Datenschutz und digitale Ethik
Grundlage guter Technik

Walter Swoboda, Marina Fotteler, Michael Örtl, Felix Holl, Martin Schmieder, Elmar Buchner

Was ist Digitalisierung?

Computer im heutigen Sinne, also programmierbare und digital-elektronisch gesteuerte Automaten, gibt es schon seit der ersten Hälfte des letzten Jahrhunderts, wobei sich die Basistechnologie (aufbauend auf drei einfachen logischen Operationen) nicht grundlegend geändert hat. Die entscheidende Beschleunigung hat die Technologie im Jahre 1974 erfahren: In diesem Jahr begann die Firma *Intel* mit der Produktion des Mikroprozessors, der Computer nicht nur miniaturisierte, sondern radikal preiswerter machte. In den folgenden 40 Jahren verbreitete sich die Technologie rasch. Heute sprechen wir von der *Digitalisierung* praktisch aller Lebensbereiche.

Damit ist gemeint, dass es keine menschliche Tätigkeit mehr gibt, in der computergesteuerte Anwendungen nicht zum Einsatz kämen; einige Anwendungen haben sogar Bedürfnisse geschaffen, die es vorher noch gar nicht gab: *Social Networking* ist hierfür ein gutes Beispiel, aber bei weitem nicht das einzige. Ob die Digitalisierung dabei die zugrunde liegenden Prozesse immer verbessert, oder ob insgesamt durch Digitalisierung eine Verbesserung eintritt, ist durchaus umstritten: Den unumstrittenen Vorteilen (z.B. Wegstreckeneinsparung durch Navigationsgeräte, ubiquitäre Verfügbarkeit von Information durch das Internet, Wettervorhersagen durch massiv parallele Großrechner) stehen nicht wegzudiskutierende Risiken gegenüber. Moderne Computersysteme sind grundsätzlich mit großer Speicherkapazität ausgestattet und miteinander vernetzt, das heißt, es können Daten in einer Menge gespeichert und ausgetauscht werden, wie es noch vor einigen Jahren undenkbar gewesen wäre. Gegenüber herkömmlichen Datenspeichern, wie beispielsweise Aktenordnern oder *Mikrofiches*, hat sich die *potenzielle Quantität* erhöht, nicht aber die Qualität des Datenschutzrisikos. Dies führt in der öffentlichen Diskussion manchmal zu voreiligen Schlüssen, wie etwa dem Einwand, dass auch früher Patient*innenakten versehentlich Dritten zur Einsicht gelangten. Das mag richtig sein, aber durch datentechnische Unzulänglichkeiten moderner Informa-

https://doi.org/10.14361/9783839454695-005 - am 13.02.2026, 21:33:43. https://www.inlibra.com/de/agb - Open Access -

tionssysteme gelangen eben nicht nur einzelne Datensätze, sondern häufig ganze Datenarchive mit vielen Tausend Datensätzen in die Hände nicht autorisierter Personen.

Durch Einsatz von neuen, teilweise revolutionären Technologien wie *Big Data*, maschinellem Lernen und eventuell künftig von *Quantencomputern* können riesige Datenmengen zudem sehr effizient gefiltert und verarbeitet werden, womit auch kommerziell verwertbares Wissen extrahiert werden kann. Plattformen wie *Amazon* oder *Alibaba* arbeiten daran, ihre Kund*innendaten derartig effizient auszuwerten, dass es möglich ist, die nächste Bestellung vorzubereiten, *bevor* die Kund*innen bestellen. Der Anfang ist gemacht und diesbezügliche Versuche laufen bereits.

Warum Digitalisierung für Senior*innen?

Die menschlichen Lebensgewohnheiten werden bereits heute durch die mit Miniaturisierung und Verbilligung ausgelöste technologische und soziale Revolution der Digitalisierung mehr verändert als durch die drei industriellen Revolutionen der Mechanisierung, Massenproduktion und Automatisierung zuvor. Bisher ist kein Ende in Sicht, im Gegenteil scheint sich die Entwicklung sogar noch weiter zu beschleunigen. Allerdings nehmen nicht alle Bevölkerungsschichten gleichermaßen an dieser Entwicklung teil. Der vielbesprochene ›social divide‹, das heißt, der schlechtere Zugang zur Technologie und die daraus resultierende Benachteiligung vor allem von älteren, sozial schwachen und behinderten Menschen, ist Realität und kann auch in jüngerer Zeit bestätigt werden (Hollier 2007), wenngleich das Problem mittlerweile differenzierter betrachtet werden muss (Paul/Stegbauer 2005). Entsprechend wird von staatlichen Institutionen gegengesteuert; einige Maßnahmen sind im 8. Altersbericht des *Bundesministeriums für Familie, Senioren, Frauen und Jugend* (BMFSFJ) zusammengefasst (BMFSFJ 2020).

Nicht zwingende Gründe

Besteht hier Nachholbedarf, oder anders ausgedrückt: Sollen wir die Digitalisierung der Lebensumstände von Älteren überhaupt fördern? Brauchen Senior*innen unbedingt Digitalisierung? Viele würden hier sicher argumentieren: Nicht unbedingt. Allerdings entstehen dann durch die sich ändernden gesellschaftlichen Rahmenbedingen Einschränkungen, die nicht ohne Weiteres aus dem Weg geräumt werden können, so zum Beispiel:

- Finanzielle Einschränkungen (z.B. wird eine Banküberweisung künftig für diejenigen deutlich teurer werden, die den herkömmlichen, analogen Weg bevor-

https://doi.org/10.14361/9783839454695-005 - am 13.02.2026, 21:33:43. https://www.inlibra.com/de/agb - Open Access -

zugen; Verbraucher*innen, die mittels App und/oder Kund*innenkarte Mitglied in einem digitalen Bonusprogramm sind, bekommen einlösbare Punktegutschriften oder erhalten Rückzahlungen).
- Gesellschaftliche Einschränkungen (z.B. soziale Kontakte finden vermehrt über die digitalen Netzwerke statt, physische Veranstaltungen werden darüber geplant).

Obwohl diese Nachteile zwar messbar sind, werden sie wohl aber nicht als derart gravierend angesehen, die Digitalisierung der Lebensbereiche von Senior*innen zu fördern oder eventuell gar zu fordern: Die Einzelperson mag die Konsequenzen abwägen und individuell entscheiden.

