Kein Backup – kein Mitleid

15.10.2024

PD Dr. Christian Stephan

Die Gesundheitsbranche ist zum drittgrößten Ziel von Cyberangriffen weltweit geworden

1 Education

2 Gov/Military

3 Healthcare

4 Comms.

5 ISP/MSP

Einrichtungen des Gesundheitswesens sind Nicht-IT-Organisationen

Angriffe auf Gesundheitssysteme stellen lebensbedrohliche Risiken dar

Daten aus dem Gesundheitswesen sind von Natur aus vertraulich

Advanced Persistent Threats (APT) und Ransomware-Banden machen sich diese Risiken zunutze, um Druck auszuüben, was zu kompromittierten Patientendaten und unterbrochenen medizinischen Diensten führt.

Hijack einer Infusionspumpe, 2015

Fernzugriff auf Hospira-Infusionspumpen und Fernsteuerung gefährlicher Medikamentendosen

MedStar Health breach, 2016

Ransomware erzwang die Abschaltung von Systemen in 10 Krankenhäusern und 250 Kliniken

GE MRI Sicherheitslücke, 2018

Kritische Schwachstelle in GE-MRT-Geräten könnte Fernübernahme und Manipulation ermöglichen

Ryuk ransomware, 2018-2019

Betroffen waren über 100 Gesundheitseinrichtungen weltweit, darunter Krankenhäuser, Kliniken und medizinische Zentren

