Verwendungszweck

**Ziel dieser Vorlage ist es, Organisationen, die mit Personenidentifizierenden Daten (IDAT) arbeiten, dabei zu unterstützen, eine eigene Arbeitsanweisung zu erstellen, um IDAT für die Implementierung und Evaluierung von Schnittstellen datenschutzkonform verarbeiten zu können.**

Die Vorlage sollte an die Fähigkeiten, Rollen und Prozesse der jeweiligen Organisation angepasst werden.

* Die relevanten Fähigkeiten, Rollen und Prozesse können technischer Natur sein, wie z.B. das Management von V2-Nachrichten, oder
* mit der in jeder einzelnen Organisation bestehenden Rolle für Datenschutz, Qualitätsmanagement und Qualitätskontrolle zusammenhängen.

Diese Vorlage behandelt die **projektübergreifenden Arbeitsschritte zur Anonymisierung von Testdaten**. Das Zielpublikum einer auf dieser Vorlage aufbauenden Arbeitsanweisung bildet sich aus Personen, die die Anonymisierung von Testdaten projektübergreifend vorbereiten.

Die projektspezifischen Arbeitsschritte bauen auf den Ergebnissen der hier aufgeführten Arbeitsschritte auf und werden in einer gesonderten Vorlage beschrieben.

**Anonymisierung klinischer Daten im HL7 V2 Format zum Zweck von *Data Profiling* - Vorlage für die Umsetzung projektübergreifender Prozesse**

Vorlage für die Umsetzung hauseigener Verfahrensanweisungen; ggf. in hauseigene Dokumentenvorlage zu überführen.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| |  | | --- | | General Information | | |  |  | | --- | --- | | Project name | Qualitätsmanagementsystem (QMS) | | Document owner | Vorname Nachname | |
| |  | | --- | | Review | | |  |  |  |  | | --- | --- | --- | --- | | Name | Role/Comments | Signature | Date | | Vorname Nachname | Rolle |  |  | |  |  |  |  | |
| |  | | --- | | Approval | | |  |  |  |  | | --- | --- | --- | --- | | Name | Role/Comments | Signature | Date | | Vorname Nachname | Rolle |  |  | |  |  |  |  | |
| |  | | --- | | Document History | | |  |  |  |  | | --- | --- | --- | --- | | Author | Version | Reason for change | Date | | Vorname Nachname | 0.1 | Erster Entwurf | TT.MM.JJJJ | |  |  |  |  | |

Index

**1.** **Hintergrund 4**

**2.** **Ziel 4**

**3.** **Geltungsbereich 4**

**4.** **Anonymisierung 4**

**5.** **Prozessbeschreibung 5**

**6.** **Definition der zu anonymisierenden Datenfelder 7**

6.1. Segment IN1 und IN2 7

6.2. Das PID Segment 8

6.3. NK1 Attribute 8

6.4. National definierte Z-Segmente 8

6.5. Hauseigene Z-Segmente 8

**7.** **Referenzen und Anlagen 8**

**8.** **Glossar 8**

**9.** **Anlagen 9**

9.1. Anlage 1 – Handbuch zum Healex Anonymisierungswerkzeug 9

9.1.1. Healex.HL7v2Anonymizer 9

9.1.2. Funktionen 9

9.1.3. Bereitstellung 9

9.1.4. Konfiguration 9

# Hintergrund

Krankenhaussysteme sind auf Kommunikation und Austausch von Daten untereinander stark angewiesen. Auch bei der Verwendung von Standards, wie HL7 V2, für die Anbindung der Systeme, ist eine starke Variabilität in der Zusammenstellung der Nachrichten möglich.

Anonymisierte Daten sind für die Analyse und Validierung von Schnittstellenformaten von großer Bedeutung. Die jeweils eingesetzten Systeme, Anwendungen und Konnektoren sollen vor dem Live-Betrieb zunächst in einer realitätsnahen Umgebung systematisch geprüft werden, um sicherzustellen, dass sie lokale Formate sowie deren Zusammensetzungen und Varianten unterstützen. Dies ist insbesondere wichtig, wenn Format-Standards, wie z.B. HL7 v2, Variabilität in der Zusammensetzung von Segmenten und Segmenttypen erlauben.

