Transferforum: Digitales Arbeiten vs. Datenschutz

"Vertrauensvolle Kommunikation bei offener Tür?!"

Montag 23.11.2020
16.00 - 19.00 Uhr

Vorstellungsrunde – die HSHL:

Vorstellungsrunde – die KatHO NRW:

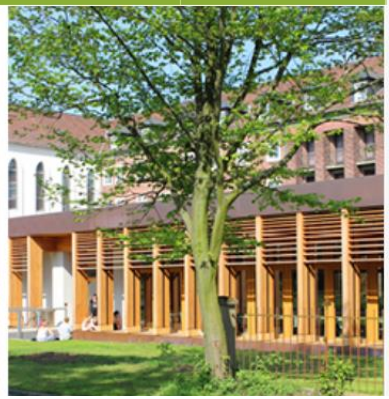
KatHO NRW

Katholische Hochschule Nordrhein-Westfalen
Catholic University of Applied Sciences

AACHEN | KÖLN | MÜNSTER | PADERBORN

Hochschule | Studium & Lehre | Praxisorientierung | Forschung & Entwicklung | Third Mission | Weiterbildung | Internationales





Im Wintersemester 1971/72 startete die Katholische Fachhochschule NW – die heutige Katholische Hochschule NRW – mit 1.374 Studierenden in drei Fächern den Vorlesungsbetrieb. Sie ist die Nachfolgeeinrichtung von 15 Ausbildungsstätten für Sozialarbeit /Sozialpädagogik und Religionspädagogik in Nordrhein-Westfalen. Träger der Fachhochschule sind die fünf (Erz-)Bistümer in NRW. Im Jahr 2021 feiert die Hochschule ihr 50-jähriges Bestehen vor allem mit drei Veranstaltungen:

Was ist das Internet: die Grundlagen


PC


Server


Laptop


Smart-phone

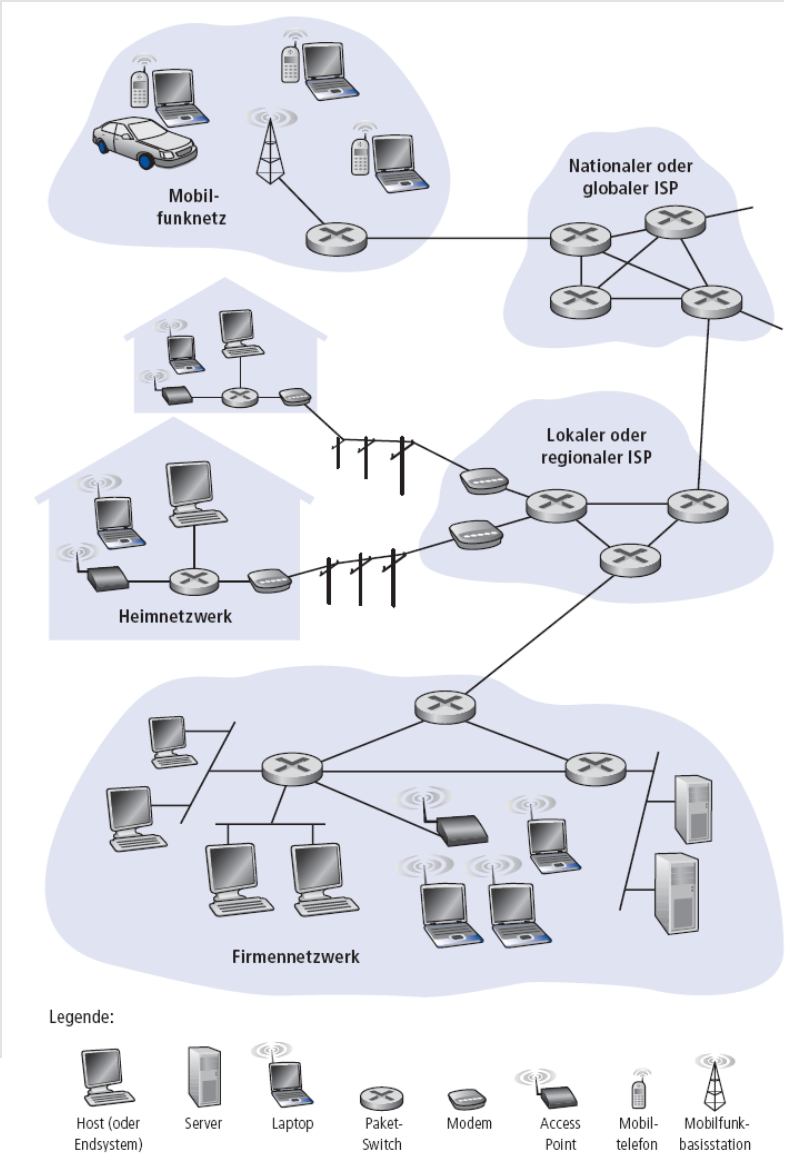
- Millionen vernetzter Computer:
  Hosts = Endsysteme
  - Auf denen Netzwerkanwendungen laufen
- *Leitungen/Funkstrecken (links)*
  - Glasfaser, Kupfer, Funk, Satellit
  - Übertragungsrate = *Bandbreite*


Access Points

Leitungen

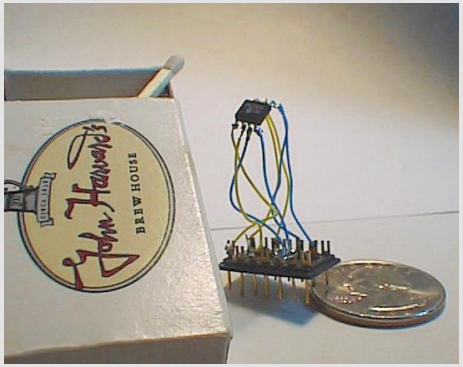

Router

- *Router:* leiten Datenpakete (Einheiten von Daten) weiter



„Coole“ Endsysteme und Anwendungen

IP picture frame
http://www.ceiva.com/



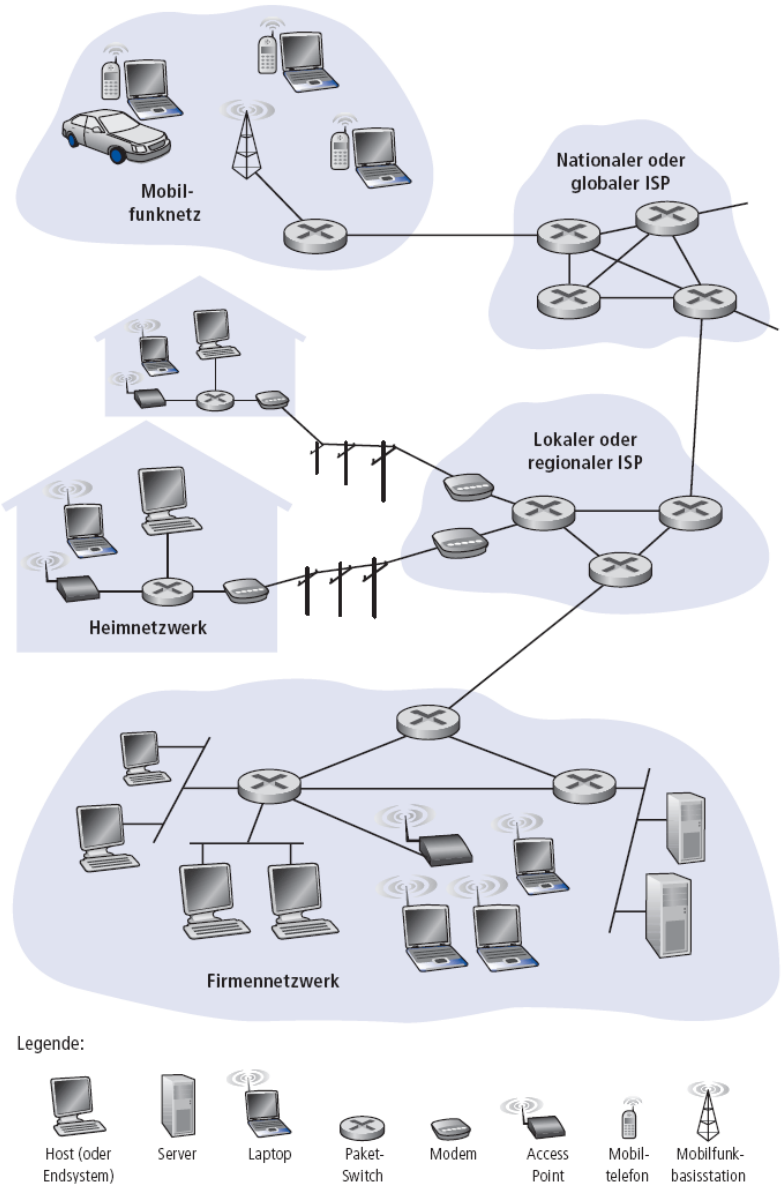
Kleinster Webserver der Welt:
http://www-ccs.cs.umass.edu/~shri/iPic.html

Internetfähige Medizinprodukte

Internettelefonie

Was ist das Internet: die Grundlagen

- *Protokolle* kontrollieren das Senden und Empfangen von Nachrichten
  - z.B., TCP, IP, HTTP, Skype, Ethernet
- *Internet:* "Netzwerk von Netzwerken"
  - Hierarchisch
  - Öffentliches Internet und privates Intranet
- Internetstandards
  - RFC: Request For Comments
  - IETF: Internet Engineering Task Force



Was ist ein Protokoll?