Zwingende Gründe

Allerdings existiert mindestens ein weiterer Punkt, der sich ganz grundlegend von den angeführten Einschränkungen unterscheidet und eine zumindest teilweise Digitalisierung voraussetzt. Es handelt sich um die Möglichkeit der adäquaten künftigen pflegerischen und medizinischen Versorgung Älterer, beziehungsweise um die Unmöglichkeit dieser, wenn die etablierten Prozesse ohne grundlegende Änderung fortgesetzt werden. Es gibt in Deutschland, wie in anderen Ländern, außerdem einen gravierenden Mangel an Pflegepersonal, der zwar durch äußere Umstände (Bezahlung, Arbeitsbedingungen) beeinflussbar ist, aber ganz grundsätzlich durch zu wenig verfügbare personelle Ressourcen verursacht wird, wobei sich diese Faktoren natürlich gegenseitig beeinflussen (siehe Abbildung 1).

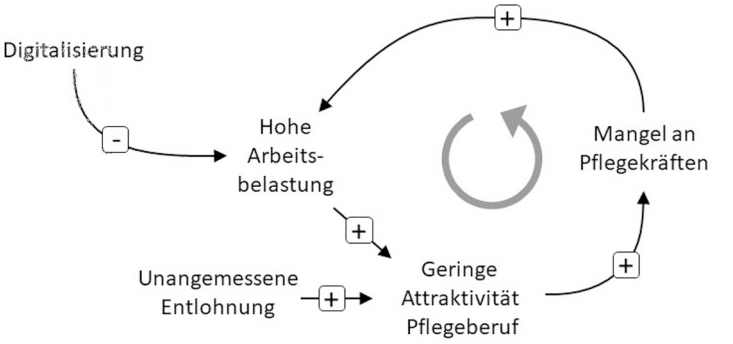
Der dargestellte, sich selbst verstärkende Kreislauf kann nur durchbrochen werden, wenn mindestens einer der Faktoren Arbeitsbelastung, Attraktivität, und/oder Arbeitskräftemangel *entscheidend positiv* beeinflusst wird.

Dem Mangel an Personal wird mit überschaubarem Erfolg entgegengetreten, indem Pflegekräfte aus dem Ausland gezielt angeworben werden. Auch Versuche, die Höhe der Bezahlung den verantwortungsvollen und risikoreichen Aufgaben anzupassen, haben eher enge Grenzen finanzieller Art. Dagegen lässt sich die Belastung am Arbeitsplatz voraussichtlich deutlich durch Einsatz der Digitalisierung verringern, vor allem wenn man bedenkt, dass mindestens ein Drittel der pflegerischen Arbeitszeit mit eigentlich pflegefremden Tätigkeiten verbracht wird, zum Beispiel Tätigkeiten der Verwaltung oder Dokumentation (Hendrich et al. 2008). Werden Pflegekräfte selbst befragt, so würden sie übrigens selbst bessere Arbeitsbedingungen einer besseren Bezahlung vorziehen (Vereinigung der Bayerischen Wirtschaft 2020).

Zudem, und dieser Punkt wird häufig übersehen, ist davon auszugehen, dass eine moderne und effiziente Arbeitsumgebung dazu beitragen kann, die Attraktivität des Berufs zu steigern. Zeitgerechte Ausstattung hebt durchaus die Motivati-

https://doi.org/10.14361/9783839454695-005 - am 13.02.2026, 21:33:43. https://www.inlibra.com/de/agb - Open Access -

Abbildung 1: Abhängigkeitsmodell berufliche Attraktivität Pflege



Quelle: Eigene Darstellung

on und gerade in den pflegerischen Berufen besteht hier Nachholbedarf. Während zum Beispiel Automechaniker*innen zu Mechatroniker*innen werden und selbstverständlich nicht nur mit Motoren umgehen, sondern auch programmieren und Software aktualisieren, wird in der Pflege – abgesehen von vereinzelten Inselversuchen mit Pflegeinformationssystemen – zumeist immer noch mit herkömmlichen Methoden, wie beispielsweise papierbasierter Dokumentation, gearbeitet.

Die Sinnhaftigkeit der Digitalisierung von medizinischer und pflegerischer Versorgung von Senior*innen sollte damit außer Frage stehen, allerdings gilt es, vorhandene Risiken hinreichend kritisch zu bewerten und zu berücksichtigen.

Was ist sinnvoll?

Außer Frage steht, dass es sich bei medizinischer Versorgung um einen sehr arbeitsteiligen Prozess handelt. Das gilt auch für die Pflege und zwar sogar zunehmend. Durch die Bemühungen, die Pflege von Senior*innen verstärkt ambulant zu betreiben, sind häufig unterschiedliche Dienstleister*innen am Prozess beteiligt. Vernetzung und Abstimmung erfolgen dabei nicht immer in ausreichendem Maße (Lavander/Meriläinen/Turkki 2016). Davon ausgehend muss die Frage gestellt werden: Was ist weiterhin sinnvoll?

https://doi.org/10.14361/9783839454695-005 - am 13.02.2026, 21:33:43. https://www.inlibra.com/de/agb - Open Access -

Literaturrecherche

Wir haben eine breit angelegte Literaturrecherche zu assistiven Technologien für Senior*innen begonnen, die als vorläufige Veröffentlichung vorliegt (Fotteler et al. 2019). Einschlusskriterien waren unter anderem, dass es sich um eine randomisierte kontrollierte Studie (engl. ›randomized controlled trial‹, RCT) mit mindestens einer Kontrollgruppe handelt, die peer-reviewed nach dem 01.01.2009 veröffentlicht wurde und sich mit üblichen Digitalisierungsschwerpunkten der assistiven Versorgung älterer Menschen (Durchschnittsalter ≥ 65 Jahre) beschäftigt. Ausgeschlossen wurden die Themen Telemedizin, Virtual Reality, Robotik, Lifestyle-Interventionen und weitere Technologien für rehabilitative und therapeutische Ansätze. Die Suche wurde in den Datenbanken *Medline*, *CINAHL* und *IEEEXplore* durchgeführt. Es wurden 11.400 Studien gesichtet; nach eingehender Prüfung blieben neunzehn Studien übrig, die sich durch einen hohen Grad der Heterogenität auszeichneten. Sechs Kategorien wurden in der Auswertung identifiziert: Hören, Medikation, Sehen, mentale Unterstützung, Mobilität und persönliches Krankheitsmanagement. Lediglich Hörgeräte und Anwendungen zum persönlichen Krankheitsmanagement erscheinen den vermeintlich größten Nutzen für ältere Menschen zu haben. Es gibt jedoch noch zu wenige randomisiert-kontrollierte Studien zur Thematik, zudem kaum RCTs zu den aktuell populären Technologien wie Sturz-Sensorik et cetera, weshalb die Evidenzlage nicht eindeutig bestimmt werden kann.

