

E DIN EN ISO 25237:2026-06 (D/E)

Erscheinungsdatum: 2026-05-15

Medizinische Informatik - Pseudonymisierung (ISO/DIS 25237:2026); Deutsche und Englische Fassung prEN ISO 25237:2026

Health informatics - Pseudonymization (ISO/DIS 25237:2026); German and English version prEN ISO 25237:2026

Inhalt

Seite

Europäisches Vorwort	4
Vorwort	5
Einleitung	6
1 Anwendungsbereich	7
2 Normative Verweisungen	7
3 Begriffe	7
4 Abkürzung	13
5 Prinzipien der Pseudonymisierung	14
5.1 Allgemeines	14
5.2 Trennung der Bezeichner	15
5.3 Daten-Minimierung	15
6 Anforderungen an die Pseudonymisierung im Gesundheitswesen	15
6.1 Pseudonymisierung	15
6.2 Anonymisierung	16
6.3 Direkte und indirekte Bezeichner	17
6.4 Klassifizierung von Dateninhabern	17
6.4.1 Allgemeines	17
6.4.2 behandelte Person	18
6.4.3 Ärztliches Personal und Organisationen	18
6.4.4 Gerätedaten	18
6.5 Vertrauenswürdiger Dienst	19
6.6 Daten von Opfern von Gewalttaten und öffentlich bekannten Personen	19
6.7 Geninformationen	19
7 Pseudonymisierung in der Praxis	19
7.1 Allgemeines	19
7.2 Datensicherheitsstufe 1: Eliminierung von eindeutig zur Identifizierung geeigneten Daten oder von leicht erhältlichen zur indirekten Identifizierung geeigneten Daten	20
7.3 Datensicherheitsstufe 2: Berücksichtigung von Angreifern, die externe Daten nutzen	20
7.4 Datensicherheitsstufe 3: Berücksichtigung von Datenausreißern	21
8 Praktische Anwendung der Pseudonymisierung und der kontrollierten Wiedererkennung von pseudonymisierten Daten	21
8.1 Allgemeines	21
8.2 Pseudonymisierungsansatz	21
8.3 Wiedererkennung-Zweckcodes	21
9 Eigenschaften von Pseudonymisierungsdiensten	22
9.1 Allgemeines	22
9.2 Mindestanforderungen an vertrauenswürdige Praktiken	22
10 Schutz der Privatsphäre durch Pseudonymisierung	23
10.1 Allgemeines	23
10.2 Eignung von personenbezogenen Informationen zur direkten und zur indirekten Identifizierung	23
10.2.1 Allgemeines	23
10.2.2 Zur Identifizierung von Personen geeignete Variablen	24
10.2.3 Kumulationsvariablen	24
10.2.4 Ausreißervariablen	25
10.2.5 Strukturierte Datenvariablen	26
10.2.6 Nicht-strukturierte Datenvariablen	26

11	Wiedererkennungprozess	27
11.1	Kontext	27
11.1.1	Allgemeines	27
11.1.2	Wiedererkennung als Teil der normalen Verfahren	27
11.1.3	Wiedererkennung als außergewöhnliches Ereignis	28
11.2	Technische Realisierbarkeit	29
12	Pseudonymisierungstechniken	29
12.1	Allgemeines	29
12.2	Schlüsseltechniken	29
12.2.1	Tokenisierung	29
12.2.2	Verschlüsselungsbasierte Pseudonymisierung	30
12.2.3	Hashing	30
12.2.4	Deterministische Pseudonymisierung	30
12.2.5	Nicht-deterministische oder zufällige Pseudonymisierung	30
12.2.6	Datenmaskierung	30
Anhang A	(informativ) Pseudonymisierungsszenarien im Gesundheitswesen	31
A.1	Allgemeines	31
A.2	Erläuterung der Szenarien	31
A.3	Szenarien im Gesundheitswesen	32
A.3.1	Reihenfolge nach der klinischen Pathologie (pseudonymisierte Pflege)	36
A.3.2	Klinische Studie	37
A.3.3	Klinische Forschung	40
A.3.4	Überwachung der öffentlichen Gesundheit	42
A.3.5	Berichte zur Patientensicherheit (unerwünschte Ereignisse im Zusammenhang mit Arzneimitteln)	44
A.3.6	Nicht das Gesundheitswesen betreffende Forschung, die personenbezogene mediale Daten verwendet	45
A.3.7	Marktforschung	45
A.3.8	Lehrdateien	46
A.3.9	Außendienst	46
Anhang B	(informativ) Spezifikation von Verfahren und Implementierung	51
Anhang C	(informativ) Genetische Informationen	53
Anhang D	(informativ) Beispielhafte Kategorien personenbezogener Daten für die Risikobewertung der Re-Identifizierung bei Pseudonymisierung	55
Literaturhinweise		57

Bilder

Bild A.1	— Veränderung der Daten zu klinischen Studien	38
Bild A.2	— Informationsflüsse bei klinischen Studien	40
Bild A.3	— Informationsflüsse bezüglich der Patientensicherheit	45
Bild A.4	— Datenflüsse	47
Bild A.5	— Datenvorbereitung	48
Bild A.6	— Pseudonymisierungsprozess	49

Tabellen

Tabelle A.1	— Eigenschaften der Szenarien	34
Tabelle A.2		47
Tabelle D.1		55