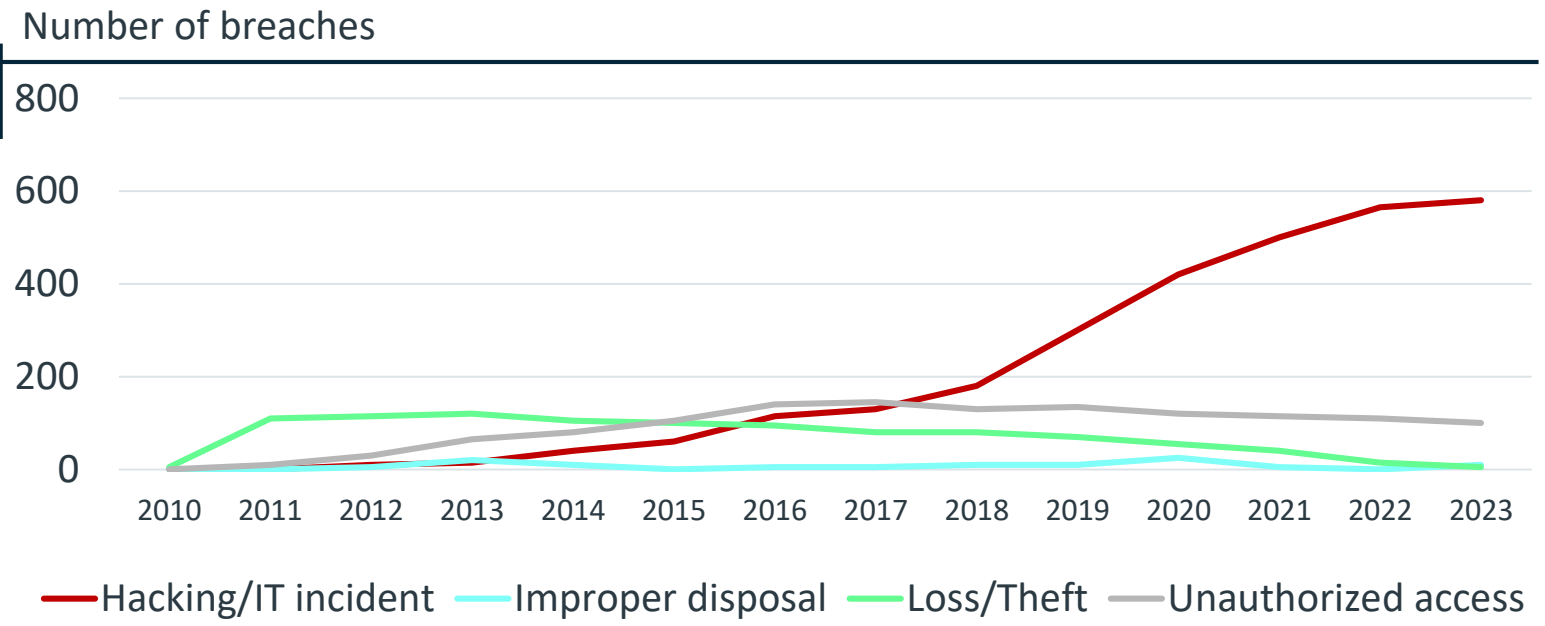
Conti ransomware, 2020-2021

Hunderte von Krankenhäusern und Kliniken, die der Pandemie zum Opfer fielen und die Versorgung unterbrachen

Digitalization and outsourcing has increased the number of security breaches in the industry

IT-Systeme sind die Hauptursache für Breaches

Die Digitalisierung im Gesundheitswesen hat sich seit 2013 beschleunigt und ist während Covid-19 stark angestiegen
Die beispiellose Nachfrage während der Pandemie führte zu einer schnellen Einführung digitaler Lösungen, manchmal ohne angemessene Tests
Dies führte zu einer Zunahme von IT-Sicherheitsvorfällen im Gesundheitswesen, bei denen bis 2023 über 124 Millionen Datensätze "verloren" gingen



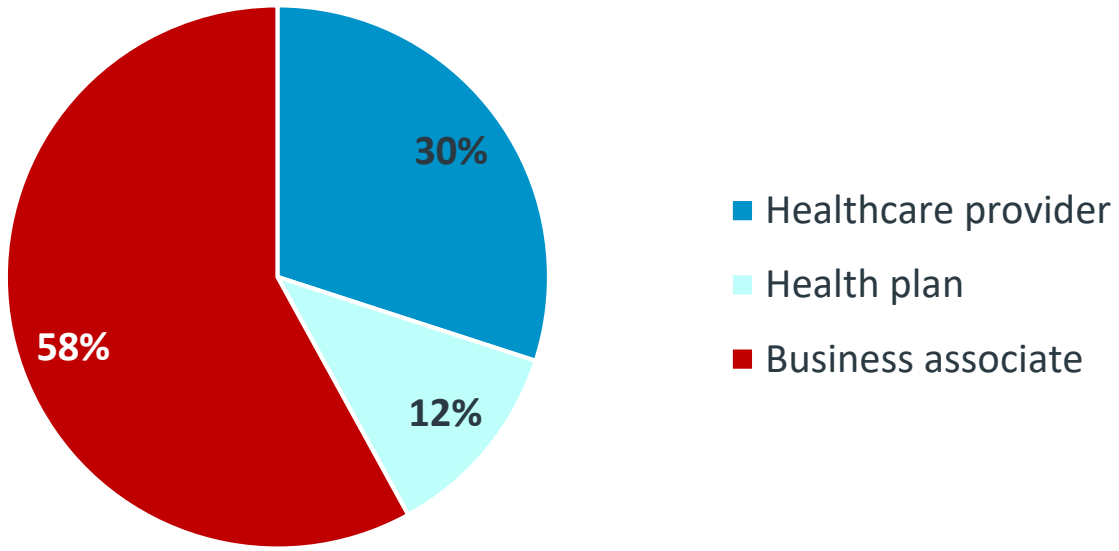
Source: https://www.hipaajournal.com – USA statistics

2

Digitalization and outsourcing has increased the number of security breaches in the industry

Vielen medizinischen Einrichtungen fehlt es an Fachwissen oder Ressourcen für komplexe Netzwerkeinrichtungen. Sie verlassen sich in verschiedenen Bereichen wie IT-Infrastruktur, Gehaltsabrechnungen, Verarbeitung und Speicherung medizinischer Daten häufig auf externe Geschäftspartner. Die Geschäftspartner sind die Hauptursache für Datenschutzverletzungen, da sie Zugang zu mehreren medizinischen Einrichtungen haben.

