4.2 Datenschutz und -sicherheit

Daten managen – 4 Datenpflege und Schutz

Das folgende Scary Tale des Thüringer Kompetenznetzwerks Forschungsdatenmanagement (TKFDM) zeigt, warum der Schutz von personenbezogenen Daten so wichtig ist: https://forschungsdaten-thueringen.de/geschichten/articles/20241024-der-bestohlene-dieb.html

Unterschied Datenschutz und Datensicherheit

Die Begriffe „Datenschutz“ und „Datensicherheit“ werden häufig synonym verwendet, meinen aber tatsächlich unterschiedliche Konzepte. Der Datenschutz konzentriert sich auf den Schutz von personenbezogenen Daten, also beschäftigt sich mit Fragen, welche Daten überhaupt verarbeitet werden dürfen und ob dies rechtmäßig und zweckgebunden passiert. Datensicherheit ist der technische und organisatorische Bestandteil des Ganzen und schützt nicht nur personenbezogene – sondern alle – Daten vor unbefugtem Zugriff, Verlust oder Beschädigung. Datensicherheit ist also eine notwendige Voraussetzung für den Datenschutz.

Schutz von personenbezogenen Daten

Insbesondere Gesundheitsdaten erfordern einen besonderen Schutz, da sie häufig sensible Informationen enthalten und sich gegebenenfalls auch mit vulnerablen Personengruppen beschäftigen. Sie werden zwar von Forschenden erhoben, aber gehören im ethischen Sinne den Teilnehmenden. Der Begriff „Datenschutz“ ist hierbei missverständlich: Es geht nicht um den Schutz der Daten, sondern den Schutz von Personen!

Im europäischen Raum gibt die DSGVO (Datenschutz-Grundverordnung), insb. Artikel 5 (Grundsätze für die Verarbeitung personenbezogener Daten) und 9 (Verarbeitung besonderer Kategorien personenbezogener Daten), den Rahmen und die Grundlage für den richtigen Umgang mit personenbezogenen Daten. Im Folgenden werden kurz die wichtigsten rechtlichen Vorgaben zum Management von Gesundheitsdaten dargestellt. Weitere und detailliertere Informationen zu den rechtlichen Aspekten im Umgang mit Gesundheitsdaten finden sie im Modul „Ethische, rechtliche und soziale Betrachtung“.

Anonymisierung und Pseudonymisierung

Insbesondere für die Forschung muss die Identität der datengebenden Personen geschützt werden. Die Identität von Personen kann dabei auf unterschiedliche Arten bewahrt werden: Konkret spricht man von Anonymisierung und Pseudonymisierung.

Es wird zwischen drei Graden der Anonymisierung unterschieden:

- **Formal:** Alle direkten Identifizierungsmerkmale wie Eigennamen, Bilder und Stimmen werden entfernt.
- **Faktisch:** Daten werden so verändert (meist Informationen mit Personenbezug entfernt), dass Rückverfolgung zu der spezifischen Person nur mit unverhältnismäßig großem Aufwand an Zeit, Kosten oder Arbeitskraft möglich ist.
- **Absolut:** Die Daten werden so verändert, dass die Re-Identifizierung einer Untersuchungsperson unmöglich ist.

Bei der Pseudonymisierung werden Identifikationsmerkmale durch willkürlich gewählte Kennzeichen (Pseudonyme) ersetzt. So wird die Eindeutigkeit dieses Werts gewahrt, aber es wird schwieriger Rückschlüsse auf einen ursprünglichen Datenwert zu ziehen. Die Re-Identifikation von einzelnen Datenwerten bleibt also

Gefördert durch:
Bundesministerium für Forschung, Technologie und Raumfahrt
Finanziert von der Europäischen Union
NextGenerationEU

möglich, wenn der Zuordnungsschlüssel von Pseudonym und Daten bekannt ist. Auch pseudonyme Daten sind personenbezogene Daten und unterfallen somit immer noch dem Datenschutzrecht.