Konsortialprojekt CARE REGIO

Das Projektkonsortium CARE REGIO wurde im Raum Bayerisch-Schwaben ins Leben gerufen, um speziell die Möglichkeiten der Digitalisierung der Pflege zu erproben. In der bereits abgelaufenen Vorphase des Projekts wurden mehrere Befragungen durchgeführt, um den Bedarf der Pflegekräfte zu evaluieren (Veröffentlichung in Vorbereitung). Ein ganz eindeutiges Ergebnis ist, dass die Befragten einen erhöhten Bedarf bei der Erleichterung der als sehr arbeitsintensiv empfundenen Dokumentationspflichten und bei der inter-institutionellen Nachrichtenvernetzung sehen. Demzufolge wird CARE REGIO neben dem Einsatz von assistiver robotischer Technologie auch einen besonders aufwendigen Dokumentations- und Kommunikationsprozess (Überleitungsmanagement) und einen zentralen Datenpool für pflegerische Datensätze (›Data Lake‹) erproben.

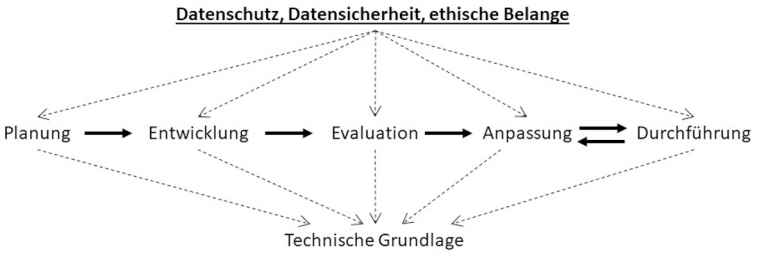
https://doi.org/10.14361/9783839454695-005 - am 13.02.2026, 21:33:43. https://www.inlibra.com/de/agb - Open Access -

Wie wird aus Digitalisierung gute Technik?

In diesem Artikel sollen weniger die technischen Lösungsansätze beleuchtet werden, da diese teilweise vorhanden, wenn auch nicht im gegebenen Umfeld erprobt sind. Vor allem die Einbindung der pflegerischen Prozesse in die deutsche *Telematik*-Infrastruktur wird eine wesentliche Aufgabe darstellen. Bisher gibt es diesbezüglich kaum etablierte Ansätze, zumal der Fokus der mit der Bereitstellung beauftragten Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH, genannt *gematik* (Drees 2007), in der Vergangenheit mehr auf die medizinische Versorgung ausgerichtet war. Dies wird nunmehr für die Pflege nachgeholt, entsprechende Module und Modifikationen sind bereits eingeleitet.

Im Folgenden wird detailliert auf Anforderungen von Datenschutz, Datensicherheit und ethische Belange eingegangen, die im sensiblen Umfeld der Digitalisierung von Medizin und Pflege während des gesamten Einführungs- und Betriebsprozesses Vorrang vor technischen und ökonomischen Gegebenheiten haben sollten (siehe Abbildung 2).

Abbildung 2: Einflussfaktoren auf den Einführungs- und Betriebsprozess



Quelle: Eigene Darstellung

Datenschutz und Datensicherheit

Insbesondere in Medizin und Pflege stellt der Schutz der patient*innenrelevanten Daten eine besonders wichtige Aufgabe dar. Dabei ist Datenschutz von der Datensicherheit zu unterscheiden: Das Erste meint den Schutz vor Zugriffen unautorisierter Dritter, das Zweite die sichere Speicherung und Übertragung der Datensätze. Hierunter fallen zum Beispiel der Schutz vor Löschung und Veränderung, die Verfügbarkeit und die Nichtabstreitbarkeit von Daten.

https://doi.org/10.14361/9783839454695-005 - am 13.02.2026, 21:33:43. https://www.inlibra.com/de/agb - Open Access -

Gesetzliche Grundlagen

Ganz grundsätzlich ist für jede Maßnahme der Digitalisierung in der (Alten-)Pflege ein ›Datenschutzbeauftragter‹ nach Artikel 37 der *Datenschutz-Grundverordnung* (DSGVO) zu benennen, welcher aufgrund der beruflichen Qualifikation und des Fachwissens gewählt werden muss.

Eine weitere wichtige Voraussetzung ist die Einhaltung der Richtlinien des *Bundesdatenschutzgesetzes* (Nagel/Kiefer 2008) und der *Datenschutz-Grundverordnung* der Europäischen Union (Voigt/von dem Bussche 2018). Hier wird vor allem das Persönlichkeitsrecht der Patient*innen geschützt: Unbedingt erforderlich ist die Einholung einer freiwilligen, für den jeweiligen Einsatz zweckgebundenen, schriftlichen Patient*innenzustimmung mit vorgehender vollständiger Aufklärung in einer für die Patient*innen verständlichen Sprache. Selbstverständlich dürfen Erhebung, Verarbeitung und Nutzung der personenbezogenen Daten nur für die medizinisch-pflegerische Behandlung (unter Patient*inneneinwilligung) verwendet werden. Die Erhebung, Verarbeitung und Nutzung von ausschließlich nicht personenbezogenen Daten für eine wissenschaftliche Auswertung ist möglich, muss jedoch in der Patient*inneneinwilligung ausdrücklich vermerkt werden. Ganz grundsätzlich unterliegen alle Datensätze der Erforderlichkeit und Zweckbindung, das heißt, Daten werden nur erhoben, wenn sie für den medizinisch-pflegerischen und eventuell wissenschaftlichen Einsatzzweck erforderlich und zweckmäßig sind.

Einige wichtige neuere Anforderungen ergeben sich durch das *Patientendatenschutzgesetz* (Fricke 2020). Dieses beinhaltet im Wesentlichen, dass Patient*innen in Deutschland das Recht besitzen, dass ihre medizinisch und auch pflegerisch relevanten Daten in den Datensenken der deutschen Telematik-Infrastruktur (auf Verlangen) eingetragen werden. Unabdingbare Voraussetzung dafür ist, dass Digitalisierungsvorhaben für Senior*innen mittels Konnektoren überhaupt eingebunden werden und die betreuenden Fachkräfte Zugang zur Telematik-Infrastruktur erhalten. Dies scheitert im Moment noch an der Tatsache, dass der dafür notwendige *elektronische Heilberufe-Ausweis* (eHBA) an Ärzt*innen, jedoch noch nicht an Pflegekräfte ausgegeben wird. Der Grund hierfür liegt in einer uneinheitlichen organisatorischen Verteilerstruktur, die zwar im medizinischen Bereich mit der Bundesärztekammer vorhanden ist (und von den Ärzt*innen finanziert wird); eine entsprechende Einrichtung für die Pflege hingegen jedoch fehlt. Eine Lösung mittels Gruppenzugang ist im Sinne der Nachverfolgbarkeit von Datenzugriff, -änderung und -eingabe kein geeigneter Weg.