Prozentualer Beitrag der Datenschutzverletzungen



Source: https://www.hipaajournal.com – USA statistics

3

Studie zeigt: Über 90 % der Gesundheitseinrichtungen in Deutschland haben Datenschutzvorfall erlitten

AUA!!!

Okt • 26 • 2022

9 von 10 IT-Fachkräften in der Gesundheitsbranche attestieren Mängel bei der Sicherheit von Patientendaten

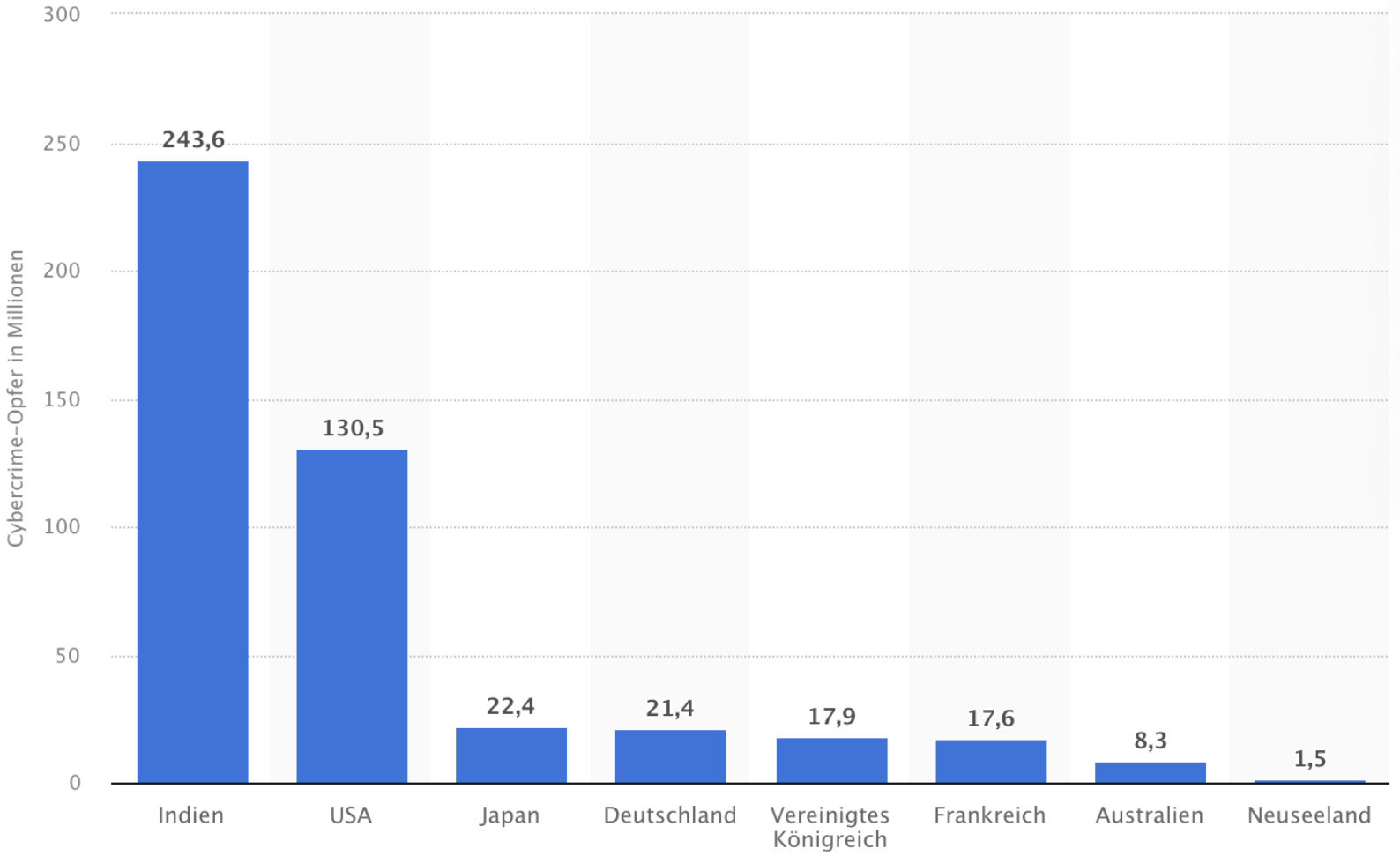
stock.adobe.com

München. Laut einer aktuellen Studie von SOTI mit dem Titel *„Eine entscheidende Investition: Am Puls der Technologie im Gesundheitswesen“* haben 91 % der Gesundheitseinrichtungen in Deutschland (70 % weltweit) seit dem Jahr 2020 mindestens einen Datenschutzvorfall erlitten. Dennoch sind 83 % der Befragten (76 % weltweit) der Meinung, eine vollständige Digitalisierung von Patientenakten könne die Datensicherheit verbessern und die Gefahr von Datenverlusten verringern.

- Datenverlust durch vorsätzliches oder fahrlässiges Fehlverhalten der Mitarbeiter (63 % in Deutschland; 49 % weltweit)
- Datenschutzverletzungen aufgrund externer Ursachen, beispielsweise durch DDoS-Attacken (59 % in Deutschland; 48 % weltweit)

https://ku-gesundheitsmanagement.de/2022/10/26/studie-zeigt-ueber-90-der-gesundheitseinrichtungen-in-deutschland-haben-datenschutzvorfall-erlitten/

Cybercrime Opfer in Millionen



KAIROS GmbH – DIN ISO 13485 und 9001

The Cybersecurity Connection

While ISO 13485 doesn't explicitly cover cybersecurity, the standard's emphasis on risk management provides a natural extension into cybersecurity considerations. The integration of cybersecurity into the QMS under ISO 13485 can significantly enhance the security posture of medical devices by:

1. **Risk Management:** ISO 13485 mandates a comprehensive risk management approach throughout the device lifecycle. Extending this to include cybersecurity risks ensures a holistic view of all potential threats to device safety and effectiveness.
2. **Design and Development:** The standard requires documented procedures for design and development, including validation of the design's ability to meet specified requirements. This aligns with cybersecurity best practices, emphasizing secure design principles and validating security features.