Protokolle zur Kommunikation zwischen Menschen:

- “Wie viel Uhr ist es?”
- “Ich habe eine Frage”
- Gegenseitiges Vorstellen

… es werden „standardisierte“ Nachrichten übertragen

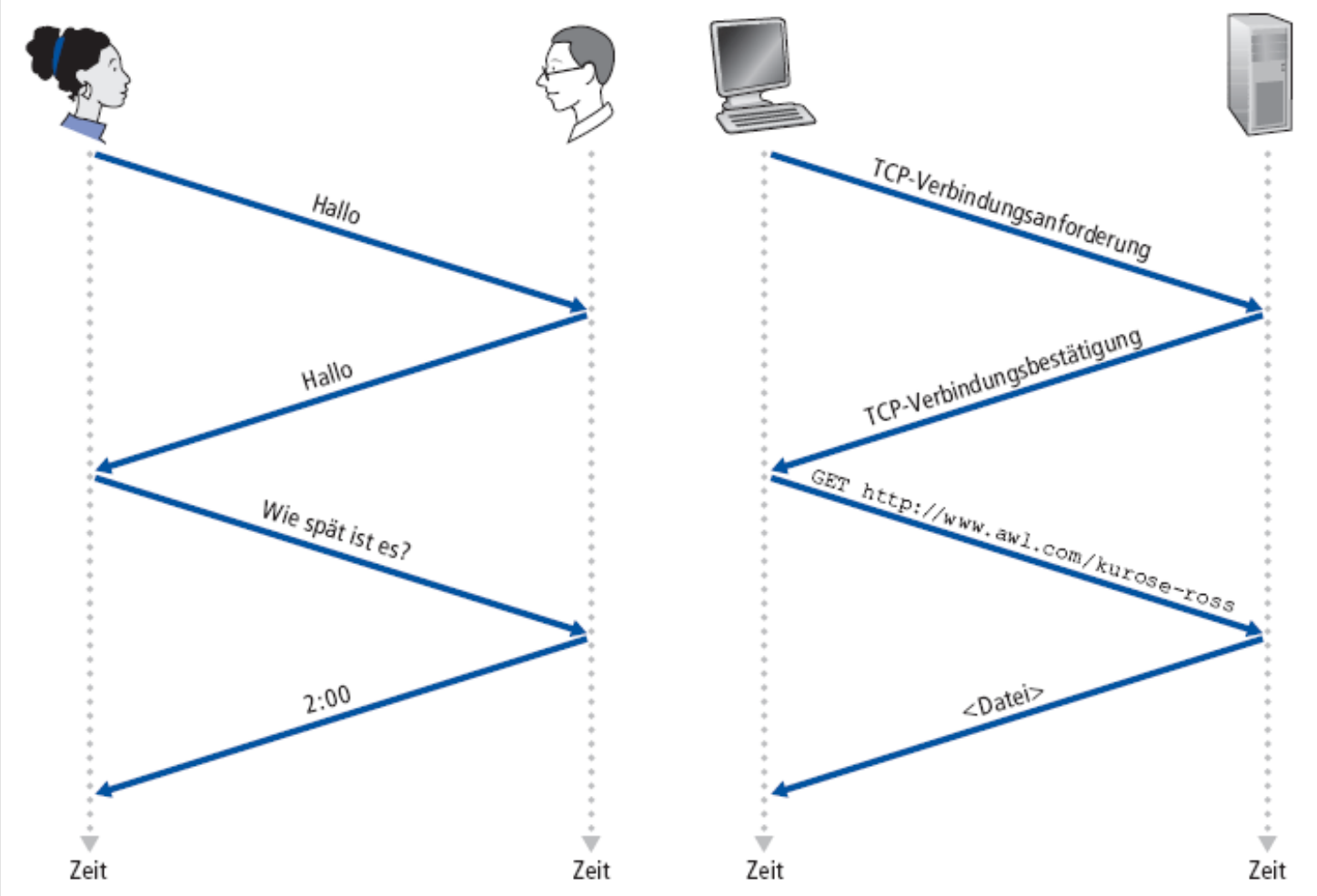
… durch den Empfang dieser Nachrichten werden „standardisierte“ Aktionen ausgelöst

Netzwerkprotokolle:

- Maschinen statt Menschen
- Sämtliche Kommunikation im Internet wird durch Protokolle geregelt

Protokolle definieren das Format und die Reihenfolge, in der Nachrichten von Systemen im Netzwerk gesendet und empfangen werden, sowie die Aktionen, welche durch diese Nachrichten ausgelöst werden.

Ein Protokoll zwischen Menschen und ein Protokoll in Computernetzwerken:



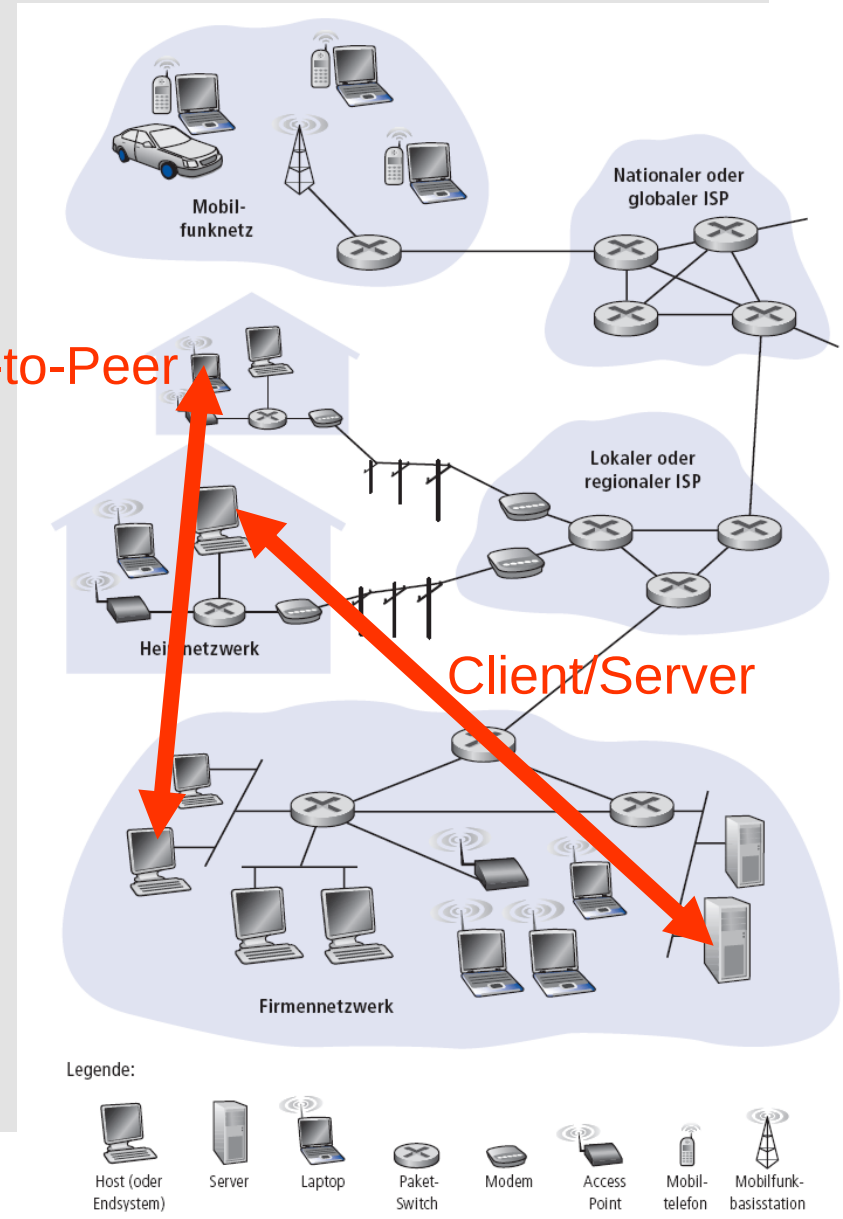
Frage: Andere Protokolle zwischen Menschen?

Der Randbereich des Netzwerkes:

- Endsysteme (Hosts):
  - Für Anwendungsprogramme
  - z.B. für Web, E-Mail
  - Am Rand des Netzwerkes

❑ Client/Server-Architektur
- ❖ Client fragt Dienste von einem Server an
- ❖ z.B. Webbrowser/Server; E-Mail-Client/Server

❑ Peer-to-Peer-Architektur:
- ❖ Minimaler oder gar kein Einsatz von dedizierten Servern
- ❖ z.B. Skype, BitTorrent



Kennen wir die zukünftigen Nutzer_innen ?

Generation Z –

Die Geburtenjahrgänge nach 1996 geben z.B. an, dass sie nie ein Sekretariat oder Büro ohne Internetanschluss gesehen haben.

HOCHSCHULE
HAMM-LIPPSTADT

SAMSTAG | 27. OKTOBER 2012 | 20.00 UHR

FILM-KONZERT im Gemeindezentrum Waldkirch, Kirchplatz

Die ganze Karriere der Beatles im Querschnitt, von 1962 bis 1970, inklusive vieler Songs aus der Zeit in der die Beatles viel im Studio experimentierten und die sie selbst nie live gespielt haben:

Nr. 1 Hits, B-Seiten, Kracher, schöne Melodien, Harmoniegesang und vor allem das Eine, das den Beatles immer am wichtigsten war: Rock'n'Roll.

Außerdem noch einiges drumherum, was die 60er-Jahre sonst noch ausmachte.
Auch musikalisch.

Die No Plastic Band gibt es seit 1990 in fast unveränderter Besetzung.

EINLASS 19.30 Uhr
EINTRITT 10 + 1€*

* je 1 € des Eintritts geht an den Verein "Hoffnung für Kinder im Elztal und den Seitent."

DIETER ECK Gitarre,Leadgesang KLAUS DIETER KIENZLER Bass, Gesang RALF PASKE Gitarre, Gesang
TOM SCHWÖRER Keyboards VOLKER ECK Schlagzeug, Leadgesang

Die Digitalisierung prägt die Gesellschaft und auch das Sozial- und Gesundheitswesen:

Was sind die Gründe für diesen umfassenden Wandel ?

Welche Chancen und Herausforderungen ergeben sich für die Akteure?

Digitale Transformation –

das Beobachtungsproblem

Warum werden Innovationen in den nächsten 2 Jahren überschätzt

und in den nächsten 10 Jahren unterschätzt ?

Was hat das mit dem Sozial- und dem Gesundheitswesen zu tun?

