



Klinische Studien und Patientendaten in der sicheren Cloud eines Pharma-IT-Dienstleisters: Chancen, Grenzen, Hintergründe, Beispiele.

Dr. Gundula Garbe, T-Systems International GmbH
Senior Consultant Public / Health / Pharma



ERLEBEN, WAS VERBINDET.



Klinische Studien und Patientendaten in der sicheren Cloud eines Pharma-IT-Dienstleisters: Chancen, Grenzen, Hintergründe, Beispiele.

1 Zentrale (Sicherheits-) Richtlinien in der Pharmaindustrie – verschiedene Sichten

2 Good Practices Pharma-Beispiele – Bedeutung für ICT / Cloud Dienstleister

3 Best Practices Beispiel – T-Systems ESARIS Sicherheitsframework

4 Cloud Lösungen – Chancen, Grenzen, Hintergründe, Beispiele

5 Fazit



Klinische Studien und Patientendaten in der sicheren Cloud eines Pharma-IT-Dienstleisters: Chancen, Grenzen, Hintergründe, Beispiele.

zentrale Richtlinien in der Pharmaindustrie – verschiedene Sichten

(Behördliche) Richtlinien der Pharmaindustrie zu Qualität, Sicherheit und Compliance orientieren sich an:

- Patientensicherheit
- Arzneimittelqualität
- Qualität aller Prozesse mit Einfluss auf Patientensicherheit bzw. Arzneimittelqualität

Verbraucher-/Patientensicht

- Medikamente mit hoher Wirksamkeit und möglichst geringen Risiken und Nebenwirkungen

Fachlich / technische Sicht

- Durchgängig korrekten, sicheren, unverfälschten dokumentierten Umgang mit allen relevanten Daten in:
 - Forschung & Entwicklung von Medikamenten
 - Klinischen Studien zur Medikamentenzulassung
 - Langzeit- und Pharmakovigilanz-Betrachtung für im Markt befindliche Arzneimittel

Sicht der Beteiligten

- Einzelperson
- Pharmaunternehmen
- Behörde
- Lieferant
- Dienstleister
- Mitarbeiter, Laborant, MTA
- Mitarbeiter, Pfleger, Arzt
- Mitarbeiter, Arzt, Apotheker, Patient, Versicherter



Klinische Studien und Patientendaten in der sicheren Cloud eines Pharma-IT-Dienstleisters: Chancen, Grenzen, Hintergründe, Beispiele.

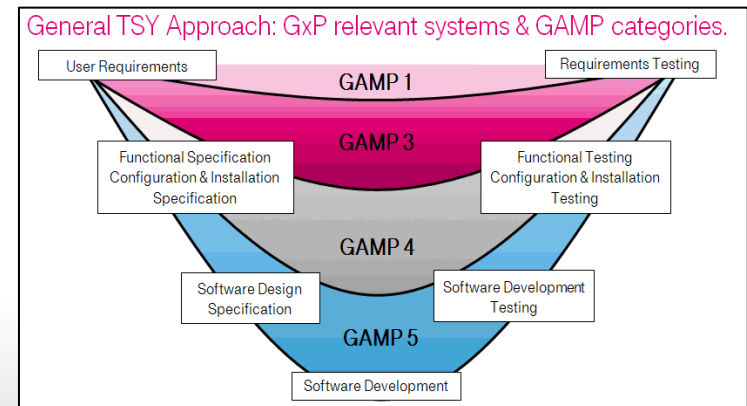
zentrale Richtlinien in der Pharmaindustrie – Good xxx Practices (GxP)

(Behördliche) Richtlinien der Pharmaindustrie zu Qualität, Sicherheit und Compliance orientieren sich an:

- Patientensicherheit
- Arzneimittelqualität
- Qualität aller Prozesse mit Einfluss auf Patientensicherheit bzw. Arzneimittelqualität

Für jeden Dienstleister bedeutet das konkret

- nach „Good xxx Practices“ (GxP):
 - GCP: Good Clinical Practices
 - GLP: Good Laboratory Practices
 - GMP: Good **Manufacturing** Practices
 - GAMP: Good **Automated Manufacturing** Practices
- durch geschultes Personal
- durch qualifizierte Infrastruktur und validierte Prozessen
- durch dokumentiertes Vorgehen über den gesamten Lebenszyklus eines Produkts/Medikaments
 - „Was nicht dokumentiert ist, hat nicht stattgefunden“



GAMP Category 1: Standard Hardware and Infrastructure Software
GAMP Category 3: Non-Configured Standard Software
GAMP Category 4: Configured Software
GAMP Category 5: Individual/Customer-specific Software



Klinische Studien und Patientendaten in der sicheren Cloud eines Pharma-IT-Dienstleisters: Chancen, Grenzen, Hintergründe, Beispiele.

