

DIN EN ISO 25237:2017-05 (D)

Medizinische Informatik - Pseudonymisierung (ISO 25237:2017); Deutsche Fassung
EN ISO 25237:2017

Inhalt	Seite
Europäisches Vorwort.....	4
Vorwort.....	5
Einleitung.....	6
1 Anwendungsbereich.....	7
2 Normative Verweisungen.....	7
3 Begriffe.....	7
4 Abkürzungen.....	14
5 Anforderungen an den Schutz von personenbezogenen Daten im Gesundheitswesen.....	14
5.1 Ziele des Schutzes von personenbezogenen Daten.....	14
5.2 Allgemeines.....	15
5.3 Entpersonalisierung als Prozess der Risikominderung.....	16
5.3.1 Allgemeines.....	16
5.3.2 Pseudonymisierung.....	17
5.3.3 Anonymisierung.....	17
5.3.4 Direkte und indirekte Bezeichner.....	17
5.4 Schutz der personenbezogenen Daten von Entitäten.....	17
5.4.1 Vergleich von personenbezogenen und entpersonalisierten Daten.....	17
5.4.2 Konzept der Pseudonymisierung.....	19
5.5 Pseudonymisierung in der realen Welt.....	22
5.5.1 Begründung.....	22
5.5.2 Stufen des Schutzes von personenbezogenen Daten.....	22
5.6 Kategorien der betroffenen Personen.....	25
5.6.1 Allgemeines.....	25
5.6.2 Zu betreuende Personen.....	25
5.6.3 Ärztliches Personal und Organisationen.....	26
5.6.4 Gerätedaten.....	26
5.7 Klassifizierungsdaten.....	26
5.7.1 Nutzdaten.....	26
5.7.2 Beobachtungsdaten.....	26
5.7.3 Pseudonymisierte Daten.....	27
5.7.4 Anonymisierte Daten.....	27
5.8 Forschungsdaten.....	27
5.8.1 Allgemeines.....	27
5.8.2 Generierung von Forschungsdaten.....	28
5.8.3 Sekundäre Nutzung von personenbezogenen Gesundheitsinformationen.....	28
5.9 Zur Identifizierung geeignete Daten.....	28
5.9.1 Allgemeines.....	28
5.9.2 Patientenbezeichner.....	28
5.10 Daten von Opfern von Gewalttaten und öffentlich bekannten Personen.....	29
5.10.1 Allgemeines.....	29
5.10.2 Geninformationen.....	29
5.10.3 Vertrauenswürdiger Dienst.....	29
5.10.4 Bedarf bezüglich der Wiedererkennung von pseudonymisierten Daten.....	29
5.10.5 Eigenschaften von Pseudonymisierungsdiensten.....	30

6	Datenschutz durch Pseudonymisierung	31
6.1	Begriffsmodell der Problembereiche	31
6.2	Eignung von personenbezogenen Informationen zur direkten und zur indirekten Identifizierung	31
6.2.1	Allgemeines	31
6.2.2	Zur Identifizierung von Personen geeignete Variablen	32
6.2.3	Kumulationsvariablen	32
6.2.4	Ausreißervariablen	33
6.2.5	Strukturierte Datenvariablen	34
6.2.6	Nicht-strukturierte Datenvariablen	34
6.2.7	Inferenzrisikobewertung	35
6.2.8	Privatheit und Sicherheit	35
7	Wiedererkennungsprozess	35
7.1	Allgemeines	35
7.2	Teil der normalen Verfahren	36
7.3	Ausnahme	36
7.4	Technische Realisierbarkeit	37
	Anhang A (informativ) Szenarien für die Pseudonymisierung im Gesundheitswesen	38
	Anhang B (informativ) Anforderungen an die Analyse des Risikos für den Schutz von personenbezogenen Daten	53
	Anhang C (informativ) Pseudonymisierungsprozess (Verfahren und Implementierung)	64
	Anhang D (informativ) Spezifikation von Verfahren und Implementierung	70
	Anhang E (informativ) Grundstruktur einer Policy für den Betrieb von Pseudonymisierungsdiensten (Verfahren und Implementierung)	72
	Anhang F (informativ) Genetische Informationen	76
	Literaturhinweise	77