Die folgende kurze Geschichte aus der Scary Tale-Reihe des Thüringer Kompetenznetzwerks Forschungsdatenmanagement (TKFDM) zeigt anschaulich, warum eine Anonymisierung häufig nicht so simpel ist, wie man denkt, und einige Überlegungen und Abwägungen bei der Datenerhebung getätigt werden müssen, um die Identität der Forschungsteilnehmer:innen zu schützen: https://forschungsdaten-thueringen.de/geschichten/articles/20211029-wer-bin-ich.html

Neben den eindeutigen Identifikationsmerkmalen sollten auch Rücksicht auf Datenkombinationen genommen werden: Beispielsweise ist das Alter an sich kein eindeutiges Identifikationsmerkmal, aber je nach Datensatz kann durch das gegebene Alter, Geschlecht, Wohnort, Ethnie und sexuelle Orientierung eine Person durch Dritte eindeutig identifiziert werden. Eine faktische oder absolute Anonymität ist also meist schwer oder gar nicht erreichbar, ohne relevante Informationen zu verlieren. Deswegen müssen häufig weitere Maßnahmen ergriffen werden, um die Identität von Personen zu schützen.

Bei der Aggregation werden Informationen „vergröbert“ und zu Klassen und Kategorien zusammengefasst, um den Personenbezug zu erschweren. Beispielsweise wird - anstatt das konkrete Alter einer Person zu speichern - die Kategorie „21-30 Jahre“ zugewiesen oder statt des konkreten Wohnorts wird nur das Bundesland gespeichert. Bei der Wahl der Kategoriengröße sollte sich die Stichprobe angeschaut werden. Es macht keinen Sinn eine Kategorie der Variable Einkommen von „> 10.000 € im Monat“ zu bilden, wenn diese bei einer Zufallsbefragung der durchschnittlichen Gesellschaft nur einen einzelnen seltenen Randwert umfasst. Bei einer Befragung unter Spitzen-Verdienern macht eine solche Kategorie wiederum Sinn. Eine Faustregel der empirischen Forschung besagt, dass Variablenausprägungen mindestens 5 Personen im Datensatz zugeordnet werden sollten.

Personen-bezogene Daten	Original	Anonymisierung/ Starke Abstraktion	Pseudonym-isierung	Aggregation
Name	Van der Pol	Person	De Weerdt	Frau
Geschlecht	Frau	Person	Herr	Frau
Wohnort	Köln	Ort	Düsseldorf	Nordrhein-Westfalen
Geburtsjahr	1995	Jahr	1997	Zwischen 1991 und 2000
Berufs-bezeichnung	Gymnasiallehrerin	Beruf	Erzieher	Pädagogischer Beruf

Anleitungen, Beispielszenarien und Materialien zur Anonymisierung und Pseudonymisierung finden sich zusammengestellt vom Projekt „GesundFDM“ unter folgenden Links:

- https://www.gesund-fdm.de/anonymisierung-pseudonymisierung-von-daten/
- https://www.gesund-fdm.de/pseudonymisierungsmodelle/

Datensicherheit

Situationen die Sicherheitsbedenken in Bezug auf Daten auslösen sieht man im Arbeitsalltag immer wieder: Papierakten liegen offen rum. Der Rechner ist nicht mit einem Passwort geschützt (oder dieses ist mit einem Post-it an den Bildschirm geklebt) und wird häufig offen oder unbeaufsichtigt gelassen. Dokumente werden, wenn sie gelöscht werden sollen, nur in den Papierkorb verschoben. Daten werden über Fax oder unverschlüsselte Mails geteilt.

Gefördert durch:
Bundesministerium für Forschung, Technologie und Raumfahrt
Finanziert von der Europäischen Union
NextGenerationEU

Offener Zugang zu Dokumenten ist brandgefährlich, egal ob analog oder digital. Ziel von Datensicherheitsmaßnahmen ist es, Daten vor Datendiebstahl zu schützen, Missbrauch von Daten zu verhindern und die sensiblen Daten von Personen zu schützen.