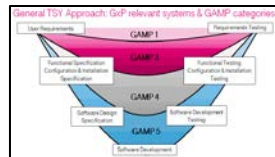
zentrale Richtlinien in der Pharmaindustrie – Bedeutung für ICT Dienstleister

(Behördliche) Richtlinien der Pharmaindustrie zu Qualität, Sicherheit und Compliance orientieren sich an:

- Patientensicherheit
- Arzneimittelqualität
- Qualität aller Prozesse mit Einfluss auf Patientensicherheit bzw. Arzneimittelqualität

Für jeden Dienstleister bedeutet das konkret

- nach „Good xxx Practices“ (GxP) :
 - GCP: Good Clinical Practices
 - GLP: Good Laboratory Practices
 - GMP: Good **Manufacturing** Practices
 - GAMP: Good **Automated Manufacturing** Practices



- durch geschultes Personal
- durch qualifizierte Infrastruktur und validierte Prozessen
- durch dokumentiertes Vorgehen über den gesamten Lebenszyklus eines Produkts/Medikaments

→ „Was nicht dokumentiert ist, hat nicht stattgefunden“

=> für TK- / IT- / Cloud Dienstleister:

- gemäß der Best Practices der ICT Branche:
 - Methodiken: PM-Book; SE-Book, Prince2, V-Model XT, ITIL v3: IT Infrastructure Library
 - Datenschutz/sicherheit: Telekommunikationsgesetz, ADV, VSnfD, BSI / Cert,
 - T-Systems ESARIS Sicherheitsframework und GxP-Approach (ready for FDA / EU audits)
 - Zertifizierung nach: ISO 9001, 20.000, 27.001, DataCenter Level C
 - Extern auditiert gemäß SOX70 / ISAE3402



Klinische Studien und Patientendaten in der sicheren Cloud eines Pharma-IT-Dienstleisters: Chancen, Grenzen, Hintergründe, Beispiele.

Cloud Dienstleister Branchenbeispiel: T-Systems ESARIS Sicherheitsframework 1/3

(Behördliche) Richtlinien der Pharmaindustrie zu Qualität, Sicherheit und Compliance orientieren sich an:

- Patientensicherheit
- Arzneimittelqualität
- Qualität aller Prozesse mit Einfluss auf Patientensicherheit bzw. Arzneimittelqualität

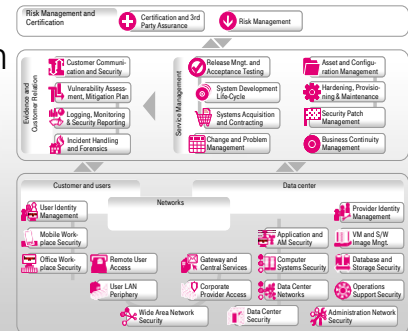
technische Bereiche

- TK-Leitungen, Netz-Infrastruktur
- Hardware, IaaS
- Betriebssysteme
- Plattformen, PaaS
- Standard-Software, IT-Lösungen, SaaS
- Rechenzentren (Hosting, Housing, ...aaS*)
- sowie alle Prozesse zum Management dieser Hard-/Software-Infrastruktur



=> T-Systems ESARIS: Enterprise Security Architecture For Reliable ICT Service

- T-Systems ESARIS Sicherheitsframework für alle ICT-Bereiche für:
 - diverse Branchenspezifika
 - und Länder / Standards
- gruppiert in 6 Clustern:
 - Risk Management and Certification
 - Evidence and Customer Relation
 - Service Management
 - Customer and users
 - Network
 - Data center Service Management



*„as a Service“ Cloud Lösung: IaaS, SaaS, PaaS: Infrastructure (Network, Hardware, Server, Storage); Platform (Middleware, Standardssoftware); Software (Applications)

