

Dass Maschinen
miteinander reden –
ok.
Aber mit dem
Betriebsrat ...?



INDUSTRIE 4.0 - CHANCE ODER HYPE?

Dr. Bernd Schütze

Innovationsforum „Krankenhaus 4.0“ / hospitalconcepts 2017, 2017-10-14



HEALTHCARE SOLUTIONS



Deutsche Telekom Healthcare and Security Solutions GmbH

Dr. Bernd Schütze
Senior Experte Medical Data Security

+49 (160) 9566 - 3145

Bernd.Schuetze@T-Systems.com



Studium

- Informatik (FH-Dortmund)
- Humanmedizin (Uni Düsseldorf / Uni Witten/Herdecke)
- Jura (Fern-Uni Hagen)

Ergänzende Ausbildung

- Datenschutzbeauftragter (Ulmer Akademie für Datenschutz und IT-Sicherheit)
- Datenschutz-Auditor (TüV Süd)
- Medizin-Produkte-Integrator (VDE Prüf- und Zertifizierungsinstitut)

Berufserfahrung

- Über 10 Jahre klinische Erfahrung
- Mehr als 20 Jahre IT im Krankenhäusern
- > 20 Jahre Datenschutz im Gesundheitswesen

Mitarbeit in wiss. Fachgesellschaften

- Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V. (GMDS)
- Gesellschaft für Datenschutz und Datensicherung e.V. (GDD)
- Gesellschaft für Informatik (GI)

Mitarbeit in Verbänden

- Berufsverband der Datenschutzbeauftragten Deutschlands e.V. (BvD)
- Berufsverband Medizinischer Informatiker e.V. (BVMi)
- Fachverband Biomedizinische Technik e.V. (fbmt)
- HL7 Deutschland e.V.
- HE Deutschland e.V.

AGENDA

„To-do-Liste“

- Warum eigentlich Datenschutz/IT-Sicherheit?
- Begriffsbestimmung Industrie 4.0
- Industrie 4.0 und Datenverarbeitung: Wo kommen die Gesundheitsdaten her?
- Datenschutzrechtliche Anforderungen
- Anforderungen bzgl. IT-Sicherheit
- Industrie 4.0 - Chance oder Hype?

**MOTIVATION:
WARUM EIGENTLICH
DATENSCHUTZ/IT-SICHERHEIT?**

WARUM EIGENTLICH DATENSCHUTZ/IT-SICHERHEIT?

SPIEGEL ONLINE

Menü | Politik Meinung Wirtschaft

NETZWELT

Nachrichten > Netzwelt > Netzpolitik > Medizintechnik

Angriff im OP

Hacker könnten Nar...

Patienten droht eine neue Gefahr: H...
verändern. Nach Informationen des



Also ging Grunow eine Kooperation mit...
stellten ihm die Geräte zur Verfügung...
Computer auseinander.

DAS SPIEGELMAGAZIN

Nr. 2/9.1.12

Deutschland: 4,- €



Horror im OP - Hacker steuern Personal aus der Ferne!



Hier könnte auch Ihr
Produkt „beworben“
werden...

... vor Hackerangriffen auf...

Blogs

...che. Wie sie
...das

...sonders die Medizintechnik ist
...tsches Unternehmen tut sich

...sicherheitslücken:
...egerät

...chutz | DoS-A

...rät fern

...gert die
...chen ungemein,
...erste Stelle
...greifer Zugriff

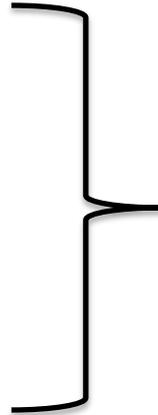
BEGRIFFSBESTIMMUNG INDUSTRIE 4.0

INDUSTRIE 4.0: WAS IST DAS?

Es gibt keine Definition!