Diese Validierung der Systeme, Anwendungen und Konnektoren an sich ist kein legitimer Zweck für die Verarbeitung der personenbezogenen Daten. Künstliche Datensätze helfen jedoch nicht bei der Validierung des konkreten technischen Schnittstellenformats, da es nicht möglich ist, ohne Einblick in Echtdaten Testdaten zu bilden, die exakt die gleichen Strukturmerkmale aufweisen wie die realen Daten. Es ist daher essentiell auf der Basis von realen Daten Datensätze zu bilden, die durch die Anonymisierung derart modifiziert wurden, dass sie keinerlei Informationen über die einzelnen Personen mehr aufweisen. Zur rechtlichen Begründung siehe Abschnitt 4 “Anonymisierung”.

# Ziel

Die Durchführung des Anonymisierungsprozesses soll Maßstäbe der örtlichen Datenschutzbeauftragten befolgen und nach definierten und dokumentierten Schritten erfolgen.

Mithilfe des vorliegenden Dokuments sollen alle im Auftrag des im [Krankenhaus] Arbeitenden, welche mit der Anonymisierung von personenbezogenen Daten beauftragt sind, bei der Durchführung und erfolgreichen Umsetzung dieser Prozesse unterstützt werden. Dadurch soll eine korrekte und qualitativ hochwertige und datenschutzkonforme Verarbeitung gewährleistet werden.

# Geltungsbereich

Die Arbeitsanweisung (**WI-xxx -** Englisch **W**orking **I**nstruction**)** besitzt für alle im Auftrag des Krankenhaus Arbeitenden, die an der Verarbeitung von personenbezogenen Daten zwecks Schnittstellenimplementierung und -Validierung beteiligt sind, Gültigkeit.

# Anonymisierung

Weder die DSGVO noch das Bundesdatenschutzgesetz (BDSG) enthalten Definitionen des Begriffs „Anonymisierung“.

Das BDSG a.F. stellt in § 3 Abs. 6 fest, dass *Anonymisieren das Verändern personenbezogener Daten in der Art ist*, *„dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr“* (sog. absolute Anonymität) *oder „nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft“* (sog. faktische Anonymität) *einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können*.

Eine aussagekräftige Definition hat der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) im [Rahmen eines öffentlichen Konsultationsverfahrens](https://www.bfdi.bund.de/DE/Infothek/Pressemitteilungen/2020/03_Konsultationsverfahren.html) zum Thema Anonymisierung erläutert und dabei eine pragmatische Auslegung der DSGVO-Vorgabe vorgestellt. So ist eine Anonymisierung in der Art, dass eine Re-Identifizierung – die Wiederherstellung des Personenbezugs – für niemanden möglich ist, in der Praxis sehr schwer zu erreichen und wird aus Sicht des BfDI auch nicht durch die Verordnung gefordert. *Eine faktische Anonymisierung, die sicherstellt, dass der Personenbezug nur mit unverhältnismäßigen Aufwand an Kosten, Zeit und Arbeitskräften wiederhergestellt werden kann, ist somit ausreichend*.

