Glossar zur Orientierungshilfe Krankenhausinformationssysteme

Anonyme Daten

Gemäß EG 26 DSGVO handelt es sich bei anonymen Daten um Informationen, die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen oder um ehemals personenbezogene Daten, die auf eine Weise verändert (anonymisiert) wurden, dass die Person nach allgemeinem Ermessen nicht mehr identifiziert werden kann.

Anonymisierung

Anonymisierung ist eine Verarbeitung personenbezogener Daten, deren Ergebnis nicht (mehr) personenbezogen ist und dementsprechend nicht der DSGVO unterliegt. Ob personenbezogene Daten tatsächlich anonymisiert worden sind oder ob pseudonymisierte Daten für den jeweiligen Verantwortlichen (noch) personenbezogene Daten darstellen, hängt insbesondere davon ab, ob die entsprechenden Maßnahmen aufgehoben werden können und ob im Einzelfall andere Mittel zur Zuordnung zur Verfügung stehen[1].

Archiv (Altfälle)

Datenbestand mit Daten aus abgeschlossenen Behandlungsfällen, für die die Behandler nach Bundes- oder Landesrecht eine Aufbewahrungspflicht haben. Das Archiv wird gebildet durch Überführung von Daten aus dem laufenden Bestand in ein Archivsystem bzw. die → ***Trennung von Datenbeständen***. Archivdaten bleiben logisch Teil der → ***Patientenakte***. Für den Zugriff auf Archivdaten gelten besondere Berechtigungen. Diese Anforderung geht zurück auf gesetzliche Anforderungen. Der hier verwendete Archivbegriff meint nicht Archive im Sinne der Archivgesetze oder Archive, die aus Performancegründen gebildet werden und Daten aufnehmen, auf die über einen definierten Zeitraum nicht mehr zugegriffen wurde, die jedoch bei Bedarf direkt bereitgestellt werden können. Im letztgenannten Fall muss das Rollen- und Berechtigungskonzept greifen, welches auch für den laufenden Bestand gilt.

Behandlungsfall

Eine medizinische Behandlung umfasst alle Anamnese-, Diagnose-, Therapie- und Nachbehandlungsmaßnahmen zu derselben Krankheit, Verdachtsdiagnose oder Symptomatik, wegen der die Patientin bzw. der Patient stationär aufgenommen wurde. Medizinisch kann eine Behandlung aus mehreren ambulanten und stationären Behandlungsfällen bestehen und über Jahrzehnte andauern (chronische Krankheiten). Unter Behandlungsfall ist bei einer stationären Behandlung die gesamte Behandlung derselben Erkrankung zu verstehen, die ein Patientin bzw. ein Patient

[1] Vgl. EuGH C-413/23

in einem Krankenhaus von der stationären Aufnahme bis zur Entlassung aus der stationären Behandlung erhält. Eingeschlossen sind die dem Behandlungsfall zuzuordnenden vor- und nachstationären Behandlungen im Sinne von § 115a SGB V, sowie Wiederaufnahmen innerhalb der oberen Grenzverweildauer im Sinne von § 8 Abs. 5 Krankenhaus-Entgeltgesetz (KHEntG).

Cloud-Computing-Dienst

Ein Cloud-Computing-Dienst ist ein digitaler Dienst, der auf Abruf die Verwaltung und den umfassenden Fernzugang zu einem skalierbaren und elastischen Pool gemeinsam nutzbarer Rechenressourcen ermöglicht, auch wenn diese Ressourcen auf mehrere Standorte verteilt sind (Legaldefinition aus § 384 Satz 1 Nr. 5 SGB V).

Confidential Cloud-Computing

Unter dem Begriff „Confidential Cloud Computing" [2] wird nicht eine einzige Technologie, sondern die Summe verschiedener Maßnahmen wie bspw. eine Verschlüsselung von Daten im Arbeitsspeicher oder aber auch eine reine Zugriffsbeschränkung auf reservierte Speicherbereiche verstanden. Sie kann das allgemeine Sicherheitsniveau erhöhen und typischerweise einen wertvollen Schutz gegen andere Nutzende auf der gleichen Hardware und gegen einzelne Innentäter bieten. Grundsätzlich ist davon auszugehen, dass ein Cloud-Betreiber Zugriffsmöglichkeiten auf die zu schützenden Daten besitzt.