- Definition schwierig: Alles, was mit „Digitalisierung zusammenhängt, scheint „4.0“ zu sein
- Digitalisierung der Industrie - Die Plattform Industrie 4.0 : Fortschrittsbericht¹⁾
 - ➔ Digitalisierung der Produktion
- Aber was ist die „Digitalisierung der Produktion“?

- Industrieroboter?
- Cloud?
- Big/Smart Data?
- Machine learning?
- Internet der Dinge?
- ...?



- 1) **Das alles als Grundlage**
- 2) **Ergänzend: Extraktion von Wissen aus Daten**
(D.h. nicht mehr alleinige Gewinnung von Wissen aus menschlicher Erfahrung)

1) Bundesministerium für Wirtschaft und Energie: Digitalisierung der Industrie - Die Plattform Industrie 4.0 Fortschrittsbericht

<http://www.bmwi.de/Redaktion/DE/Publikationen/Industrie/digitalisierung-der-industrie.html>

INDUSTRIE 4.0 UND DATENVERARBEITUNG

Wo kommen die Gesundheitsdaten her?

HERKUNFT DER DATEN

Die Vernetzung der Welt bietet unzählige Datenquellen, z.B. ...

- **Netzwerke**
 - Facebook, Twitter, Google, Xing, LinkedIn. Apple, Microsoft, Skype, Friendship24, Parship, ...
- **Einkauf im Netz**
 - Payback, Happy Digits
- **Kundenkarten**
 - Douglas-Kundenkarte, Lufthansa Milres&More, EC-Karte, Kreditkarte, Krankenkassenkarte
- **Handy**
 - Standort, Wann wurde mit wem gesprochen, Termine, Kamera, Mikrofon
- **Navy des Autos**
- **Serviceschnittstelle des intelligenten Stromzählers**
- **E-Mails**
- **Regierung**
 - Schweizer Bundesarchiv (opendata.admin.ch): Energie, Ökonomie, Umwelt, Verkehr, Finanzen, Wirtschaft und Gesundheit
- ...

HERKUNFT DER DATEN

Gesundheitsdaten

- **„Wellness“-Daten**
 - Fitness-Tracker, Sportstudio, Heimtrainer, ...
- **Patientenversorgung**
 - Arztpraxis, Krankenhaus, Reha-Zentren, Krankenkassen, ...
 - Krankheitsregister, z.B. Krebsregister oder Infektionsregister
- **Forschung**
 - Analyse von menschlichen und bakteriellen Genomen
 - Untersuchung von Stoffwechselabläufen in gesunden und kranken Organismen
 - Erforschung von Molekülstrukturen und -funktionen zur Krankheitsbekämpfung
 - ...
- **Statistische Gesundheitsberichterstattung**
 - Deutschland, Europa, USA, ...
- **Gesundheitsdaten durch „Smarte“ Technik**
 - Smartphone, Smart-Home, ...
- **Internet**
 - Portale bzgl. Krankheit bzw. deren medizinischer Versorgung, Erfahrungsaustausch Patienten, ...
- ...

DATEN SIND DA...

... sind es auch die richtigen? Und können wir damit umgehen?

- **Täglich neu produzierten Menge > 2,5 Exabytes, also 2,5 10¹⁸ Bytes***
- **Jährlich wachsende Telekommunikationskapazität von fast 30 %****
- **Technologische Entwicklungen**
 - mobile content
 - sensor-based content

bieten zuvor nicht vorhandene Möglichkeiten der Datenerfassung.

➔ **Sind wir in der Lage, die Daten angemessen zu verarbeiten?**

- ➔ Erfahrungen aus der Terrorismusbekämpfung zeigen: Nicht die zur Verfügung stehenden Daten sind das Problem, sondern deren Verarbeitung.
- ➔ Stehen die Daten denen, die sie brauchen zur Verfügung?
- ➔ Sind wir in der Lage, aus dem Berg der Daten die für die Fragestellung relevanten in einer angemessenen Zeit herauszusuchen?
- ➔ Können wir den Missbrauch der gesammelten Daten verhindern?