Corti et al. formulieren drei Ebenen der Datenverschlüsselung, durch die die Datensicherheit erreicht werden soll:

- **Physische Sicherheit (der physische Zugriff auf die Daten wird geschützt):**
  Diese ist realisierbar durch beschränkten Zugang zu Gebäuden und das Einschließen von Dokumenten (entweder in physischer oder digitaler Form, als Akten oder Datenträger). Computer können mit Gehäusen oder Klemmen vor Mitnahme gesichert werden, sensible Daten sollten nur in Ausnahmefällen transportiert werden und Dokumente sollen nicht unverschlossen in Hotelzimmern gelassen werden. Eine saubere Entsorgung von Dokumenten und digitalen Daten kann durch Softwareoptionen, die eine Wiederherstellung von Daten verhindern (vgl. Datenpflege), sowie eine physische Vernichtung durch Schreddern oder Zerschlagen von Festplatten erreicht werden. Bildschirme sind so zu platzieren, dass sie nur durch die datenverarbeitenden Personen eingesehen werden können und nicht von Externen. Beispielsweise sollte der Bildschirm in einer Behandlungszimmer von den für Patient:innen vorgesehene Plätze weggerichtet sein oder sogar in für diese unzugängliche Bereiche platziert werden. Nach einer gewissen Zeit ohne Benutzerinteraktion sollte sich ein passwortgeschützter Bildschirmschoner einschalten.
- **Netzwerksicherheit:**
  Sensible Daten sollten nur auf internen Servern gespeichert werden, Firewalls sollten auf dem neusten Stand gehalten und regelmäßig aktualisiert werden, Anti Virus Software sollten regelmäßig geupdatet werden. Jegliche Funktionen, Serverdienste und offene Kommunikationsports nach außen ermöglichen eine Sicherheitslücke, weswegen die Notwendigkeit dieser insbesondere bei Computern mit darauf gespeicherten sensiblen Daten geprüft werden sollte.
  Für Arztpraxen existiert die Empfehlung den Computer mit Patient:innendaten nicht direkt mit dem Internet zu verbinden.
- **Informations- und Computersicherheit:**
  Daten sollten zusätzlich durch Authentifikation absichert werden. Das heißt nur Personen die beweisen können, wer sie sind und dass sie die Berechtigung haben, erhalten Zugriff. Die Authentifikation kann passieren durch
  1. Etwas, das man weiß, wie z.B. Passwörter. Hierbei ist es wichtig, sichere Passwörter wählen. Sie sollten also lang genug sein, keine Begriffe die im Wörterbuch stehen sein und möglichst komplex aus Buchstaben, Zahlen und Sonderzeichen zusammengesetzt sein. Individuelle Passwörter sollten nicht weitergeben werden, nicht offensichtlich schriftlich festhalten werden (der Klassiker hier ist ein Post-it am Bildschirm) und nicht mehrmals verwendet werden.
  2. Etwas, das man hat, wie z.B. Schlüssel oder Smart Cards.
  3. Etwas über einen selbst z.B. Fingerabdrücke, Face ID, Stimmerkennung.
  Für noch mehr Sicherheit kann man noch einen Schritt weitergehen und eine Zwei-Schritte-Verifizierung nutzen, um Zugriff für Unbefugte noch mehr zu erschweren. Beispielsweise hätte ein Dieb so trotz gestohlenem Passwort keinen Zugriff, wenn Zusätzlich noch mit einem Fingerabdruck entsperrt werden muss.
  Möglich sind auch rollenbasierte Zugänge z.B. durch Benutzerkonten: Hier sollte sich die Frage gestellt werden, welche Rollen die unterschiedlichen beteiligten Personen haben und welche Rechte diese Personen (nur Lesen, Schreibberechtigung, eigene

Gefördert durch:
Bundesministerium für Forschung, Technologie und Raumfahrt
Finanziert von der Europäischen Union
NextGenerationEU

Dateien anlegen,…) auf welche Daten haben (für alles, je nach Order oder spezifische Dateien?).
Es gibt auch automatische Verschlüsselungsoptionen der verschiedenen Betriebssysteme, die Festplatten vor fremden Zugriffen schützt wie z.B. FileVault für Mac, Bitlocker für Windows oder dm-crypt für Linux.