Verschlüsselung

Erster und wichtigster Schritt für die Sicherstellung der datenschutzrechtlichen Anforderungen ist die Verschlüsselung von Daten. Je nach verwendetem Verfah-

https://doi.org/10.14361/9783839454695-005 - am 13.02.2026, 21:33:43. https://www.inlibra.com/de/agb - Open Access -

ren ist eine Entschlüsselung durch unautorisierte Dritte mehr oder weniger leicht möglich. Im Sinne eines mathematischen Nachweises kann *keine* der heute verwendeten Verschlüsselungsalgorithmen einen absolut sicheren Schutz bieten.[1] Gängige Verfahren erhöhen nur den Aufwand, der zur Entschlüsselung betrieben werden muss, auf ein Maß, das sie heute faktisch unmöglich macht. Allerdings geht jede*r Anwender*in das Risiko ein, dass verschlüsselte Daten gespeichert werden und in Zukunft mit neuen Verfahren relativ einfach in Klartext verwandelt werden können. Wesentlichste Unsicherheitsfaktoren sind dabei die Möglichkeit wissenschaftlicher Fortschritte auf verschiedenen Gebieten der Kryptografie, zum Beispiel zeitlich verzögerte ›Brute-Force-Attacke‹ oder die Anwendung eventuell entwickelter neuer Möglichkeiten der Primzahlenzerlegung. Auch schlichtes menschliches Versagen trägt dazu bei, dass Daten entschlüsselt werden können.

Herkömmliche Verfahren basieren grundsätzlich auf einem *symmetrischen* Schlüsselaustausch, bevor der eigentliche Datenaustausch erfolgt. Alle am Verfahren beteiligten Partner*innen nutzen dann (eventuell für einen sehr kurzen Zeitraum) denselben Schlüssel, mit dem die Daten über einen bekannten Prozess behandelt werden. Das inverse Verfahren liefert dann wieder den ursprünglichen Text. Formal betrachtet verhält es sich wie folgt: Sei C eine beliebige Zeichenkette, f ein Verschlüsselungsverfahren, S der zugehörige Schlüssel, C' die verschlüsselte Zeichenkette und f' das Umkehrverfahren zu f:

$$C = \left\{ c \in (a.z, A.Z, \ldots) \middle| c_0 . c_n \right\}$$

$$f(S, C) = C'$$

$$f'\left(S, C'\right) = C$$

Es ist leicht einsehbar, dass eine dritte Person alle Nachrichten entschlüsseln kann, wenn ihr der Schlüssel bekannt ist. Wird dieser über denselben Nachrichtenkanal wie die eigentliche Nachricht ausgetauscht, ist dies sogar besonders einfach (›Man-In-The-Middle-Attack‹). Trotzdem wird das Verfahren häufig wegen seiner verhältnismäßigen Einfachheit, des geringen Ressourcenverbrauchs und seiner Perfor-

1 Es gibt zwar ›beweisbar sichere Verfahren‹, diese fußen aber auf Annahmen, die heute noch nicht bewiesen werden können. Außerdem werden diese Verfahren in der Praxis wegen des damit verbundenen hohen Aufwands kaum eingesetzt.

https://doi.org/10.14361/9783839454695-005 - am 13.02.2026, 21:33:43. https://www.inlibra.com/de/agb - Open Access -

mance angewendet, auch bei der Verschlüsselung von WLAN-Übertragungen über das Protokoll *Wired Equivalent Privacy* (WEP).

Bei der *asymmetrischen* Verschlüsselung werden zwei Schlüssel verwendet, ein sogenannter *privater Schlüssel* und ein *öffentlicher Schlüssel*:

$$f\left(S_{\text{"}\ddot{o}ffentlich}, Z\right) = S'$$

$$f'\left(S_{privat}, Z'\right) = S$$

Der private Schlüssel kann frei verteilt werden; damit behandelte Dateien lassen sich nur dann wieder in den Klartext verwandeln, wenn der geheime Schlüssel zur Verfügung steht. In der Praxis verteilt ein*e potenzielle*r Empfänger*in einer Nachricht seinen*ihren öffentlichen Schlüssel zum Beispiel über eine Web-Page, die jede*r einsehen kann. Ein*e potenzielle*r Nachrichtensender*in verschlüsselt dann seine*ihre Datei mit diesem öffentlichen Schlüssel und entzieht sie damit dem Zugriff (auch durch ihn*sie selbst, d.h., der*die Sender*in kann dann die Nachricht ebenfalls nicht mehr lesen). Kommt die Nachricht bei dem*der Empfänger*in an, so entschlüsselt diese*r die Nachricht mittels seines*ihres geheimen privaten Schlüssels.

Wie kann dies funktionieren? Dieses Verfahren basiert auf der Tatsache, dass bestimmte mathematische Rechnungen auf Computern in einer Richtung sehr schnell, in der anderen Richtung aber extrem langsam ablaufen. So lässt sich jede beliebige ganze Zahl in ein Produkt aus Primzahlen zerlegen, diese Operation kann aber bei großen Zahlen sehr viel Zeit erfordern, bei Zahlen mit 200 Stellen zehntausende Jahre oder mehr bei heutiger Computertechnik. Aus beliebigen ganzen Primzahlen lässt sich aber in Bruchteilen von einer Sekunde ein Produkt bilden, dessen Ergebnis eine Zahl mit den genannten 200 Stellen ergibt.

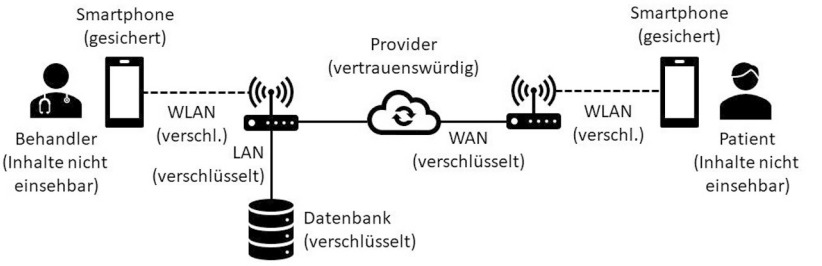
In der Praxis werden sinnvollerweise beide Verfahren, also symmetrische und asymmetrische Verschlüsselung, kombiniert. Der Algorithmus, der sich hinter ›sicheren‹ Web-Pages befindet, ist *Hypertext Transfer Protocol Secure* (HTTPS). Das Verfahren bewerkstelligt den Schlüsselaustausch über asymmetrische, die Nachrichtenverschlüsselung über symmetrische Verfahren.