* McAfee A, Brynjolfsson E (2012) Big data: the management revolution. Harvard Business Review

** Hilbert M, López P (2011) The world's technological capacity to store, communicate, and compute information. Science 332:60–65

DATENSCHUTZRECHTLICHE ANFORDERUNGEN

DATENSCHUTZRECHT – NUR EIN ASPEKT

Zugang zu Patientendaten = Vierfacher Schutz



Arbeitsrecht

Datenschutzrecht

Standes-, Berufsrecht

Strafrecht

DATENSCHUTZ

Voraussetzung: Personenbezogene Daten

- **Art. 4 Ziff. 1 DS-GVO**
 - **alle** Informationen, die sich auf eine identifizierte oder **identifizierbare** natürliche Person beziehen
 - als identifizierbar wird eine natürliche Person angesehen, die **direkt** oder **indirekt** [...] identifiziert werden kann;
- **Auch Pseudonyme sind personenbezogene Daten, z. B.**
 - Öffentliches Personenpseudonym (Telefonnummer, ...)
 - Nicht-Öffentliches Personenpseudonym (Konto-Nummer, ...)
 - Anonymes Personenpseudonym (eigenes Genom, ...)
 - Geschäftsbeziehungspseudonym (Chat-Name, ...)
 - Transaktionspseudonym (PIN, TAN, ...)
- **Auch IP-Adressen, KFZ-Nummernschilder usw. sind Personen identifizierende Daten!**

DATENSCHUTZRECHTLICHE RAHMENBEDINGUNGEN

Es gibt ein paar datenschutzrechtliche Regeln im Gesundheitswesen ...

Bundesrecht

- Bundesdatenschutzgesetz (BDSG)
- Telekommunikationsgesetz (TKG)
- Telemediengesetz (TMG)
- Signaturgesetz (SigG)
- Verordnung zur elektronischen Signatur (SigV)
- Mediendienstaatsvertrag (MDSStV)

Landesrecht (z.B. NRW)

- Archivgesetz (ArchivG)
- Gesetz über die Ausführung des Gesetzes zu Artikel 10 Grundgesetz (AG G 10 NW)
- Berufsordnung der Ärztekammer Westfalen-Lippe
- Berufsordnung für die nordrheinischen Ärztinnen und Ärzte
- Berufsordnung für Apothekerinnen und Apotheker der Apothekerkammer Nordrhein
- Berufsordnung für Apothekerinnen und Apotheker der Apothekerkammer Westfalen-Lippe
- Datenschutzgesetz (DSG NRW)
- Gesetz über den öffentlichen Gesundheitsdienst (ÖGDG)
- Gesetz über den Feuerschutz und die Hilfeleistung
- Gesetz über Hilfen und Schutzmaßnahmen bei psychischen Krankheiten (PsychKG)
- Gesetz über Tageseinrichtungen für Kinder (GTK)
- Gesundheitsdatenschutzgesetz (GDSG NW)
- Gutachterausschussverordnung (GAVO NRW)
- Heilberufsgesetz (HeilBerG)
- Hochschulgesetz (HG)
- Krankenhausgesetz (KHG NRW)
- Meldedatenübermittlungsverordnung (MeldDÜV NRW)
- Meldegesetz (MG NRW)
- Sicherheitsüberprüfungsgesetz (SÜG NRW)
- Verordnung zur Durchführung des Meldegesetzes (DVO MG NRW)

Sozialrecht

- Sozialgesetzbuch V (SGB V)
 - § 73 Kassenärztliche Vereinigung
 - § 140a Integrierte Versorgung
- Sozialgesetzbuch X
- ...