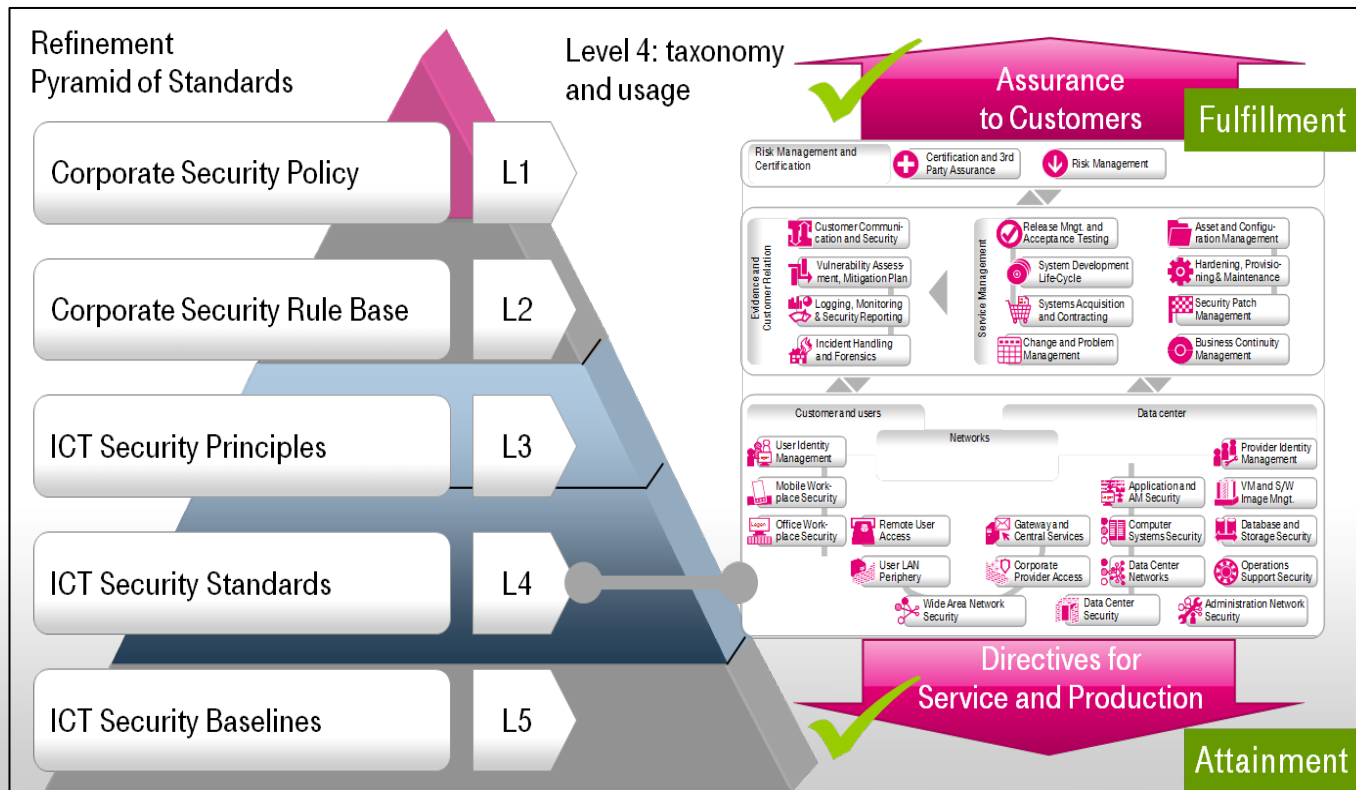




Klinische Studien und Patientendaten in der sicheren Cloud eines Pharma-IT-Dienstleisters: Chancen, Grenzen, Hintergründe, Beispiele.