Manchmal wird übersehen, dass die Daten nicht nur während der eigentlichen Übertragung geschützt werden müssen, sondern auch bei der Datenspeicherung in allen beteiligten System-Modulen (siehe Abbildung 3).

Auch jene Daten, die auf dem Server liegen, müssen verschlüsselt werden. Das gilt auch für die Zugriffsmöglichkeiten der Administrator*innen! Beteiligte Perso-

https://doi.org/10.14361/9783839454695-005 - am 13.02.2026, 21:33:43. https://www.inlibra.com/de/agb - Open Access -

Abbildung 3: Notwendige Absicherungen von Modulen in einem Beispielsystem (WLAN=Funkverbindung, LAN=Lokales Netzwerk, WAN=Weitverkehrsnetzwerk)



Quelle: Eigene Darstellung

nen müssen dafür Sorge tragen, dass Bildschirminhalte, Töne und so weiter nicht von Dritten eingesehen oder abgehört werden können. In den meisten Fällen wird es nötig sein, eigene Räume für die angemessene physische IT-Sicherheit zur Verfügung zu stellen.

Anonymisierung

Bei jeglicher Auswertung von Ergebnissen durch nicht am Behandlungsprozess Beteiligte ist es notwendig, dass Daten entfernt werden, die nicht für die Auswertung erforderlich sind, aber eine Identifizierung ermöglichen. Dieser Transfer von patient*innenrelevanten Daten (für die Behandlung) hin zu nicht-patient*innenrelevanten Daten erfolgt grundsätzlich durch die *Anonymisierung* der Datensätze. Hierbei werden persönliche Daten in einer möglichst räumlich, organisatorisch und personell getrennten *Vertrauensstelle* vor Weiterleitung entfernt und alle noch vorhandenen Datensätze mittels eines Randomisierung-Algorithmus zwischen den Datensätzen permutiert. Dabei bleiben zwar summarische Auswertungen (z.B. durchschnittlicher zeitlicher Arbeitsaufwand) erhalten, die Daten eignen sich aber nicht mehr für die eingehende wissenschaftliche Untersuchung, insbesondere, wenn verschiedene Gruppen unter Einbeziehung von Kofaktoren evaluiert werden sollen. Deshalb wird bei einer geplanten Untersuchung normalerweise die Methode der *Pseudonymisierung* angewendet, bei der auf die permutierende Neuverteilung der Daten verzichtet wird. Es ist leicht nachvollziehbar, dass durch auftretende Datenmuster bei Diagnosen und Behandlungen auch nach der Pseudonymisierung eine teilweise sichere Zuordnung zur Persönlichkeit der Patient*innen

https://doi.org/10.14361/9783839454695-005 - am 13.02.2026, 21:33:43. https://www.inlibra.com/de/agb - Open Access -

möglich bleiben kann. Deshalb wird das Verfahren als alleinige Maßnahme für den Datenschutz als nicht ausreichend angesehen.

Eine höhere Konformität zum Bundesdatenschutzgesetz bietet die *k-Anonymität* (Sweeney 2002) kombiniert mit einer Pseudonymisierung. Hierzu werden neben den personenrelevanten Datensätzen (›Identifier‹, diese werden entfernt) andere Variablen als quasi-*identifizierend* (›Quasi-Identifier‹) definiert. Quasi-Identifikatoren sind solche, die für sich genommen keine Zuordnung erlauben würden, aber in Kombination mit anderen Daten eine Zuordnung ermöglichen. Ein Anwendungsbeispiel: Die Vertrauensstelle gibt einen Datensatz erst dann weiter, wenn mindestens zwei Datensätze mit gleichen quasi-identifizierenden Einträgen vorhanden sind, da erst dann davon ausgegangen werden kann, dass eine sichere Zuordnung nicht mehr möglich ist. Etwas formeller lässt sich der Zusammenhang so darstellen: Gegeben sei eine Gruppe von Patient*innen G, die über die identifizierende Datenmenge Imit ihren Variablen $V_{0.n}$, einer quasi-identifizierenden Datenmenge Q mit ihren Variablen $V_{n+1.m}$ und eine weitere sensible Datenmenge S mit ihren Variablen $V_{m+1.o}$ beschrieben wird:

$$G = \left\{ I\left(V_{0.n}\right) \cup Q(V_{n+1.m}) \cup S(V_{m+1.o}) \right\}$$

Der für eine Untersuchung zur Verfügung stehende Datensatz lautet G':

$$G' = \left\{ Q(V_{n+1.m}) \cup S(V_{m+1.o}) \right\}$$

Dabei gibt es eine Zuordnung f der Vertrauensstelle:

$$f\colon G' \rightarrow G$$

T sei eine Tabelle von Werten der Variablen aus Q. Der Datensatz G'ist genau dann k-anonym, wenn jede Teilmenge jeder Zeile x aus T mindestens k-mal in T vorkommt:

https://doi.org/10.14361/9783839454695-005 - am 13.02.2026, 21:33:43. https://www.inlibra.com/de/agb - Open Access -

$$t\,(x) \subset T(x)$$

$$\forall t\,(x) : \exists x_{1.k} \text{mit} \left\{1.k \in \aleph \middle| x = x_1, \ldots, x = x_k\right\}$$

Man spricht bei diesen Einträgen auch von einer ›Äquivalenzklasse‹. Damit ergibt sich:

$$\nexists f' : Q \to G$$

In der praktischen Arbeit ergeben sich trotzdem Möglichkeiten zur Deanonymisierung, die bekannteste davon ist die ›Homogenitäts-Attacke‹. Wenn alle Einträge einer Äquivalenzklasse in einem sensiblen Datensatz den gleichen Wert haben, ist eine Zuordnung sensibler Daten möglich (Beispiel: Alle 85-jährigen Männer haben eine Prostata-Hyperplasie). Auch lassen sich durch Verknüpfungen mit anderen Datenbanken einzelne Datensätze direkt zuordnen (›Background-Knowledge-Attack‹).

Schutzziele

Es gibt eine Reihe weiterer zu realisierenden Maßnahmen, um Schutzziele bei allen Digitalisierungsvorhaben in der Medizin zu verfolgen, insbesondere bei solchen, bei denen keine statistische Auswertung erfolgt.

Zunächst ist hier die *Vertraulichkeit* von Daten zu nennen. Darunter versteht man, dass Daten nur von den Personen eingesehen oder offengelegt werden dürfen, die dazu auch berechtigt sind, was normalerweise über Verschlüsselungen erreicht wird.