Datenübermittlung

Um Daten zu übermitteln existieren vielfältige Optionen:

Fax: Das Fax stammt noch aus einer Zeit, in der Datenschutz kaum bis gar kein Thema war. Das spiegelt sich auch in der Sicherheit dieses Übertragungsmediums wieder: Die Dokumente werden offen und unverschlüsselt übermittelt und können von jedem, der Zugang zu dem Empfängergerät hat, eingesehen werden. Eine Zugriffskontrolle kann nicht gewährleistet werden. Auch kann es zu Übermittlungsfehlern kommen und das Fax landet (unbemerkt) an einer ganz anderen Adresse. Gerade vertrauliche Daten sollten deswegen auf gar keinen Fall per Fax übermittelt werden.

E-Mail: Eine (unverschlüsselte) Mail ist vergleichbar mit einer Postkarte: Jeder kann theoretisch mitlesen, was drauf bzw. drinnen steht. Deswegen müssen sensible Daten in E-Mails zusätzlich mit Verschlüsselung geschützt werden. Meist ist die Dateigröße, die man im Anhang versenden kann auch stark begrenzt, je nach Anbieter, weswegen für größere Datenmengen auf andere Optionen zurückgegriffen werden muss.

Datenübertragungs- und Clouddienste: Dropbox, Google Drive, Microsoft OneDrive, WeTransfer und Co bieten unterschiedliche Modelle, um auch größere Daten teilen zu können. Meist ist das Teilen bis zu einer bestimmten Datenmenge kostenlos, danach wird ein kostenpflichtiges Abo verlangt. Bei WeTransfer wird zusätzlich damit geworben, dass die Daten nur kurzfristig gespeichert werden. Bei alle diesen Anbietern können Sicherheitsbedenken angemerkt werden, da die Daten teilweise unverschlüsselt auf US-amerikanischen Servern gespeichert werden. Zertifikate wie TCDP (Trusted Cloud Datenschutz-Profil), EuroCloud-Star-Audit und TÜV-Prüfzeichen bestätigen die Einhaltung von DSGVO-Vorgaben. Achtung: Häufig wird auch die internationalen Norm ISO/IEC 27001 aufgeführt, diese weist aber nur strukturierte Prozesse für die Informationssicherheit nach, trifft aber keine Aussage über die tatsächlich eingesetzten Sicherheitsmaßnahmen. Merkmale eines sicheren Cloud-Dienstes sind Serverstandorte in der EU oder Ländern mit vergleichbarem Datenschutzniveau, Datenschutzmaßnahmen wie Verschlüsselung, regelmäßige Sicherheitsupdates und Backups, sichere Zugriffskontrollen z.B. durch Mehr-Faktor-Authentifizierung und transparente Nutzungsbedingungen. Auf https://www.trusted-cloud.de/, der Seite des gemeinnützige Vereins Kompetenznetzwerk Trusted Cloud finden sich Listungen von vertrauenswürdigen Cloud Services & Dienstleistern.

Am sichersten ist schlussendlich die Übertragung von Daten verschlüsselt auf portablen Datenträgern mit persönlicher Entgegennahme.

Datenschutz in Arztpraxen

Patient:innendaten dürfen nur unter bestimmten Voraussetzungen erhoben, gespeichert, genutzt und verarbeitet werden. Patient:innen müssen hierfür zustimmen und die Daten müssen den gesundheitlichen Interessen des/der Patient:in dienen z.B. für Vorsorge, Diagnostik oder Behandlung.

