

MAGDA-LENA

Kommunikation in Forschung und Lehre

Datenschutz-Policy

Version 1.1, 1.9.2001

**Klaus M. Simonic
Günther Gell**



INSTITUT FÜR MEDIZINISCHE INFORMATIK, STATISTIK UND DOKUMENTATION
LKH/UNIVERSITÄTSKLINIKUM GRAZ

Inhalt

Inhalt	i
1. Einleitung.....	1
1.1. Kontext und Zielsetzung	1
1.2. Gliederung der vorliegenden Arbeit	1
1.3. Sprachliche Gleichbehandlung	2
2. Allgemeine Grundlagen	3
2.1. Rechtliche Grundlagen.....	3
2.1.1. Grundsätze bei der Verwendung von Daten	3
2.1.2. Verwendung von Daten für wissenschaftliche Forschung und Statistik	3
2.1.3. Bemerkungen zu § 46 DSGVO 2018	4
2.1.4. Rollenmodelle in der wissenschaftlichen Forschung und Statistik.....	5
2.1.5. Zur Verfügungstellung von Adressen zur Benachrichtigung und Befragung von Betroffenen	6
2.1.6. Verwendung von Daten in der Lehre	7
2.2. Anonymisierung.....	7
2.2.1. Indirekt personenbezogene Daten.....	7
2.2.2. Primäre Identifikationsdaten	8
2.2.3. Sekundäre Identifikationsdaten	8
2.2.4. Beschränkte Übermittlung von Daten	9
2.2.5. <i>k</i> -Anonymität	10
3. Datenschutz-Policy	11
3.1. Allgemeine Datensicherheitsmaßnahmen	11
3.1.1. Rahmenbedingungen.....	11
3.1.2. Vorgehensmodell	11
3.2. Datengeheimnis.....	12
3.2.1. Rahmenbedingungen.....	12
3.2.2. Vorgehensmodell	12
3.3. Meldepflicht des Auftraggebers.....	12
3.3.1. Rahmenbedingungen.....	12
3.3.2. Vorgehensmodell	13
3.4. Informationspflicht des Auftraggebers	14
3.4.1. Rahmenbedingungen.....	14
3.4.2. Vorgehensmodell	15
3.5. Zustimmung des Betroffenen	15
3.5.1. Rahmenbedingungen.....	15
3.5.2. Vorgehensmodell	15
3.6. Pflichten des Dienstleisters	16
3.6.1. Rahmenbedingungen.....	16
3.6.2. Vorgehensmodell	17
3.7. Primäre Identifikationsdaten.....	18
3.7.1. Rahmenbedingungen.....	18
3.7.2. Vorgehensmodell	18
3.8. Sekundäre Identifikationsdaten.....	19
3.8.1. Rahmenbedingungen.....	19
3.8.2. Vorgehensmodell	20
3.8.3. <i>k</i> -Anonymität bei Untersuchungen mit kleiner Fallzahl.....	21
3.8.4. Sonderfälle	22

3.9. Übermittlung von Daten	22
3.9.1. Rahmenbedingungen.....	22
3.9.2. Vorgehensmodell	23
3.10. Lokale Datenschutzkommissionen	24
4. Systemstrukturen zur Anonymisierung personenbezogener Daten	25
4.1. Reversible Anonymisierung	25
4.1.1. Definition	25
4.1.2. RDN des Auftraggebers	25
4.1.3. Lokale RDNs.....	26
4.1.4. Vorgehensmodell	26
4.2. Vorgehensmodell zur Anonymisierung personenbezogener Daten.....	28
4.3. Vorschläge für weitere Entwicklungen.....	30
5. Health Level 7.....	31
5.1. HL7 Nachrichtenaufbau	31
5.2. Segmente mit demographischen Patientendaten	31
5.2.1. ACC – Accident Segment	31
5.2.2. AL1 – Patient Allergy Information Segment	32
5.2.3. DB1 – Disability Segment.....	32
5.2.4. NK1 – Next of Kin, Associated Parties Segment	33
5.2.5. PD1 – Patient Additional Demographic Segment	34
5.2.6. PID – Patient Identification Segment.....	36
5.3. Weitere Segmente mit primären und/oder sekundären Identifikationsdaten.....	39
5.4. Spezielle HL7 Segmente	39
5.4.1. NTE – Notes and Comments Segment	39
5.4.2. Z-Segmente.....	39
5.5. HL7 Nachrichten für klinische Studien	40
5.5.1. CRM – Clinical Study Registration Message	40
5.5.2. SCU – Unsolicited Study Data Message	40
6. DICOM.....	42
6.1. Information Object Definition.....	42
6.1.1. Composite IOD	42
6.1.2. Normalized IOD.....	42
6.1.3. Attributes	42
6.2. Common Composite Image IOD.....	43
6.2.1. Patient Module	43
6.2.2. Patient Study Module	44
6.3. Basic Study Descriptor IOD.....	44
6.3.1. Patient Summary Module.....	45
6.4. Patient Information Object Definition.....	45
6.4.1. Patient Identification Module	45
6.4.2. Patient Demographic Module	46
6.4.3. Patient Medical Module	48
6.5. Anmerkungen.....	48
7. CEN/TC 251 Electronic Healthcare Communication	49
7.1. Informationsmodell.....	49
7.2. EHCR Nachrichten	49
7.2.1. Patient Matching Information	50
7.2.2. EHCR Extract	51
7.2.3. EHCR Data Items	52
7.3. Anmerkungen.....	53
8. Referenzen	54
9. Glossar	56

1. Einleitung

1.1. Kontext und Zielsetzung

Mit der Einführung des Datenschutzgesetzes 2000 folgt der Gesetzgeber den Harmonisierungsbestrebungen der Datenschutzvorschriften in den Mitgliedstaaten der Europäischen Union. Als wesentliche Neuerungen respektive Änderungen sind aufzuzählen:

1. Die Zulässigkeitsvoraussetzungen für die Verwendung von Daten wurden neu geregelt.
2. Die Betroffenenrechte, die schon bisher im Grundrecht gegenüber einer automationsunterstützten Verwendung von Daten garantiert waren, wurden nunmehr auch auf die Verwendung von Daten in manueller, strukturierter Form (z.B. Karteien, Listen usw.) ausgedehnt.
3. Damit sich die Betroffenen besser über Art und Zweck einer Datenanwendung informieren können, wurden die Kriterien für die Meldepflicht an das Datenverarbeitungsregister nachhaltig verschärft. Dieser Informationspflicht steht eine Verminderung des Registrierungsaufwands gegenüber, zudem sind etliche Standard-Datenanwendungen von der Meldepflicht ausgenommen.
4. Änderungen hinsichtlich des Datenverkehrs mit dem Ausland. So existieren nunmehr innerhalb des EU-Gebiets keine Beschränkungen des Datenverkehrs.

Das Ziel dieser Arbeit ist es Wissenschaftler und Lehrende über die aktuelle Gesetzeslage zu informieren und die rechtliche Situation praxisnah zu kommentieren. Weiters werden wirksame Regeln spezifiziert, die dem Grundrecht auf Datenschutz genügen ohne dabei einen allzu hohen bürokratischen Aufwand zu verursachen.

Solche Regelungen zu finden ist oftmals ein Balanceakt: Einerseits erkennt das Datenschutzgesetz eine privilegierende Stellung von wissenschaftlicher Forschung und Statistik als sachlich gerechtfertigt an. Dementsprechend enthält das DSG eingehende Richtlinien für die Verarbeitung von personenbezogenen Daten in diesen Bereich. Auf der anderen Seite ist der Austausch von wissenschaftlichen Daten – eine Notwendigkeit in der heutigen Zeit – im Allgemeinen in „nur indirekt personenbezogener“ Form erlaubt. Die Umwandlung von personenbezogenen Daten in indirekt personenbezogene Daten aber ist in der Praxis häufig eine veritable Hürde. Es ist genau diese Art von Fragen, auf die die vorliegende Datenschutz-Policy Antworten geben will, unter Aufbietung von organisatorischen, technischen und methodischen Ansätzen.

1.2. Gliederung der vorliegenden Arbeit

Kapitel 2 informiert über die rechtlichen Rahmenbedingungen des DSG 2000, insbesondere aus der Sicht der wissenschaftlichen Forschung und Statistik sowie der Lehre. In diesem Kontext ist der Begriff der „indirekt personenbezogenen Daten“ von zentraler Bedeutung und führt über den Weg einer Klassifikation in primäre und sekundäre Identifikationsdaten zur mathematischen Definition der „beschränkten Übermittlung“ und der „k-Anonymität“.

Aufbauend auf diese Grundlagen wird in Abschnitt 3 eine Datenschutz-Policy entwickelt, die Empfehlungen für einen gut Teil der fraglichen Themenkomplexe gibt, nämlich Datensicherheitsmaßnahmen, Datengeheimnis, Melde- und Informationspflicht, Zustimmung des Betroffenen, Pflichten des Dienstleisters, eine Analyse von typischen primären und sekundären Identifikationsdaten sowie deren Übermittlung. Dabei verstehen sich die Empfehlungen im Sinne von minimalen Maßnahmen bzw. „good practise“.

Die Frage, wie die einzelnen Forderungen der Datenschutz-Policy praktisch umsetzbar sind, versucht Kapitel 4 zu beantworten, wobei auch hier wiederum der abgestuften Vorgehensweise aus

Teil 3 Rechnung getragen wird. Es folgt der Begriff der „reversiblen Anonymität“ und seine praktische Realisierung. Praktikabilität ist überhaupt das zentrale Motto in dieser Sektion, und wo dies nicht in einfacher Art und Weise mit bestehenden Werkzeugen erzielbar ist, werden Vorschläge für Entwicklungen skizziert, um diesen Prozess zu unterstützen.

Welche Auswirkungen hat die gegebene Datenschutz-Policy auf die gängigen Standards für den elektronischen Austausch von medizinischen Daten? Diese Überlegungen werden im Detail für HL7, DICOM und das Domain Information Model der CEN TC 251 geführt (Kapitel 5, 6 u. 7).

Den Abschluss der Arbeit bilden ein Verzeichnis der relevanten Gesetze und Normen (Abschnitt 8) sowie das in derartigen Dokumenten übliche Glossar (Nummer 9).

1.3. Sprachliche Gleichbehandlung

Soweit in dieser Richtlinie auf natürliche Personen bezogene Bezeichnungen nur in männlicher Form angeführt sind, beziehen sie sich auf Frauen und Männer in gleicher Weise. Bei der Anwendung der Bezeichnungen auf bestimmte natürliche Personen ist die jeweils geschlechtsspezifische Form zu verwenden.

2. Allgemeine Grundlagen

2.1. Rechtliche Grundlagen

Als Basis für die folgenden Ausführungen dienen

1. die „Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr“, weiters
2. das Datenschutzgesetz 2000 (DSG 2000),
3. die „Verordnung des Bundeskanzlers über das bei der Datenschutzkommission eingerichtete Datenverarbeitungsregister (Datenverarbeitungsregister-Verordnung 2000)“ sowie
4. die „Verordnung des Bundeskanzlers über Standard- und Musteranwendungen nach dem Datenschutzgesetz 2000“.

Man beachte, dass die im Rahmen dieser Richtlinie wiedergegebenen Rechtsnormen nur so weit ausgeführt sind, als dies für den aktuellen Kontext notwendig erscheinen. Für alle darüber hinausreichenden Fragen ist die jeweilige Norm heranzuziehen.

2.1.1. Grundsätze bei der Verwendung von Daten

In Übereinstimmung mit § 6 Abs. 1 DSG 2000 dürfen Daten nur

1. nach Treu und Glauben und auf rechtmäßige Weise verwendet werden;
2. für festgelegte, eindeutige und rechtmäßige Zwecke ermittelt und nicht in einer mit diesen Zwecken unvereinbaren Weise weiterverwendet werden;
3. soweit sie für den Zweck der Datenanwendung wesentlich sind, verwendet werden und über diesen Zweck nicht hinausgehen;
4. so verwendet werden, dass sie im Hinblick auf den Verwendungszweck im Ergebnis sachlich richtig und, wenn nötig, auf den neuesten Stand gebracht sind;
5. solange in personenbezogener Form aufbewahrt werden, als dies für die Erreichung der Zwecke, für die sie ermittelt wurden, erforderlich ist; eine längere Aufbewahrungsdauer kann sich aus besonderen gesetzlichen, insbesondere archivrechtlichen Vorschriften ergeben.

Der Auftraggeber trägt bei jeder seiner Datenanwendungen die Verantwortung für die Einhaltung der genannten Grundsätze; dies gilt auch dann, wenn er für die Datenanwendung Dienstleister heranzieht (§ 6 Abs. 2 DGS 2000).

2.1.2. Verwendung von Daten für wissenschaftliche Forschung und Statistik

Gemäß § 46 Abs. 1 DSG 2000 darf ein Auftraggeber für Zwecke wissenschaftlicher oder statistischer Untersuchungen, die keine personenbezogenen Ergebnisse zum Ziel haben, alle Daten verwenden, die

1. öffentlich zugänglich sind oder
2. der Auftraggeber für andere Untersuchungen oder auch andere Zwecke zulässigerweise ermittelt hat oder
3. für den Auftraggeber nur indirekt personenbezogen sind.

In Übereinstimmung mit § 4 Z 1 DSG 2000 gelten Daten für einen Auftraggeber, Dienstleister oder Empfänger einer Übermittlung als „nur indirekt personenbezogen“, wenn der Personenbezug der Daten derart ist, dass dieser Auftraggeber, Dienstleister oder Übermittlungsempfänger die Identität des Betroffenen mit rechtlich zulässigen Mitteln nicht bestimmen kann.

Andere, nicht öffentlich zugängliche Daten dürfen laut § 46 Abs. 2 DSG 2000 für Zwecke der wissenschaftlichen Forschung und Statistik, nur

1. gemäß besonderer gesetzlicher Vorschriften oder
2. mit Zustimmung des Betroffenen oder
3. mit Genehmigung der Datenschutzkommission verwendet werden, wobei

eine Genehmigung der Datenschutzkommission zu erteilen ist, wenn (§ 46 Abs. 3 DSG 2000)

1. die Einholung der Zustimmung der Betroffenen mangels ihrer Erreichbarkeit unmöglich ist oder sonst einen unverhältnismäßigen Aufwand bedeutet und
2. ein öffentliches Interesse an der beantragten Verwendung besteht und
3. die fachliche Eignung des Antragstellers glaubhaft gemacht wird.