Digitale Transformation – ein Interaktionsmodell

das Beobachtungsproblem – einfaches Beispiel

Digitale Transformation – ein Interaktionsmodell

das Beobachtungsproblem

Beispiel:

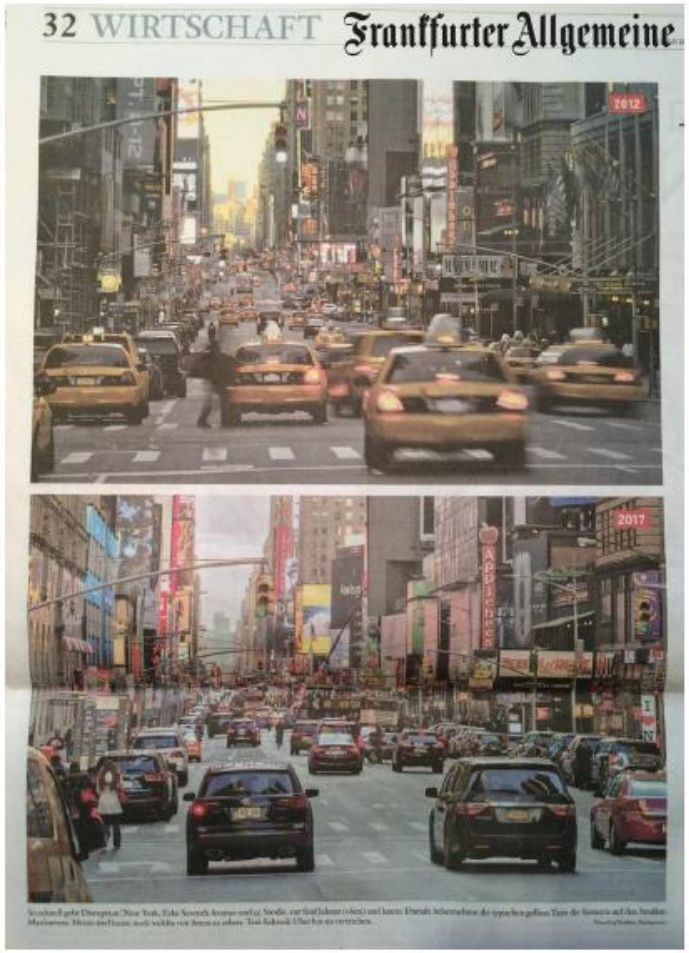
Hat sich das Smartphone die letzten 5 Jahre grundlegend verändert ?

iPhone 5 aus dem Jahr 2012

iPhone X aus dem Jahr 2017

Digitale Transformation – ein Interaktionsmodell

das Beobachtungsproblem – schwieriges Beispiel



New York, 7th Ave

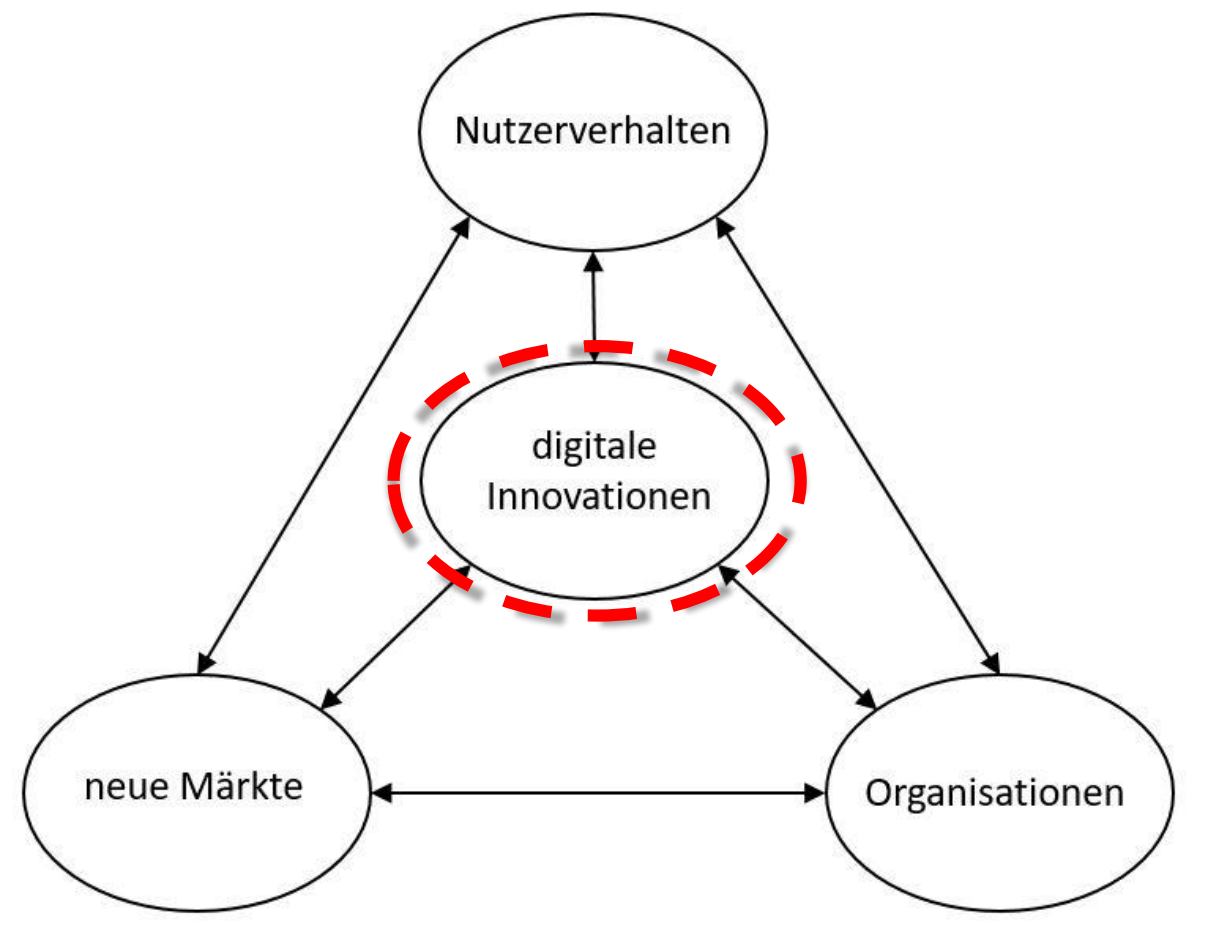
2012

...und

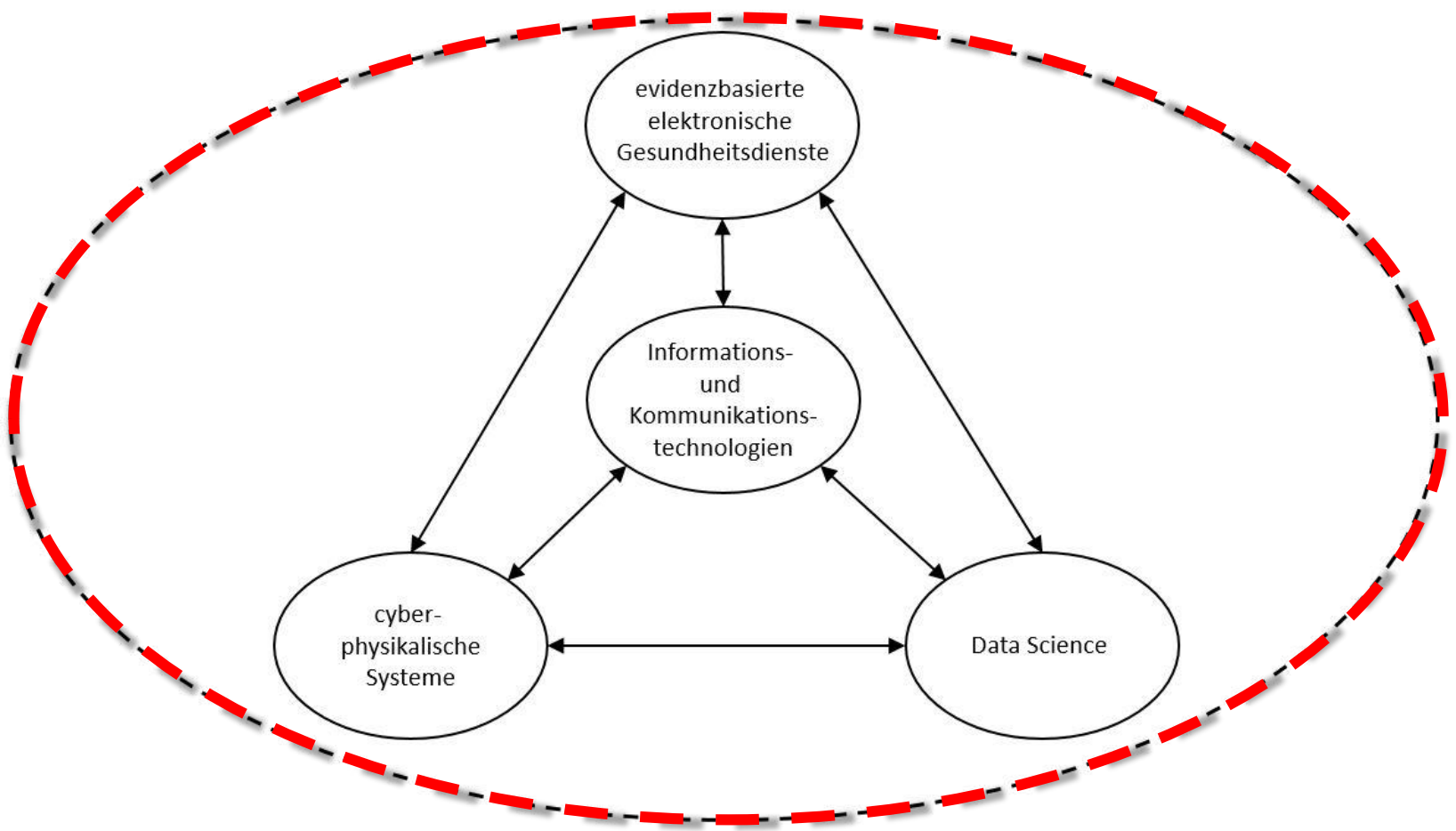
2017

FAZ Sonntagszeitung, 5.2.2017, S.32

Digitale Transformation – ein Interaktionsmodell



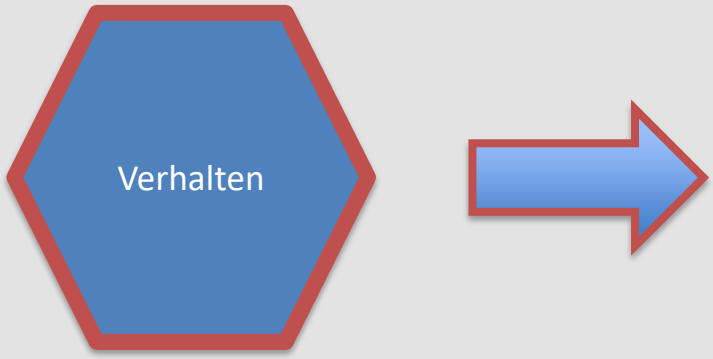
Digitale Innovation – ein Interaktionsmodell



Interpretation von Hypothesen:

Mithilfe des Interaktionsmodells lassen sich Hypothesen interpretieren.