Für niedergelassene Ärzt:innen in Arztpraxen formulieren die DSGVO und das Bundesdatenschutzgesetz (BDSG) für die Verarbeitung von

Gefördert durch:
Bundesministerium für Forschung, Technologie und Raumfahrt
Finanziert von der Europäischen Union
NextGenerationEU

Gesundheitsdaten Rechenschafts- und Nachweispflichten, denen mit einem guten Datenschutzmanagement und der Führung eines Verzeichnisses von Verarbeitungstätigkeiten begegnet werden kann. Aus § 22 BDSG ergibt sich, dass Verarbeitung von Gesundheitsdaten bei der ärztlichen Behandlung (unter der Bearbeitung von Personen mit Geheimhaltungspflicht (Art. 9 Abs. 3 i. V. m. § 22 Abs. 1 Nr. 1 Buchst. b BDSG), zur Erfüllung spezieller Pflichten aus dem Sozialrecht oder im öffentlichen Gesundheitsinteresse, zum Schutz lebenswichtiger Interessen bei Einwilligungsunfähigkeit des Patienten oder zur Wahrung von Rechtsansprüchen erlaubt ist.

Arztpraxen sind hierbei zur Führung eines Verzeichnisses von Verarbeitungstätigkeiten von Gesundheitsdaten verpflichtet (Art. 30 DSGVO). Eine Muster-Vorlage und weitere Hinweise dazu werden von der deutschen Aufsichtsbehörde für Datenschutz gegeben und Hinweise zur Erstellung von der Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie (GMDS) e.V.. Wenn die Form der Verarbeitung aufgrund von Art, Umfang, Umstand oder Zweck voraussichtlich ein hohes Risiko für den Datenschutz hat, ist zusätzlich eine Datenschutz-Folgeabschätzung zu tätigen (Artikel 35 DSGVO). Eine solche Folgenabschätzung enthält nach den Vorgaben von Art. 35 Abs. 7 DSGVO eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und deren Zwecke, darauf basierend eine Bewertung von Notwendigkeit und Verhältnismäßigkeit, eine Bewertung der Risiken für die Patienten sowie die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen. Ergibt sich aus dieser Folgenabschätzung ein zu hohes Risiko muss die zuständige Aufsichtsbehörde kontaktiert werden.

Die KBV bietet für Praxisteams und Niedergelassene einen Praxischeck zur Bewertung von Datenschutz und Informationssicherheit in der eigenen Praxis an. Dieser ist hier zu finden.

Quellenverzeichnis

Bundesamt für Sicherheit und Informationstechnik (2021). Cloud: Risiken und Sicherheitstipps. Abgerufen am 30.09.2025, von https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cloud-Computing-Sicherheitstipps/Cloud-Risiken-und-Sicherheitstipps/cloud-risiken-und-sicherheitstipps_node.html

Bundesärztekammer & Kassenärztliche Bundesvereinigung (2021). Hinweise und Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis. Deutsches Ärzteblatt. https://doi.org/10.3238/arztebl.2021.ds02. Abgerufen am 30.09.2025, von https://www.kbv.de/documents/infothek/rechtsquellen/weitere-vertraege/praxen/datenschutz-schweigepflicht/Empfehlungen_aerztliche_Schweigepflicht_Datenschutz.pdf

Canavan, MJ, McGinty, S, Reznik-Zellen, R (2022). Module 4: Data Storage, Backup and Security. New England Collaborative Data Management Curriculum. Abgerufen am 30.09.2025, von https://oercommons.org/courses/new-england-collaborative-data-management-curriculum

Ford, S. (2014). Information Security : Physical Information Security (06:02). Abgerufen am 30.09.2025, von https://www.youtube.com/watch?v=b70-hr8RLzM

Ford, S. (2014). Information Security : Authentication (06:03). Abgerufen am 30.09.2025, von https://www.youtube.com/watch?v=t4kTgjQabV4