Ergänzend führt der Gesetzgeber aus: Sollen sensible Daten übermittelt werden, muss ein wichtiges öffentliches Interesse an der Untersuchung vorliegen; weiters muss gewährleistet sein, dass die Daten beim Empfänger nur von Personen verwendet werden, die hinsichtlich des Gegenstandes der Untersuchung einer gesetzlichen Verschwiegenheitspflicht unterliegen oder deren diesbezügliche Verlässlichkeit sonst glaubhaft ist. In § 4 Z 2 DSG 2000 wird der Begriff „sensible Daten“ („besonders schutzwürdige Daten“) als Daten natürlicher Personen über ihre rassische und ethnische Herkunft, politische Meinung, Gewerkschaftszugehörigkeit, religiöse oder philosophische Überzeugung, Gesundheit oder ihr Sexualleben definiert.

Auch in jenen Fällen, in welchen gemäß den vorstehenden Bestimmungen die Verwendung von Daten für Zwecke der wissenschaftlichen Forschung oder Statistik in personenbezogener Form zulässig ist, ist der direkte Personenbezug unverzüglich zu verschlüsseln, wenn in einzelnen Phasen der wissenschaftlichen oder statistischen Arbeit mit nur indirekt personenbezogenen Daten das Auslangen gefunden werden kann. Sofern gesetzlich nicht ausdrücklich anderes vorgesehen ist, ist der Personenbezug der Daten gänzlich zu beseitigen, sobald er für die wissenschaftliche oder statistische Arbeit nicht mehr notwendig ist (§ 46 Abs. 5 DSG 2000).

2.1.3. Bemerkungen zu § 46 DSG 2000

Die Richtlinie 95/46/EG des Europäischen Parlaments erkennt eine besondere, privilegierende Stellung von wissenschaftlicher Forschung und Statistik bei der Verwendung personenbezogener Daten als sachlich gerechtfertigt an. Dementsprechend enthält das Datenschutzgesetz 2000 eingehende Richtlinien für diesen Bereich. Sofern nicht spezielle gesetzliche Regelungen (wie etwa das Bundesstatistikgesetz) bestehen, sind grundsätzlich zwei verschiedene Gebrauchssituationen zu unterscheiden:

1. Die Daten werden für eine „Untersuchung“ verwendet, das ist ein konkretes Forschungsprojekt oder eine konkrete statistische Erhebung, bei der als Ergebnis Aussagen in nicht personenbezogener Form gewonnen werden sollen. Für diese Fälle sieht § 46 Abs. 1 DSG 2000 eine privilegierte Verwendungsmöglichkeit bestimmter Daten vor, insbesondere Daten, die beim selben Auftraggeber bereits für andere Zwecke vorhanden sind.
2. Unter § 46 Abs. 2 DSG 2000 fallen wissenschaftliche oder statistische Aktivitäten, die keine konkrete Untersuchung (Erhebung) darstellen, z.B. die Führung von personenbezogenen Hilfsregistern für statistische Zwecke oder andere personenbezogene permanente Datensammlungen im Umfeld von Forschung und Statistik.

In der Regel gelten die Bedingungen des § 46 Abs. 1 DSG 2000 in der klinischen Forschung als erfüllt. Zum einen haben wissenschaftliche Untersuchungen dieses Typs naturgemäß einen bestimmten Zweck und selbst das Führen von medizinischen Registern dient, wenn auch allgemeineren so doch konkreten Fragestellungen (Aussagen über zeitliche Änderungen, epidemiologische Zusammenhänge etc.). Andernfalls wäre eine Datenauswahl für ein derartiges Register schwerlich definierbar. Zum anderen haben Untersuchungen in der medizinischen Forschung keine personenbezogenen Aussagen zum Ziel, sondern vielmehr allgemeine Zusammenhänge. Werden exemplarisch Kasuistiken publiziert, so ist nicht das Ziel zu zeigen, dass ein bestimmter Sachverhalt bei einer individuellen Person beobachtet wurde, sondern dass dieser Fall (mindestens) einmal im Krankengut aufgetreten ist. Als Beispiel einer wissenschaftlichen Forschung, die personenbezogene Ergebnisse anstrebt, sei die Zeitgeschichte angeführt: hier werden tatsächlich Aussagen über die historische Rolle von bestimmten Personen gemacht.

Der Begriff „wissenschaftliche Forschung“ ist definiert als Bereich, in dem eine bestimmte Methode der Vorgehensweise, nämlich eine „wissenschaftliche“ angewendet wird. Auch der Begriff „Statistik“ wird dahingehend verstanden, dass es sich um methodologisch „wissenschaftliche Statistik“ handelt, da nur unter dieser Voraussetzung eine Privilegierung sachlich zu rechtfertigen ist. Abgesehen davon soll aber dieser Begriff sowohl die sogenannte „amtliche Statistik“ als auch sonstige (mit wissenschaftlichen Methoden durchgeführte) Statistik umfassen.

2.1.4. Rollenmodelle in der wissenschaftlichen Forschung und Statistik

Der für das Erhebungskonzept und die Erhebungsmethodik verantwortliche Datennutzer ist ein Auftraggeber iSd. § 4 Z 4 DSG 2000, das sind natürliche oder juristische Personen, Personengemeinschaften oder Organe einer Gebietskörperschaft beziehungsweise die Geschäftsapparate solcher Organe, wenn sie allein oder gemeinsam mit anderen die Entscheidung getroffen haben, Daten für einen bestimmten Zweck zu verarbeiten, und zwar unabhängig davon, ob sie die Verarbeitung selbst durchführen oder hierzu einen anderen heranziehen. Als Auftraggeber gelten die genannten Personen, Personengemeinschaften und Einrichtungen auch dann, wenn sie einem anderen Daten zur Herstellung eines von ihnen aufgetragenen Werkes überlassen und der Auftragnehmer die Entscheidung trifft, diese Daten zu verarbeiten.

Als sekundäre Datennutzer gelten natürliche oder juristische Personen, Personengemeinschaften oder Organe einer Gebietskörperschaft beziehungsweise die Geschäftsapparate solcher Organe, wenn sie Daten durch Übermittlung iSd. § 4 Z 12 DSG 2000 erhalten haben. Gemäß § 7 Abs. 2 DSG 2000 dürfen Daten nur übermittelt werden, wenn

1. sie aus einer zulässigen Datenanwendung stammen und
2. der Empfänger dem Übermittelnden seine ausreichende gesetzliche Zuständigkeit oder rechtliche Befugnis – soweit diese nicht außer Zweifel steht – im Hinblick auf den Übermittlungszweck glaubhaft gemacht hat und
3. durch Zweck und Inhalt der Übermittlung die schutzwürdigen Geheimhaltungsinteressen des Betroffenen nicht verletzt werden.

Gemäß § 9 DSG 2000 werden die schutzwürdigen Geheimhaltungsinteressen bei der Verwendung sensibler Daten ausschließlich dann nicht verletzt, wenn (auszugsweise)

1. die Daten in nur indirekt personenbezogener Form verwendet werden (Z 2) oder
2. der Betroffene seine Zustimmung zur Verwendung der Daten ausdrücklich erteilt hat, wo bei ein Widerruf jederzeit möglich ist und die Unzulässigkeit der weiteren Verwendung der Daten bewirkt (Z 6), oder
3. Daten für wissenschaftliche Forschung oder Statistik gemäß § 46 oder zur Benachrichtigung oder Befragung des Betroffenen gemäß § 47 verwendet werden (Z 10) oder

4. die Daten zum Zweck der Gesundheitsvorsorge, der medizinischen Diagnostik, der Gesundheitsversorgung oder -behandlung oder für die Verwaltung von Gesundheitsdiensten erforderlich ist, und die Verwendung dieser Daten durch ärztliches Personal oder sonstige Personen erfolgt, die einer entsprechenden Geheimhaltungspflicht unterliegen (Z 12).

Man beachte, dass die Definition „Auftraggebers einer Untersuchung“ als bezüglich Erhebungskonzept und Erhebungsmethodik verantwortlichen Datennutzer eine hinreichend genaue Abgrenzung zu den möglichen Datennutzern erlaubt, insbesondere was die Verwendung von bereits für andere Zwecke oder Untersuchungen ermittelte Daten betrifft. Ein Beispiel möge dies verdeutlichen. Eine Person sei Auftraggeber einer Datenanwendung zum Zweck der Gesundheitsvorsorge, der medizinischen Diagnostik, der Gesundheitsversorgung oder -behandlung im Sinne des § 9 Z 12 DSGVO 2000 und verwende die dabei ermittelten Daten auch gemäß § 46 Abs. 1 für die wissenschaftliche Forschung und Statistik. Zusammen mit Partnern, etwa im Rahmen eines Konsortiums zur Durchführung einer multizentrischen Studie, fungiere diese Person auch als Auftraggeber einer Datenanwendung nach § 9 Z 10 DSGVO 2000. Sollen nun einzelne, in der Routine erhobene Daten im Rahmen der multizentrischen Studien verwendet werden, so darf dies aufgrund der unterschiedlichen Auftraggeber nur in indirekt personenbezogener Form oder mit Zustimmung des Betroffenen bzw. mit Genehmigung der Datenschutzkommission erfolgen. Dies gilt auch für die Übermittlung der Multicenterdaten in die umgekehrte Richtung.

Der Datenverkehr in das Ausland ist gemäß § 12 DSGVO 2000 genehmigungsfrei, wenn die Übermittlung oder Überlassung von Daten an Empfänger in Mitgliedstaaten der Europäischen Union (Abs. 1) oder an Empfänger in Drittstaaten mit angemessenem Datenschutz¹ (Abs. 2) erfolgt. Darüber hinaus ist der Datenverkehr ins Ausland dann genehmigungsfrei, wenn (auszugsweise)

1. die Daten im Inland zulässigerweise veröffentlicht wurden (Abs. 3 Z 1) oder
2. Daten, die für den Empfänger nur indirekt personenbezogen sind, übermittelt oder überlassen werden (Abs. 3 Z 2) oder
3. der Betroffene ohne jeden Zweifel seine Zustimmung zur Übermittlung oder Überlassung seiner Daten ins Ausland gegeben hat (Abs. 3 Z 5).

Soweit der Datenverkehr mit dem Ausland nicht gemäß § 12 DSGVO 2000 genehmigungsfrei ist, hat der Auftraggeber vor der Übermittlung oder Überlassung von Daten in das Ausland eine Genehmigung der Datenschutzkommission einzuholen (§ 13 DSGVO 2000).

Laut § 14 Abs. 2 Z 7 DSGVO 2000 ist über eine durchgeführte Übermittlung Protokoll zu führen, damit ihre Zulässigkeit im notwendigen Ausmaß nachvollzogen werden kann.

2.1.5. Zur Verfügungstellung von Adressen zur Benachrichtigung und Befragung von Betroffenen

Gemäß § 47 Abs. 1 DSGVO 2000 bedarf die Übermittlung von Adressdaten eines bestimmten Kreises von Betroffenen zum Zweck ihrer Benachrichtigung oder Befragung der Zustimmung der Betroffenen.

Wenn allerdings angesichts der Auswahlkriterien für den Betroffenenkreis und des Gegenstands der Benachrichtigung oder Befragung eine Beeinträchtigung der Geheimhaltungsinteressen der Betroffenen unwahrscheinlich ist, bedarf es laut § 47 Abs. 2 keiner Zustimmung, wenn

1. Daten desselben Auftraggebers verwendet werden oder
2. bei einer beabsichtigten Übermittlung der Adressdaten an Dritte

¹ Welche Drittstaaten angemessenen Datenschutz gewährleisten, wird unter Beachtung des § 55 Z 1 durch Verordnung des Bundeskanzlers festgestellt. Maßgebend für die Angemessenheit des Schutzes ist die Ausgestaltung der Grundsätze des § 6 Abs. 1 in der ausländischen Rechtsordnung und das Vorhandensein wirksamer Garantien für ihre Durchsetzung.

- a. an der Benachrichtigung oder Befragung auch ein öffentliches Interesse besteht oder
- b. der Betroffene nach entsprechender Information über Anlass und Inhalt der Übermittlung innerhalb angemessener Frist keinen Widerspruch gegen die Übermittlung erhoben hat.

Liegen die Voraussetzungen des § 47 Abs. 2 nicht vor und würde die Einholung der Zustimmung der Betroffenen gemäß § 47 Abs. 1 einen unverhältnismäßigen Aufwand erfordern, so ist nach § 47 Abs. 3 Z 3 die Übermittlung der Adressdaten an Dritte zur Befragung der Betroffenen für wissenschaftliche oder statistische Zwecke mit Genehmigung der Datenschutzkommission zulässig. Die übermittelten Adressdaten sind zu löschen, sobald sie für die Benachrichtigung oder Befragung nicht mehr benötigt werden (§ 47 Abs. 5).

In jenen Fällen, in welchen es gemäß den vorstehenden Bestimmungen zulässig ist, Namen und Adresse von Personen, die einem bestimmten Betroffenenkreis angehören, zu übermitteln, dürfen auch die zum Zweck der Auswahl der zu übermittelnden Adressdaten notwendigen Verarbeitungen vorgenommen werden.

2.1.6. Verwendung von Daten in der Lehre

Sofern nicht öffentlich zugänglich, ist die Verwendung von personenbezogenen Daten in der allgemeinen Lehre einer Veröffentlichung dieser Daten gleichzusetzen,² unabhängig davon, ob eine Verwendung im Rahmen einer Präsentation oder für publizistische Zwecke inklusive der Anwendung „Neuer Medien“ (Computer- bzw. Web-based Training) erfolgt. Für die Praxis bedeutet dies, dass – neben der ausdrücklichen Zustimmung des Betroffenen zur Veröffentlichung der Daten nach § 9 Z 1 bzw. § 9 Z 6 DSGVO 2000 – nur anhand abstrakter Beispiele bzw. mit Materialien gearbeitet werden darf, die aufgrund ihrer mangelnden Rückführung auf den Betroffenen einem Geheimhaltungsanspruch nicht zugänglich sind (§ 1 Abs. 1 DSGVO 2000).

Werden Personen zu Ausbildungszwecken in den Dienstbetrieb eines Auftraggebers oder Dienstleisters integriert, so sind diese datenschutzrechtlich wie Mitarbeiter zu behandeln, d.h. die Auszubildenden haben Daten aus Datenanwendungen, die ihnen im Rahmen der Unterweisung oder auch bei selbstständiger Anwendung und Festigung des Erlernten zugänglich geworden sind, geheim zu halten (Datengeheimnis gemäß § 15 Abs. 1 DSGVO 2000). Darüber hinaus sind nach § 15 Abs. 2 die Auszubildenden vertraglich zu verpflichten, das Datengeheimnis auch nach Beendigung der Ausbildung einzuhalten.