3. **Supplier Management:** Given the complex supply chains involved in medical device manufacturing, ISO 13485's focus on supplier evaluation and monitoring is crucial. This includes ensuring that software and IT service providers adhere to stringent cybersecurity standards, reducing the risk of vulnerabilities in the device ecosystem.
4. **Continuous Improvement:** A core principle of ISO 13485 is the commitment to continuous improvement, which is critical for cybersecurity. It involves regular updates, vulnerability management, and staying ahead of emerging threats.
5. **Training and Awareness:** The standard underscores the importance of training personnel involved in the QMS. Expanding this training to cover cybersecurity awareness and practices can mitigate risks associated with human error.

Black Duck Audit

Security test

Static application security testing audits combine automated, tool-based scans with expert source code review to systematically find critical software security vulnerabilities such as SQL injection, cross-site scripting, buffer overflows, and the rest of the OWASP Top 10. They provide an inside-out view of the security of the code.

Penetration test audits are essentially ethical hacking to assess the security robustness of a software asset. They provide an examination of the applications from the outside-in, in their full running state. These tests include exploratory risk analysis in which auditors try to bypass security controls (such as WAFs and input validation) and attempt to abuse business logic and user authorization to demonstrate how hackers could gain access and cause damage.

Secure design review audits find system defects related to security controls in the design of an application. These audits include interviews with the engineers responsible for application security to evaluate the design of key security controls. Password storage, identity and access management, and use of cryptography, among others, are compared against industry best practices to determine whether any are misconfigured, weak, misused, or missing. No testing or analysis of the application or code is performed.