Zweitens ist die *Verfügbarkeit* von Daten zu nennen. Sind Daten, die in einer Behandlung sinnvoll eingesetzt werden können, digital verfügbar, so müssen sie auch mit vertretbarem Aufwand einsehbar sein. Es wäre nicht vertretbar, wenn ein entsprechender Server gerade gewartet würde und daher nicht auf ihn zugegriffen werden könnte, sei es auch nur für eine begrenzte Zeit. Dieses Schutzziel wird normalerweise durch Einsatz redundanter Systeme erreicht, das heißt, durch mehrere Server, bei denen im Fall eines Einzelausfalls zusätzliche Hard- und Software vorgehalten wird. Um es gar nicht so weit kommen zu lassen, wird auch der

https://doi.org/10.14361/9783839454695-005 - am 13.02.2026, 21:33:43. https://www.inlibra.com/de/agb - Open Access -

Einsatz von unterbrechungsfreien Stromversorgungen diskutiert, die aber jeweils für sich wieder eine zusätzliche Fehlerquelle darstellen.

Die Daten-*Integrität*, also der Schutz vor unerlaubter (und eventuell sogar unentdeckter) Einsicht, Verfälschung oder gefälschtem Herkunftsnachweis, kann durch technische Maßnahmen wirkungsvoll verhindert werden. Verschlüsselung, *Hash*-Algorithmen und digitale Signaturen sind wirksame technische Methoden bei Speicherung und Kommunikation, die in jedem Fall durch zusätzliche organisatorische Maßnahmen (›Closed Room‹, Zugangsbeschränkung) ergänzt werden müssen. Der Verwendung von asymmetrischen Methoden, bei denen kein vorhergehender Austausch von privaten Schlüsseln notwendig ist (Andalib/Azad 2015), ist dabei zu bevorzugen.

Zusätzlich bestehen folgende ergänzende Schutzziele: *Revisionssicherheit* (revisionssichere Archivierung), *Transparenz* (ständige Möglichkeit des Einblicks gespeicherter Datensätze), *Nichtverkettbarkeit* von Datensätzen (s.o.) und *Invertierbarkeit*, also die vollständige Kontrolle durch Patient*innenrechte. Hierbei sind zu gewährleisten:

- Recht auf *Widerspruch*: Patient*innen haben ein Recht auf Widerspruch, dieses Recht gilt auch für Daten, welche zu Forschungszwecken eingesetzt werden unter Nennung von Gründen. Damit wird eine Teilnahmevereinbarung unter sofortiger Wirkung ungültig und alle Daten sind zu löschen.
- Recht auf *Widerrufung*: Patient*innen haben zu jeder Zeit die Möglichkeit, das Einverständnis zur Verarbeitung der personenbezogenen Daten zurückzuziehen. Im Unterschied zur Widerrufung wird dabei das Zustandekommen und die Gültigkeit einer Teilnahmevereinigung nicht bestritten, aber zu einem späteren Zeitpunkt beendet. Eventuell bereits gespeicherte Daten können damit erhalten bleiben.
- Recht auf *Löschung* von Daten, auch teilweise.
- Recht auf *Auskunft* über das Vorhandensein eigener Daten.
- Recht auf *Nichtwissen*: Patient*innen können sich dazu entscheiden, nicht über eventuelle Erkrankungen und Vorkommnisse aufgeklärt zu werden und Informationen über Ergebnisse nicht zu erfahren.

Weitere Schutzziele

Es gibt eine Reihe von zusätzlichen Forderungen, die schon in die ethischen Erfordernisse hineinreichen, aber technisch bedingt sind, weshalb sie hier besprochen werden:

- *Unaufdringlichkeit*: Die eingesetzten digitalen Methoden zwingen aus sich selbst heraus nicht zum Handeln der Patient*innen.

https://doi.org/10.14361/9783839454695-005 - am 13.02.2026, 21:33:43. https://www.inlibra.com/de/agb - Open Access -

- *Situationsangemessenheit*: Die eingesetzten digitalen Methoden reagieren angemessen auf die Bedürfnisse der Nutzer*innen, der Umgebung und der Situation.
- *Zulassung* von Sensoren und Aktoren: Sämtliche Sensoren, Aktoren und jegliche weitere Hard- und Software unterliegen der *Medizingeräteverordnung* (Nöthlichs/Weber 2003) und müssen diesbezüglich freigegeben sein.
- *Robustheit*: Die Robustheit der Systeme muss dem Einsatzzweck angemessen sein.
- *Technikfolgenabschätzung*: Grundsätzlich sind die Folgen des Einsatzes einer Digitalisierungs-Technologie für Patient*innen, Personal und Gesellschaft vor dem Einsatz geeignet abzuschätzen. Zu dieser Abschätzung gehört die Einbeziehung von medizinisch-pflegerischen, technischen, aber auch soziologischen und wirtschaftlichen Faktoren. Aktuell mangelt es noch an pflegebezogenen Technikfolgenabschätzungen. Sinnvoll erscheint daher analog zum etablierten *Health Technology Assessment* (HTA) ein ›Care Technology Assessment‹. Dazu gehören Nutzenbewertung und Technikfolgeabschätzung. Ein klassisches HTA hat die Aufgabe, die beste Lösung für eine Entscheidung hinsichtlich der Gesundheitsversorgung insgesamt wissenschaftlich zu unterstützen. Dies setzt jedoch eine gründliche vorausgegangene Evaluierung einer Anwendung voraus, das heißt, klinische Studien liegen bereits vor und die Anwendung wird bereits genutzt und erprobt. Ein prospektives HTA, das in früheren Phasen ansetzt, kann Einsatzpotenziale und Schwachstellen einer Innovation aufzeigen und so helfen, Chancen und Risiken frühzeitig zu bewerten und damit als strategisches Entscheidungsinstrument für die Umsetzung dienen.

Tabelle 1 fasst alle oben genannten Maßnahmen zusammen.

https://doi.org/10.14361/9783839454695-005 - am 13.02.2026, 21:33:43. https://www.inlibra.com/de/agb - Open Access -

Tabelle 1: Maßnahmen zu Datenschutz und Datensicherheit

Gesetzliche Anforderungen	Datenschutzgesetze Patientendatenschutzgesetz
Verschlüsselung	Symmetrische Verfahren Asymmetrische Verfahren Kombinierte Verfahren
Anonymisierung	Klassische Anonymisierung Pseudonymisierung k-Anonymisierung
Schutzziele	Vertraulichkeit Verfügbarkeit Datenintegrität Transparenz Nichtverkettbarkeit Invertierbarkeit
Weitere Schutzziele	Unaufdringlichkeit Angemessenheit Zulassung Robustheit Folgenabschätzung

Quelle: Eigene Darstellung

Erfordernisse der digitalen Ethik

Abgrenzung und Ethikkommission

Datenschutz und Datensicherheit sind Teil der ethischen Anforderungen, da ihre Nichtbeachtung zu entsprechenden Nachteilen für die Klient*innen führen kann. Weitere ethische Erfordernisse werden im Folgenden genannt. Zu beachten ist, dass eine formale Aufzählung nicht vollständig sein kann, da sie von den spezifischen Gegebenheiten eines Systems abhängt, womit dann neue Einträge erzwungen werden können. Im Zweifelsfall wird die zuständige *Ethikkommission* auf einzelne Punkte hinweisen, bevor sie ein Vorhaben positiv bewerten kann.