2.2. Anonymisierung

2.2.1. Indirekt personenbezogene Daten

Die Richtlinie 95/46/EG des Europäischen Parlaments geht davon aus, dass Daten nicht nur dann „personenbezogen“ sind, wenn die Identität des Betroffenen für den jeweiligen Verwender bestimmbar ist, sondern auch dann, wenn sie nur für einen Dritten (z.B. den Inhaber des Entschlüsselungscodes bei codierten Identitätsdaten) bestimmbar sind. Um in Hinblick auf das Schutzinteresse eine sinnvolle Abstufung vornehmen zu können, wird nun im DSGVO zwischen direkter und (nur) indirekter Identifizierbarkeit unterschieden; wenn es für den konkreten Verwender der Daten nicht möglich ist, den – z.B. in Form einer laufenden oder sprechenden Nummer – vorhandenen Personenbezug auf eine in ihrer Identität bestimmte Person zurückzuführen, dann ist der Gebrauch solcher „nur indirekt personenbezogener“ Daten durch diesen Verwender unter erleichterten datenschutzrechtlichen Bedingungen erlaubt.³ Was als möglich anzusehen ist, wird in Erwägungsgrund 26 der EU-Richtlinie ausgeführt: „Als mögliches Mittel der

² Das Datengeheimnis bzw. eine Verpflichtung zur Geheimhaltung ist in der allgemeinen Lehre nicht verwirklicht, da – etwa bei der Überprüfung des Erreichens der Lehrziele – häufig eine Wieder- bzw. Weitergabe dieser Daten notwendig ist.

³ Von den „nur indirekt personenbezogenen“ Daten sind die üblicherweise als „anonymisiert“ bezeichneten Daten zu unterscheiden. Bei anonymisierten Daten gibt es keinen Personenbezug; hierbei handelt es sich um Daten, die niemand auf eine in ihrer Identität bestimmte Person zurückführen kann. Derartige Daten sind daher auch nicht datenschutzrelevant.

Identifikation ist ein solches anzusehen, das „vernünftigerweise“ angewendet wird, d.h. das weder seiner Art nach, noch seinem Aufwand nach vollkommen ungewöhnlich ist.“

Vor dem Hintergrund einer Informationsgesellschaft mit einem stark dynamischen Technologieverständnis bedarf die Frage, welche Mittel als „vernünftig“ bzw. als „vollkommen ungewöhnlich“ anzusehen sind einer präziseren, d.h. von den verfügbaren Technologien und Datensammlungen unabhängigen Antwort. So ist ein häufiges Missverständnis, dass der Personenbezug von Daten durch Verschlüsselung oder Löschung jener Attribute zuverlässig eliminiert wird, welche offensichtlich geeignet sind, eine Person zu identifizieren (z.B. Name, Adresse, Sozialversicherungs- oder Telefonnummer etc.). Ist – etwa durch Kombination der verbleibenden Datenelemente – ein einzelner Datensatz eindeutig auszeichnbar, so kann diese Information dazu verwendet werden, beispielsweise durch Verknüpfung mit öffentlich verfügbaren Daten, die Identität des Betroffenen festzustellen.

Welche Daten öffentlich verfügbar sind oder welche Daten der Empfänger einer Übermittlung im Detail zulässigerweise verwenden darf, entzieht sich häufig der Kenntnis des Übermittlers. Diese Situation kann bei der praktischen Entscheidung, ob Daten als indirekt personenbezogen eingestuft werden können, zu erheblicher Unsicherheit führen. Aufgrund der Bedeutung der wissenschaftlichen Forschung und Statistik für die Gesellschaft erscheint eine allgemein restriktive Datenschutz-Policy (Disclosure avoidance) als wenig produktiv. Umgekehrt erzeugen einfache, klare und vor allem nachhaltig wirksame Regeln zur Geheimhaltung persönlicher Daten vielfach erst die Bereitschaft, wissenschaftliche Untersuchungen als Betroffener zu unterstützen. Eine adäquate Datenschutz-Policy, welche die im DSG 2000 gegebene Definition von „indirekt personenbezogen Daten“ in praxi hinreichend erfüllt, muss daher

1. selektiv auf die zu verarbeitenden bzw. zu übermittelnden Daten eingehen, diese
2. bezüglich eines möglichen Personenbezugs analysieren und kategorisieren sowie
3. entsprechende Methoden beschreiben, die eine Rückführung der Daten auf einen Betroffenen verhindern (Disclosure control bzw. Disclosure limitation).

Dabei ist wesentlich, dass die zu etablierende Policy von anderen als den beim Auftraggeber zulässigerweise verarbeitbaren bzw. von den zu übermittelnden Daten unabhängig ist.

Für die Definition der Datenschutz-Policy ist zwischen primären und sekundären Identifikationsdaten zu unterscheiden.

2.2.2. Primäre Identifikationsdaten

Primäre Identifikationsdaten sind Attribute oder Attributkombinationen, die von Natur her oder aufgrund ihrer Definition oder Verwendung dazu dienen, eine Person eindeutig zu identifizieren, auch wenn dazu eine Verknüpfung mit anderen Daten notwendig ist. Beispiele für primäre Identifikationsdaten sind „Name und Adresse“, „Sozialversicherungsnummer“, die „Telefonnummer“ unter der ein Betroffener erreichbar ist, eine „Aufnahmezahl“ oder „Untersuchungsnummer“ in einem Krankenhaus usw. Zur Elimination des Personenbezugs ist die Möglichkeit einer Verwendung all dieser Daten zur Bestimmung der Identität des Betroffenen zuverlässig auszuschließen, d.h. jedes Attribut der primären Identifikationsdaten ist entweder zu löschen oder sicher zu verschlüsseln. Die auf die primären Identifikationsdaten anzuwendende Datenschutz-Policy ist dementsprechend eine Beschränkung der zu übermittelnden Attribute. Eine detaillierte Diskussion primärer Identifikationsdaten findet sich in Abschnitt 3.7.

2.2.3. Sekundäre Identifikationsdaten

Als sekundäre Identifikationsdaten werden jene Attribute einer Person bezeichnet, die bei Kombination und aufgrund der möglichen Attributwerte ein eindeutiges Muster ausprägen können, so dass in dieser Form eine Identifikation des Betroffenen durch Verknüpfung mit anderen Daten möglich ist. Ein Beispiel für sekundäre Identifikationsdaten einer natürlichen

Person sind die Attribute „Wohnort“ und „Beruf“, wenn der Betroffene in einer kleinen Gemeinde lebt und einer relativ seltenen Beschäftigung (etwa Tierarzt) nachgeht. In diesem Fall kann durch Verknüpfung der Daten mit dem Telefonbuch des Wohnorts die Identität der Person bestimmt werden, falls der Betroffene – vielleicht aus wirtschaftlichen Gründen – die Veröffentlichung seines Berufs im Rufnummernverzeichnis veranlasst hat.⁴ Ein wesentliches Unterscheidungsmerkmal der sekundären Identifikationsdaten von den primären ist die Eigenschaft, dass nicht die Besonderheit der Attribute per se sondern die Kombination der Attributwerte einen Datensatz auszeichnet und typischerweise trifft dies nur auf einen Teil des Kollektivs zu. Ist die Berufsbezeichnung im beschriebenen Beispiel etwa Landwirt, so mag gut sein, dass keine Eindeutigkeit vorliegt und folglich eine Identifikation nicht möglich ist. Dieser Umstand gilt insbesondere dann, wenn bereits die übermittelten Daten keine Eindeutigkeit bezüglich der sekundären Attribute aufweisen, d.h. wenn für jeden Datensatz im Rahmen einer Übermittlung mindestens ein weiterer mit den gleichen sekundären Identifikationsdaten existiert. Für diese Klasse von Daten ist somit eine Datenschutz-Policy anzustreben, die allgemein auf einer Beschränkung der übermittelten Attributwerte beruht (siehe auch Sektion 3.8.).

2.2.4. Beschränkte Übermittlung von Daten

Sei \mathbf{X} eine (m, n) -Matrix von Daten für m Personen mit n Attributen. Unter einer beschränkten Übermittlung \mathbf{M} der Daten \mathbf{X} versteht man eine Abbildung der Form

$$\mathbf{M} = \mathbf{A} \mathbf{X} \mathbf{B} + \mathbf{C}, \quad (1)$$

wobei die Matrix \mathbf{A} die Fälle und \mathbf{B} die Variablen transformiert, und \mathbf{C} ein Rauschen in den Komponenten von \mathbf{X} , genauer von $\mathbf{A} \mathbf{X} \mathbf{B}$, beschreibt. Im Rahmen dieser allgemeinen Form können eine Reihe von bekannten Vorgehensweisen zur Anonymisierung der Daten \mathbf{X} als Spezialfälle von \mathbf{M} betrachtet werden:

1. Freigabe einer Teilmenge der Daten (von Samples) durch Löschen von Zeilen in \mathbf{X} ,
2. Beifügen von simulierten Daten als weitere Zeilen in \mathbf{X} ,
3. Aggregation einzelner Personen zu Clustern durch Kombination von Zeilen in \mathbf{X} ,
4. Zusätzen von stochastischen Störungsfunktionen mittels \mathbf{C} ,
5. Unterdrücken einzelner Attribute durch Löschen von Spalten in \mathbf{X} ,
6. Weitergabe der Varianz-Kovarianz Matrix ($\mathbf{A} = \mathbf{X}^T$).

Weitere Beispiele für mögliche Transformationen, welche aber nicht strikt der Form \mathbf{M} entsprechen sind: das Austauschen von Zeilen für einen Teil der Spalten in \mathbf{X} sowie Coarsening, Kategorisieren oder das Abschneiden (Truncation) von Attributwerten.

Werden die Daten \mathbf{X} in der Form \mathbf{M} weitergeben, so sind je nach der gewählten Methode zusätzliche Informationen über \mathbf{A} , \mathbf{B} und \mathbf{C} notwendig. Gilt etwa $\mathbf{B} \neq \mathbf{I}$, so sind i. Allg. Kenntnisse über Teile von \mathbf{B} vonnöten, andernfalls ist die Bedeutung der Attributwerte nicht ersichtlich. Ist \mathbf{C} eine stochastische Störungsfunktion, benötigt man für eine teilweise Umkehr der Maskierung neben dem Erwartungswert $E(\mathbf{C})$ auch $\text{Var}(\mathbf{C})$, die Varianz von \mathbf{C} . Es sei an dieser Stelle darauf hingewiesen, dass sowohl die gewählte Methode \mathbf{M} wie auch die Frage welche Informationen über \mathbf{A} , \mathbf{B} und \mathbf{C} veröffentlicht werden zu den Bereichen aktiver Forschung zählen.

Man beachte, dass das allgemeine Modell \mathbf{M} auch auf longitudinale Daten anwendbar ist. Sei dazu \mathbf{X}_t eine (m, n) -Matrix von Daten für m Personen mit n Attributen zum Zeitpunkt t , $1 \leq t \leq q$. Dann kann die Folge der Daten $\mathbf{X}_1, \mathbf{X}_2, \dots, \mathbf{X}_q$ durch Transformation des $m \times n \times q$ -Raums als (mq, nq) -Matrix dargestellt werden.

⁴ Die im Beispiel skizzierte Vorgehensweise kann freilich zu einem falschen Ergebnis führen. Man bedenke allerdings, dass i. Allg. auch Dritte nicht in der Lage sind, diese fehlerhafte Zuordnung zu erkennen.

2.2.5. k -Anonymität

Im weiteren wird davon ausgegangen, dass alle primären Identifikationsdaten in \mathbf{X} zuverlässig eliminiert wurden.

Sei \mathbf{X} wiederum eine (m, n) -Matrix von Daten für m Personen mit n Attributen. Bezeichne weiters J die Menge der Spaltenindizes, die den sekundären Identifikationsdaten entsprechen. Eine beschränkte Übermittlung \mathbf{M} heißt k -anonymisiert, wenn jede Kombination von Bildern der Projektionen (x_{ij}) , mit $i = 1, 2, \dots, m$ und $j \in J$, mindestens k -mal in \mathbf{M} vorkommt.

Aus der Definition folgt, dass für eine Anonymisierung $k \geq 2$ gelten muss, wobei allgemein bei der Festlegung von k auf die Anzahl der Datensätze m bedacht zu nehmen ist. In der Praxis gilt bei Wahl von $k \geq 5$ die Definition von „indirekt personenbezogen“ als hinreichend erfüllt.

Die Zahl k repräsentiert eine untere Schranke für die Identifizierbarkeit eines Betroffenen, da zu jeder Wertkombination sekundärer Identifikationsdaten mindestens k identische Datensätze in \mathbf{M} bestehen und es ist annehmen, dass in der realen Welt noch deutlich mehr Personen existieren, die durch die gegebene Kombination von Merkmalen nicht unterscheidbar sind. Kann etwa nach der Anwendung von Transformation (1) auf einer Obermenge von \mathbf{X} k -Anonymität gezeigt werden, so ist die Bedingung der k -Anonymität auch für \mathbf{M} hinreichend erfüllt. Mit anderen Worten: sind etwa in einer Datenanwendung zum Zweck der medizinischen Diagnostik und Behandlung mindestens k Personen mit den gleichen sekundären Identifikationsdaten wie in einem fraglichen Datensatz auffindbar, dann ist auch die Bedingung der k -Anonymität für diesen Datensatz bewiesen.

Man bedenke allerdings, dass jede beschränkte Übermittlung von Daten die Wahrscheinlichkeit der Identifizierbarkeit eines Betroffenen erhöht. Diese Situation wird in der Literatur manchmal als Inferential disclosure bezeichnet und konsequenterweise sind für k möglichst große Werte anzustreben.

3. Datenschutz-Policy

3.1. Allgemeine Datensicherheitsmaßnahmen

3.1.1. Rahmenbedingungen

Gemäß § 14 Abs. 1 DSG 2000 sind für alle Organisationseinheiten eines Auftraggebers oder Dienstleisters, die Daten verwenden, Maßnahmen zur Gewährleistung der Datensicherheit zu treffen. Dabei ist je nach der Art der verwendeten Daten und nach Umfang und Zweck der Verwendung sowie unter Bedachtnahme auf den Stand der technischen Möglichkeiten und auf die wirtschaftliche Vertretbarkeit sicherzustellen, dass die Daten vor zufälliger oder unrechtmäßiger Zerstörung und vor Verlust geschützt sind, dass ihre Verwendung ordnungsgemäß erfolgt und dass die Daten Unbefugten nicht zugänglich sind.