Beispiel:



Hypothese:

Das Verhältnis zwischen Patient_innen und Ärzt_innen ändert sich!

Das Verhältnis zwischen Adressat_innen und Sozialarbeiter_innen aber auch!

Quelle:
hautnah dermatologie
July 2016, Volume 32, Issue 4, pp 58–58 |
Umfrage unter Niedergelassenen
Dr. Google setzt Ärzte unter Druck

OPEN Access PDF-Dokument:
https://content-select.com/de/portal/media/download_oa/9783779952589

Digitalisierung in der Sozialen Arbeit

Beispiele:

- Digitale Alltagskommunikation zwischen Fachkräften und Adressat_innen
- Onlineberatung
- Videoberatung
- Falladministration
- Softwarebasierte Falldiagnostik u.v.m.

Technikskepsis und Technikeuphorie

Technikdistanz und Technikaffinität

Datenschutz im Sozial- und Gesundheitswesen

Die Verarbeitung **besonderer Kategorien personenbezogener Daten** (§ 22 BDSG) sind durch öffentliche und nichtöffentliche Stellen zulässig, wenn sie zum Zweck der Gesundheitsvorsorge, für die Beurteilung der Arbeitsfähigkeit des Beschäftigten, für die medizinische Diagnostik, **die Versorgung oder Behandlung im Gesundheits- oder Sozialbereich oder für die Verwaltung von Systemen und Diensten im Gesundheits- und Sozialbereich** oder aufgrund eines Vertrags der betroffenen Person mit einem Angehörigen eines Gesundheitsberufs erforderlich ist und diese Daten von ärztlichem Personal oder durch sonstige Personen, die einer entsprechenden Geheimhaltungspflicht unterliegen, oder unter deren Verantwortung verarbeitet werden.

https://www.caritas.de/hilfeundberatung/onlineberatung/onlineberatung abgerufen am 22.11.2020

- Was bedeutet anonym und sicher in der Sozialen Arbeit?
- Welche Standards liegen Onlineberatungsangeboten der Sozialen Arbeit zu Grunde?
- Wie kann „vertrauensvolle Kommunikation ohne offene Hintertür“ online sichergestellt werden?
- Wer ist verantwortlich?
- Wer prüft die Angebote?

Institut für IT-Sicherheit
im Sozial- und
Gesundheitswesen

KatHO NRW
Aachen | Köln | Münster | Paderborn
Katholische Hochschule Nordrhein-Westfalen
Catholic University of Applied Sciences

HOCHSCHULE
HAMM-LIPPSTADT

Berliner Beauftragte
für Datenschutz
und Informationsfreiheit

Datenschutzanforderungen an Online-Beratungsangebote[1]

Beratungsangebote, teilweise auch in sensiblen Bereichen, werden vielfach und verstärkt derzeit vor dem Hintergrund der Coronavirus-Pandemie nicht mehr nur vor Ort oder per Telefon, sondern zusätzlich auch online durch rein textliche Kommunikation angeboten. Ziel ist es, ein möglichst niederschwelliges Angebot zu ermöglichen. Das Angebot holt die Beratungssuchenden idealerweise in denjenigen digitalen Medien ab, in denen sie sich regelmäßig bewegen. Die Hemmschwellen für eine persönliche Kontaktaufnahme sollen auf diese Weise verringert werden.

Da die Beratung normalerweise vertraulich erfolgen soll, sind aus datenschutzrechtlicher Sicht die folgenden Aspekte unbedingt zu beachten:

1. Die mit dem Angebot einhergehende Datenverarbeitung muss den Beratungssuchenden transparent und nachvollziehbar dargestellt werden. Hierzu gehört, dass deutlich wird, für welche Zwecke und durch wen Daten (Inhaltsdaten wie z. B. Fragen und Antworten, IP-Adressen und Metadaten wie Zeitpunkte, Cookies, Nutzernamen etc.) verarbeitet werden und wie lange welche Daten gespeichert bleiben. Die Anbieter entsprechender Angebote sind verpflichtet, ihren Informationspflichten nach Art. 12 ff. DS-GVO nachzukommen.

2. Die Beratung darf keinesfalls innerhalb von Online-Angeboten erfolgen, deren Geschäftsmodell auch die Auswertung personenbezogener Daten der Nutzenden ist. Beispiele hierfür sind die werbefinanzierten Kommunikationsdienste von Facebook oder Google.

https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/orientierungshilfen/2020-BlnBDI-Online-Beratungsdienste.pdf abgerufen am 22.11.2020

Datenschutzanforderungen an Online-Beratungsangebote[1]

3. Um eine anonyme oder pseudonyme Beratung zu ermöglichen, darf diese nicht über Plattformen oder Dienste erfolgen, die eine Anmeldung mit identifizierenden Daten verlangen.

4. Beratungen per Messenger-Dienst, SMS oder auch E-Mail sind daher i. d. R. nicht möglich. Ausnahmen könnten ggf. Messenger-Dienste bieten, die unabhängig von Identitätsdaten wie Telefonnummer oder E-Mail arbeiten. Informationen dazu finden sich im Beitrag zum datenschutzgerechten Einsatz von Messenger-Diensten im aktuellen Jahresbericht der Berliner Beauftragten für Datenschutz und Informationsfreiheit[2].

5. Einer Beratung per E-Mail steht zudem entgegen, dass nicht einmal die Grundanforderung an die vertrauliche Übermittlung personenbezogener Daten sichergestellt werden kann, wenn die Übertragung ohne Ende-zu-Ende-Verschlüsselung erfolgt.

6. Wird eine anonyme Beratung versprochen, dürfen nur die für den Betrieb des Beratungsangebotes technisch unbedingt erforderlichen identifizierenden Daten erhoben und für den kürzest notwendigen Zeitraum gespeichert werden. Sowohl für die Inhaltsdaten als auch für die Nutzungsdaten ist ein Löschkonzept zu entwickeln und die Notwendigkeit der darin festgelegten Speicherdauer zu begründen.

7. Die Verarbeitung von IP-Adressen ist nur innerhalb der jeweiligen Sitzung des Nutzenden technisch notwendig. Eine vorsorgliche Speicherung von personenbezogenen Daten wie beispielsweise der IP-Adresse lässt die Anonymität des Beratungsangebotes entfallen. Eine vorsorgliche Speicherung mit dem Ziel, die verbindlich zugesagte Anonymität in bestimmten Fällen, z. B. für Zwecke der Gefahrenabwehr, zu brechen, ist nicht zulässig.

https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/orientierungshilfen/2020-BlnBDI-Online-Beratungsdienste.pdf abgerufen am 22.11.2020

Datenschutzanforderungen an Online-Beratungsangebote[1]

8. Der Einsatz von Dritt-Inhalten, insbesondere externen Tracking- und Analysefunktionen sowie die Einbindung von Social-Plug-Ins, d. h. Funktionen, über die die Inhalte des Angebots mit sozialen Netzwerken geteilt werden können, sind auf Webseiten von Beratungsangeboten nicht zulässig. Ansonsten würden bereits bei Aufruf der Webseite unzulässig personenbezogene Daten an Dritte übermittelt oder von diesen erhoben werden.

9. Online-Beratungsangebote müssen so gestaltet werden, dass ein hohes Niveau an IT-Sicherheit erreicht wird. Trotz eines vornehmlich anonymen Beratungsangebots ist eine zumindest temporäre Verarbeitung identifizierender Daten, wie z. B. IP-Adressen, identifizierende Angaben in den Nachrichten der Beratungssuchenden, bei manchen Plattformen auch freiwillig angegebene E-Mail-Adressen, nicht völlig vermeidbar. Da bei der Erbringung von Beratungsangeboten häufig auch besonders sensitive Daten im Sinne des Art. 9 Abs. 1 der Datenschutz-Grundverordnung (DS-GVO) wie beispielsweise Gesundheitsdaten, Daten zum Sexualleben oder auch über die ethnische Herkunft verarbeitet werden, sind IT-Sicherheitsmaßnahmen zu treffen, die bezüglich des Schutzziels der Vertraulichkeit möglichst das Schutzniveau „hoch“ entsprechend BSI-IT-Grundschutz erreichen.

https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/orientierungshilfen/2020-BlnBDI-Online-Beratungsdienste.pdf abgerufen am 22.11.2020

SERVICE FÜR DIE PRAXIS

ABRECHNUNG
VERORDNUNGEN
FORMULARE
AMBULANTE LEISTUNGEN
PRAXISFÜHRUNG
PRAXIS-IT

- Praxisverwaltungssysteme
- Sicheres Netz
- Telematikinfrastruktur
- eDMP
- eDoku
- Telekonsilium
- Videosprechstunde
- IT-Sicherheitsrichtlinie

Stand 18.09.2020

VIDEOSPRECHSTUNDE

Videosprechstunde: telemedizinisch gestützte Betreuung von Patienten

Gerade bei langen Anfahrtswegen oder nach Operationen können telemedizinische Leistungen eine sinnvolle Hilfe sein, so wie die Videosprechstunde. Ärzte und Psychotherapeuten können ihren Patientinnen und Patienten dabei die weitere Behandlung am Bildschirm erläutern, den Heilungsprozess einer Operationswunde begutachten oder ein psychotherpeutisches Gespräch führen. So müssen Patientinnen und Patienten nicht für jeden Termin in die Praxis kommen.

Dabei ist die Organisation denkbar einfach: Der Arzt oder Psychotherapeut wählt einen zertifizierten Videodienstanbieter aus, der für einen reibungslosen und sicheren technischen Ablauf der Videosprechstunde sorgt. Praxis und Patient benötigen im Wesentlichen einen Bildschirm mit Kamera, Mikrofon und Lautsprecher sowie eine Internetverbindung. Eine zusätzliche Software ist nicht erforderlich.