KAIROS GmbH – Deming-Cycle (Plan, Do, Check, Act)

- Backups bei der Kairos erfolgen den Vorgaben der entsprechenden Normen
- Dazu gibt es entsprechende Software Design Spezifikationen (SWD)
- Kritische Strukturen definieren (Netzwerke, Server und Clientarbeitsplätze)
- Datenbanken sichern
- Programmkonfigurationen sichern
- Full Backup der verwendeten Services
- Dateisicherung von wichtigen Verzeichnissen (Benutzerverantwortung)
- Dokumentation der Sicherungen
- Simulation Desaster Recovery
- IQVIA ermöglicht auch das Hosting von Daten (LEVEL2 und LEVEL3)
- Viel Zeit!!!!!!

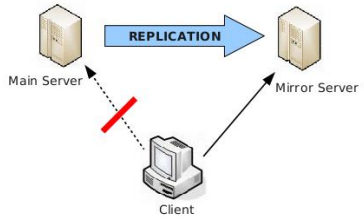
Seid ihr alle DIN ISO 27001?

Bridging the Gap with Cybersecurity Frameworks

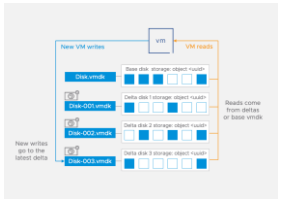
To address cybersecurity comprehensively, manufacturers are encouraged to integrate specific cybersecurity frameworks, such as ISO/IEC 27001 or the NIST Cybersecurity Framework, into their QMS. This dual approach ensures that the quality and security of medical devices are managed effectively, addressing not only the physical safety of devices but also the protection of sensitive health data.

Was ist kein Backup

- Eine Replikation/Mirror-Server



- Snapshot der virtuellen Maschine



- „was soll denn passieren“-Aussagen

BMI

- „Hoffnung“

Einwilligung benötigt auch ein Backup

Einwilligung (elektronisch)

Thieme Compliance

ID-Management (elektronisch)

bdr.
BUNDESDRUCKEREI

Speicherung (elektronisch)

KAIROS
an IQVIA business

Datenbank Backup

The heart of data

Datensicherung (englisch *backup*) bezeichnet den Vorgang zum Sichern von Daten mit der Absicht, diese im Falle eines Datenverlustes wiederherzustellen.

Vorschlag der Kairos GmbH:

- Full Backup alle 2 Wochen
- Incrementelle Backups täglich
- “transcaction log“ alle 2 Stunden
- Das Backup kann zwar lokal erstellt werden muss aber unbedingt mindestens auf ein anderes Laufwerk, besser auf einen anderen Server in einem anderen Gebäude, an einem anderen Ort, in einem anderen Land
- Alle Konfigurationsfiles nach jeder Änderung gesondert speichern.