Elektronische Patientendaten

Elektronische Patientendaten sind alle in einem → ***Krankenhausinformationssystem (KIS)*** verarbeiteten administrativen und klinischen Daten einer Patientin oder eines Patienten.

Fallakte

Alle Daten, die einem → ***Behandlungsfall*** zugeordnet sind. Alle Fallakten zusammen bilden die → ***Patientenakte***.

Funktionsbezogene Organisationseinheit

Eine funktionsbezogene Organisationseinheit (OE) ist eine kleinste organisatorische Einheit innerhalb eines → ***Krankenhauses***, in der Patientinnen bzw. Patienten von einer oder interdisziplinär von mehreren Fachrichtungen behandelt, gepflegt oder versorgt werden - z.B. eine Fachabteilung, eine Gruppe von Konsiliarärztinnen oder -ärzten, eine Station, ein Labor, eine Abteilung für Medizincontrolling und ähnliches. Die OE kann sich somit je nach Berufsgruppe unterscheiden. Während Ärzte häufig auf die Daten aller Patientinnen und Patienten eines Fachbereichs Zugriff haben, umfassen die pflegerischen OEs eine oder mehrere Stationen innerhalb dieses Fachbereichs. Abzugrenzen sind diese von größeren Versorgungsbereichen (z.B. Zentren). Patientinnen bzw. Patienten und Krankenhausbeschäftigte können mehreren funktionsbezogenen Organisationseinheiten zugeordnet sein.

[2] Entschließung Confidential Cloud Computing, verfügbar unter: https://www.datenschutzkonferenz-online.de/media/en/DSK-Entschliessung_Confidential_Cloud_Computing.pdf

Identifikationsdaten

Unter Identifikationsdaten fallen insbesondere folgende Daten: Vor- und Zuname, Geburtsname, Geburtsdatum, Geburtsort, Geschlecht, Titel, Anschrift, Krankenversichertennummer, Patienten-ID.

Konsil / Konsiliardienst

Konsil ist die patientenbezogene Beratung der behandelnden Ärztin bzw. des behandelnden Arztes durch eine andere Ärztin bzw. einen anderen Arzt. Konsiliardienst ist das in einem Krankenhaus bestehende Angebot zur Beurteilung und Mitbetreuung von Patientinnen und Patienten, das von den behandelnden Ärztinnen und Ärzten für deren Patientinnen bzw. Patienten angefordert werden kann.

Krankenhaus

Ein Krankenhaus ist ein zusammengehörender Funktionskomplex im Sinne von § 107 SGB V. Welche Einrichtungen als zusammengehörig betrachtet werden, kann nach den jeweiligen Landeskrankenhausplänen, dem Auftreten unter einheitlichem Institutskennzeichen nach § 293 SGB V und der Existenz einer einheitlichen ärztlichen Leitung beurteilt werden. Die Orientierungshilfe richtet sich primär an Krankenhäuser im Sinne des § 107 Abs. 1 SGB V. Soweit die einzelnen Empfehlungen dem Sinn nach auf Vorsorge- und Rehabilitationseinrichtungen nach § 107 Abs. 2 SGB V anwendbar sind, können sie auch diesen als Orientierungshilfe dienen. Krankenhausketten oder -konzerne zählen nicht als ein Krankenhaus. Unabhängig von der Einordnung als Krankenhaus bestimmt sich die Einordnung als datenschutzrechtlich Verantwortlicher nach den Vorgaben der Datenschutz-Grundverordnung, der Landeskrankenhaus- und Datenschutzgesetze und der kirchlichen Rechtsvorschriften.

Krankenhausinformationssystem (KIS)

Unter dem Begriff Krankenhausinformationssystem wird die zentrale Arbeitskomponente für den Prozess der medizinischen Versorgung des Patienten verstanden. Das KIS führt in der Regel die zentrale Patientenakte und enthält administrative Daten, Abrechnungsdaten und medizinische Daten. An das KIS angebunden sind diverse Subsysteme wie Laborinformationssystem, Radiologieinformationssystem, DMS oder Spezialsysteme, für die die Anforderungen an das KIS entsprechend auch gelten.

Krankenhauskonzern

Unternehmen, das mehrere Krankenhäuser sowie ggf. auch andere medizinische Einrichtungen betreibt.

Löschung

Löschung bedeutet die irreversible Unkenntlichmachung gespeicherter personenbezogener Daten. Eine Markierung von Daten als „gelöscht", mit der Folge, dass die Daten lediglich nicht mehr angezeigt werden, ist keine Löschung.