EU

- Datenschutz-Grundverordnung (ab 25. Mai 2018)
- EIDAS-Verordnung
- Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr
- Richtlinie 2002/22/EG Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten (Universaldienstrichtlinie)
- Richtlinie 2002/58/EG (Datenschutzrichtlinie für elektronische Kommunikation)
- Richtlinie 2006/24/EG über die Vorratsspeicherung von Daten
- Richtlinie 2009/136/EG („Cookie“-Richtlinie)

Kirchenrecht

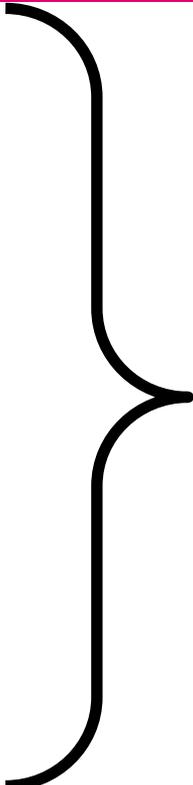
- Datenschutzgesetz der Evangelischen Kirche in Deutschland (DSG-EKD)
- Verordnung über die in das Gemeindeverzeichnis aufzunehmenden Daten der Kirchenmitglieder mit ihren Familienangehörigen
- Verordnung über den automatisierten zwischenkirchlichen Datenaustausch
- Verordnung mit Gesetzeskraft zur Einführung des Datenschutzes in der Vereinigten Evangelisch-Lutherischen Kirche Deutschlands
- Anordnung über die Sicherung und Nutzung der Archive der Katholischen Kirche
- Anordnung über das kirchliche Meldewesen (KMAO) für Bistum ...
- Anordnung über den kirchlichen Datenschutz (KDO) für Bistum ...
- Durchführungsverordnung zur KDO (KDO-DVO)

Medizinisches Umfeld

- Musterberufsordnung für deutsche Ärztinnen und Ärzte (MBO)
 - §9 Abs. 1 Schweigepflicht des Arztes
- Strafprozessordnung (StPO)
 - §53 Abs. 1 Zeugnisverweigerungsrecht
 - §97 Abs.1 Beschlagnahmeverbot
 - §103 Abs.1 eingeschränktes Durchsuchungsrecht für Arztpraxen
- Strafgesetzbuches (StGB)
 - §203 Abs.1 4.2.1.2.c Ärztliche Schweigepflicht
- Zivilprozessordnung (ZPO)
 - § 383 Zeugnisverweigerung aus persönlichen Gründen

DATENSCHUTZRECHTLICHE ANFORDERUNGEN ...

... sind eigentlich überschaubar. Und umsetzbar.

- EU
 - Europäische Grundrechte-Charta
 - Datenschutz-Grundverordnung
 - Datenschutz-Richtlinie
Wirkung über Umsetzung in deutsche Gesetze
 - Bundesdatenschutzgesetz (BDSG)
 - Privatpersonen
 - Privatwirtschaft
 - Bundesbehörden
 - Kirchliche Datenschutzgesetze
 - Einrichtungen der evang. und kath. Kirche
 - Landesdatenschutzgesetze
 - öffentliche Verwaltung in Land und Kommunen
 - Spezialgesetze
(Vorrang vor allg. Gesetzen)
 - Telemediengesetz
 - Gesundheitsdatenschutz
 - Hochschulgesetz
 - SGB, AO, Polizeigesetz, Passgesetz,
Personalausweisgesetz, Aufenthaltsgesetz,
Landesmeldegesetz, Landesverwaltungsgesetz, ...
- 
- Rechtmäßigkeit der Datenverarbeitung
 - Gesetzliche Grundlagen
 - Einwilligung
 - Grundsatz der Zweckbindung
 - Grundsatz der Erforderlichkeit
 - Grundsatz der Datenvermeidung und Datensparsamkeit
 - Grundsatz der Transparenz
 - Grundsatz der klaren Verantwortlichkeiten
 - Grundsatz der Kontrolle
 - Grundsatz der Gewährleistung der Betroffenenrechte
 - Verbot der Profilbildung
 - Verbot der Datensammlung auf Vorrat
 - Verbot der automatisierten Einzelentscheidung
 - Nutzung pseudonymisierter oder anonymisierter Daten
 - Verpflichtung zum Schutz der Daten