FÜR PRAXEN

VIDEOSPRECHSTUNDE ANZEIGEN

Wenn Sie als Arzt oder Psychotherapeut einen zertifizierten Videodienst nutzen, müssen Sie dies zunächst bei Ihrer Kassenärztlichen Vereinigung anzeigen. Das Verfahren ist regional unterschiedlich. Weitere Informationen finden sich im folgenden Dokument.

KV-Verfahren Videosprechstunde (PDF, 101 KB)

FÜR ANBIETER

Regelungen zur Videosprechstunde in der Psychotherapie

Technische Anforderungen

Die technischen Anforderungen für die Praxis und den Videodienst – insbesondere zur technischen Sicherheit und zum Datenschutz – sind in der Anlage 31b zum Bundesmantelvertrag-Ärzte geregelt.

Anforderungen an Praxen

Anforderungen an Videodienstanbieter

Zertifizierte Videodienstanbieter

Übersicht zur Vergütung

Grund-, Versicherten- und Konsiliarpauschale

Zusätzlich abrechenbare Leistungen

Anschubfinanzierung: 10 Euro pro Videosprechstunde

Zuschlag für Authentifizierung neuer Patienten

Technik- und Förderzuschlag

FÜR ANBIETER

VIDEODIENST MELDEN

Sie bieten einen Dienst zur Durchführung von Videosprechstunden an und verfügen über die notwendigen Zertifikate? Wir veröffentlichen den Namen Ihres Produktes auf unserer Internetseite. Dazu senden Sie bitte eine ausgefüllte Selbstauskunft an:

KBV
Dezernat VuG, Abteilung EBM
Postfach 12 02 64
10592 Berlin

Hinweis: Bis zum 30.9.20 können Sie Ihren Videodienst übergangsweise noch mit dem alten Selbstauskunftsformular nach den vormals geltenden Anforderungen anzeigen.

Formular zur Selbstauskunft für Anbieter von Videosprechstunden (PDF, 199 KB)

Quelle: https://www.kbv.de/html/videosprechstunde.php abgerufen am 22.11.2020

Die Kassenärztliche Bundesvereinigung, K.d.ö.R., Berlin,

– einerseits –

und

der GKV-Spitzenverband (Spitzenverband Bund der Krankenkassen), K.d.ö.R., Berlin,

und

– andererseits –

schließen als Anlage 31b zum Bundesmantelvertrag-Ärzte (BMV-Ä) die nachstehende

Vereinbarung über die Anforderungen an die technischen Verfahren zur Videosprechstunde gemäß § 291g Absatz 4 SGB V

vom 21. Oktober 2016 in der Fassung vom 27. Juli 2020*

https://www.kbv.de/media/sp/Anlage_31b_Videosprechstunde.pdf abgerufen am 22.11.2020

(Anlage 31b BMV-Ä)

Inhaltsverzeichnis

§ 2 Bestimmungen zum Datenschutz

(1) Der Videodienstanbieter und der Vertragsarzt haben für die Verarbeitung personenbezogener Patientendaten die rechtlichen Rahmenbedingungen zu beachten, die sich insbesondere aus den Vorschriften der Datenschutzgrundverordnung (DS-GVO), des Bundesdatenschutzgesetzes (BDSG) sowie des Fünften Sozialgesetzbuchs (SGB V) und – soweit anwendbar – des Zehnten Sozialgesetzbuchs (SGB X) ergeben. Bei der konkreten Umsetzung kann sich der Vertragsarzt an den „Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis“ der Bundesärztekammer und der Kassenärztlichen Bundesvereinigung orientieren.

(2) Im Hinblick auf die Sicherheit der Verarbeitung der Daten hat der Vertragsarzt in seinen Räumlichkeiten und IT-Systemen zu gewährleisten, dass die erforderlichen technischen und organisatorischen Maßnahmen eingehalten werden.

(3) Der Videodienstanbieter ist verantwortlich für die Daten, die bei der Verwendung seines Dienstes verarbeitet werden.

(4) Die Übertragung der Videosprechstunde soll über eine Peer-to-Peer-Verbindung zwischen Vertragsarzt und Patienten oder der Pflegekraft, ohne Nutzung eines zentralen Servers, erfolgen. Bei einem Abweichen von einem Peer-to-Peer-Verfahren ist der Videodienstanbieter verpflichtet, durch geeignete technische und organisatorische Maßnahmen ein angemessenes Schutzniveau zu gewährleisten.

(5) Der Videodienstanbieter muss gewährleisten, dass sämtliche Inhalte der Videosprechstunde während des gesamten Übertragungsprozesses nach dem Stand der

https://www.kbv.de/media/sp/Anlage_31b_Videosprechstunde.pdf abgerufen am 22.11.2020

§ 2 Bestimmungen zum Datenschutz

(Anlage 31b BMV-Ä)

Technik Ende-zu-Ende verschlüsselt sind. Der Stand der Technik ergibt sich insbesondere aus der Technischen Richtlinie 02102 des Bundesamtes für Sicherheit in der Informationstechnik in der jeweils aktuell gültigen Fassung.

(6) Sämtliche Inhalte der Videosprechstunde dürfen durch den Videodienstanbieter weder eingesehen noch gespeichert werden können. Die Metadaten/technischen Verbindungsdaten müssen nach spätestens drei Monaten gelöscht werden und dürfen nur für die zur Abwicklung der Videosprechstunde notwendigen Abläufe genutzt werden. Die Weitergabe der Daten ist untersagt.

(7) Die Verarbeitung von Daten auch im Auftrag darf nur im Inland, in einem Mitgliedsstaat der Europäischen Union oder in einem diesem nach § 35 Absatz 7 des Ersten Buches Sozialgesetzbuch gleichgestellten Staat, oder, sofern ein Angemessenheitsbeschluss gemäß Artikel 45 der Verordnung (EU) 2016/679 vorliegt, in einem Drittstaat erfolgen.

https://www.kbv.de/media/sp/Anlage_31b_Videosprechstunde.pdf abgerufen am 22.11.2020

Anforderungen an Praxen

- Die Patientin oder der Patient muss für die Videosprechstunde eine Einwilligung abgeben.
- Die Videosprechstunde muss in Räumen stattfinden, die Privatsphäre bieten. Außerdem müssen die eingesetzte Technik und die elektronische Datenübertragung eine angemessene Kommunikation gewährleisten.
- Die Videosprechstunde muss vertraulich und störungsfrei verlaufen – wie eine normale Sprechstunde auch. So darf die Videosprechstunde beispielsweise von niemandem aufgezeichnet werden, auch nicht von der Patientin oder dem Patient.
- Der Klarname der Patientin oder des Patienten muss für die Praxis erkennbar sein.
- Die Videosprechstunde muss frei von Werbung sein.

Quelle: https://www.kbv.de/html/videosprechstunde.php abgerufen am 22.11.2020

(Anlage 31b BMV-Ä)

Anlage 1: Technische Anforderungen an die apparative Ausstattung der Arztpraxis

Die Vereinbarungspartner sind sich einig, dass zur Durchführung der Videosprechstunde mindestens folgende Voraussetzungen gegeben sein müssen:

- Kamera
- Bildschirm (Monitor, Display etc.):
  - Bildschirmdiagonale: mindestens 3 Zoll
  - Auflösung: mindestens: 640x480 px
- Bandbreite: Mindestens 2000 kbit/s im Download
- Mikrofon
- Tonwiedergabeeinheit

https://www.kbv.de/media/sp/Anlage_31b_Videosprechstunde.pdf abgerufen am 22.11.2020

Anforderungen an Videodienstanbieter

- Der Videodienstanbieter muss zertifiziert sein und dazu eine Selbstauskunft bei der KBV sowie beim GKV-Spitzenverband eingereicht haben. Die Praxis erhält vom gewählten Anbieter nach Vertragsschluss eine Bescheinigung, dass der Videodienst gemäß Anlage 31b zur IT-Sicherheit und zum Datenschutz zertifiziert ist sowie die Anforderungen zu den Inhalten erfüllt.
- Der Videodienstanbieter muss zudem gewährleisten, dass die Videosprechstunde während der gesamten Übertragung Ende-zu-Ende verschlüsselt ist.

Wichtig zu wissen: Ärzte oder Psychotherapeuten können Leistungen im Rahmen der Videosprechstunde erst dann abrechnen, wenn sie ihrer Kassenärztlichen Vereinigung zuvor angezeigt haben, einen zertifizierten (Anlage 31b zum BMV-Ä) Videodienstanbieter zu nutzen. In einigen KV-Regionen ist diese Regelung zurzeit ausgesetzt. Praxen sollten sich dazu bei ihrer zuständigen Kassenärztlichen Vereinigung informieren.

Quelle: https://www.kbv.de/html/videosprechstunde.php abgerufen am 22.11.2020

Zertifizierte Videodienstanbieter

Hinweis: Die KBV und der GKV-SV führen selbst keine Zertifizierungen von Anbietern von Videodiensten und deren Diensten durch. Die Erfüllung der Anforderungen an Videodienstanbieter und deren Dienste gemäß Anlage 31b zum BMV-Ä wird von unabhängigen zertifizierenden Stellen im Rahmen der beizubringenden Nachweise geprüft. Ein in die Liste der zertifizierten Videodienstanbieter aufgenommener Dienst ist somit nicht „KBV-zertifiziert" sondern ein von zertifizierenden Stellen zertifizierter Dienst gemäß den Regelungen von GKV-Spitzenverband und KBV.

Zertifizierte Videodienstanbieter (Stand: 19.10.2020, PDF, 103 KB)

Quelle: https://www.kbv.de/html/videosprechstunde.php abgerufen am 22.11.2020

Meilenstein: das Digitale-Versorgung-Gesetz vom 2019

Datenschutz und Telemedizin

Allgemeine datenschutzrechtliche Anforderungen

Für die Verarbeitung personenbezogener Patientendaten im Rahmen telemedizinischer Anwendungen gelten grundsätzlich die allgemeinen rechtlichen Rahmenbedingungen, die für die Verarbeitung personenbezogener Patientendaten außerhalb telemedizinischer Anwendungen gelten.