Cloud Dienstleister Branchenbeispiel: T-Systems ESARIS Sicherheitsframework 2/3

T-Systems ESARIS: Enterprise Security Architecture For Reliable ICT Service

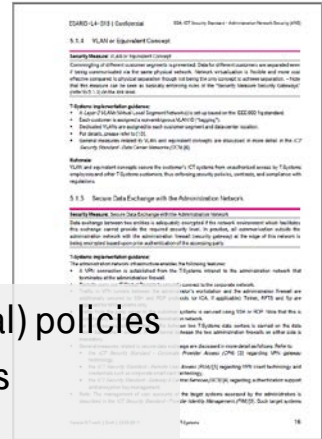
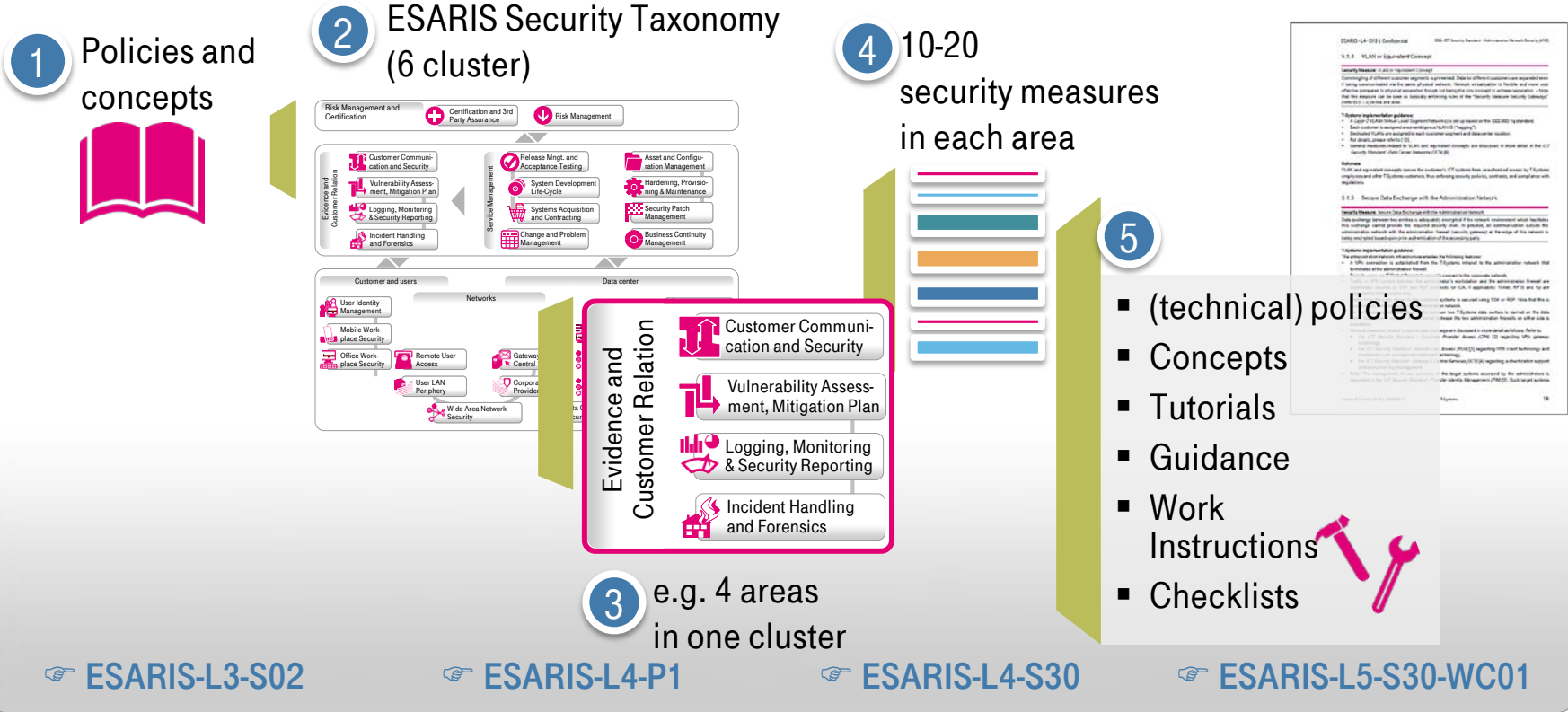




Klinische Studien und Patientendaten in der sicheren Cloud eines Pharma-IT-Dienstleisters: Chancen, Grenzen, Hintergründe, Beispiele.

Cloud Dienstleister Branchenbeispiel: T-Systems ESARIS Sicherheitsframework 3/3

T-Systems ESARIS: Enterprise Security Architecture For Reliable ICT Service





Klinische Studien und Patientendaten in der sicheren Cloud eines Pharma-IT-Dienstleisters: Chancen, Grenzen, Hintergründe, Beispiele.