Kramer, P. (2020). Datenschutz im Betrieb. Eine Handreichung für Beschäftigte. Abgerufen am 30.09.2025, von

Gefördert durch:

Bundesministerium für Forschung, Technologie und Raumfahrt

Finanziert von der Europäischen Union
NextGenerationEU

https://stiftungdatenschutz.org/fileadmin/Redaktion/Dokumente/Broschuere/SDS_Datenschutz_im_Betrieb_SDS_2022-12_DE_Web.pdf

Mcleod, J. (2022). DATUM for Health: Research data management training for health studies. Abgerufen am 30.09.2025, von https://oercommons.org/courses/datum-for-health-research-data-management-training-for-health-studies

Mertzen, D., Neuroth, H., Schneemann, C., Woywod, K., Haase, C., Jacob, B., Kroehling, M., Mittelbach, J., Straka, J., Szczukowski, A., & Weise, K. (2023). Zertifikatskurs "Forschungsdatenmanagement für Studierende": Spring School 2023 der Landesinitiative für Forschungsdatenmanagement in Brandenburg. Zenodo. https://doi.org/10.5281/zenodo.7936966

RatSWD [Rat für Sozial- und Wirtschaftsdaten] (2020). Handreichung Datenschutz. 2. vollständig überarbeitete Auflage. RatSWD Output 8 (6). https://doi.org/10.17620/02671.50

Weiterführende Info

Bundesärztekammer & Kassenärztliche Bundesvereinigung (2021). Hinweise und Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis. Deutsches Ärzteblatt. https://doi.org/10.3238/arztebl.2021.ds02. Abgerufen am 30.09.2025, von https://www.kbv.de/documents/infothek/rechtsquellen/weitere-vertraege/praxen/datenschutz-schweigepflicht/Empfehlungen_aerztliche_Schweigepflicht_Datenschutz.pdf

Ebel, T.; Meyermann, A. (2015). Hinweise zur Anonymisierung von quantitativen Daten. Frankfurt am Main : DIPF | Leibniz-Institut für Bildungsforschung und Bildungsinformation 2015, 11 S. -(forschungsdaten bildung informiert; 3) - URN: urn:nbn:de:0111-pedocs-219703 - DOI:10.25656/01:21970

Ford, Scott (2014). Information Security : Protecting Your Data (06:02). Abgerufen am 30.09.2025, von https://www.youtube.com/watch?v=WBulJytSnak

Koch, H., Schütze, B., Spyra, G., & Wefer, M. (2017). Datenschutzrechtliche Anforderungen an die medizinische Forschung unter Berücksichtigung der EU Datenschutz-Grundverordnung (DS-GVO). Abgerufen am 30.09.2025, von https://gesundheitsdatenschutz.org/download/forschung_ds-gvo.pdf

Meyermann, A.; Porzelt, M. (2014). Hinweise zur Anonymisierung qualitativer Daten. Frankfurt am Main : DIPF | Leibniz-Institut für Bildungsforschung und Bildungsinformation 2014, 17 S. - (forschungsdaten bildung informiert; 1) - URN: urn:nbn:de:0111-pedocs-219682 - DOI: 10.25656/01:21968

Gefördert durch:
Bundesministerium für Forschung, Technologie und Raumfahrt
Finanziert von der Europäischen Union
NextGenerationEU

Das Material ist im Rahmen des Projekts „DIM.RUHR: Datenkompetenzzentrum für die interprofessionelle Nutzung von Gesundheitsdaten in der Metropole Ruhr“ (Förderkennzeichen: 16DKZ2008[A-F]) entstanden. Dementsprechend spiegelt das Material in Version 1.0 den Stand von 2025 wider.

„Daten managen - 4.2 Datenpflege und -schutz – Datenschutz und -sicherheit“ von Anne Mainz und Sven Meister.

Gefördert durch:
Bundesministerium für Forschung, Technologie und Raumfahrt
Finanziert von der Europäischen Union
NextGenerationEU