# Prozessbeschreibung

Im Folgenden werden die einzelnen Prozessschritte, welche im Rahmen der Analyse der identifizierenden Daten (IDAT) und Umsetzung der Anonymisierung projektübergreifend durchlaufen werden, genauer beschrieben. Diese Prozessschritte dienen der Vorbereitung von Anonymisierungen zur Erstellung von projektspezifischen Testdaten.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **#** | **Prozessschritt** | **Aktionen/ Beschreibung** | **Ergebnis** | **Zuständigkeiten** |
| **1** | Personen mit V2 Kenntnissen werden vom Haus benannt. | Benennung der Verantwortlichen | Liste von benannten Personen mit V2 Erfahrung | - Forschungskoordinator\*innen des Hauses koordinieren Benennungen |
| **2** | Evaluation der relevanten V2 Nachrichten im Haus. | Identifikation von IDATs in allen V2 Nachrichten am Haus. | Liste von V2 Nachrichten und Segmenten (am Haus) mit IDAT | Designierte Personen gemäß Prozess:  - Datenschutzbeauftragte des Hauses  - Lokale Anwendungsbetreuung der Quellsysteme (COM Server Beauftragter)  Und/Oder  - Eine Person mit V2 Erfahrung |
| **3** | Festlegung der IDAT Elemente, die anonymisiert werden müssen. | Aufbauend auf den Ergebnissen von 2.:  Entscheidung über die zu anonymisierenden IDAT in den hausspezifischen V2 Nachrichten/ Segmente | Liste von V2 Nachrichten und Segmenten mit zu anonymisierenden IDATs am Haus | - Datenschutzbeauftragte des Hauses  - Lokale Anwendungsbetreuung der Quellsysteme (COM Server Beauftragte)  Und/Oder  - Eine Person mit V2 Erfahrung |
| **4** | Verfahrensanweisungen werden von lokalen Datenschutzbeauftragten geprüft, ggf. angepasst und freigegeben. | Die Verfahrensanweisungen (projektübergreifend und projektspezifisch) werden von dem lokalen Datenschutzbeauftragten gemeinsam mit den COM Server Betreuenden auf Basis der Vorlagen erstellt und geprüft. | hausspezifische Verfahrensanweisungen (projektübergreifend und projektspezifisch) | - Forschungskoordinator\*innen (verantwortlich)  - Datenschutzbeauftragte des Hauses (ausführend)  - Forschungskoordinator\*innen können designierte Personen mit einbeziehen |
| **5** | Beteiligte werden in der Bedienung des V2 Anonymisierungstools geschult. | Designierte Personen aus dem Haus, für die Durchführung des Anonymisierungsprozesses werden vom Servicecenter Medical Data Science oder UK OWL-Dienstleistern geschult. | ggf. Schulungs-Nachweis (je nach QM Vorgabe der Organisation) | Servicecenter Medical Data Science oder externer UK OWL-Dienstleister |
| **6** | Beteiligte werden in der Verfahrensanweisung geschult. | Designierte Personen aus dem Haus für die Durchführung des Anonymisierungsprozesses werden von der Forschungskoordination oder vom DSB des Hauses geschult. | ggf. Schulungs- Nachweis (je nach QM Vorgabe der Organisation) | Nach Ermessen des Hauses (gemäß Fähigkeiten im Team) |
| **7** | Festlegung der Rollen und der Umgebung zur Ausführung des Anonymisierungstools | Datenschutzbeauftragte legen die Rollen und die Umgebung fest in der die Anonymisierung qualifiziert und sicher durchgeführt werden kann | Dokument mit Festlegung der Umgebung und der Rollen | * Datenschutzbeauftragte des Hauses * Technischer Sicherheitsadministrator |
| **8** | Einrichtung der hausspezifischen Konfiguration des Anonymisierungstools. | Technische Umsetzung der Festlegungen aus 3., um durch das Anonymisierungstool die relevanten IDAT in hausspezifischen V2 Nachrichten zu anonymisieren | hausspezifische Konfiguration des Anonymisierungstools | - Eine Person mit V2 Erfahrung, die geschult wird, das Anonymisierungstool zu bedienen  - Zweite Person mit V2 Erfahrung für 2nd Look/ Review |
| **9** | Antragsprozess | Erstellung einer Vorlage für die Beantragung | Vorlage | - Forschungskoordinator\*innen (verantwortlich)  - Datenschutzbeauftragte des Hauses (ausführend) |

# Definition der zu anonymisierenden Datenfelder

Das folgende Kapitel illustriert die zu anonymisierenden Datenfelder. Diese Definition ist als Basisreferenz zu betrachten, sollte aber nicht ausschließlich für die Anonymisierung maßgeblich sein. Sie deckt die Segmente ab, die in der Praxis in Deutschland regelmäßig vorkommen. Sie muss jedoch zwingend mit den hauseigenen Nachrichten abgeglichen werden, um sicherzustellen, dass alle Instanzen von tatsächlichen IDAT anonymisiert wurden.

Bitte beachten Sie, dass Hersteller und Krankenhäuser neue Felder erstellen können, um ihre eigenen Anforderungen zu unterstützen. Dies ist in HL7 V2 mittels sog. *Z-Segmente* möglich: Ein Z-Segment ist ein Nachrichten Segment, das lokal definiert wird und nicht verbindlicher Teil des HL7-V2 Standards ist. Daher ist es notwendig, eine Übersicht der Z-Segmente, die für ihr Haus definiert wurde, zu haben.

Bitte erfragen Sie eine Übersicht der definierten Z-Segmente bei Ihrer Krankenhaus IT-Leitung.

Einige Z-Segmente sind national festgelegt worden. Nachfolgend ist eine Liste der durch HL7-D veröffentlichten Z-Segmente zu finden: <https://wiki.hl7.de/index.php?title=Z-Segmente>

Diese Übersicht ist auf Deutschland fokussiert. Eine globale Anweisung müsste weitere Segmente berücksichtigen, beispielsweise sind die Segmente GT1, UB1 und UB2 in Deutschland nicht von Bedeutung und somit nicht zugelassen in USA jedoch gängig.