DATEN DER BESONDEREN KATEGORIEN

Gesundheitsdaten, genetische Daten = „besondere Kategorien von Daten“

- „Daten besonderer Kategorien“ (Art. 9 DS-GVO)
 - Rassistische und ethnische Herkunft
 - Politische Meinungen
 - Religiöse oder weltanschauliche Überzeugungen
 - Gewerkschaftszugehörigkeit
 - **Genetische Daten**
 - Biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person
 - **Gesundheitsdaten**
 - Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person
- Ist eine Verarbeitung nicht ausdrücklich erlaubt, so ist sie verboten (Art. 9 Abs. 1 DS-GVO)
- Cave: Art. 6 stellt keinen Erlaubnistatbestand für besondere Kategorien von Datenarten dar!

ART. 9: VERARBEITUNG BESONDERER KATEGORIEN PERSONENBEZOGENER DATEN

Erlaubnistatbestand: Einwilligung

- **Art. 9 Abs. 2: Absatz 1 gilt nicht in folgenden Fällen (= Verarbeitung ist erlaubt 😊)**
 - a) betroffene Person hat in die Verarbeitung der genannten personenbezogenen Daten für einen oder mehrere festgelegte Zwecke ausdrücklich eingewilligt
- **Dabei beachten:**
 - Art. 4 Abs. 11: Definition (die Anforderungen beinhaltet)
 - freiwillig (=ohne Zwang)
 - für den bestimmten Fall
 - in informierter Weise (= in Kenntnis der Sachlage)
 - unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung (= eindeutig „ich will“)
 - mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist (= ausdrückliche Willenserklärung)

ART. 9: VERARBEITUNG BESONDERER KATEGORIEN PERSONENBEZOGENER DATEN

Erlaubnistatbestand: Einwilligung

- **Art. 9 Abs. 2: Absatz 1 gilt nicht in folgenden Fällen (= Verarbeitung ist erlaubt 😊)**
 - a) betroffene Person hat in die Verarbeitung der genannten personenbezogenen Daten für einen oder mehrere festgelegte Zwecke ausdrücklich eingewilligt
- **Dabei beachten:**
 - Art. 7: Bedingungen für die Einwilligung
 - Beweislast beim Datenverarbeiter (Art. 7 Abs. 1)
 - Bei Einholung Einwilligung in Zusammenhang mit anderen Sachverhalten:
„verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache so erfolgen, dass es von den anderen Sachverhalten klar zu unterscheiden ist“ (Art. 7. Abs. 2)
(= ist für den Betroffenen transparent dargestellt, worum es geht und welche Auswirkungen es hat oder haben könnte“)
 - Recht zum Widerruf, Hinweis auf das Recht dazu bei Einwilligung (Art. 7 Abs. 3)
 - Hinweis, dass Widerruf die Rechtmäßigkeit der erfolgten Datenverarbeitung bis Erteilung des Widerrufs nicht berührt (Art. 7 Abs. 3)
 - Widerruf mindestens so einfach abzugeben wie die Einwilligung
 - Kopplungsverbot der Einwilligung mit Vertragsabschluss, Erbringung Dienstleistung o.ä.
 - Keine Schriftform mehr vorgegeben

BETROFFENENRECHTE: ARTT. 12 -23

Überwiegend geblieben

Recht auf

– **Transparenz (Art. 12)**

- Verantwortlicher informiert über Betroffenenrechte
- Informationen müssen in präziser, transparenter, verständlicher und leicht zugänglicher Form vorliegen
- Mitteilungspflicht Artt. 15ff innerhalb 4 Wochen, ggfs. Info über Fristverlängerung durch Verantwortlichen
- Unentgeltlich