Die Einführung telemedizinischer Anwendungen darf nicht zu einer rechtlichen oder faktischen Verschlechterung der Patientenrechte führen.

Die Durchsetzung bzw. Konkretisierung der Patientenrechte unter den veränderten technischen Bedingungen bedarf teilweise neuer datenschutzrechtlicher Konzepte.

Quelle: Marion Bultmann Der Landesbeauftragte für den Datenschutz und das Recht auf Akteneinsicht Brandenburg , Dr. Rita Wellbrock Der Hessische Datenschutzbeauftragte,
Heinz Biermann Der Bundesbeauftragte für den Datenschutz, Jürgen Engels Die Landesbeauftragte für den Datenschutz Nordrhein-Westfalen, Walter Ernestus Der Bundesbeauftragte für den Datenschutz,
Udo Höhn Der Bayerische Landesbeauftragte für den Datenschutz , Rüdiger Wehrmann Der Hessische Datenschutzbeauftragte, Andreas Schurig Der Sächsische Datenschutzbeauftragte

Datenschutz und Telemedizin

Rechtsgrundlagen

Für die Verarbeitung von Patientendaten durch niedergelassene Ärzte gelten die Vorschriften des **BDSG**. Für die Verarbeitung von **Patientendaten durch die Krankenhäuser gelten in Bund und Ländern unterschiedliche Rechtsvorschriften**. In einzelnen Ländern liegen sog. bereichsspezifische Regelungen der Verarbeitung personenbezogener Daten in Krankenhäusern (**Landeskrankenhausgesetze, Gesundheitsdatenschutzgesetze**) vor.

Soweit keine bereichsspezifischen Regelungen vorhanden sind, gelten die allgemeinen datenschutzrechtlichen Vorschriften. Die Religionsgesellschaften treffen für ihren Bereich zum Teil Regelungen in eigener Zuständigkeit. **Darüber hinaus sind die Regelungen der Berufsordnung und des Strafgesetzbuchs zu beachten**.

Quelle: Marion Bultmann Der Landesbeauftragte für den Datenschutz und das Recht auf Akteneinsicht Brandenburg , Dr. Rita Wellbrock Der Hessische Datenschutzbeauftragte, Heinz Biermann Der Bundesbeauftragte für den Datenschutz, Jürgen Engels Die Landesbeauftragte für den Datenschutz Nordrhein-Westfalen, Walter Ernestus Der Bundesbeauftragte für den Datenschutz, Udo Höhn Der Bayerische Landesbeauftragte für den Datenschutz , Rüdiger Wehrmann Der Hessische Datenschutzbeauftragte, Andreas Schurig Der Sächsische Datenschutzbeauftragte

Datenschutz und Telemedizin

Rechtsgrundlagen

Auf der Grundlage des Behandlungsvertrages in Verbindung mit den jeweils maßgeblichen datenschutzrechtlichen Vorschriften **darf der Arzt die für die Durchführung der Behandlung erforderlichen Daten verarbeiten**. Soweit die Verarbeitung der Daten **nicht für die Durchführung der Behandlung erforderlich ist** (z.B. zusätzliche Datenerhebungen für ein Forschungsvorhaben), **bedarf es einer besonderen Einwilligung des Patienten**.

Quelle: Marion Bultmann Der Landesbeauftragte für den Datenschutz und das Recht auf Akteneinsicht Brandenburg , Dr. Rita Wellbrock Der Hessische Datenschutzbeauftragte, Heinz Biermann Der Bundesbeauftragte für den Datenschutz, Jürgen Engels Die Landesbeauftragte für den Datenschutz Nordrhein-Westfalen, Walter Ernestus Der Bundesbeauftragte für den Datenschutz, Udo Höhn Der Bayerische Landesbeauftragte für den Datenschutz , Rüdiger Wehrmann Der Hessische Datenschutzbeauftragte, Andreas Schurig Der Sächsische Datenschutzbeauftragte

Datenschutz und Telemedizin

Rechtsgrundlagen

Unabhängig vom verwendeten Datenträger muss der Arzt parallel zu den datenschutzrechtlichen Vorschriften die in der Berufsordnung und in **§ 203 StGB normierte Schweigepflicht** beachten, ferner das in **§ 5 BDSG** und den entsprechenden landesrechtlichen Bestimmungen geregelte **Datengeheimnis**.

Gehilfen des Arztes unterliegen ebenfalls der ärztlichen Schweigepflicht.

Quelle: Marion Bultmann Der Landesbeauftragte für den Datenschutz und das Recht auf Akteneinsicht Brandenburg , Dr. Rita Wellbrock Der Hessische Datenschutzbeauftragte,
Heinz Biermann Der Bundesbeauftragte für den Datenschutz, Jürgen Engels Die Landesbeauftragte für den Datenschutz Nordrhein-Westfalen, Walter Ernestus Der Bundesbeauftragte für den Datenschutz,
Udo Höhn Der Bayerische Landesbeauftragte für den Datenschutz , Rüdiger Wehrmann Der Hessische Datenschutzbeauftragte, Andreas Schurig Der Sächsische Datenschutzbeauftragte

Datenschutz und Telemedizin

Dokumentationspflicht

Nach der Berufsordnung ist der Arzt verpflichtet, die erforderlichen Aufzeichnungen über die in Ausübung seines Berufs gemachten Feststellungen und getroffenen Maßnahmen anzufertigen. Es handelt sich um eine unselbständige vertragliche Nebenpflicht aus dem Behandlungsvertrag. **Ist die Dokumentation lückenhaft, kann dies im Haftungsprozess eine Umkehr der Beweislast zugunsten des Patienten nach sich ziehen**, wenn die Aufklärung des Sachverhalts für den Patienten insgesamt erschwert wird.

Quelle: Marion Bultmann Der Landesbeauftragte für den Datenschutz und das Recht auf Akteneinsicht Brandenburg , Dr. Rita Wellbrock Der Hessische Datenschutzbeauftragte, Heinz Biermann Der Bundesbeauftragte für den Datenschutz, Jürgen Engels Die Landesbeauftragte für den Datenschutz Nordrhein-Westfalen, Walter Ernestus Der Bundesbeauftragte für den Datenschutz, Udo Höhn Der Bayerische Landesbeauftragte für den Datenschutz , Rüdiger Wehrmann Der Hessische Datenschutzbeauftragte, Andreas Schurig Der Sächsische Datenschutzbeauftragte

Datenschutz und Telemedizin

Befugnis zur Übermittlung bzw. Weitergabe von Patientendaten

Der Arzt darf personenbezogene Patientendaten nur im Rahmen der datenschutzrechtlichen Vorschriften und befugt i.S.v. § 203 StGB offenbaren.

Eine Befugnis zur Offenbarung kann sich insbesondere aus einer gesetzlichen Regelung (z.B. Krebsregistergesetze, Infektionsschutzgesetz, Sozialgesetzbuch V), aus dem Behandlungs-vertrag oder der speziellen Einwilligung des Patienten ergeben.
Die ärztliche Schweigepflicht gilt grundsätzlich auch zwischen Ärzten.

Eine Übermittlung personenbezogener Daten an einen vor-,mit- oder nach behandelnden Arzt bedarf daher der Einwilligung des Patienten.

Quelle: Marion Bultmann Der Landesbeauftragte für den Datenschutz und das Recht auf Akteneinsicht Brandenburg , Dr. Rita Wellbrock Der Hessische Datenschutzbeauftragte,
Heinz Biermann Der Bundesbeauftragte für den Datenschutz, Jürgen Engels Die Landesbeauftragte für den Datenschutz Nordrhein-Westfalen, Walter Ernestus Der Bundesbeauftragte für den Datenschutz,
Udo Höhn Der Bayerische Landesbeauftragte für den Datenschutz , Rüdiger Wehrmann Der Hessische Datenschutzbeauftragte, Andreas Schurig Der Sächsische Datenschutzbeauftragte

Datenschutz und Telemedizin

In § 140a ff. SGB V sind Regelungen zur sog. integrierten Versorgung enthalten.

Die Teilnahmeder Versicherten an den integrierten Versorgungsformen ist freiwillig. **Die Vertragspartner müssen u.a. die Gewähr dafür übernehmen**, dass sie eine an dem Versorgungsbedarf orientierte Zusammenarbeit zwischen allen an der Versorgung Beteiligten sicherstellen, einschließlich der Koordination zwischen den verschiedenen Versorgungsbereichen und einer ausreichenden Dokumentation, die allen an der integrierten Versorgung Beteiligten im jeweils erforderlichen Umfang zugänglich sein muss.

Quelle: Marion Bultmann Der Landesbeauftragte für den Datenschutz und das Recht auf Akteneinsicht Brandenburg , Dr. Rita Wellbrock Der Hessische Datenschutzbeauftragte, Heinz Biermann Der Bundesbeauftragte für den Datenschutz, Jürgen Engels Die Landesbeauftragte für den Datenschutz Nordrhein-Westfalen, Walter Ernestus Der Bundesbeauftragte für den Datenschutz, Udo Höhn Der Bayerische Landesbeauftragte für den Datenschutz , Rüdiger Wehrmann Der Hessische Datenschutzbeauftragte, Andreas Schurig Der Sächsische Datenschutzbeauftragte

Datenschutz und Telemedizin

Der Leistungserbringer darf aus der gemeinsamen Dokumentation die den Versicherten betreffenden Behandlungsdaten und Befunde **nur dann abrufen, wenn der Versicherte ihm gegenüber seine Einwilligung erteilt hat,** die Information für den konkret anstehenden Behandlungsfall genutzt werden soll und der Leistungserbringer zu dem Personenkreis gehört, der nach § 203 StGB zur Geheimhaltung verpflichtet ist.