Ein Votum einer Ethikkommission ist immer dann erforderlich, wenn Forschung an lebenden oder verstorbenen Menschen oder an entnommenen Körpergeweben vorgenommen wird oder epidemiologische Untersuchungen erfolgen, bei denen personenbezogene Daten verarbeitet (nicht unbedingt ausgewertet) werden.

Forderungen

Zur Orientierung werden hier einige Sachverhalte angesprochen, die in den meisten Projekten für die technische Versorgung Älterer zur Anwendung kommen dürften:

https://doi.org/10.14361/9783839454695-005 - am 13.02.2026, 21:33:43. https://www.inlibra.com/de/agb - Open Access -

- *Risiken*: Die *Deklaration von Helsinki* (Bundesärztekammer 2013) fordert schon seit 1964 eine Chancen-/Risiko-Abwägung, allerdings nur für medizinisch-pflegerische Forschungsvorhaben: Ganz grundsätzlich dürfen Vorhaben nur dann umgesetzt werden, wenn die positiven Effekte für die Klient*innen überwiegen. Einzelne negative Effekte müssen durch einen Gewinn für die Gesamtheit aller Beteiligten mehr als ausgeglichen werden. Diese Forderung hat erhebliche Bedeutung für alle Digitalisierungsvorhaben und sollte daher auch hier Berücksichtigung finden.
- *Selbstbestimmung*: Eines der Hauptziele von senior*innengerechten technischen Hilfen ist es, den Klient*innen ein selbstbestimmtes Leben zu ermöglichen. Kein System oder Teilsystem sollte deshalb ausschließlich autonom agieren. In allen Fällen werden unter Einbeziehung der Klient*innen Entscheidungen von Menschen getroffen. Hierzu gehört auch, dass alle Personen das Recht haben, auf ein Hilfsmittel zu verzichten (s.u.).
- *Eingeschränkte Selbstbestimmung*: Ein Unterstützungsangebot sollte sich ausschließlich an entscheidungsfähige Patient*innen richten, deren kognitive Fähigkeiten weder durch Krankheit noch durch Behinderung soweit eingeschränkt sind, dass obige Voraussetzung nicht mehr gegeben ist. Diese Forderung ist in vielen Fällen nicht zu erfüllen, vor allem dann, wenn die Empfänger*in der Leistung diese zwar benötigen würde, aber aufgrund beispielsweise mangelnder kognitiver Leistung dazu nicht mehr oder vorübergehend nicht mehr in der Lage ist (Beispiel: Frühmobilisation großer Gelenke nach Schlaganfall mit Unterstützung durch Bewegungsroboter). Hier sollte versucht werden, Angehörige hinzuzuziehen. Ist dies nicht möglich, sollte eine rechtliche Vertretung gefunden werden.[2] Eine eventuell vorhandene Patient*innenverfügung ist auf alle Fälle bindend.
- *Teilhabe*: Alle Teilnehmer*innen des Projekts (Personal, Patient*innen, Angehörige) werden in das Projekt einbezogen und befragt, auch zu Verbesserungsmöglichkeiten. Alle Meinungsäußerungen sind gleichwertig zu behandeln.
- *Gerechtigkeit und Vermeiden von Diskriminierung*: Alle Personen werden ausschließlich durch Anwendung der Ein- und Ausschlusskriterien ohne Ansehen von Geschlecht, Religion oder ethnischer Gruppenzugehörigkeit einbezogen. Die erwähnten Kriterien werden *vor* der eigentlichen Untersuchung festgelegt und nachträglich nicht verändert, solange sich daraus keine ethischen Konflikte (Risikoerhöhung) ergeben. Um dies auszuschließen, werden regelmäßig Zwischenuntersuchungen anhand der bereits verfügbaren Daten durchgeführt.

2 Das gilt ausschließlich für nicht-invasive Verfahren, andernfalls sind deutlich verschärfte Bedingungen bindend.

https://doi.org/10.14361/9783839454695-005 - am 13.02.2026, 21:33:43. https://www.inlibra.com/de/agb - Open Access -

- *Privatheit*: Daten aus der Privatsphäre aller beteiligten Personen werden nur insoweit gespeichert, als sie der medizinischen Behandlung dienen und für diese unabdingbar sind. Die wissenschaftliche Auswertung findet nur unter der Minimalvoraussetzung der Pseudonymisierung der Datensätze (s.o.) statt.
- *Aufklärung*: Bei allen Klient*innen findet eine schriftliche Aufklärung statt, die im Falle der Zustimmung zur Projektteilnahme mit Unterschrift der Aufklärenden und der Patient*innen bestätigt wird. Die Aufklärenden werden vor der Durchführung des ersten Aufklärungsgesprächs im Projekt über Risiken und Gefahren geschult. Die Aufklärungsdokumente werden an zentraler Stelle aufbewahrt und vor nachträglicher Änderung geschützt. Siehe hierzu auch die Forderung nach Selbstbestimmung, beziehungsweise eingeschränkter Selbstbestimmung.
- *Sicherheit und Haftung*: Sicherheit für alle Beteiligten steht an erster Stelle und wird durch Anwendung geprüfter Technologie gewährleistet. Sollten dennoch unerwünschte Wirkungen auftreten, so werden diese dokumentiert und den zuständigen Behörden gemeldet (*Bundesinstitut für Arzneimittel und Medizinprodukte*, BfArM). Ansonsten tritt die Haftung der betreuenden Einrichtungen in Kraft, die durch eine entsprechende Pflichtversicherung abgedeckt sein muss.
- *Anwender*innenfreundlichkeit*: Um den Projekterfolg nicht zu gefährden, werden alle digitalen Verfahren anwender*innenfreundlich gestaltet und diesbezüglich optimiert (›Usability‹).
- *Vertragsabstimmung*: Klient*innen haben das Recht, im Projektverlauf aus dem Projekt jederzeit auszusteigen und die Teilnahme zu beenden (s.u.).
- *Weiterbildung*: Beteiligtes Personal wird vor Beginn einer Maßnahme ausführlich, nachvollziehbar und nachweisbar geschult, um das Risiko einer negativen Behandlungswirkung für alle Beteiligten auszuschließen.
- *Verantwortung*: Alle Projektmitarbeiter*innen und alle beteiligten Lieferant*innen werden in ihrer Verantwortung gegenüber Bedürfnissen, Wünschen und Lebensprozessen der Patient*innen belehrt; die Einhaltung wird überprüft und dokumentiert.
- *Sozialräumliche Strukturen*: Bei der Teilnehmer*innenakquise spielt weder die ökonomische Situation, die Bildung, oder Herkunft eine Rolle, außer sie sind Gegenstand der Untersuchung selbst. Alle unterstützungsbezogenen Aufwendungen werden ersetzt.
- *Technisierung*: Die eingesetzten Methoden bleiben im alltäglichen Hintergrund und tragen nicht mehr als notwendig zur Technisierung des Alltags bei. Insbesondere wird keine Technik verwendet, die aus sich selbst heraus eine Reaktion oder Eingabe der Patient*innen erfordert.