Insbesondere ist (soweit erforderlich)

1. die Aufgabenverteilung bei der Datenverwendung zwischen den Organisationseinheiten und zwischen den Mitarbeitern ausdrücklich festzulegen,
2. die Verwendung von Daten an das Vorliegen gültiger Aufträge der anordnungsbefugten Organisationseinheiten und Mitarbeiter zu binden,
3. jeder Mitarbeiter über seine nach DSG 2000 und nach innerorganisatorischen Datenschutzvorschriften einschließlich der Datensicherheitsvorschriften bestehenden Pflichten zu belehren,
4. die Zutrittsberechtigung zu den Räumlichkeiten des Auftraggebers oder Dienstleisters zu regeln,
5. die Zugriffsberechtigung auf Daten und Programme und der Schutz der Datenträger vor der Einsicht und Verwendung durch Unbefugte zu regeln,
6. die Berechtigung zum Betrieb der Datenverarbeitungsgeräte festzulegen und jedes Gerät durch Vorkehrungen bei den eingesetzten Maschinen oder Programmen gegen die unbefugte Inbetriebnahme abzusichern,
7. Protokoll zu führen, damit tatsächlich durchgeführte Verwendungsvorgänge, wie insbesondere Änderungen, Abfragen und Übermittlungen, im Hinblick auf ihre Zulässigkeit im notwendigen Ausmaß nachvollzogen werden können,
8. eine Dokumentation über die nach Z 1 bis 7 getroffenen Maßnahmen zu führen, um die Kontrolle und Beweissicherung zu erleichtern.

Sofern gesetzlich nicht ausdrücklich anderes angeordnet ist, sind Protokoll- und Dokumentationsdaten drei Jahre lang aufzubewahren. Davon darf in jenem Ausmaß abgewichen werden, als der von der Protokollierung oder Dokumentation betroffene Datenbestand zulässigerweise früher gelöscht oder länger aufbewahrt wird (§ 14 Abs. 5 DSG 2000).

Datensicherheitsvorschriften sind so zu erlassen und zur Verfügung zu halten, dass sich die Mitarbeiter über die für sie geltenden Regelungen jederzeit informieren können (§ 14 Abs. 6).

3.1.2. Vorgehensmodell

Für den Betrieb von Datenanwendungen wird dem Auftraggeber die Spezifikation einer allgemeinen Sicherheits-Policy angeraten, welche die einzuhaltenden organisatorischen und technischen Datensicherheitsmaßnahmen in Art und Umfang regelt. Typische, in dieser Policy abzuhandelnde Themen sind Bestimmungen zur Benutzer- und Zugriffskontrolle (Authentifizierung

und Autorisierung), Maßnahmen zur Gewährleistung der Datenintegrität, Mechanismen zur Übermittlungs- und Organisationskontrolle usw. Eine ausführliche Darstellung von notwendigen und empfohlenen Maßnahmen findet sich in den „Rahmenbedingungen für ein logisches österreichisches Gesundheitsdatennetz – MAGDA-LENA“.

Zusätzlich zu den in MAGDA-LENA beschriebenen Maßnahmen ist für eine Datenanwendung zum Zweck der wissenschaftlichen Forschung und Statistik zu entscheiden, wie mit den Daten nach Abschluss der Untersuchung zu verfahren ist. Kommt eine dauerhafte Löschung der Daten nicht in Betracht, so wird empfohlen, eine Archivierung der Daten „offline“ auf einem Wechselspeichermedium durchzuführen und die Kopie an einem sicheren Ort zu verwahren. Auf diese Weise kann eine zufällige oder unrechtmäßige Zerstörung bzw. unbefugte Verwendung der Daten weitgehend ausgeschlossen werden.

Bei der Implementierung von Datensicherheitsmaßnahmen wird empfohlen, entsprechende Regelungen der lokalen Rechenzentren zu berücksichtigen.

3.2. Datengeheimnis

3.2.1. Rahmenbedingungen

Auftraggeber, Dienstleister und ihre Mitarbeiter haben gemäß § 15 Abs. 1 DSG 2000 Daten aus Datenanwendungen, die ihnen ausschließlich auf Grund ihrer berufsmäßigen Beschäftigung anvertraut wurden oder zugänglich geworden sind, unbeschadet sonstiger gesetzlicher Verschwiegenheitspflichten, geheim zu halten, soweit kein rechtlich zulässiger Grund für eine Übermittlung der anvertrauten oder zugänglich gewordenen Daten besteht (Datengeheimnis). Weiters haben nach § 15 Abs. 2 Auftraggeber und Dienstleister, sofern eine solche Verpflichtung ihrer Mitarbeiter nicht schon kraft Gesetzes besteht, diese vertraglich zu verpflichten, dass sie das Datengeheimnis auch nach Beendigung des Arbeits(Dienst)verhältnisses zum Auftraggeber oder Dienstleister einhalten werden.

3.2.2. Vorgehensmodell

Für die praktische Umsetzung des § 15 DSG 2000 wird Auftraggebern bzw. Dienstleistern eine regelmäßige (jährliche) datenschutzrechtliche Belehrung ihrer Mitarbeiter empfohlen. Diese ist in Art und Umfang durch den Mitarbeiter zu bestätigen.

Neben der in § 15 Abs. 1 formulierten rechtlichen Zulässigkeit der Datenübermittlung ist das Datengeheimnis auch an die praktische Notwendigkeit ebendieser zu binden. Es wird daher angeraten, in das Datengeheimnis auch auf indirekt personenbezogene Daten einzubeziehen.

3.3. Meldepflicht des Auftraggebers

3.3.1. Rahmenbedingungen

Gemäß § 17 Abs. 1 DSG 2000 hat jeder Auftraggeber vor Aufnahme einer Datenanwendung eine Meldung an die Datenschutzkommission zum Zweck der Registrierung im Datenverarbeitungsregister zu erstatten. Neben der Aufnahme der Datenverarbeitung sind gemäß § 4 Datenverarbeitungsregister-Verordnung 2000 zu melden:

1. jede Änderung oder Ergänzung einer bereits registrierten Datenanwendung vor Aufnahme der geänderten oder ergänzten Datenanwendung;
2. der Eintritt eines Grundes für die Streichung einer registrierten Datenanwendung, insbesondere der Wegfall ihrer Rechtsgrundlage, unverzüglich nachdem er sich ereignet hat;
3. jede Änderung des Namens oder der sonstigen Bezeichnung oder der Anschrift des Auftraggebers, unverzüglich nach Eintritt der Änderung.

Von dieser Meldepflicht ausgenommen sind Datenanwendungen, die (auszugsweise)

1. ausschließlich veröffentlichte Daten umfassen oder
2. nur indirekt personenbezogene Daten enthalten oder
3. einer Standardanwendung⁵ entsprechen.

Eine Meldung im Sinne des § 17 hat zu beinhalten (siehe § 19 DGS 2000):

1. den Namen (die sonstige Bezeichnung) und die Anschrift des Auftraggebers sowie eines allfälligen Vertreters gemäß § 6 Abs. 3 oder eines Betreibers gemäß § 50 Abs. 1 DSG 2000, weiters die Registernummer des Auftraggebers, sofern ihm eine solche bereits zugeteilt wurde, und
2. den Nachweis der gesetzlichen Zuständigkeit oder der rechtlichen Befugnis für die erlaubte Ausübung der Tätigkeit des Auftraggebers, soweit dies erforderlich ist, und
3. den Zweck der zu registrierenden Datenanwendung und ihre Rechtsgrundlagen, soweit sich diese nicht bereits aus den Angaben nach Z 2 ergeben, und
4. die Kreise der von der Datenanwendung Betroffenen und die über sie verarbeiteten Datenarten und die Kreise der von beabsichtigten Übermittlungen Betroffenen, die zu übermittelnden Datenarten und die zugehörigen Empfängerkreise – einschließlich allfälliger ausländischer Empfängerstaaten sowie die Rechtsgrundlagen der Übermittlung und
5. soweit eine Genehmigung der Datenschutzkommission notwendig ist die Geschäftszahl der Genehmigung durch die Datenschutzkommission sowie
6. allgemeine Angaben über die getroffenen Datensicherheitsmaßnahmen im Sinne des § 14 DSG 2000, die eine vorläufige Beurteilung der Angemessenheit der Sicherheitsvorkehrungen erlauben.

Gemäß § 18 Abs. 1 DSG 2000 darf der Vollbetrieb einer meldepflichtigen Datenanwendung unmittelbar nach Abgabe der Meldung aufgenommen werden. Von dieser Regelung sind nach § 18 Abs. 2 meldepflichtige Datenanwendungen ausgenommen, wenn sie sensible Daten enthalten. In diesem Fall darf die Verarbeitung erst nach Prüfung (Vorabkontrolle) durch die Datenschutzkommission nach den näheren Bestimmungen des § 20 DSG 2000 aufgenommen werden.⁶

3.3.2. Vorgehensmodell

Zur Erleichterung und Vereinheitlichung der Meldungen hat die Datenschutzkommission elektronische Formblätter aufgelegt, die auch im Wege der automationsunterstützten Datenübertragung eingebracht werden können. Eine elektronische Meldung gilt als erstattet, wenn sie an der von der Datenschutzkommission im Formblatt hierfür angegebenen E-Mail-Adresse eingegangen ist. Es wird empfohlen, die elektronische Meldung mit einer sicheren elektronischen Signatur im Sinne des § 4 Abs. 1 SigG 1999 zu versehen.

⁵ Der Bundeskanzler kann durch Verordnung Typen von Datenanwendungen und Übermittlungen aus diesen zu Standardanwendungen erklären, wenn sie von einer großen Anzahl von Auftraggebern in gleichartiger Weise vorgenommen werden und angesichts des Verwendungszwecks und der verarbeiteten Datenarten die Gefährdung schutzwürdiger Geheimhaltungsinteressen der Betroffenen unwahrscheinlich ist. In der Verordnung sind für jede Standardanwendung die zulässigen Datenarten, die Betroffenen- und Empfängerkreise und die Höchstdauer der zulässigen Datenaufbewahrung festzulegen.

In diesem Zusammenhang sei auf die Standardanwendung SA024 „Patientenverwaltung und Honorarabrechnung“ mit dem Zweck der „Führung von Patientenkarteen zur Dokumentation (§ 51 ÄrzteG 1998), Erstellung von medizinischen Gutachten und Honorarverrechnung durch Ärzte, Zahnärzte und Dentisten, einschließlich automationsunterstützt erstellter und archivierter Textdokumente (wie z.B. Korrespondenz) in diesen Angelegenheiten“ hingewiesen.

⁶ Aus dieser Vorgehensweise ist i. Allg. mit keiner zeitlichen Verzögerung von wissenschaftlichen Projekten zu rechnen, da dieser Schritt parallel zur Begutachtung des Vorhabens durch die lokale Ethikkommission durchgeführt werden kann.

Wird bei der Meldung einer Datenanwendung zum Zweck der Gesundheitsvorsorge, der medizinischen Diagnostik, der Gesundheitsversorgung oder -behandlung iSd. § 9 Z 12 DSG 2000 allgemein auf die Verwendung der Daten für wissenschaftliche Forschung und Statistik hingewiesen, so gilt die Meldepflicht des Auftraggebers bei einer Verwendung dieser Daten nach § 46 Abs. 1 DSG 2000 als erfüllt. Alle anderen meldepflichtigen Datenanwendungen iSd. § 46 sind der Datenschutzkommission unter Angabe des konkreten Zwecks (Fragestellung) der Untersuchung anzuzeigen. Man beachte, dass eine Meldung immer auch dann durchzuführen ist, wenn

1. der Betroffene seine Zustimmung zur Verwendung der Daten erteilt hat (siehe Abschnitt 3.5.) oder
2. ein Auftraggeber eine Untersuchung unter Verwendung von Daten einer früheren, gemeldeten Anwendung durchführen will und die nunmehrige Fragestellung nicht in einem direkten Bezug zur früheren Anwendung steht.

Der Zeitpunkt der Meldung und der Aufnahme der Datenanwendung ist zu protokollieren.

3.4. Informationspflicht des Auftraggebers

3.4.1. Rahmenbedingungen

In Übereinstimmung mit § 24 Abs. 1 DSG 2000 hat der Auftraggeber einer Datenanwendung aus Anlass der Ermittlung von Daten die Betroffenen in geeigneter Weise

1. über den Zweck der Datenanwendung, für die die Daten ermittelt werden, und
2. über Namen und Adresse des Auftraggebers,

zu informieren, sofern diese Informationen dem Betroffenen nach den Umständen des Falles nicht bereits vorliegen. Darüber hinausgehende Informationen sind gemäß § 24 Abs. 2 DSG 2000 in geeigneter Weise zu geben, wenn dies für eine Verarbeitung nach Treu und Glauben erforderlich ist; dies gilt insbesondere dann, wenn

1. gegen eine beabsichtigte Verarbeitung oder Übermittlung von Daten ein Widerspruchsrecht des Betroffenen gemäß § 28 besteht oder
2. es für den Betroffenen nach den Umständen des Falles nicht klar erkennbar ist, ob er zur Beantwortung der an ihn gestellten Fragen rechtlich verpflichtet ist.

Werden Daten nicht durch Befragung des Betroffenen, sondern durch Übermittlung von Daten aus anderen Aufgabengebieten desselben Auftraggebers oder aus Anwendungen anderer Auftraggeber ermittelt, darf die Information gemäß Abs. 1 entfallen, wenn sie angesichts der Unwahrscheinlichkeit einer Beeinträchtigung der Betroffenenrechte einerseits und der Kosten der Information aller Betroffenen andererseits einen unverhältnismäßigen Aufwand erfordert. Dies liegt insbesondere dann vor, wenn Daten für Zwecke der wissenschaftlichen Forschung oder Statistik gemäß § 46 oder Adressdaten im Rahmen des § 47 ermittelt werden und die Information des Betroffenen in diesen Bestimmungen nicht ausdrücklich vorgeschrieben ist.