Cloud Lösungen: Chancen – Grenzen – Hintergründe – Beispiele

| Chancen | Grenzen | Beispiele | Hintergründe / Gegenmaßnahmen |
|--|---|---|---|
| Standardisierung von Infrastruktur von Netzen, Hardware, Software | | | |
| <ul style="list-style-type: none"> + Kostenvorteile / Skaleneffekte + Flexibilität + Redundanzen + Transparenz / Traceability + Stabilität + Glaubwürdigkeit / Nachweispflicht (gegenüber Dritten) + Schutz / Sicherheit | <ul style="list-style-type: none"> - Abhängigkeit vom Lieferant / Dienstleister - wenn Fehler auftreten, haben sie größere Auswirkungen | <ul style="list-style-type: none"> • Flatrates, Pay as you use Modelle • Wechsel von Hardware oder VLAN (Optimierte Downtimes, Konfiguration) • “WannaCry”: Hackerangriff auf Netz- und Software-Lücken | <ul style="list-style-type: none"> • Weltweite Angebote • Internationale Branchen-Controls und Zertifizierungen (Vulnerability / Hardening) • Trust Center / Trusted Provider • Interessens-Verbünde: BSI / Cert |
| Standardisierung von Betrieb und Prozessen | | | |
| <ul style="list-style-type: none"> + Kostenvorteile / Skaleneffekte + Flexibilität + Redundanzen + Transparenz / Traceability + Stabilität + Glaubwürdigkeit / Nachweispflicht (gegenüber Dritten) + Schutz / Sicherheit | <ul style="list-style-type: none"> - ... - Vertrauensabhängigkeiten von Dritten (ISO, Auditoren) - Branchenübergreifende Standardisierungen kosten | <ul style="list-style-type: none"> • ... • IaaS / PaaS / SaaS-Lösungen* • Lizenzoptimierung • Vertrauen / Segregation of Duty • Branchen Best Practices: GxP/GAMP, ITIL, SOX • Unternehmens-Best Practices: ESARIS, Zero Outage | <ul style="list-style-type: none"> • ... • Datenschutz / Sicherheitsbestimmungen (US- vs. EU- / CH- / DE Datenschutzgesetz) • Umgang mit Vertrauensabhängigkeiten -> EU-Initiative bis 2015 zur Datenhaltung außerhalb von Pharma-Unternehmen -> MRA: Mutual Recognition Agreement zwischen Arzneimittel-Zulassungs- und Inspektionsbehörden der USA und der EU (v1:1998 v2: 2017) |
| <p>Anwendungsbeispiele: Klinik-Informationen-Systeme (KIS/HIS, LIS, RIS/PACS), Klinische Studien / Pharmakovigilanz-Datenbank, zentrales Krebsregister, Transplantation- / Knochenmarksspender-Datenbank, Rheumaregister, eFA / elektronische Patientenakte / persönliche Gesundheitsakten, Fitness / Wellness-App...</p> | | | |

*:„as a Service“ Cloud Lösungen: IaaS, SaaS, PaaS: Infrastructure (Network, Hardware, Server, Storage); Platform (Middleware, Standardsoftware); Software (Applications)





Klinische Studien und Patientendaten in der sicheren Cloud eines Pharma-IT-Dienstleisters: Chancen, Grenzen, Hintergründe, Beispiele.

Fazit

Aus Sicht von Datenschutz und Datensicherheit im Patienten- / Klinik- / Pharma-Umfeld sollten nur die Dienstleister ausgewählt / beauftragt / zugelassen werden, die durchgängig dokumentierte und unabhängig überprüfbare Leistungen erbringen.

Dies ist Aufgabe und zugleich Change aller Beteiligten:

- **Politik und Behörden**
 - sollten wachsam bleiben und gesetzliche Vorgaben kontinuierlich prüfen und an den Stand der (ICT- und Sicherheits-) Technik anpassen
- **Wirtschaft** speziell Pharmaunternehmen und ihre Dienstleister
 - sollte sich aktiv an der Verbesserung der Good Practices beteiligen und verstärkt Technik- und Branchen-übergreifend planen
- **Patienten, Ärzte, Spitäler** sowie deren „Auftraggeber“ / Versicherungsunternehmen
 - sollten die aktuellen Branchenstandards fordern und selbst beachten