Ist eigentlich jedem klar, dass der heilige Grahl (DICOM/HL7)…

- … keine Verschlüsselung hat
- … keine Authentifizierung hat

Cybersicherheit

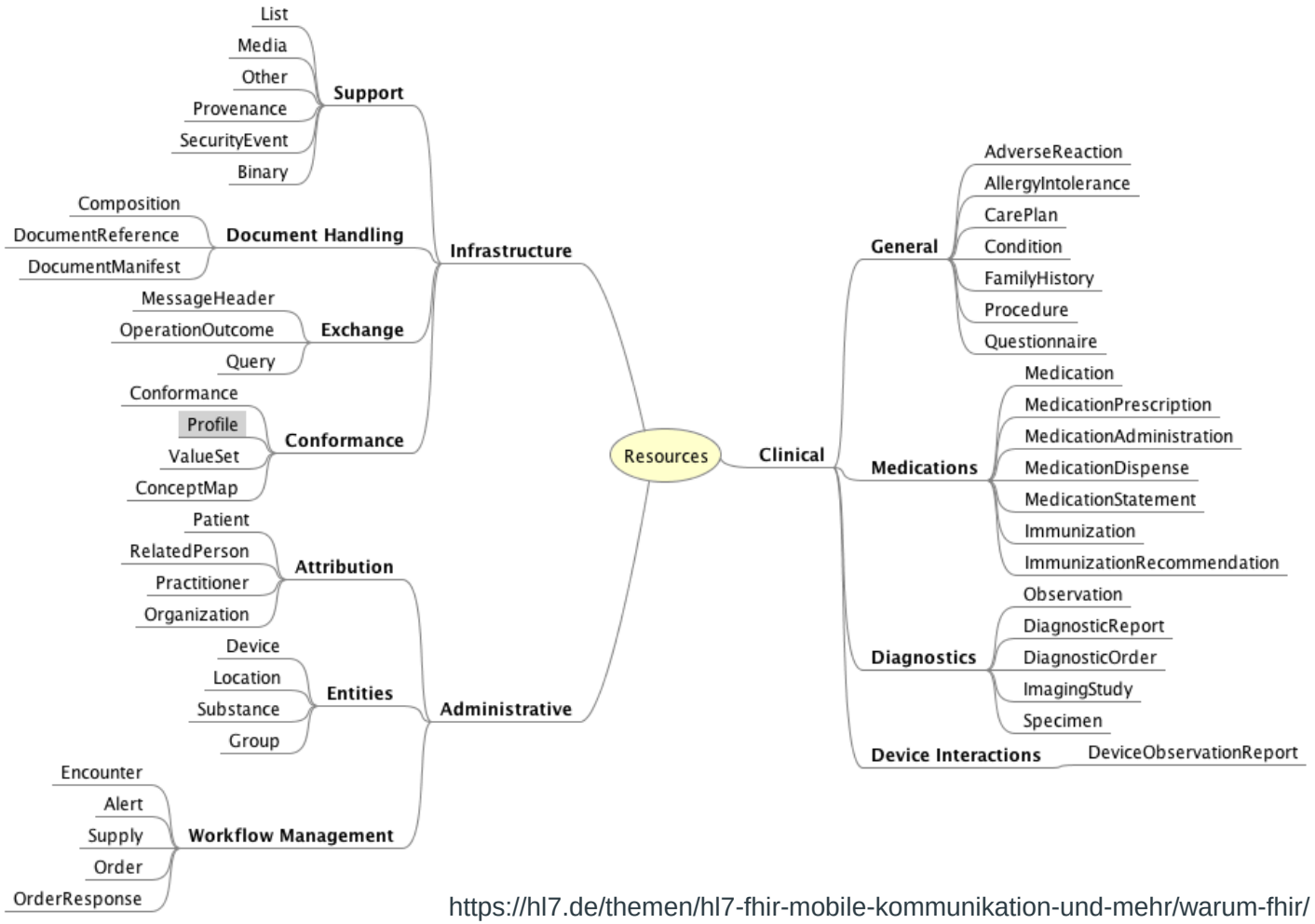
„DICOM und HL7 sind generell unsicher“

26.05.2022 · Von Natalie Ziebolz

- … keine Einwilligungen berücksichtigen kann
- … nicht automatisch eine Senderkennung oder Empfängerkennung hat
- … btw das ist Email-ähnlich