Die Informationspflicht des Auftraggebers soll es dem Betroffenen erleichtern, seine Rechte zu wahren. Weitere, ergänzende Instrumente für diesen Zweck sind das Datenverarbeitungsregister, die Offenlegung nach § 23 und schließlich die Auskunft gemäß § 26 DSG 2000. Vor dem Hintergrund des Bestehens einer Registrierungspflicht ist der Sinn einer zusätzlichen Informationspflicht darin zu sehen, dass dem Betroffenen immer dann, „wenn ihm diese Information nicht bereits vorliegt“, der Hinweis darauf gegeben wird, dass seine Daten von einem bestimmten Auftraggeber für einen bestimmten Zweck verarbeitet werden sollen. Dadurch wird er in die Lage versetzt, sich – falls er dies wünscht – aller Hilfsmittel zu bedienen, um „ordnungsgemäß und

umfassend informiert zu werden“, und und zwar ohne unzumutbare Anstrengungen seinerseits, aber auch ohne unzumutbare und unnötige Belastung des Auftraggebers.

3.4.2. Vorgehensmodell

Werden Patientendaten gemäß § 7 in Verbindung mit § 9 Z 12 DSG 2000 für die medizinische Diagnostik und Behandlung erhoben, so kann der Datenermittler davon ausgehen, dass der Verarbeitungszweck für den Betroffenen unmittelbar einsichtig ist bzw. eine ausdrückliche Information des Betroffenen bei ihm wahrscheinlich Befremden hervorrufen würde. Aufgrund der expliziten Ausformung des § 46 Abs. 1 DSG 2000 schließt dies auch die Verwendung der Daten für die wissenschaftliche Forschung und Statistik ein.

Werden Daten aber im Sinne des § 9 Z 10 DSG 2000 zum Zweck der wissenschaftlichen Forschung und Statistik (§ 46) oder zur Benachrichtigung oder Befragung des Betroffenen (§ 47) erhoben, so ist der Betroffene entsprechend zu informieren. Dies schließt die Anwendung des § 24 Abs. 2 DSG 2000 ein.

Erfolgt die Verwendung der Daten aufgrund der Zustimmung des Betroffenen iSd. § 9 Z 5 DSG 2000, so ist der Betroffene jedenfalls vor bzw. im Rahmen der Zustimmung umfassend zu informieren (siehe dazu auch den folgenden Abschnitt „Zustimmung des Betroffenen“). Es wird dem Auftraggeber empfohlen, die Erfüllung der Informationspflicht in Art und Umfang vom Betroffenen bestätigen zu lassen.

3.5. Zustimmung des Betroffenen

3.5.1. Rahmenbedingungen

Allgemein werden gemäß § 8 Abs. 1 Z 2 bzw. § 9 Z 6 DGS 2000 die schutzwürdigen Geheimhaltungsinteressen bei der Verwendung nicht-sensibler bzw. sensibler Daten nicht verletzt, wenn der Betroffene seine Zustimmung zur Verwendung der Daten ausdrücklich erteilt hat, wobei ein Widerruf jederzeit möglich ist und die Unzulässigkeit der weiteren Verwendung der Daten bewirkt. Dies gilt nach § 12 Abs. 3 auch für den Datenverkehr ins Ausland, wenn der Betroffene ohne jeden Zweifel seine Zustimmung zur Übermittlung oder Überlassung seiner Daten ins Ausland gegeben hat. Dabei ist der Begriff der „Zustimmung“ laut § 4 Z 14 DSG 2000 definiert als eine gültige, insbesondere ohne Zwang abgegebene Willenserklärung des Betroffenen, dass er in Kenntnis der Sachlage für den konkreten Fall in die Verarbeitung oder Übermittlung seiner Daten einwilligt.

3.5.2. Vorgehensmodell

In den Erläuterungen zum DSG 2000 ist ausgeführt, dass eine datenschutzrechtliche Zustimmung bei der Verwendung von sensiblen Daten ausdrücklich vorliegen muss, wobei die Schriftlichkeit nur dann notwendig ist, wenn es um den Nachweis geht, dass die Zustimmung zweifelsfrei vorliegt.

Unabhängig von der Form der Zustimmung sind der Zweck und die Verwendung der Daten so ausreichend darzulegen, dass die daraus zu erwartenden Konsequenzen für den Betroffenen ersichtlich sind. Unter Berücksichtigung der jeweiligen Sachlage hat eine Aufklärung die folgenden Punkte zu beinhalten:

1. den Zweck der wissenschaftlichen oder statistischen Untersuchung;
2. den für das Erhebungskonzept und die Erhebungsmethodik verantwortlichen Datennutzer (Auftraggeber);
3. die betroffene Personengruppe, also das Auswahlkriterium für eine Aufnahme in die konkrete Untersuchung;

4. die in der Datenanwendung verarbeiteten Datenarten;
5. die Form der Verarbeitung und die Darstellung der Ergebnisse (personenbezogenen, indirekt-personenbezogen bzw. anonymisiert);
6. allfällige Dienstleister oder sekundäre Datennutzer, insbesondere ob dabei eine Überlassung oder Übermittlung der Daten in das Ausland notwendig ist;
7. die Handhabung der Daten nach dem Erreichen des Untersuchungszwecks.

Es wird empfohlen, Art und Umfang der Aufklärung des Betroffenen zusammen mit der (ausdrücklichen) Zustimmung zur Verwendung der Daten in schriftlicher Form festzuhalten.

Eine besondere Situation entsteht, wenn eine personenbezogene wissenschaftliche Datensammlung zur Beantwortung einer retrospektiven Fragestellung herangezogen werden soll und dieser Verwendungszweck nicht durch die Zustimmung der Betroffenen abgedeckt ist. In diesem Falle stellt das Einholen der Zustimmung der Betroffenen häufig einen unverhältnismäßig hohen Aufwand dar, und es wird empfohlen die Verarbeitung gemäß § 46 Abs. 2ff DSG 2000 mit Genehmigung der Datenschutzkommission durchzuführen.

Für eine Verwendung von personenbezogenen Daten in der allgemeinen Lehre ist jedenfalls die Zustimmung des Betroffenen einzuholen.

3.6. Pflichten des Dienstleisters

3.6.1. Rahmenbedingungen

Auftraggeber dürfen laut § 10 Abs. 1 DSG 2000 bei ihren Datenanwendungen Dienstleister in Anspruch nehmen, wenn diese ausreichende Gewähr für eine rechtmäßige und sichere Datenverwendung bieten. Der Auftraggeber hat mit dem Dienstleister die hierfür notwendigen Vereinbarungen zu treffen und sich von ihrer Einhaltung durch Einholung der erforderlichen Informationen über die vom Dienstleister tatsächlich getroffenen Maßnahmen zu überzeugen.

Unabhängig von allfälligen vertraglichen Vereinbarungen haben Dienstleister bei der Verwendung von Daten für den Auftraggeber gemäß § 11 Abs. 1 DSG 2000 jedenfalls folgende Pflichten:

1. die Daten ausschließlich im Rahmen der Aufträge des Auftraggebers zu verwenden; insbesondere ist die Übermittlung der verwendeten Daten ohne Auftrag des Auftraggebers verboten;
2. alle gemäß § 14 DSG 2000 erforderlichen Datensicherheitsmaßnahmen zu treffen; insbesondere dürfen für die Dienstleistung nur solche Mitarbeiter herangezogen werden, die sich dem Dienstleister gegenüber zur Einhaltung des Datengeheimnisses verpflichtet haben oder einer gesetzlichen Verschwiegenheitspflicht unterliegen;
3. weitere Dienstleister nur mit Billigung des Auftraggebers heranzuziehen und deshalb den Auftraggeber von der beabsichtigten Heranziehung eines weiteren Dienstleisters so rechtzeitig zu verständigen, dass er dies allenfalls untersagen kann;
4. sofern dies nach der Art der Dienstleistung in Frage kommt – im Einvernehmen mit dem Auftraggeber die notwendigen technischen und organisatorischen Voraussetzungen für die Erfüllung der Auskunft-, Richtigstellungs- und Löschungspflicht des Auftraggebers zu schaffen;
5. nach Beendigung der Dienstleistung alle Verarbeitungsergebnisse und Unterlagen, die Daten enthalten, dem Auftraggeber zu übergeben oder in dessen Auftrag für ihn weiter aufzubewahren oder zu vernichten;
6. dem Auftraggeber jene Informationen zur Verfügung zu stellen, die zur Kontrolle der Einhaltung der unter Z 1 bis 5 genannten Verpflichtungen notwendig sind.

Bei Überlassungen ins Ausland muss die schriftliche Zusage des ausländischen Dienstleisters an den inländischen Auftraggeber vorliegen, dass er diese Dienstleisterpflichten einhalten werde. Allgemein sind Vereinbarungen über die nähere Ausgestaltung der genannten Pflichten zum Zweck der Beweissicherung schriftlich festzuhalten.

3.6.2. Vorgehensmodell

Der Auftraggeber trägt – auch bei der Heranziehung von Dienstleistern – für jede seiner Datenanwendungen die Verantwortung für die Einhaltung der in § 6 Abs. 1 DSGVO 2018 statuierten „Grundsätze bei der Verwendung von Daten“ (siehe Abschnitt 2.1.1.). Vor diesem Hintergrund ist für die jeweilige Situation zu prüfen, ob die vorliegende Form der Kooperation tatsächlich einer Auftraggeber-Dienstleister Beziehung entspricht. Gerade im Bereich der wissenschaftlichen Forschung mit den heute typischen interdisziplinären Teamstrukturen ist diese Frage nicht ohne weiteres beantwortbar. So ist als alternative Form der Kooperation allgemein die Personengemeinschaft als Auftraggeber zu nennen, selbst dann, wenn eine klare Abgrenzung der Aufgabenverteilung vorliegt und jeder Partner seinen Beitrag selbstständig und eigenverantwortlich leistet. Auch die monetäre Abgeltung von (Dienst-)Leistungen erscheint in diesem Zusammenhang als kein hinreichendes Selektionskriterium. Vielmehr ist die Rolle bei der Untersuchung von Bedeutung. Wird das Erbringen einer Leistung als Teil der wissenschaftlichen Fragestellung gesehen, so handelt es sich wohl um einen strukturierten Auftraggeber. Demgegenüber steht die Dienstleistung losgelöst von der konkreten Fragestellung der wissenschaftlichen Untersuchung. Von dieser Regelung auszunehmen ist nur die Verifikation von Untersuchungsergebnissen, etwa durch eine anerkannte Methode im Vergleich zu einem neuen Verfahren. Hier handelt es sich gerade aufgrund der identischen Fragestellung um eine typische Dienstleistung iSd. DSGVO.

Eine analoge Überlegung ist bei der Differenzierung zwischen sekundären Datennutzern und Dienstleistern anzustellen, insbesondere um ein „Aufweichen“ der Übermittlung von Daten hin zur Überlassung zu verhindern (siehe Sektion 3.9.). Das in diesem Fall schlagende Unterscheidungskriterium liegt in der eigenständigen Verwertung der Untersuchungsergebnisse. Während das Interesse eines Dienstleisters, wie bereits oben beschrieben, in der Erbringung der Leistung per se liegt, ist das Ziel des sekundären Datennutzers in der Beantwortung von eigenen wissenschaftlichen Fragestellungen zu suchen, auch wenn diese thematisch mit jenen des Auftraggebers korrelieren.

Eine vertragliche Vereinbarung zwischen Auftraggeber und Dienstleister soll die folgenden Punkte beinhalten:

1. Die implementierten Datensicherheitsmaßnahmen im Organisationsbereich des Dienstleisters sind dem Auftraggeber in schriftlicher Form bekannt zu geben (siehe dazu auch 3.1.). Diese Sicherheits-Policy ist Teil der Vereinbarung.
2. Der Auftraggeber hat Art und Umfang der zu erbringenden Dienstleistungen so detailliert festzulegen, dass die in der Folge zur Erfüllung dieser Leistungen durchzuführenden Verarbeitungsschritte begründbar sind und daraus die Zulässigkeit der Datenanwendung beim Dienstleister folgert.
3. Die, für die Herstellung des aufgetragenen Werks, notwendigen und dem Dienstleister zu überlassenden Datenarten sind in der Vereinbarung zu spezifizieren.
4. Für den Fall der Beendigung der Dienstleistung hat der Auftraggeber die final durchzuführenden Aktivitäten des Dienstleisters zu definieren; der Vollzug der vereinbarten Maßnahmen ist dem Auftraggeber anzuzeigen.

Allfällige Verletzungen des Datenschutzes im Bereich des Dienstleisters sind dem Auftraggeber unverzüglich mitzuteilen und die weitere Vorgehensweise ist – sofern die Situation nicht ein sofortiges Handeln erzwingt – mit dem Auftraggeber abzustimmen.

Sieht die Planung einer wissenschaftlichen Untersuchung die Beauftragung eines Dienstleisters vor und wird das Vorhaben der lokalen Ehtikkommission zur Zulassung vorgelegt, so ist die zwischen Auftraggeber und Dienstleister zu schließende vertragliche Vereinbarung dem Antrag beizufügen.

3.7. Primäre Identifikationsdaten

3.7.1. Rahmenbedingungen

Primäre Identifikationsdaten sind Attribute oder Attributkombinationen, die von Natur her oder aufgrund ihrer Definition oder Verwendung dazu dienen, eine Person eindeutig zu identifizieren, auch wenn dazu eine Verknüpfung mit anderen Daten notwendig ist. Eine Zusammenstellung von typischen primären Identifikationsdaten findet sich in der nachstehenden Tabelle.

DATENART	KOMPONENTEN	DATENNUTZERKREIS
Name	Zuname, Vorname, Zusatz, Geburtsname, Titel	Öffentlichkeit
Adresse	Straße, Zusatz, Postleitzahl, Ort, Land	Öffentlichkeit
Telefonnummer		Öffentlichkeit
Sozialversicherungsnummer		Verwaltung
Polizzenummer		Versicherungen
Dokumentnummer z.B. Führerschein, Reisepass, Personalausweis		Verwaltung
Grundbuchblattnummer		Landesverteidigung
Registernummer		Verwaltung
KFZ-Nummer		Verwaltung
Matrikelnummer		Verwaltung
Veranlagungsnummer		Verwaltung
Kontonummer		Geldinstitute
Personalnummer		Dienstgeber
Patientenidentifikation z.B. Aufnahmeummer, Fallnummer, PID-Nummer, Untersuchungsnummer		Leistungserbringer
Mitgliedsnummer		Vereine

Man bedenke, dass in einem zu übermittelnden Datensatz neben den primären Identifikationsdaten eines Patienten auch solche von weiteren Personen wie nächster Angehöriger oder des zuweisenden Arztes enthalten sein können. Aus der Sicht des DSG 2000 sind alle diese Personen als Betroffene einzustufen.