https://doi.org/10.14361/9783839454695-005 - am 13.02.2026, 21:33:43. https://www.inlibra.com/de/agb - Open Access -

Zusammenfassung

Gute Technik im Alter erfordert die Beachtung der Grundsätze von Datenschutz und digitaler Ethik, da ansonsten die Verbesserung der Lebensbedingungen durch schwerwiegende Nachteile, wie Verletzung des Persönlichkeitsrechts, Verlust der Selbstbestimmung und so weiter erkauft wird. Dies hat nicht nur Auswirkungen auf die Anwender*innen, sondern auch auf die Anbietenden: Werden derart grundlegende Werte nicht beachtet, wird vermutlich die Akzeptanz der Produkte sinken. Dabei ist es nicht so, dass Senior*innen gute Technik ablehnen würden; das Gegenteil ist eher der Fall (Demiris et al. 2004). Es herrscht ein gewisses Vertrauen von Senior*innen, dass der Einsatz von Technik das Leben im Alter erleichtert und insbesondere eine längere Selbstständigkeit ermöglichen kann. Es gilt, dieses Vertrauen nicht zu enttäuschen.

Hier wurde der Versuch unternommen, einerseits die Notwendigkeit der Digitalisierung für Ältere darzulegen, andererseits die damit verbundenen datenschutzrechtlichen und ethischen Anforderungen aufzuzeigen. Die Fülle mag überraschen und es wird schwer sein, zu jedem Einzelvorhaben alle aufgeführten Punkte zu realisieren. Ob und inwieweit dies sinnvoll ist, muss immer die Betrachtung des Einzelfalls zeigen. Zudem ist es wahrscheinlich, dass in der konkreten Durchführung eines Projekts Anforderungen auftreten, die hier nicht vorkommen, deren Einhaltung jedoch wesentlich sein können.

Literatur

Andalib, Saad/Azad, Saiful (2015): »The RSA Algorithm«, in: Saiful Azad/Al-Sakib Khan Pathan (Hg.), Practical Cryptography: Algorithms and Implementations Using C++, Boca Raton: CRC Press, 135-146.

BMFSFJ Bundesministerium für Familie, Senioren, Frauen und Jugend (2020): »Achter Altersbericht. Ältere Menschen und Digitalisierung«, https://www.bmfsfj.de/blob/159938/3970eecafb3c3c630e359379438c6108/achter-altersbericht-langfassung-data.pdf vom 02.12.2020.

Bundesärztekammer (2013): »Deklaration von Helsinki«, https://www.bundesaerztekammer.de/fileadmin/user_upload/downloads/pdf-Ordner/International/Deklaration_von_Helsinki_2013_20190905.pdf vom 02.12.2020.

Demiris, George/Rantz, Marilyn/Aud, Myra/Marek, Karen/Tyrer, Harry/Skubic, Marjorie/Hussam, Ali (2004): »Older adults' attitudes towards and perceptions of ›smart home‹ technologies: A pilot study«, in: Med. Inform. Int. Med. 29, 87-94.

Drees, Dirk (2007): ISSE/SECURE 2007 – Securing Electronic Business Processes, Braunschweig: Vieweg.

https://doi.org/10.14361/9783839454695-005 - am 13.02.2026, 21:33:43. https://www.inlibra.com/de/agb - Open Access -

Fotteler Marina/Mühlbauer Viktoria/Holl, Felix/Swoboda, Walter/Dallmeier, Daria/Denkinger, Michael (2019): »The Usefulness of Assistive Technologies for Older Adults: Preliminary Results of a Systematic Literature Review«, in: 14. Jahrestagung der DGEpi, Ulm: HNU.

Fricke, Arno (2020): »Koalition bringt E-Patientenakte Richtung Versorgung«, in: InFo Hämatol. + Onkol. 9, 60-61.

Hendrich, Ann/Chow, Marilyn/Skierczynski, Boguslaw/Lu, Zhenqiang (2008): »A 36-Hospital Time and Motion Study: How Do Medical-Surgical Nurses Spend Their Time? », in: Perm. J. 12, 25-34.

Hollier, Scott (2007): »The Disability Divide: A Study into the Impact of Computing and Internet-related Technologies on People who are Blind or Vision Impaired«, Doctoral Thesis, Faculty of Media, Society and Culture, Perth: Curtin University.

Lavander, Päivi/Meriläinen, Merja/Turkki, Leena (2016): »Working time use and division of labour among nurses and health-care workers in hospitals – a systematic review«, in: J. Nurs. Manag. 24, 1027-1040.

Nagel, Kurt/Kiefer, Erich (2008): Informationsbroschüre zum Bundesdatenschutzgesetz in der Fassung der Neubekanntmachung vom 14. Januar 2003 mit den Änderungen vom 22. August 2006, Berlin: De Gruyter.

Nöthlichs, Matthias/Weber, Horst Peter (2003): Sicherheitsvorschriften für Medizinprodukte, Berlin: Erich Schmidt.

Paul, Gerd/Stegbauer, Christian (2005): »Is the digital divide between young and elderly people increasing?«, in: First Monday 10.

Sweeney, Latanya (2002): »k-Anonymity: A Model for Protecting Privacy«, in: International Journal of Uncertainty, Fuzziness and Knowlege-Based Systems 5, 557-570.

Vereinigung der Bayerischen Wirtschaft (2020): »Zukunft der Pflege in Bayern«, https://www.wifor.com/de/studien/ vom 02.12.2020.

Voigt, Paul/von dem Bussche, Axel (2018): EU-Datenschutz-Grundverordnung (DSGVO), Berlin, Heidelberg: Springer.

https://doi.org/10.14361/9783839454695-005 - am 13.02.2026, 21:33:43. https://www.inlibra.com/de/agb - Open Access -

https://doi.org/10.14361/9783839454695-005 - am 13.02.2026, 21:33:43. https://www.inlibra.com/de/agb - Open Access -