Quelle: Marion Bultmann Der Landesbeauftragte für den Datenschutz und das Recht auf Akteneinsicht Brandenburg , Dr. Rita Wellbrock Der Hessische Datenschutzbeauftragte, Heinz Biermann Der Bundesbeauftragte für den Datenschutz, Jürgen Engels Die Landesbeauftragte für den Datenschutz Nordrhein-Westfalen, Walter Ernestus Der Bundesbeauftragte für den Datenschutz, Udo Höhn Der Bayerische Landesbeauftragte für den Datenschutz , Rüdiger Wehrmann Der Hessische Datenschutzbeauftragte, Andreas Schurig Der Sächsische Datenschutzbeauftragte

Datenschutz und Telemedizin

Informationsrechte des Patienten

Nach der Rechtsprechung des BGH hat der Patient grundsätzlich ein Recht auf Einsicht in seine Krankenunterlagen, soweit sie sog. objektive Daten betreffen. Es handelt sich um einen Nebenanspruch aus dem Behandlungsvertrag. Für den Bereich der Psychiatrie hat die Rechtsprechung Ausnahmen formuliert. Die – gegenüber der Rechtsprechung vorrangigen - datenschutzrechtlichen Regelungen (Landeskrankenhausgesetze, Gesundheits-datenschutzgesetze, allgemeine datenschutzrechtliche Regelungen) legen zum Teil weitergehende Rechte der Patienten auf Information, Auskunft und Einsicht fest.

Quelle: Marion Bultmann Der Landesbeauftragte für den Datenschutz und das Recht auf Akteneinsicht Brandenburg , Dr. Rita Wellbrock Der Hessische Datenschutzbeauftragte,
Heinz Biermann Der Bundesbeauftragte für den Datenschutz, Jürgen Engels Die Landesbeauftragte für den Datenschutz Nordrhein-Westfalen, Walter Ernestus Der Bundesbeauftragte für den Datenschutz,
Udo Höhn Der Bayerische Landesbeauftragte für den Datenschutz , Rüdiger Wehrmann Der Hessische Datenschutzbeauftragte, Andreas Schurig Der Sächsische Datenschutzbeauftragte

Datenschutz und Telemedizin

Informationsrechte des Patienten

Im Bereich der Telemedizin ist es besonders wichtig, dass der Patient in allen Verarbeitungsphasen ausreichend informiert ist über die Verarbeitung seiner personenbezogenen Daten. Dies setzt voraus, dass das ihn informierende Personal ebenfalls ausreichend informiert ist. Es muss insbesondere auch gewährleistet sein, dass dem Patienten bei Vertragsabschluss bzw. Einwilligung Umfang, Zweck und Rechtsgrundlage der Verarbeitung seiner Daten sowie ggf. die Grundzüge des technischen Verfahrens der Verarbeitung bekannt gegeben worden sind.

Quelle: Marion Bultmann Der Landesbeauftragte für den Datenschutz und das Recht auf Akteneinsicht Brandenburg , Dr. Rita Wellbrock Der Hessische Datenschutzbeauftragte, Heinz Biermann Der Bundesbeauftragte für den Datenschutz, Jürgen Engels Die Landesbeauftragte für den Datenschutz Nordrhein-Westfalen, Walter Ernestus Der Bundesbeauftragte für den Datenschutz, Udo Höhn Der Bayerische Landesbeauftragte für den Datenschutz , Rüdiger Wehrmann Der Hessische Datenschutzbeauftragte, Andreas Schurig Der Sächsische Datenschutzbeauftragte

Datenschutz und Telemedizin

Abruf von Patientendaten über ein Datennetz

Patientendaten können nach Erteilung einer Einwilligung des Patienten im Einzelfall für einen Zugriff durch den Berechtigten freigegeben werden. **Ein Zum – Abruf - Bereitstellen (vgl. z.B. § 810 BDSG) von Patientendaten durch einen Arzt über ein Datennetz ist nach der gegenwärtigen Rechtslagegrundsätzlich nicht zulässig.**

Ein Arzt ist verpflichtet, vor einer Übermittlung zu prüfen, ob eine Befugnis zur Offenbarung der Daten an den Empfänger vorliegt.

Quelle: Marion Bultmann Der Landesbeauftragte für den Datenschutz und das Recht auf Akteneinsicht Brandenburg , Dr. Rita Wellbrock Der Hessische Datenschutzbeauftragte, Heinz Biermann Der Bundesbeauftragte für den Datenschutz, Jürgen Engels Die Landesbeauftragte für den Datenschutz Nordrhein-Westfalen, Walter Ernestus Der Bundesbeauftragte für den Datenschutz, Udo Höhn Der Bayerische Landesbeauftragte für den Datenschutz , Rüdiger Wehrmann Der Hessische Datenschutzbeauftragte, Andreas Schurig Der Sächsische Datenschutzbeauftragte

Datenschutz und Telemedizin

Abruf von Patientendaten über ein Datennetz

Würde ein Arzt die Patientendaten für einen Abruf durch andere Behandlungs-einrichtungen bereithalten und käme es dann zu einem Abruf, der rechtlich nicht (z. B. durch eine Einwilligung des Patienten) legitimiert ist, so hätte sich der speichernde Arzt nach § 203 StGB **strafbar gemacht**.

Eine Offenbarung von Patientendaten kann auch dadurch vorgenommen werden, dass nicht verhindert wird, dass die Daten durch externe Dritte abgerufen werden können.

Quelle: Marion Bultmann Der Landesbeauftragte für den Datenschutz und das Recht auf Akteneinsicht Brandenburg , Dr. Rita Wellbrock Der Hessische Datenschutzbeauftragte, Heinz Biermann Der Bundesbeauftragte für den Datenschutz, Jürgen Engels Die Landesbeauftragte für den Datenschutz Nordrhein-Westfalen, Walter Ernestus Der Bundesbeauftragte für den Datenschutz, Udo Höhn Der Bayerische Landesbeauftragte für den Datenschutz , Rüdiger Wehrmann Der Hessische Datenschutzbeauftragte, Andreas Schurig Der Sächsische Datenschutzbeauftragte

Datenschutz und Telemedizin

Grundlegende Sicherheitsanforderungen

1. Vertraulichkeit

Die in der ärztlichen Berufsordnung und dem Strafgesetzbuch normierte **ärztliche Schweigepflicht schützt das Vertrauensverhältnis zwischen Patient und Arzt**. Der Arzt muss die Vertraulichkeit der erhobenen, gespeicherten, übermittelten oder sonst verarbeiteten Daten gewährleisten, d.h. nur Befugte dürfen personenbezogene Daten zur Kenntnis erhalten bzw. davon Kenntnis nehmen können. Auch die datenschutzrechtlichen Regelungen, die das Recht des Patienten auf **informationelle Selbstbestimmung** konkretisieren, schützen die Vertrauensbeziehung zwischen Patient und Arzt. Eine Kenntnisnahme **medizinischer Daten durch Unbefugte** (z.B. Arbeitgeber, Versicherungen, Pharmaindustrie) **kann erhebliche soziale bzw. materielle Folgen für den Patienten nach sich ziehen.**

Quelle: Marion Bultmann Der Landesbeauftragte für den Datenschutz und das Recht auf Akteneinsicht Brandenburg , Dr. Rita Wellbrock Der Hessische Datenschutzbeauftragte, Heinz Biermann Der Bundesbeauftragte für den Datenschutz, Jürgen Engels Die Landesbeauftragte für den Datenschutz Nordrhein-Westfalen, Walter Ernestus Der Bundesbeauftragte für den Datenschutz, Udo Höhn Der Bayerische Landesbeauftragte für den Datenschutz , Rüdiger Wehrmann Der Hessische Datenschutzbeauftragte, Andreas Schurig Der Sächsische Datenschutzbeauftragte

Datenschutz und Telemedizin

Grundlegende Sicherheitsanforderungen

2. Authentizität (Zurechenbarkeit)

Die Authentizität der erhobenen, gespeicherten, übermittelten oder sonst verarbeiteten Daten muss gewährleistet sein, d.h. **der Urheber von patientenbezogenen bzw. der Verantwortliche für patientenbezogene Daten sowie der Auslöser eines Verarbeitungs-vorgangs bzw. der Verantwortliche für einen Verarbeitungsvorgang muss jederzeit eindeutig feststellbar sein**. Ggf. kann auch die Art und Weise der Erhebung der Daten von Bedeutung sein (z.B. Datenerhebung durch ein medizinisches Gerät).

Medizinische Dokumente, die ihren Urheber bzw. Verantwortlichen nicht erkennen lassen, sind als Grundlage für Behandlungen und Begutachtungen ungeeignet.

Quelle: Marion Bultmann Der Landesbeauftragte für den Datenschutz und das Recht auf Akteneinsicht Brandenburg , Dr. Rita Wellbrock Der Hessische Datenschutzbeauftragte,
Heinz Biermann Der Bundesbeauftragte für den Datenschutz, Jürgen Engels Die Landesbeauftragte für den Datenschutz Nordrhein-Westfalen, Walter Ernestus Der Bundesbeauftragte für den Datenschutz,
Udo Höhn Der Bayerische Landesbeauftragte für den Datenschutz , Rüdiger Wehrmann Der Hessische Datenschutzbeauftragte, Andreas Schurig Der Sächsische Datenschutzbeauftragte

Datenschutz und Telemedizin

Grundlegende Sicherheitsanforderungen

3. Integrität

Die Integrität der erhobenen, gespeicherten, übermittelten oder sonst verarbeiteten Daten muss gewährleistet sein, d.h. **personenbezogene Daten müssen während aller Phasen der Verarbeitung unversehrt, vollständig, gültig und widerspruchsfrei bleiben**. Der Behandlungsauftrag in Einrichtungen des Gesundheitswesens umfasst eine sorgfältige Diagnose und Therapie mit dem Ziel der Heilung des Patienten. **Die Echtheit, Korrektheit und Vollständigkeit der Daten, vor,während und nach der Bearbeitung und Übertragung ist für die Erfüllung des Behandlungsauftrags von großer Bedeutung**. Eine Verfälschung oder Unvollständigkeit der Daten kann zu falschen medizinischen Entscheidungen m it u.U. lebensbedrohenden Folgen für den Patienten führen, verbunden mit rechtlichen Konsequenzen für den Mediziner.