– **Information (Artt. 13, 14)**

- Vor Beginn der Datenverarbeitung
- Cave Auskunftsrecht: neu ist Auskunft bzgl. Speicherdauer bzw. – falls nicht möglich – Darlegung der Kriterien für die Festlegung dieser Dauer

– **Auskunft (Art. 15)**

- Informationen nur an identifizierte Personen (Betroffene) weitergeben
- Cave: Betroffenen bzgl. Zweckänderung informieren

– **Berichtigung (Art. 16)**

BETROFFENENRECHTE: ARTT. 12 -23

Überwiegend geblieben

Recht auf

- **Löschung (Art. 17)**
 - Ggfs. auch Empfänger über Löschverlangen eines Betroffenen unterrichten
- **Sperrung (Art. 18)**
 - Nach Sperrung: außer Speichern keine Verarbeitung ohne Einwilligung betroffener mehr (abgesehen von drei Ausnahmetatbeständen)
 - Ggfs. muss über Aufhebung Sperrung Betroffener informiert werden
- **Widerspruchsrecht (Art. 21)**
 - Jederzeit möglich, bedarf keiner Einwilligung als Erlaubnistatbestand
- **Auf Widerspruchsrecht hinweisen**
 - Verarbeitung auch bei Widerspruch möglich, wenn „zwingende schutzwürdige Gründe“ die „Interessen, Rechte und Freiheiten“ des Betroffenen überwiegen → Nachweis erforderlich, also dokumentieren
- **Automatisierte Generierung von Einzelentscheidungen einschließlich Profiling (Art. 22)**



Aber auch Neues...

☀ Artikel 19 „Mitteilungspflicht im Zusammenhang mit der Berichtigung, Löschung oder Einschränkung“

- Empfängern, an die Daten weitergegeben wurden, jede Berichtigung, Löschung oder Einschränkung mitteilen
 - 👉 ToDo: Informationssystem anpassen

☀ Artikel 20 „Recht auf Datenübertragbarkeit“

- Voraussetzung: Einwilligung oder „Vertrag gemäß Art. 6 Abs. 1 lit. b“
Betroffene haben das
- Recht, Daten „in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten“
- Recht, Daten direkt von einem Verantwortlichen einem anderen Verantwortlichen übermitteln zu lassen
 - 👉 ToDo: Informationssystem anpassen

ANFORDERUNGEN BZGL. IT-SICHERHEIT

ART. 25 „DATENSCHUTZ DURCH TECHNIKGESTALTUNG UND DURCH DATENSCHUTZFREUNDLICHE VOREINSTELLUNGEN “

Privacy by Design / Privacy by Default

- Adressat: für die Daten Verantwortliche, nicht Hersteller
- ErwGr. 78: „*sollten* die Hersteller der Produkte, Dienste und Anwendungen *ermutigt werden, das Recht auf Datenschutz* bei der Entwicklung und Auslegung der Produkte, Dienste und Anwendungen *zu berücksichtigen*“
- Bußgeldbewehrter Tatbestand
- ➔ Daher Empfehlung: bei Anschaffung/Ausschreibung Anforderung berücksichtigen

ART. 32 „SICHERHEIT DER VERARBEITUNG“

Technisch-organisatorische Maßnahmen (TOMs)

Der für die Verarbeitung Verantwortliche und der Auftragsverarbeiter treffen unter Berücksichtigung