## Segment IN1 und IN2

Das IN1-Segment dient der Übermittlung der Daten zum Kostenträger und Versicherungsnehmer. Unter Kostenträger wird typischerweise die Krankenversicherung – egal ob gesetzlich (GKV) oder privat (PKV) – verstanden. Der Kostenträger kann aber auch der Patient selber sein, der dann eine direkte Rechnung erhält. Der Typ des Kostenträgers wird über IN2-5 identifiziert. Aus diesem Grund ist das IN2-Segment in dem Nachrichten Fragment (Profil Komponente) verpflichtend. Wenn der Patient die Rechnung selber bezahlt, ist er gleichzeitig Versicherter und Kostenträger.

## Das PID Segment

Das PID-Segment dient der Übermittlung der nicht fallspezifischen Patientendaten. Ein Großteil der nicht erlaubten Felder bezieht sich auf Informationen aus dem Bereich der Veterinärmedizin bzw. Informationen, deren Verarbeitung in Deutschland nicht zugelassen ist.

## NK1 Attribute

Mit diesem Segment können Informationen über Kontaktpersonen, die zu dem Patienten in einer Beziehung stehen, übermittelt werden. Das können sein: direkte Verwandte, Lebensgefährten, Freunde.

## National definierte Z-Segmente

Nachfolgend eine Liste der durch HL7-Deutschland veröffentlichten Nationalen Z-Segmente: <https://wiki.hl7.de/index.php?title=Z-Segmente#Deutschland>

## Hauseigene Z-Segmente

Bitte lassen Sie sich unbedingt von Ihrer hauseigenen Krankenhaus-IT die Liste der intern definierten Z-Segmenten geben. Wenn eine solche Übersicht nicht vorhanden ist, kann die hauseigene IT bei den einzelnen Systemhersteller / Lieferanten des Hauses eine solchen Liste anfordern.

# Referenzen und Anlagen

Auflistung aller interner und externer Referenzdokumente, auf die das Dokument Bezug nimmt.

* <https://www.bfdi.bund.de/SharedDocs/Pressemitteilungen/DE/2020/03_Konsultationsverfahren.html>
* <https://www.luc.edu/its/aboutits/itspoliciesguidelines/hipaainformation/18hipaaidentifiers/>
* <https://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Handbook_De-Identification_Rev1.1_2014-06-06.pdf>
* <https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html>
* Master Document List (MDL)
* SOP-xxx Titel
* WI-xxx Titel

# Glossar

[Auflistung und Erläuterung aller verwendeter Abkürzungen]

IDAT Personenidentifizierende Daten

QM Qualitätsmanagement

QMS Qualitätsmanagementsystem/ Quality Management System

WI Working Instruction

# Anlagen

## Anlage 1 – Handbuch zum Healex Anonymisierungswerkzeug

Die Aktuellste version der Software sowie die aktuelleste englische Version der Anleitung finden sie hier: <https://github.com/healexsystems/Healex.HL7-V2-Anonymizer>

## Download und Installation

* Laden Sie [die neueste Version](https://github.com/healexsystems/Healex.HL7-V2-Anonymizer) herunter.
* Da Sie personenbezogenen Daten damit verarbeiten werden ist es ratsam die software in einer ausreichend abgesicherter Umgebung auszuführen

Für weitere Schritte siehe Abschnitt Ausführung.

### Healex.HL7v2 Anonymizer

Diese Konsolenanwendung ermöglicht es Ihnen, HL7v2-Nachrichten zu anonymisieren. Alle von Ihnen festgelegten identifizierbaren Daten in HL7v2-Nachrichten werden mittels des Anonymisierers anonymisiert.

Felder, die personenbezogenen Informationen enthalten, werden

* durch ein von Ihnen zu definierenden Zeichenkette ersetzt

oder

* optional gehasht [1].

Die Hash-Funktion im *Healex Anonymizer* ist ‘einseitig’, so dass es keine Möglichkeit gibt, die pseudonymisierte ID in ihre ursprüngliche ID zurück zu verwandeln.