Quelle: Marion Bultmann Der Landesbeauftragte für den Datenschutz und das Recht auf Akteneinsicht Brandenburg , Dr. Rita Wellbrock Der Hessische Datenschutzbeauftragte, Heinz Biermann Der Bundesbeauftragte für den Datenschutz, Jürgen Engels Die Landesbeauftragte für den Datenschutz Nordrhein-Westfalen, Walter Ernestus Der Bundesbeauftragte für den Datenschutz, Udo Höhn Der Bayerische Landesbeauftragte für den Datenschutz , Rüdiger Wehrmann Der Hessische Datenschutzbeauftragte, Andreas Schurig Der Sächsische Datenschutzbeauftragte

Datenschutz und Telemedizin

Grundlegende Sicherheitsanforderungen

4. Verfügbarkeit

Die Verfügbarkeit der erhobenen,gespeicherten, übermittelten oder sonst verarbeiteten Daten muss gewährleistet sein, d.h. personenbezogene Daten müssen zeitgerecht zur Verfügung stehen und ordnungsgemäß verarbeitet werden können. **Die zeitgerechte Verfügbarkeit medizinischer Informationen kann entscheidend sein für eine erfolgreiche Erfüllung des Behandlungsauftrags.**

Quelle: Marion Bultmann Der Landesbeauftragte für den Datenschutz und das Recht auf Akteneinsicht Brandenburg , Dr. Rita Wellbrock Der Hessische Datenschutzbeauftragte, Heinz Biermann Der Bundesbeauftragte für den Datenschutz, Jürgen Engels Die Landesbeauftragte für den Datenschutz Nordrhein-Westfalen, Walter Ernestus Der Bundesbeauftragte für den Datenschutz, Udo Höhn Der Bayerische Landesbeauftragte für den Datenschutz , Rüdiger Wehrmann Der Hessische Datenschutzbeauftragte, Andreas Schurig Der Sächsische Datenschutzbeauftragte

Datenschutz und Telemedizin

Grundlegende Sicherheitsanforderungen

4. Verfügbarkeit

Nicht oder nicht rechtzeitig zur Verfügung stehende Daten können zur Handlungs-unfähigkeit bzw. zu einem zu späten Handeln oder Behandlungsfehlern des Mediziners führen und u.U. lebensbedrohende Folgen für den Patienten sowie rechtliche Konsequenzen für den Mediziner haben. Die Verfügbarkeit der Daten impliziert natürlich die Verfügbarkeit der zur ordnungsgemäßen Verarbeitung erforderlichen Komponenten (Hard- und Software) des IT -Systems.

Quelle: Marion Bultmann Der Landesbeauftragte für den Datenschutz und das Recht auf Akteneinsicht Brandenburg , Dr. Rita Wellbrock Der Hessische Datenschutzbeauftragte,
Heinz Biermann Der Bundesbeauftragte für den Datenschutz, Jürgen Engels Die Landesbeauftragte für den Datenschutz Nordrhein-Westfalen, Walter Ernestus Der Bundesbeauftragte für den Datenschutz,
Udo Höhn Der Bayerische Landesbeauftragte für den Datenschutz , Rüdiger Wehrmann Der Hessische Datenschutzbeauftragte, Andreas Schurig Der Sächsische Datenschutzbeauftragte

Datenschutz und Telemedizin

Grundlegende Sicherheitsanforderungen

5. Revisionsfähigkeit

Die Revisionsfähigkeit der erhobenen, gespeicherten, übermittelten oder sonst verarbeiteten Daten muss gewährleistet sein, d.h. die Verarbeitungsprozesse müssen lückenlos nachvollzogen werden können und es muss festgestellt werden können, wer wann welche patientenbezogenen Daten auf welche Weise verarbeitet hat**. Für den Arzt bzw. das Krankenhaus besteht nach der Berufsordnung die Pflicht zur Dokumentation der Behandlung.**

Quelle: Marion Bultmann Der Landesbeauftragte für den Datenschutz und das Recht auf Akteneinsicht Brandenburg , Dr. Rita Wellbrock Der Hessische Datenschutzbeauftragte,
Heinz Biermann Der Bundesbeauftragte für den Datenschutz, Jürgen Engels Die Landesbeauftragte für den Datenschutz Nordrhein-Westfalen, Walter Ernestus Der Bundesbeauftragte für den Datenschutz,
Udo Höhn Der Bayerische Landesbeauftragte für den Datenschutz , Rüdiger Wehrmann Der Hessische Datenschutzbeauftragte, Andreas Schurig Der Sächsische Datenschutzbeauftragte

Datenschutz und Telemedizin

Grundlegende Sicherheitsanforderungen

5. Revisionsfähigkeit

Sie ist eine **unselbständige Nebenpflicht aus dem Behandlungsvertrag**. Eine lückenhafte Dokumentation kann im Haftungsprozess eine Beweislastumkehr zugunsten des Patienten nach sich ziehen. **Es muss nachvollziehbar sein, wer welche Diagnose gestellt und welche Therapie verordnet hat und aufgrund welcher Daten ein Arzt seine Entscheidung über Behandlungsmaßnahmen getroffen hat.** Eine notwendige Voraussetzung für die Gewährleistung der Revisionsfähigkeit ist die Sicherstellung der Authentizität.

Quelle: Marion Bultmann Der Landesbeauftragte für den Datenschutz und das Recht auf Akteneinsicht Brandenburg , Dr. Rita Wellbrock Der Hessische Datenschutzbeauftragte, Heinz Biermann Der Bundesbeauftragte für den Datenschutz, Jürgen Engels Die Landesbeauftragte für den Datenschutz Nordrhein-Westfalen, Walter Ernestus Der Bundesbeauftragte für den Datenschutz, Udo Höhn Der Bayerische Landesbeauftragte für den Datenschutz , Rüdiger Wehrmann Der Hessische Datenschutzbeauftragte, Andreas Schurig Der Sächsische Datenschutzbeauftragte

Datenschutz und Telemedizin

Grundlegende Sicherheitsanforderungen

6. Validität

Die Validität der erhobenen, gespeicherten, übermittelten oder sonst verarbeiteten Daten muss gewährleistet sein, d.h. personenbezogene Daten müssen aktuell in der für den Nutzungszweck angemessenen Qualität verarbeitet werden. Diese Forderung betrifft insbesondere Bilddaten, bei denen es auf Qualitätsmerkmale wie Bildauflösung und Farbechtheit ankommt. **Die Validität wird von der Integrität nicht umfasst, da die Daten zwar integer im Sinne von vollständig und unversehrt sein können, die Darstellungs-qualität und Aktualität aber dennoch für medizinische Nutzungszwecke unzureichend sein kann.**

Quelle: Marion Bultmann Der Landesbeauftragte für den Datenschutz und das Recht auf Akteneinsicht Brandenburg , Dr. Rita Wellbrock Der Hessische Datenschutzbeauftragte, Heinz Biermann Der Bundesbeauftragte für den Datenschutz, Jürgen Engels Die Landesbeauftragte für den Datenschutz Nordrhein-Westfalen, Walter Ernestus Der Bundesbeauftragte für den Datenschutz, Udo Höhn Der Bayerische Landesbeauftragte für den Datenschutz , Rüdiger Wehrmann Der Hessische Datenschutzbeauftragte, Andreas Schurig Der Sächsische Datenschutzbeauftragte

Datenschutz und Telemedizin

Grundlegende Sicherheitsanforderungen

7. Rechtssicherheit

Für jeden Verarbeitungsvorgang und dessen Ergebnisse ist der **Verursachende bzw. Verantwortliche beweiskräftig nachweispflichtig**. Ist die Rechtssicherheit nicht gegeben, können Patienten eventuelle Schadensansprüche u.U. nicht geltend machen bzw. können Mediziner u.U. die Korrektheit ihres Handelns nicht nachweisen. Die notwendige Voraussetzung für die Gewährleistung der Rechtssicherheit ist die Gewährleistung der Revisionsfähigkeit. Die Revisionsfähigkeit alleine gewährleistet aber noch nicht die beweiskräftige Überprüfbarkeit von Verarbeitungsvorgängen in gerichtlichen Verfahren.

Datenschutz und Telemedizin

Grundlegende Sicherheitsanforderungen

8. Nicht-Abstreitbarkeit von Datenübermittlungen

Die Nicht-Abstreitbarkeit des Sendens und des Empfangens von patientenbezogenen Dokumenten muss gewährleistet sein. D.h. einerseits ist zu gewährleisten, dass der Sender eines patientenbezogenen Dokuments sicher sein kann**, dass das Dokument seinen Empfänger erreicht hat, und er darf nicht abstreiten können, genau dieses Dokument an genau den Empfänger gesendet zu haben**. Andererseits muss der Empfänger eines patientenbezogenen Dokuments sicher sein können, genau dieses Dokument von einem bestimmten Sender empfangen zu haben, und er darf nicht abstreiten können, genau das Dokument von einem bestimmten Sender empfangen zu haben. Die Nicht-Abstreitbarkeit ist eine Voraussetzung der Revisionsfähigkeit.

https://www.caritas.de/hilfeundberatung/onlineberatung/onlineberatung abgerufen am 22.11.2020

Caritas Online-Beratung

Die Analyse ergab, dass die Datenübertragung über einen zentralen Client-Server erfolgt. Dies widerspricht dem allgemeinen Standard, der z.B. für die Online-Videosprechstunde gilt. Eine Peer-to-Peer –Verbindung wäre wünschenswert. Zwar werden die erforderlichen persönlichen Daten auf ein Mindestmaß reduziert, jedoch werden die Kommunikationsdaten gespeichert. Eine Verschlüsselung findet nicht adäquat statt. Die Anonymität der ratsuchenden Person zum Berater ist vordergründig gewährleistet, da nur Textnachrichten ausgetauscht werden. Allerdings kann während der Verbindung die IP-Adresse der ratsuchenden Person ausgelesen werden. Dies vergrößert die Angriffsfläche für die ratsuchende Person. Ein Zugriff auf das Endgerät der ratsuchenden Person kann nicht ausgeschlossen werden.

Vielen Dank für die Aufmerksamkeit

Prof. Dr. Martin Klein
Katholische Hochschule NRW
Institut für IT-Sicherheit im Sozial- und Gesundheitswesen

Prorektor für Studium und Lehre
und Wissensmanagement
Wörthstraße 10
50668 Köln
www.katho-nrw.de

Prof. Dr. Gregor Hohenberg
Hochschule Hamm-Lippstadt
Institut für IT-Sicherheit im Sozial- und Gesundheitswesen

Leitung Stabsstelle für Digitalisierung

Marker Allee 76-78
59063 Hamm
www.hshl.de