- des **Stands der Technik**,
- der **Implementierungskosten** und
- der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie
- der **unterschiedlichen Eintrittswahrscheinlichkeit** und **Schwere** des **Risikos für die persönlichen Rechte und Freiheiten**

geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten

ART. 35 „DATENSCHUTZ-FOLGENABSCHÄTZUNG“

Risikoanalyse und -Management

- **Mehr als „Vorabkontrolle“**
- **Insbesondere verpflichtend vorzunehmen (Art. 35. Abs. 3 lit. a)**
 - systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen, wenn diese Bewertung als Grundlage für rechtswirksame Entscheidungen dient
 - umfangreiche Verarbeitung **besonderer Kategorien von personenbezogenen Daten** (Art. 9 Abs. 1) bzw. Daten über strafrechtliche Verurteilungen und Straftaten (Art. 10)
 - systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche
- **(Mindest-) Inhalte von Art. 35 Abs. 7 vorgegeben**
 - geplanten Verarbeitungsvorgänge, Zwecke der Verarbeitung
 - Bewertung der Notwendigkeit und Verhältnismäßigkeit in Bezug auf den Zweck
 - Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen
 - zur Bewältigung der Risiken geplanten Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren
 - (inkl. **Nachweis**, dass DS-GVO eingehalten wird)
- **Hinweis: Ergebnis „hohes Risiko“ → Hinzuziehung der Aufsichtsbehörde**

INDUSTRIE 4.0 – CHANCE ODER HYPE?

INDUSTRIE 4.0 - CHANCE ODER HYPE?

Hype natürlich! ;-)

- „Industrie 4.0“ stellt als Begrifflichkeit sicherlich einen Hype dar
- Inhaltlich sind die Themen aktuell:
 - Medizinische Forschung basiert auf Empirie, also auf Auswertung vorhandener Daten.
 - ➔ Moderne Fragestellungen bedingen das Vorhandensein größerer Datenmengen, genauer: qualitativ guter Daten, welche zur Fragestellung passen.
 - „Individualisierte“ Medizin: ohne hinreichende Datenmenge bzgl. der jeweils zu behandelnden Person undenkbar.
Aber auch ohne eine hinreichende Datenmenge zur Ableitung der erfolgversprechendsten Therapie nicht denkbar.
 - „Alle notwendigen Daten zur richtigen Zeit am richtigen Ort. Weltweit.“
Das Versprechen Patienten gegenüber kann nur durch eine vernetzte Gesellschaft eingelöst werden.
 - ➔ Die Sensibilität von Gesundheitsdaten bedingen ein angemessenes Schutzniveau. D. h. ohne Anforderungen aus den Bereichen Datenschutz und IT-Sicherheit sind diese Themen nicht abbildbar.
- Auch wenn der Begriff „Industrie 4.0“ verschwindet: der Inhalt wird bleiben.

Lessons Learned

- „Industrie 4.0“: Begriff mag Hype sein, aber die Inhalte, für die der Begriff steht, bergen für die Gesundheitsversorgung großes Potenzial
- Die Verarbeitung von personenbezogenen oder personenbeziehbaren Gesundheitsdaten bedarf eines Erlaubnistatbestandes
 - Im Rahmen von Industrie 4.0 i.d.R. eine (nachweispflichtige) Einwilligung
- Menschen werden ihre sensiblen Gesundheitsdaten nur zur Verfügung stellen, wenn sie sicher sind, dass diese vor Missbrauch geschützt sind
 - Datenschutz und IT-Sicherheit auch ohne gesetzliche Forderung ein „muss“
- Europarechtliche datenschutzrechtliche Anforderungen sind i.d.R. vorrangiges Recht
 - Messlatte: EU Datenschutz-Grundverordnung
 - Cave: EU ePrivacy-Richtlinie angekündigt
 - ➔ Als „lex specialis“ ggf. vorrangig gegenüber DS-GVO
 - ➔ Anwendungsbereich auch M2M-Kommunikation (IoT, Smart Home, Industrie 4.0, ...)
- IT-Sicherheit notwendig; zu beachten
 - Klassische IT-Sicherheit: Schutz von aus Unternehmenssicht wertvollen Daten
 - Datenschutzrechtliche Anforderung: Schutz der aus Sicht der betroffenen Person schützenswerten Daten

DISKUSSION / FRAGEN



Kontakt: Bernd.Schuetze@T-Systems.com



HEALTHCARE SOLUTIONS