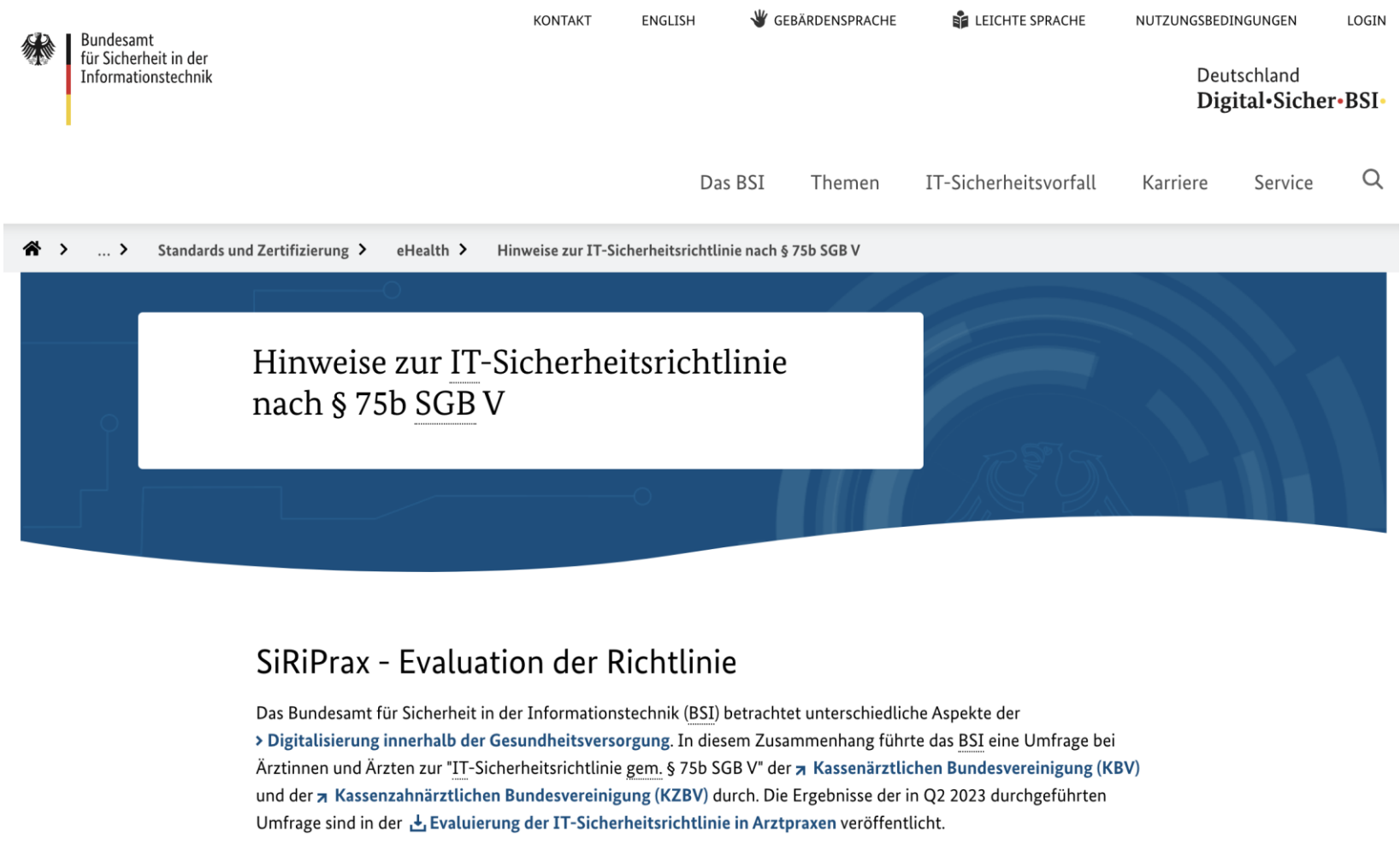
„Teilweise gibt es jedoch auch systematische Fehler. DICOM und HL7 für den Austausch von Daten zwischen Organisationen im Gesundheitswesen sind generell sehr unsicher. Diese Schwachstellen lassen sich nicht von heute auf morgen beheben“,