Mandantenfähigkeit

Der abgeschlossene Datenhaltungs- und Verarbeitungszusammenhang eines im datenschutzrechtlichen Sinne Verantwortlichen wird in diesem Papier nachfolgend als "Mandant" bezeichnet, die getrennte Speicherung und Verarbeitung als "Mandantentrennung". Ein Verfahren ist "mandantenfähig", wenn Patientendaten mandantenbezogen geführt und Verarbeitungsfunktionen, Zugriffsberechtigungen und Konfigurationseinstellungen je Mandant eigenständig festgelegt werden können.

Medizinisches Versorgungszentrum (MVZ)

Eigenständige rechtliche Einheit, in denen mehrere ambulant tätige Ärztinnen und Ärzte in gleicher oder verschiedener Fachrichtung und gegebenenfalls weitere Berufsgruppen kooperativ zusammenarbeiten. MVZ stehen unter ärztlicher oder gegebenenfalls kooperativer Leitung. MVZ im Sinne dieser Orientierungshilfe sind nur solche, die von einem Krankenhaus oder den Trägern des Krankenhauses gegründet werden (vgl. § 95 SGB V).

Mitbehandlung

Als Mitbehandlung stellen sich alle von der behandelnden Ärztin bzw. dem behandelnden Arzt veranlassten Leistungen Dritter zur medizinischen Versorgung einer Patientin bzw. eines Patienten dar.

Patientenakte

Die Gesamtheit aller zu einer Patientin bzw. einem Patienten in einem Krankenhaus im Hinblick auf die Behandlung relevanten verarbeiteten Patientendaten.

Patientenaktensystem (PAS)

Das PAS ist das Subsystem des KIS, das Krankengeschichten und Pflegedokumentationen einschließlich Anamnese- und Befunddaten, Diagnosen und Arztbriefen etc. aufnimmt. Es stellt Funktionen zur Patientenverwaltung, Behandlungsplanung und -dokumentation sowie ggf. zur Abrechnung zur Verfügung. Es ist abzugrenzen von anderen Subsystemen des KIS wie Labor- oder Radiologieinformationssystemen oder einzelnen mit dem KIS verbundenen Diagnosegeräten.

Pseudonymisierte Daten

Pseudonymisierte Daten sind das Resultat einer Verarbeitung personenbezogener Daten, das ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden kann. Pseudonymisierte Daten sind keine eigene Kategorie von Daten, sondern abhängig vom Kontext in der Regel personenbezogen oder aber bei erweiterten Maßnahmen auch bedingt anonym.

Pseudonymisierung

Pseudonymisierung ist eine technische und organisatorische Maßnahme im Sinne der Art. 25, 32 DSGVO, die die Risiken für die betroffenen Personen senken und den Verantwortlichen oder Auftragsverarbeitung bei der Einhaltung ihrer Datenschutzpflichten unterstützen kann. Dabei werden

durch eine Pseudonymisierungstransformation Teile der Originaldaten durch ein oder mehrere → ***Pseudonyme*** ersetzt.

Pseudonym

Ein Pseudonym ist das Ergebnis des Ersetzens aller Identitätsdaten einer Patientin bzw. eines Patienten durch einen Identifikator, der der betroffenen Person nur unter Verwendung zusätzlicher Informationen zugeordnet werden kann. Zur Abgrenzung vgl. → ***temporäres Patientenkennzeichen***.

Rolle

Zuständigkeit eines Beschäftigten innerhalb einer Organisation (*strukturelle Rolle*) bzw. Aufgabe, die zugewiesen oder auf Grund bestehender Fachkompetenz übernommen wurde (*funktionelle Rolle*). Strukturelle Rollen sind über längere Zeiträume statisch. Funktionelle Rollen wechseln in Abhängigkeit vom Bezug der Tätigkeit zu der Behandlung der konkreten Patienten, auf deren Daten zugegriffen werden soll. Technisch wird unter einer Rolle oft ein Bündel von Zugriffsberechtigungen verstanden, die aus den Erfordernissen einer strukturellen Rolle abgeleitet sind. Funktionelle Rollen hingegen werden durch → ***Verarbeitungskontexte*** abgebildet, durch welche die Ausübung bestehender Zugriffsrechte auf das für die jeweilige Aufgabe erforderliche Maß beschränkt wird.