3.7.2. Vorgehensmodell

Zum Entfernen des Personenbezugs in wissenschaftlichen Daten ist eine Identifizierung des Betroffenen zuverlässig auszuschließen, d.h. in einem ersten Schritt sind alle Attribute (Datenarten) der primären Identifikationsdaten entweder zu löschen oder mit einem als sicher geltenden Verfahren zu verschlüsseln. Von dieser maximalen Anforderung – und nur für die zeitlich limitierte Übergangsphase bis zur allgemeinen Verfügbarkeit entsprechender EDV-gestützter Werkzeuge – kann hinsichtlich jener Attribute abgewichen werden, die nur im Kontext des Auftraggebers als

primäre Identifikationsdaten dienen. Beispiele für solche Attribute sind lokal verwendete Aufnahmezahlen, PID-⁷, Fall-, oder Untersuchungsnummern. In Zweifelsfällen wird empfohlen, den lokal zuständigen EDV-Administrator zu befragen.

Sollen primäre Identifikationsdaten durch Verschlüsselung eliminiert werden, so wird – analog zu den in MAGDA-LENA definierten Richtlinien – der Einsatz von Verfahren, die mindestens den Anforderungen der kommerziellen Datensicherheit genügen, empfohlen. Die Mindestlänge des symmetrischen Schlüssels soll größer als 80 Bit sein und eine der folgenden Methoden zur Anwendung kommen:

1. IDEA (International Data Encryption Algorithm),
2. 3DES (triple DES) in der Variante mit zwei Schlüsseln,
3. AES (Advanced Encryption Standard).

Achtung! Die hier beschriebene Vorgehensweise darf nicht mit der Verschlüsselung von Nachrichteninhalten zum Zweck einer gesicherter Übertragung verwechselt werden. Der wesentliche Unterschied ist, dass der zur Elimination der primären Identifikationsdaten erzeugte Schlüssel vom Übermittler geheim zu halten ist und keinesfalls an den Empfänger weitergegeben werden darf!

Für eine ausführlichere Diskussion von kryptographischen Verfahren sowie für die zu beachtende Qualität eines zufällig erzeugten Schlüssels wird auf die „Rahmenbedingungen für ein logisches österreichisches Gesundheitsdatennetz – MAGDA-LENA“ verwiesen.

Man beachte, dass bei strukturierten primären Identifikationsdaten – das sind Datenarten, die in Komponenten gegliedert sind wie „Name“ oder „Adresse“ – der gemeinsamen Verschlüsselung aller Komponenten der Vorzug gegenüber einer komponentenorientierten Form zu geben ist. Beispielsweise sind für die Datenart „Name“ die Komponenten „Zuname, Vorname, Zusatz, Geburtsname, Titel“ als ein einziges Datum aufzufassen und mithin gemeinsam zu verschlüsseln. Die Chiffrierung jedes einzelnen Elements, also „Zuname“, „Vorname“, ..., „Titel“, kann aufgrund des beschränkten Wertebereichs einzelner Komponenten (z.B. „Titel“) als Ansatzpunkt für eine Kryptoanalyse (Bestimmen des Schlüssels) dienen. Sollen einzelne Komponenten von primären Identifikationsdaten, etwa der „Ort“ in „Adresse“, für den Empfänger zugänglich sein, so wird die Übermittlung als eigenes Attribut empfohlen, das entsprechend den Richtlinien des folgenden Abschnitts zu behandeln ist.

3.8. Sekundäre Identifikationsdaten

3.8.1. Rahmenbedingungen

Als sekundäre Identifikationsdaten gelten jene Attribute oder Attributkombinationen einer Person, die aufgrund der möglichen Werte dieser Attribute ein eindeutiges Muster ausprägen können, welches die Identifikation des Betroffenen durch Verknüpfung mit anderen Daten ermöglicht. Mit anderen Worten, nicht die Attribute selbst sondern der Umstand des Zusammentreffens von (vielleicht seltenen) Attributwerten schafft die Basis für eine Korrelation mit primären Identifikationsdaten.

Welche Datenarten beschreiben sekundäre Erkennungsmerkmale? Obwohl eine definitive Klassifikation einzelner Daten letztendlich nur anhand der jeweiligen Attributwerte erfolgen kann, sind doch einige heuristische Regeln definierbar, die a priori eine Einstufung ermöglichen. Typische sekundäre Identifikationsparameter sind demnach demographische Daten natürlicher Personen

⁷ Es bestehen eine Reihe von internationalen Bestrebungen, eine vereinheitlichte Patienten ID zu definieren und einzuführen.

1. mit keiner oder nur geringer Änderungswahrscheinlichkeit oder
2. die das tägliche Leben betreffen und im sozialen Umgang als bekannt anzunehmen sind.

Darüber hinaus sind medizinische Daten mit atypischen Werten in die Betrachtungen einzu-
beziehen.

Demographische Daten mit keiner oder geringer Änderungswahrscheinlichkeit sind beispielsweise Geburtsdatum, Geschlecht, ethnische oder rassische Herkunft, Mehrlinsgeburt, Religionsbe-
kenntnis, Familienstand, geographische Daten wie Geburts- oder Wohnort, weiters der Beruf,
Arbeitgeber sowie das Einkommen des Betroffenen. Daten, die das tägliche Leben betreffen, sind:
besondere Kennzeichen, angeborene oder chronische Erkrankungen, Behinderungen, Unfälle,
Sehbehelfe, Dauermedikationen, Allergien, Sucht, psychische Verhaltensmuster und persönliche
Gewohnheiten respektive Vorlieben sowie alle hinreichenden Surrogate für die genannten
Charakteristiken. Als Beispiele für medizinische Daten mit konstanten Attributwerten seien die
Blutgruppe, HLA-Parameter bzw. allgemein genetische Marker genannt.

Zum besseren Verständnis von sekundären Identifikationsmerkmalen ist eine Abgrenzung zu all-
gemein medizinischen Daten hilfreich. Medizinische Parameter unterliegen typischerweise einer
Prozessdynamik, was bedeutet, dass die zugehörigen Werte sowohl zeitlichen wie auch indivi-
duellen Schwankungen unterworfen sind. Die einzelnen Messwerte stellen quasi eine Moment-
aufnahme von Teilaspekten einer Person dar. Die Bandbreite der Variationen kann dabei inner-
halb von Normbereichen liegen oder anormale, pathologische Dimensionen annehmen. Per
Definition ist ein Norm(al)bereich jenes Intervall, in das 95% aller Messwerte einer Kenngröße
fallen⁸, d.h. Daten innerhalb der Grenzwerte sind, bei kleiner Varianz, häufig zu beobachtende
Ereignisse und für die Bestimmung der k -Anonymität ohne Bedeutung. Eine analoge Überlegung
gilt vielfach auch für moderate Abweichungen und leider sind auch pathologische Werte aus
Sicht der Medizin keine Seltenheit. In der Regel ist aus der Erfahrung der ärztlichen Tätigkeit gut
unterscheidbar, ob die Ausprägung einer Kenngröße ein zu erwartendes Ergebnis darstellt oder
aber atypische Werte annimmt, also von ihrem Vorkommen her sporadisch oder ungewöhnlich
ist. Unter Berücksichtigung des jeweiligen Kontexts ist dieser Prozess auch für eine Kombination
von Attributwerten statthaft. Eine differenzierte Sachlage ergibt sich bei zeitlichen (oder anderen)
Profilen einer Kenngröße. In diesem Fall besteht theoretisch die Möglichkeit, die Daten mit
individuellen Profilen zu vergleichen und Rückschlüsse auf den Betroffenen zu ziehen.

3.8.2. Vorgehensmodell

Bei der Planung einer wissenschaftlichen Untersuchung, insbesondere bei der Spezifikation der
für die Untersuchung zu erhebenden Daten, ist eine Analyse der Attribute hinsichtlich ihrer
Qualifikation als sekundäres Identifikationsmerkmal vorzunehmen. Obwohl keine triviale Auf-
gabe, kann in der Regel anhand der in 3.8.1. gegebenen Erläuterungen eine Klassifizierung vorge-
nommen werden. Ist dies für das eine oder andere Attribut a priori nicht möglich, etwa weil die
zu erwartenden Attributwerte zu diesem Zeitpunkt nicht abschätzbar sind, so ist das Datum
vorläufig der Klasse der sekundären Identifikationsdaten zuzuordnen. Eine alternative Vor-
gehensweise wäre, alle jene Attribute auszuschneiden, die nicht den Kriterien für sekundäre
Identifikationsdaten entsprechen. Die dermaßen verbleibenden Parameter sind als sekundäre
Erkennungsmerkmale zu behandeln.

Die Umwandlung von personenbezogenen Daten in indirekt personenbezogene erfolgt, auf
Ebene der sekundären Identifikationsdaten, durch k -Anonymisierung entsprechend der Definition
in Abschnitt 2.2.5. In der Praxis gilt bei Wahl von $k \geq 2$ (empfohlen wird $k \geq 5$) die Definition
von „indirekt personenbezogen“ im Sinne des § 4 Z 1 DSGVO 2000 als hinreichend erfüllt.
Unabhängig von dieser unteren Schranke ist ein größeres k anzustreben, wenn dies im Rahmen
einer wissenschaftlichen Untersuchung mit vertretbarem Aufwand realisierbar ist (etwa durch

⁸ Ohne Erkrankungen, die diese Kenngröße beeinflussen könnten.

Analyse der sekundären Identifikationsdaten im Bestand einer Datenanwendung zum Zweck der medizinischen Diagnostik und Behandlung).

Wird eine Studienplanung der lokalen Ethikkommission vorgelegt, so empfiehlt sich, eine Analyse von möglichen sekundären Identifikationsdaten sowie eine Abschätzung von k dem Antrag beizulegen.

In Abschnitt 2.2.4. wurde mit der beschränkten Übermittlung von Daten eine Klasse von Transformationen umrissen, die zur Erreichung der k -Anonymität herangezogen werden können. An aktueller Stelle seien nun zwei dieser Methoden näher bezeichnet, nämlich die Generalisierung von Identifikationsdaten und ein Unterdrücken einzelner Attributwerte. Bei der Generalisierung von (sekundären) Identifikationsdaten werden spezifische Attributwerte durch allgemeinere, beschreibende Daten ersetzt. So ist etwa das Geburtsdatum eines Betroffenen durch sein Alter (Generalisierung auf das Geburtsjahr) oder der Wohnort durch eine größere umliegende geographische Region substituierbar. Häufig kann eine Generalisierung ohne Einschränkung der qualitativen Aussagen von wissenschaftlichen Untersuchungen vorgenommen werden, insbesondere bei Wahl von abstrakten Formen der Verallgemeinerung; darüber hinaus sind durch Vorgabe von oberen oder unteren Schranken auch atypische Parameterwerte kategorisierbar. Bei seltenen Wertkombinationen wird allerdings der Fall eintreten, dass der mit einer Generalisierung einhergehende Informationsverlust die wissenschaftliche Auswertung der Daten stört. Eine alternative Vorgehensweise wäre, einzelne „unsichere“ Attributwerte zu unterdrücken, d.h. nicht zu übermitteln, und die verbleibenden Daten als unvollständig zu qualifizieren. In der Praxis wird die Kombination der beiden Verfahren die besten Ergebnisse liefern.

Die zielführenden Methoden zur k -Anonymisierung sind theoretisch von der zu untersuchenden Fragestellung und den unterschiedlichen Typen sekundärer Identifikationsdaten abhängig. Größen, welche die entsprechenden Überlegungen aus praktischer Sicht beeinflussen sind die Anzahl der zu diskutierenden Parameter sowie die Quantität der Datensätze. Aus diesem Zusammenhang heraus sei festgehalten, dass unter Umständen weitreichende statistische Kenntnisse zur k -Anonymisierung notwendig sind. Obwohl mit dem Anspruch wissenschaftlicher Qualität geschrieben kann und darf es nicht das Ziel dieser Policy sein, Richtlinien zu definieren, die zur Umsetzung der Wissenschaft bedürfen.⁹ Vielmehr ist auf einzelne, im Bereich der Wissenschaft tätige Personen Rücksicht zu nehmen, andernfalls ist keine Veränderung des Status quo hin zu allgemein anerkannten und routinemäßig angewendeten Standardprozeduren zu erwarten. Aus diesem Grund können – für die zeitlich limitierte Übergangsphase bis zur Verfügbarkeit adäquater EDV-gestützter Werkzeuge – medizinische Parameter aus der Analyse und k -Anonymisierung sekundärer Identifikationsdaten ausgenommen werden, wenn zu erwarten ist, dass diese Merkmale für die Dauer der wissenschaftlichen Untersuchung Dritten nicht bekannt sind und die Daten nach Abschluss der Studie vom sekundären Datennutzer gelöscht werden.

3.8.3. k -Anonymität bei Untersuchungen mit kleiner Fallzahl

Eine besondere Situation ergibt sich, wenn aufgrund der Anzahl der zu überlassenden bzw. zu übermittelnden Datensätze keine k -Anonymität innerhalb dieser Daten erzielt werden kann. So ist vorstellbar, dass eine Übermittlung im Rahmen einer Multicenterstudie aus nur einem einzigen Datensatz besteht, etwa weil die Häufigkeit des Auftretens von bestimmten, in der Untersuchung zu beobachtenden Merkmalen in der Bevölkerung sehr gering ist. In derartigen Fällen ist eine Datenschutz-Policy, die von anderen als den zu übermittelnden Daten unabhängig ist, nicht realisierbar.¹⁰ Trotzdem kann das Konzept der k -Anonymität als qualitatives Maß, ob Daten als indirekt personenbezogen einstuftbar sind, eingesetzt werden. Sind nämlich in einem vom Auftrag-

⁹ Die Befassung der Wissenschaften mit dem Ziel, einfache EDV-gestützte Verfahren zur k -Anonymisierung von personenbezogenen Daten zu entwickeln wird explizit angeregt.

¹⁰ In den Anforderungen an die zu definierende Datenschutz-Policy wird Unabhängigkeit von „anderen als den zu übermittelnden bzw. zu verarbeitenden Daten“ gefordert. Im gegenständlichen Fall muss zur Kontrolle der „ k -Anonymität“ auf das Kollektiv der zu verarbeitenden Daten zurückgegriffen werden.

geber überblickbaren Kollektiv – etwa in einer Datenanwendung zum Zweck der medizinischen Diagnostik und Behandlung – mindestens k Betroffene mit den gleichen sekundären Identifikationsdaten wie im fraglichen Datensatz auffindbar, dann ist die Bedingung der k -Anonymität für diesen Datensatz erfüllt.