Es wird brennend nach einer Lösung ist gesucht - FHIR

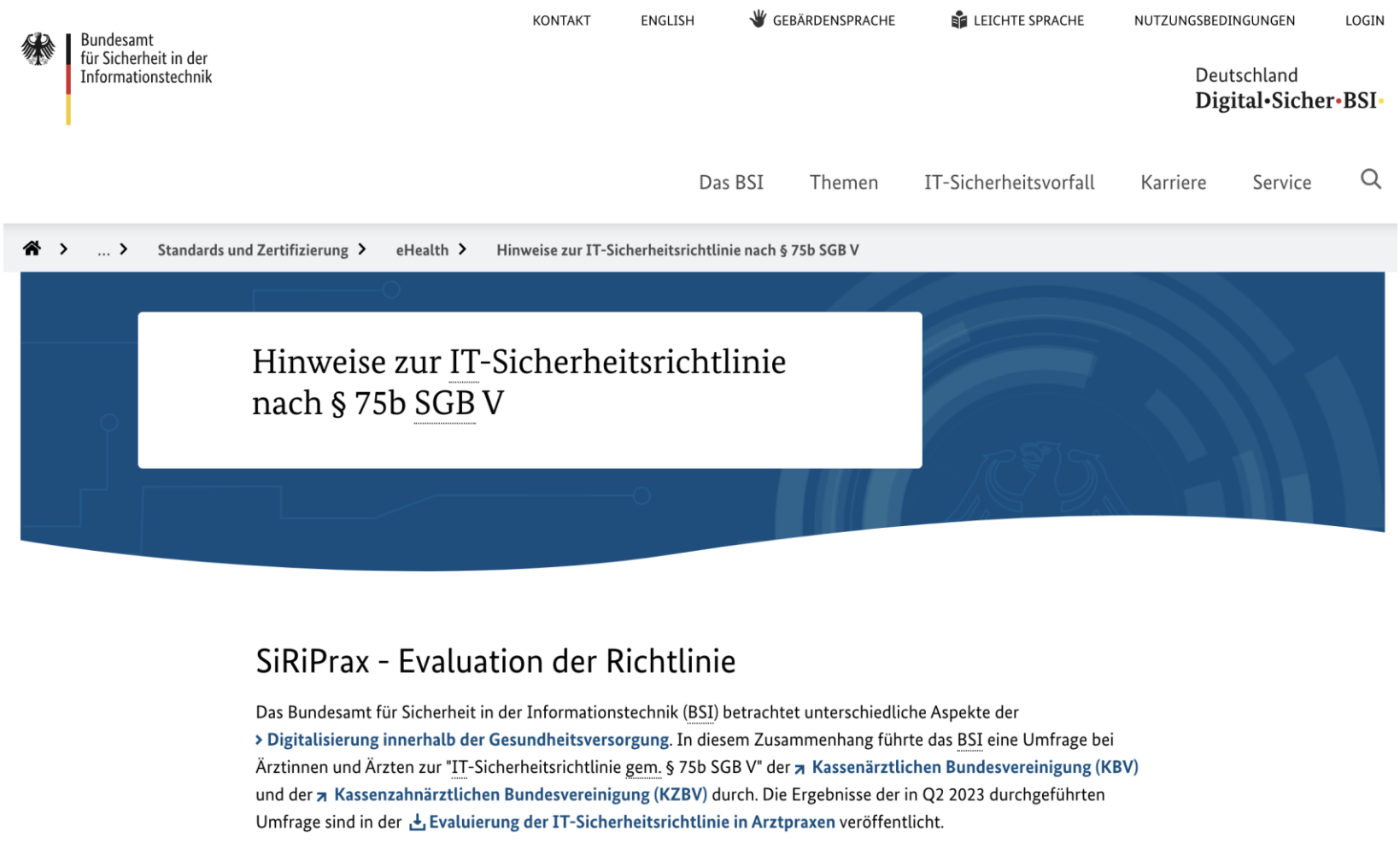


https://hl7.de/themen/hl7-fhir-mobile-kommunikation-und-mehr/warum-fhir/

Wissen ist Macht - BSI



Vorsorgen macht Sinn!



CentraXX Biobanking

ist nun

IQVIA Biobanking Solution

IQVIA

Hindsight-Bias

Nachher ist man vorher immer schlauer!