Rollen- und Berechtigungskonzept

Ein Rollen- und Berechtigungskonzept stellt eine strukturierte Zugriffsrechtevergabe dar. In dem Berechtigungskonzept werden Zugriffsbefugnisse von Mitarbeitenden auf bestimmte Daten und Anwendungen festgelegt.

Sonderzugriff, Notfallzugriff

Sonderzugriffsrechte wie im Falle eines medizinischen Notfalls sollen unvorhersehbare, dringende, zum sofortigen medizinischen Eingreifen erforderliche, jedoch anders nicht erfüllbare Verarbeitungsbedarfe befriedigen. Sie gehen über die beschränkte Rollen- und Aufgaben-bezogene Berechtigung zum Zugriff auf Patientendaten hinaus.

Sperrung bzw. Einschränkung der Verarbeitung

Die Einschränkung der Verarbeitung, umgangssprachlich auch als „Sperren" bezeichnet, ist das Kennzeichnen von Daten, um ihre weitere Verarbeitung im Sinne des Art. 4 Nr. 3 DSGVO einzuschränken. Auf gesperrte Daten kann nur noch unter eng begrenzten Voraussetzungen zugegriffen werden. Beispiele für entsprechende Sperren sind die als technisch-organisatorische Maßnahme erforderlichen Einschränkungen der Zugriffsrechte nach Abschluss der Behandlung. Um eine Sperrung handelt es sich auch dann, wenn die betroffene Person wirksam die Einschränkung der Verarbeitung im Sinne von Art. 18 DSGVO verlangt hat.

Temporäres Patientenkennzeichen

Ein temporäres Patientenkennzeichen ist das Ergebnis des Ersetzens der Identitätsdaten einer Patientin bzw. eines Patienten zu dem Zweck, diese bei der Verarbeitung *vorübergehend* zu verbergen. Dies kann z.B. in einem → **Verarbeitungskontext** Schulung sinnvoll sein, in welchem zwar die Systemfunktionen und Ausgabemasken wie unter Realbedingungen funktionieren und dargestellt werden, gleichzeitig aber identifizierende Merkmale von Patientinnen und Patienten verborgen bleiben sollen. Ein Beispiel wäre das Ersetzen des Namens mit einem generischen Begriff wie „Patient:in" ergänzt um eine fortlaufende Nummer.

Trennung von Datenbeständen

Trennung von Datenbeständen bedeutet die Organisation der Datenhaltung in einer Weise, die es erlaubt, Datenbestände funktional getrennt voneinander zu verarbeiten. Die Trennung kann durch physische Abgrenzung (z.B. Speicherung in verschiedenen Datenbankinstanzen oder auf unterschiedlichen Systemen) oder innerhalb eines Bestandes durch logische Differenzierung, durch Speicherung in separaten Datenbanktabellen und Verzeichnisstrukturen oder anhand entsprechender Kennzeichnungen sichergestellt werden.

Verarbeitungskontext

Als Verarbeitungskontext wird der sachliche und technische Zusammenhang bezeichnet, in dem Nutzende des KIS in einer bestimmten funktionellen Rolle Patientendaten verarbeiten. Verarbeitungskontexte leiten sich aus den Verarbeitungszwecken ab und verfeinern diese. Beispiele für Verarbeitungskontexte sind Behandlung der der eigenen OE zugeordneten Patientinnen und Patienten, Pflege einer Stationspatientin bzw. eines Stationspatienten, OP-Assistenz, DRG-Controlling usw. Ein Verarbeitungskontext wird im KIS über kontextbezogene Benutzerrollen, Daten- und Funktionszugriffe und Bildschirmmasken abgebildet. So unterscheidet sich z.B. eine Suchfunktion bzw. die Präsentation von deren Ergebnissen im Verarbeitungskontext „Patientenaufnahme" von der des Verarbeitungskontextes „Behandlung".

Vertretung

Eine Vertretung ist die zeitlich befristete Übernahme der Aufgabe eines Beschäftigten durch einen anderen gemäß einem Dienstplan oder einer sonstigen Regel, die von der jeweilig dafür zuständigen Leitung im Voraus festgelegt wurde.

Vorbehandlungsdaten

Vorbehandlungsdaten umfassen alle zeitlich vor dem aktuellen → ***Behandlungsfall*** liegende → ***Fallakten*** einer → ***Patientenakte***.