3.8.4. Sonderfälle

In besonderen Situationen mag es vorkommen, dass die Frage der k -Anonymität nicht beantwortbar ist beziehungsweise diese nicht erzielt werden kann. Dieser Umstand ist nicht als „Schwäche“ der vorgeschlagenen Methode zu werten sondern reflektiert das simple Faktum, dass einzelne wissenschaftliche Untersuchungen nicht in indirekt personenbezogener Form durchgeführt werden können. Der Gesetzgeber trägt dieser Sachlage Rechnung und ermöglicht – wenn auch unter verschärften Bedingungen – die Verwendung von personenbezogenen Daten in Wissenschaft und Forschung. Konkret können gemäß DSG 2000, § 46 Abs. 2f, Daten in personenbezogener Form

1. mit Zustimmung des Betroffenen oder
2. mit Genehmigung der Datenschutzkommission

verwendet werden (siehe auch Abschnitte 2.1.2 und 2.1.3.). Aus Gründen der Praktikabilität wird empfohlen, Erstere der beiden Alternativen anzuwenden (→3.5.).

Es sei an dieser Stelle nochmals ausdrücklich auf die notwendigen begleitenden Maßnahmen bei der Verarbeitung von sensiblen Daten in personenbezogener Form hingewiesen, insbesondere auf

1. die zu ergreifenden Datensicherungsmaßnahmen¹¹ (→3.1.),
2. die konsequente Durchsetzung des Datengeheimnis (→3.2) sowie
3. die Meldepflicht des Auftraggebers an das Datenverarbeitungsregister (→3.3.).

Man beachte weiters, dass gemäß § 46 Abs. 5 auch in jenen Fällen, in welchen die Verwendung von Daten für Zwecke der wissenschaftlichen Forschung oder Statistik in personenbezogener Form zulässig ist, jedenfalls die primären Identifikationsdaten unverzüglich zu verschlüsseln sind, wenn damit in einzelnen Phasen der wissenschaftlichen oder statistischen Arbeit das Auslangen gefunden werden kann (siehe dazu auch Abschnitt 3.7.).

3.9. Übermittlung von Daten

3.9.1. Rahmenbedingungen

Gemäß § 4 Z 12 DSG 2000 ist das „Übermitteln von Daten“ definiert als die Weitergabe von Daten an andere Empfänger als den Betroffenen, den Auftraggeber oder einen Dienstleister, insbesondere auch das Veröffentlichen solcher Daten sowie die Verwendung von Daten für ein anderes Aufgabengebiet des Auftraggebers.

Wesentlich für die Zulässigkeit einer Datenübermittlung ist neben der Berechtigung des Auftraggebers und der ausreichenden gesetzlichen Zuständigkeit bzw. rechtlichen Befugnis des Empfängers, dass durch Zweck und Inhalt der Übermittlung die schutzwürdigen Geheimhaltungsinteressen des Betroffenen nicht verletzt werden (§ 7 Abs. 2 DSG 2000). Schutzwürdige Geheimhaltungsinteressen werden bei der Verwendung von sensiblen Daten dann nicht verletzt, wenn (§ 9 Z 2 DSG 2000) die Daten in nur indirekt personenbezogener Form verwendet werden oder gemäß § 9 Z 6 der Betroffene seine Zustimmung zur Verwendung der Daten

¹¹ Siehe dazu auch das Formblatt „Allgemeine Angaben zu ergriffenen Datensicherungsmaßnahmen gemäß Anlage 4 DVRV BGBl. II Nr. 520/1999“ der Datenschutzkommission.

ausdrücklich erteilt hat, wobei ein Widerruf jederzeit möglich ist und die Unzulässigkeit der weiteren Verwendung der Daten bewirkt.

Aus Sicht der wissenschaftlichen Forschung und Statistik ist nach § 46 Abs. 3 die Übermittlung sensibler Daten an ein „wichtiges öffentliches Interesse an der Untersuchung“ gebunden. Weiters muss gewährleistet sein, daß die Daten beim Empfänger nur von Personen verwendet werden, die hinsichtlich des Gegenstandes der Untersuchung einer gesetzlichen Verschwiegenheitspflicht unterliegen oder deren diesbezügliche Verlässlichkeit sonst glaubhaft ist.

Gemäß § 12 DSG 2000 ist die Übermittlung (Überlassung) von Daten an Empfänger in Mitgliedstaaten der Europäischen Union (Abs. 1) bzw. an Empfänger in Drittstaaten mit angemessenem Datenschutz (Abs. 2) genehmigungsfrei. Darüber hinaus darf ein Datenverkehr ins Ausland ohne Zustimmung der Datenschutzkommission erfolgen, wenn (Abs. 3)

1. die Daten für den Empfänger nur indirekt personenbezogen sind oder
2. der Betroffene ohne jeden Zweifel seine Zustimmung zur Übermittlung seiner Daten ins Ausland gegeben hat.

Für alle anderen Fälle des Datenverkehrs mit dem Ausland hat der Auftraggeber vor der Übermittlung (Überlassung) von Daten eine Genehmigung der Datenschutzkommission einzuholen (§ 13 DSG 2000).

Laut § 14 Abs. 2 Z 7 DSG 2000 ist über eine durchgeführte Übermittlung Protokoll zu führen, damit ihre Zulässigkeit im notwendigen Ausmaß nachvollzogen werden kann.

3.9.2. Vorgehensmodell

Die Übermittlung von personenbezogenen Daten zum Zweck der wissenschaftlichen Forschung und Statistik bedarf – unabhängig von der notwendigen gesetzlichen Zulässigkeit – der Genehmigung durch die lokale Ethikkommission. Dabei ist im jeweiligen Antrag zu begründen, warum nicht mit nur indirekt personenbezogenen Daten das Auslangen gefunden werden kann. Weiters haben, in Anwendung der „Richtlinien für ein logisches österreichisches Gesundheitsdatennetz (MAGDA-LENA)“, alle an der Übermittlung beteiligten Kommunikationspartner eine Konformitätserklärung gemäß MAGDA-LENA abzugeben. Diese Konformitätserklärungen sind dem Antrag an die Ethikkommission beizulegen. Die Ethikkommission überprüft das Vorliegen der Konformitätserklärungen und entscheidet über die Notwendigkeit eines Datenaustauschs in personenbezogener Form.

Die Wahrung der schutzwürdigen Geheimhaltungsinteressen des Betroffenen (Vertraulichkeit) und die Gewährleistung der Datensicherheit (Datenintegrität, Ursprungsnachweis) sind bei der (elektronischen) Übermittlung von personenbezogenen Daten durch entsprechende technische Maßnahmen sicherzustellen. Für eine normative Aufzählung von Methoden und Verfahren zur Verschlüsselung der zu übermittelnden Daten sowie für die Authentifizierung des Senders mittels sicherer Signatur gemäß Signaturgesetz (SigG) wird auf die „Richtlinien für ein logisches österreichisches Gesundheitsdatennetz (MAGDA-LENA)“ verwiesen. Werden Daten über ein geschütztes Netzwerk übertragen, das den Sicherheitsstandards für Datenanwendungen zum Zweck der medizinischen Diagnostik und Behandlung iSd. § 9 Z 12 DSG 2000 genügt, kann eine Übermittlung personenbezogener Daten ohne Verschlüsselung und elektronische Unterschrift erfolgen.

Daten (Datensätze) gelten als indirekt personenbezogenen iSd. § 4 Z 1 DSG 2000, wenn diese der Bedingung der k -Anonymität mit $k \geq 2$, empfohlen wird $k \geq 5$, genügen. In diesem Fall ist eine Übermittlung der Daten ohne Genehmigung der Ethikkommission gestattet. Ist eine wissenschaftliche Untersuchung zum Zwecke der Zulassung einer Ethikkommission vorzulegen, wird empfohlen eventuell geplante Maßnahmen zur k -Anonymisierung, insbesondere die Größe von k , der Kommission offenzulegen.

Hinsichtlich der zu implementierenden Übertragungstechnologie wird eine Vorgehensweise analog zur Übermittlung von personenbezogenen Daten empfohlen.

Trotz der gesetzlichen Regelung in § 15 DSG (Datengeheimnis) wird angeraten, jede weitere (teilweise) Übermittlung der Daten seitens des Empfängers vertraglich an die Zustimmung des ursprünglichen Auftraggebers zu binden, insbesondere auch dann, wenn diese Daten in nur indirekt personenbezogener Form übermittelt wurden oder der Empfänger einer Übermittlung seinerseits die Daten in nur indirekt personenbezogener Form weitergeben will (siehe dazu auch Abschnitt 3.2.2.).

Über jede Übermittlung von personenbezogenen Daten ist Protokoll zu führen, wobei Zeitpunkt und Empfänger des Transfers, die übertragenen Daten sowie die zugehörige Genehmigung der Ethik- und der Datenschutzkommission zu vermerken sind. Werden indirekt personenbezogene Daten übermittelt, wird empfohlen Zeitpunkt, Empfänger, die transferierten Datenarten und die Größe von k zu protokollieren. Bei reversibler Anonymisierung (siehe 4.1.) sind zusätzlich das gewählte kryptographische Verfahren zur zuverlässigen Elimination der primären Identifikationsdaten und die TransferID im Übermittlungsprotokoll zu vermerken. Das Paar (TransferID, Key), mit Key gleich dem Schlüssel zur Chiffrierung der primären Identifikationsdaten, ist an einem sicheren Ort aufzubewahren.

3.10. Lokale Datenschutzkommissionen

Eine Reihe von Diskussionen im Zuge des Verfassens der vorliegenden Policy zeigten, dass die Umsetzung der vorgeschlagenen Maßnahmen, insbesondere die technisch-methodisch orientierten Teile der Studie, nicht zu unterschätzende Anforderungen an die verfügbare Infrastruktur stellen. Aus diesem Grund wird, neben der Kooperation mit lokalen Rechenzentren (siehe 3.2.2.) beziehungsweise der Entwicklung von speziellen Tools (siehe Abschnitt 4.3.), die Bildung von lokalen Datenschutzkommissionen angeregt. Typische Leistungen der lokalen Datenschutzkommissionen können sein:

1. das Prüfen der Angemessenheit von allgemeinen Datensicherheitsmaßnahmen,
2. Hilfestellung bei Meldungen an das Datenverarbeitungsregister,
3. Beratung bei Unklarheiten über das Ausmaß der Informationspflicht,
4. Unterstützung bei der Gestaltung von vertraglichen Vereinbarungen zwischen Auftraggeber und Dienstleister (Rollenmodelle, Musterverträge) und
5. Assistenz bei der Umwandlung von personenbezogenen in indirekt personenbezogene Daten.

Man beachte, dass die Intention für die Einrichtung lokaler Datenschutzkommissionen in der Unterstützung von Betreibern wissenschaftlicher Untersuchungen liegt und dieser Vorschlag nicht die Schaffung einer verbindlichen Instanz zum Ziel hat. Dementsprechend ist die Konsultation der jeweiligen lokalen Datenschutzkommission freiwillig und enthebt nicht von den Pflichten eines Auftraggebers im Sinne des DSG.

4. Systemstrukturen zur Anonymisierung personenbezogener Daten

4.1. Reversible Anonymisierung

4.1.1. Definition

In besonderen Fällen ist es notwendig, indirekt personenbezogene Daten auf den Betroffenen rückzuführen. Deuten zum Beispiel die Ergebnisse einer wissenschaftlichen Untersuchung auf eine Situation hin, die im Interesse des Betroffenen einer Abklärung bedarf, so muss dieser ohne Wenn und Aber benachrichtigt werden. Sind im Rahmen einer Studie Daten zu ergänzen oder weitere Fragestellungen durch ein Follow-up zu beantworten, kann dies mittels Befragung¹² der Betroffenen auf ökonomische Art und Weise geschehen.

Für die Benachrichtigung bzw. Befragung von Betroffenen sind primäre Identifikationsdaten, insbesondere Name und Adresse, vonnöten — Informationen, über die ein sekundärer Datennutzer in der Regel nicht verfügt (siehe Abschnitt 3.9.). Folglich muss sich dieser an den Übermittler der Daten wenden und die Kontaktaufnahme anregen. Obwohl auf den ersten Blick bürokratisch anmutend, ist diese Vorgehensweise wohl motiviert. Zum einen würde es beim Betroffenen wahrscheinlich Befremden hervorrufen, eine Benachrichtigung von einem, i. Allg. ihm unbekanntem, sekundären Datennutzer zu erhalten. Hier ist, schon aus ethischer Sicht, die mit der ursprünglichen Datenerhebung befasste natürliche oder juristische Person zu favorisieren. Zum anderen ist diese Methode im Einklang mit § 47 DSGVO 2018 (siehe Abschnitt 2.1.5.).

Das Verfahren zur Rückführung von *k*-anonymen Daten auf den Betroffenen durch und nur durch den Auftraggeber wird als reversible Anonymisierung bezeichnet und bedingt eine Kennzeichnung der übermittelten Daten. Zu diesem Zweck wird jedem zu transferierenden Datensatz ein Distinguished Name (DN) mit folgender Struktur vorangestellt:

```
QualifiedName ::= <AuthorityID> "/" <LocalName>
AuthorityID ::= <RegistrationAuthority> ":" <NamingEntity>
RegistrationAuthority ::= "ISO" | "DNS" | ...
LocalName ::= <TransferID> "/" <SetID>
```

Ein Qualified Name besteht also aus einer Sequenz von Relative Distinguished Names (RDNs), wobei das international eindeutige Präfix „AuthorityID“ den Auftraggeber identifiziert, das lokal zu vergebende eindeutige Suffix, bestehend aus „TransferID“ und „SetID“, bezeichnet die Übermittlung und die dabei transferierten Datensätze:

```
QualifiedName ::= <AuthorityID> "/" <TransferID> "/" <SetID>
```

Somit entspricht der Aufbau des Distinguished Name sowohl aus administrativer Sicht wie auch vom technischen Standpunkt her den Anforderungen einer verteilten Systemarchitektur.

4.1.2. RDN des Auftraggebers

Ein global eindeutiger Name eines Auftraggebers ist immer in Abhängigkeit vom jeweiligen Name Space der unterschiedlichen Naming Authorities zu betrachten. Folglich kann – je nachdem, welche Root zur Anwendung kommt – ein und derselbe Auftraggeber unter mehreren Namen bekannt sein. Mangels standardisierter Abbildungsschemata zwischen differenten Name Spaces wird allerdings empfohlen, konsequent nur eine AuthorityID einzusetzen. Zur Kennzeichnung der Be-

¹² Der Begriff „Befragung“ versteht sich in einem allgemeinen Sinn und beinhaltet alle zulässigen Methoden der Datenerhebung.

züglichkeit eines Name Space wird der Naming Entity die Registration Authority¹³ vorangestellt und durch einen Doppelpunkt begrenzt. Die zwei verbreitetsten Registration Authorities seien im Weiteren näher betrachtet.

