50 00
Fax: +49 (0)89 / 45 22 77 – 59 00

Web: www.xclinical.com
Mail: info@xclinical.com