**Bitte Beachten Sie: Diese Anwendung überschreibt die Originalnachricht. Stellen Sie sicher, dass Sie die Originaldateien also kopie aufbewahren solange Sie diese für die Verarbeitung benötigen.**

*[1] Hinweis zu ‘Hashing’: Unter Hashing versteht man die Umwandlung eines beliebigen Schlüssels oder einer Zeichenkette in einen anderen Wert. Dieser wird in der Regel durch einen kürzeren Wert oder Schlüssel mit fester Länge dargestellt, der die ursprüngliche Zeichenfolge repräsentiert und leichter auffindbar oder verwendbar macht. Die beliebteste Anwendung für Hashing ist die Implementierung von Hash-Tabellen.*

### Funktionen

* Anonymisierung von bestimmten Segmentfeldern
* Hashing von bestimmten Segmentfeldern

### Ausführung

Die Software wird als Kommandozeilenanwendung ausgeführt, die einen Pfad zu dem Ordner erwartet, der die zu anonymisierenden HL7-Nachrichten enthält.

1. Dekomprimieren Sie den Freigabeordner.
2. Führen Sie die Anwendung aus
3. geben Sie den Pfad zu Ihren v2-Nachrichten-Ordner ein.
4. Mit ‘Enter’ führen Sie die Anwendung aus

### Konfiguration

Diese Anwendung verwendet die Datei [appsettings.json](https://github.com/healexsystems/Healex.HL7-V2-Anonymizer/blob/main/Healex.HL7v2Anonymizer/appsettings.json), um die zu ersetzenden Werte für jedes Segment und die entsprechenden Felder zu lesen.

Ein Segment wird durch seine Eigenschaft "Segment" erkannt. Jedes Segment enthält ein Array von Ersetzungen. Die Untersegmente eines Segments können durch die Eigenschaft "Path" innerhalb des Ersetzungs-Arrays identifiziert werden. Untersegmente haben auch eine Eigenschaft "value", die den Wert enthält, durch den ein Wert in einer HL7v2-Nachricht ersetzt werden soll.

Nehmen wir an, Sie möchten den Wert ersetzen, der derzeit für den angegebenen Namen eines NK1-Segments zugewiesen ist. Navigieren Sie zu appsettings.json, suchen Sie das NK1-Segment und ersetzen Sie den Wert für Pfad "Path": "NK1.2.2" wie folgt:

{

"Segment": "NK1",

"Replacements": [

// ausgelassen

{

"Path": "NK1.2.2",

"Value": "Vorname" <---- diesen Wert ersetzen

},

// ausgelassen

]

}

Idealerweise entspricht der Wert seiner Semantik - wenn also ein Datum ersetzt werden soll, geben Sie ein zufälliges Datum wie 01.01.2020 ein, anstatt einen Zufallswert einzugeben.

Sie sollten auch die Zeichenbeschränkungen für Felder und Werte beachten, die in der von Ihnen verwendeten HL7 v2-Version festgelegt sind. Je nach HL7 v2-Version könnten Ersetzungen sonst die Nachricht gemäß dieser Version ungültig machen. In Version 2.5 sind für das Feld NK1.2.2 beispielsweise nur maximal 30 Zeichen zulässig.

Verwenden Sie das Schlüsselwort "HASH", um persistente, pseudonymisierte IDs zu erzeugen. Diese Funktion erzeugt immer dieselbe anonymisierte ID für eine bestimmte ID in der HL7 v2-Nachricht. Die Hash-Funktion ist einseitig, so dass es keine Möglichkeit gibt, die pseudonymisierte ID in ihre ursprüngliche ID zurück zu verwandeln.

{

"Segment": "PID",

"Replacements": [

// ausgelassen

{

"Path": "PID.1.1",

"Value": "HASH" <---- Der Wert in PID.1.1 wird gehasht, nicht überschrieben

},

// ausgelassen

]

}

Das Hinzufügen weiterer Segmente funktioniert auf ähnliche Weise. Fügen Sie einfach ein neues Segment in der appsettings.json nach "Segment" hinzu: "IN2". Stellen Sie sicher, dass Sie ein Komma an die schließende Klammer dieses Segments anhängen, damit die JSON-Datei gültig bleibt, und verwenden Sie dann diese Vorlage, um ein neues Segment hinzuzufügen.

{

"Segment": "SEGMENT\_ID",

"Replacements": [

{

"Path": "Pfad\_zum\_Untersegment1",

"Value": "Ersatz\_wert1"

},

{

"Path": "Pfad\_zum\_Untersegment2",

"Value": "Ersatz\_wert2"

}

]

}

Speichern Sie und starten Sie die Anwendung neu, damit die Änderungen wirksam werden.