Die International Standards Organization spezifiziert eine Registrierungshierarchie bestehend aus einer Folge von durch Leerzeichen getrennte Relative Distinguished Names, wobei die Namens-teile selbst gemäß der „NameForm“ von ASN.1 (ISO/IEC 8824) kodiert werden. Ein Beispiel möge diese Struktur verdeutlichen: Sei das Institut für Medizinische Informatik, kurz IMI, an der Universität Graz ein Auftraggeber, so ist der String „ISO:AT Graz-University IMI“ eine mögliche AuthorityID. Der ISO Name Space wird nach ISO/IEC 9594 mittels eines Verzeichnissystems realisiert, in dem die Naming Entity des Beispiels durch „C=AT, O=Graz-University, OU=IMI“ auffindbar ist; der Local Name wird im Directory Information Tree als Canonical Name (CN) abgelegt. Ein Auftraggeber kann eine ISO Naming Entity über das Österreichische Normungs-institut eintragen lassen (ON A 2642).

Eine Alternative zur X.500 Verzeichnisstruktur stellt das Domain Name System (DNS) dar. Internet Domain Names werden nach RFC 1034 global registriert, Subdomains lokal vergeben. In Ergänzung des obigen Beispiels ist somit „DNS:imi.uni-graz.at“ eine gültige AuthorityID innerhalb des DNS. Wie gut erkennbar besteht keine 1 zu 1 Beziehung zwischen den RDNs in den unterschiedlichen Name Spaces. Der Local Name wird als Pfad dem Domain Name zugesetzt. Internet Domain Names werden über den Internet Service Provider des Auftraggebers registriert.

Welches der beiden Verfahren zur Anwendung kommen soll, ist von der Situation und den implementierten Diensten beim Auftraggeber abhängig.

4.1.3. Lokale RDNs

Wie in Abschnitt 3.9. beschrieben, ist jede durchgeführte Übermittlung zu protokollieren. Im Rahmen einer reversiblen Anonymisierung ist ein Relative Distinguished Name als TransferID zu vergeben und im Übermittlungsprotokoll zu vermerken. Obwohl prinzipiell ein beliebiger (eindeutiger) Identifier als TransferID wählbar ist, wird empfohlen, den in der Protokollierung aufgetragenen Zeitpunkt der Übermittlung als RDN zu verwenden:

```
TransferID ::= YYYY MM DD [ HH [ MM [ SS [ "." SS ] ] ] ]
```

Die Genauigkeit des Timestamp ist von der Frequenz der Übermittlungen beim Auftraggeber abhängig und muss jedenfalls das Datum des Transfers umfassen. Die Einbeziehung der Uhrzeit (Stunde) wird angeraten.

Als SetID wird die Verwendung einer bei „1“ beginnenden, fortlaufenden Nummer als RDN empfohlen. Wird von diesem Procedere abgewichen, so ist sicherzustellen, dass die SetID unabhängig von den primären Identifikationsdaten im jeweiligen Datensatz generiert wird.

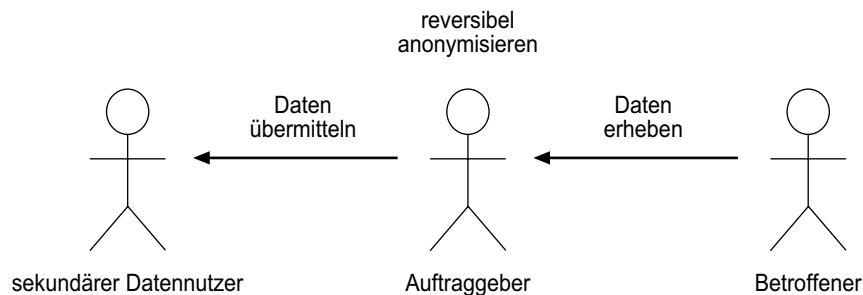
4.1.4. Vorgehensmodell

Die Methode der reversiblen Anonymisierung ist ein 2-stufiger Prozess und beinhaltet die folgenden Schritte:

1. Vor der Übermittlung von Daten ist vom Auftraggeber neben der *k*-Anonymisierung eine Kennzeichnung aller zu transferierender Datensätze durch Distinguished Names durchzuführen.
2. Im Bedarfsfall retourniert der sekundäre Datennutzer den betreffenden Datensatz an den Auftraggeber zum Zweck der Rückführung auf den Betroffenen. Der Auftraggeber selbst kann die Zuordnung aufgrund des Distinguished Name im Datensatz vornehmen.

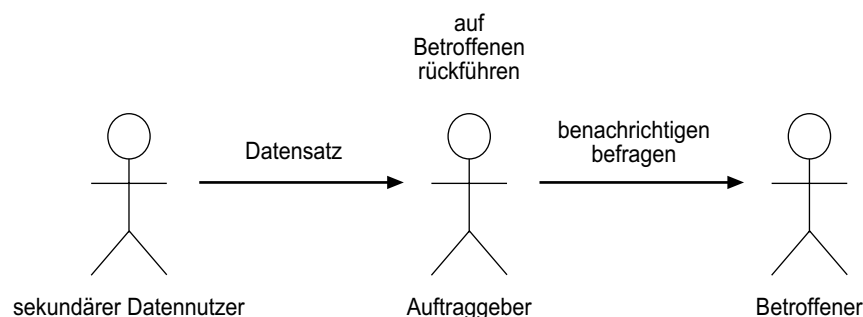
¹³ Die Registration Authority repräsentiert die Root eines Name Space.

Gemäß den Ausführungen in 3.7. sind alle Attribute der primären Identifikationsdaten entweder zu löschen oder mit einem als sicher geltenden Verfahren zu verschlüsseln. Werden zur Elimination des Personenbezugs die primären Identifikationsdaten gelöscht, so muss der Auftraggeber zwecks späterer Rückführung zumindest Name und Adresse des Betroffenen in Kombination mit der TransferID und SetID des zugehörigen Datensatzes speichern. Beim Einsatz von kryptographischen Methoden sind das zur Anwendung kommende Verfahren, der gewählte Schlüssel sowie die TransferID aufzuzeichnen. Es wird empfohlen, den Key „offline“ an einem sicheren Ort zu verwahren, idealerweise auf einer Chipkarte. Für eine prinzipielle Darstellung der reversiblen Anonymisierung siehe die folgenden zwei Abbildungen.



Es sei an dieser Stelle angemerkt, dass bei reversibler Anonymisierung eine Verschlüsselung der primären Identifikationsdaten das Procedere zwar kompliziert, dafür aber den Auftraggeber von der Verwaltung der Namen und Adressen der Betroffenen sowie der SetIDs befreit. Aus diesem Grund wird, bei reversibler Anonymisierung, der Einsatz von kryptographischen Verfahren zur Elimination des Personenbezugs als Mittel der Wahl empfohlen.

Die Wiederherstellung des Personenbezugs beim Auftraggeber erfolgt gemäß den folgenden Verarbeitungsschritten. Sind die primären Identifikationsdaten des Betroffenen vor der Übermittlung gelöscht worden, müssen diese anhand von TransferID und SetID im Datenbestand des Auftraggeber gesucht und bestimmt werden. Erfolgte die Elimination der primären Identifikationsdaten durch Verschlüsseln, so ist vom Auftraggeber vermöge der TransferID der zugehörige Key festzustellen, um in der Folge die primären Identifikationsdaten im retournierten Datensatz zu dechiffrieren. Die Bedeutung der Attribute ist aus den im Übermittlungsprotokoll gespeicherten Datenarten ersichtlich.¹⁴ Eine schematische Darstellung des Ablaufs zur Rückführung von übermittelten Daten auf den Betroffenen zeigt die nachstehende Abbildung.



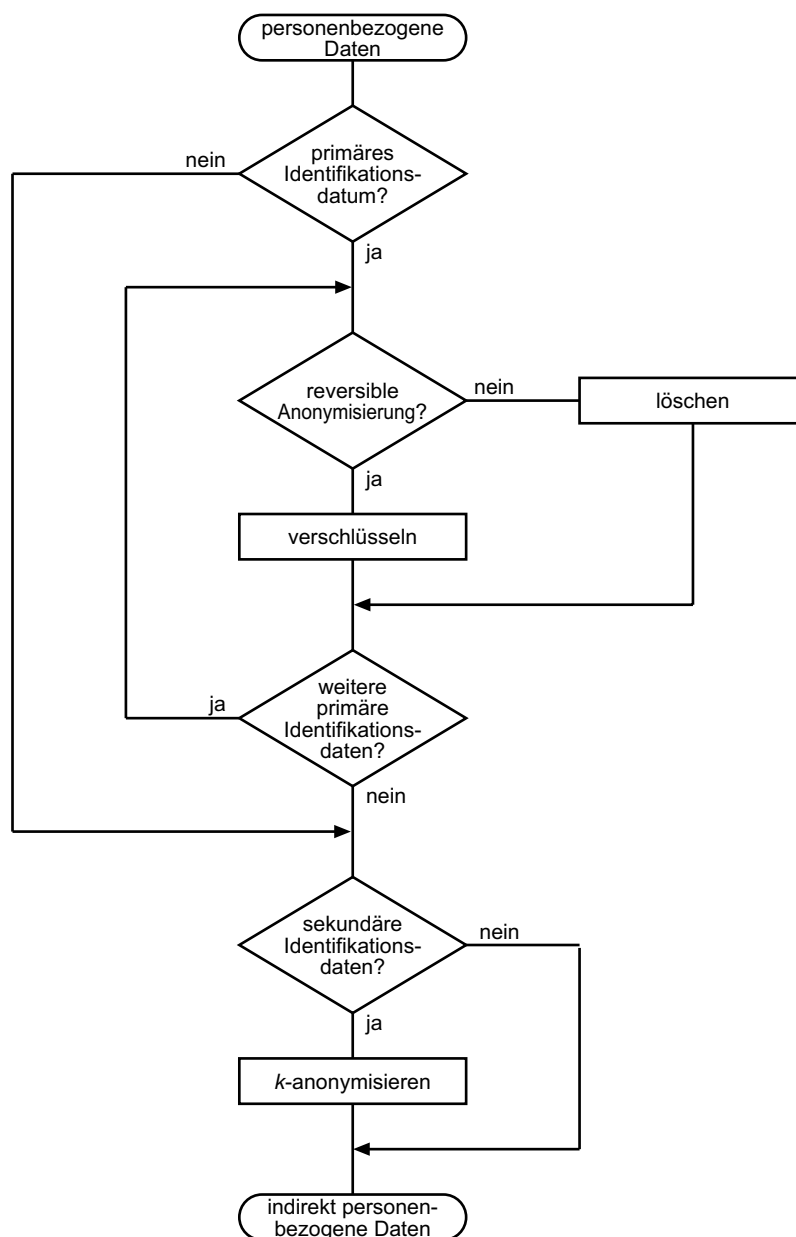
Im Weiteren vollzieht der Auftraggeber die Benachrichtigung des Betroffenen und führt eine eventuelle Befragung durch. Schließlich wird ein komplettierter Datensatz neuerlich reversibel

¹⁴ Die Bedeutung der Attribute eines Datensatzes ist i. Allg. nur dann aus dem Übermittlungsprotokoll ersichtlich, wenn der sekundäre Datennutzer keine der in 2.2.4. beschriebenen Transformationen vorgenommen hat.

anonymisiert (bei Verschlüsselung mit dem ursprünglichen Key) und unter Verwendung des originalen Distinguished Name an den sekundären Datennutzer übermittelt. Man beachte, dass für den nun erweiterten Datensatz die k -Anonymität zu prüfen ist. Kann diese nicht erzielt werden (siehe Abschnitt 3.8.3.), so bleibt alternativ nur der Weg, den Betroffenen aufzuklären und ihn unter der Angabe des Distinguished Name an den sekundären Datennutzer zu verweisen bzw. gemäß § 46 Abs. 2 die Genehmigung der Datenschutzkommission einzuholen.

4.2. Vorgehensmodell zur Anonymisierung personenbezogener Daten

Zusammenfassend wird, für die Umwandlung von personenbezogenen Daten in eine indirekt personenbezogene Entsprechung, die in der nachstehenden Abbildung skizzierte Vorgehensweise empfohlen.



Die folgende Checkliste für die Übermittlung von indirekt personenbezogenen Daten versteht sich als Ergänzung des obigen Flussdiagramms im Sinne einer „good practice“:

1. Kontrolliere die ausreichende gesetzliche Zuständigkeit oder rechtliche Befugnis des Empfängers im Hinblick auf den Übermittlungszweck. Protokolliere die getroffene Entscheidung.
2. Definiere die zu übermittelnden Daten, insbesondere die vom sekundären Datennutzer benötigte Anzahl an Datensätzen und die darin enthaltenen Datenarten. Dokumentiere Anzahl und Attributliste im Übermittlungsprotokoll.
3. Wird eine reversible Anonymisierung gewünscht, so ist jeder Datensatz mit einem Distinguished Name zu versehen. Die gewählte TransferID ist im Protokoll festzuhalten.
4. Bestimme die primären Identifikationsdaten innerhalb der zu transferierenden Datensätze.
5. Eliminiere den Personenbezug in den jeweiligen Datensätzen durch
 - a. löschen der primären Identifikationsdaten oder
 - b. verschlüsseln der primären Identifikationsdaten (reversible Anonymisierung). Wähle dazu das Verschlüsselungsverfahren, generiere den notwendigen Key und protokolliere das Procedere. Verwahre das Paar (TransferID, Key) an einem sicheren Ort.
6. Bestimme die sekundären Identifikationsdaten in den zu kommunizierenden Datensätzen. Lege die untere Schranke der k -Anonymität fest (mindestens $k \geq 2$, empfohlen wird $k \geq 5$).
7. Bestimme k für die zu übermittelnden Datensätze.
8. Ist k kleiner als die vorgegebene untere Schranke:
 - a. Führe entsprechende Transformationen für eine beschränkte Übermittlung der Daten durch. Verwende insbesondere Methoden zur Generalisierung von Attributwerten bzw. Attributunterdrückung. Gehe zu Schritt 7.
 - b. Alternativ kann k im Bestand von Dateien beim Auftraggeber nachgewiesen werden.
9. Dokumentiere den erzielten Wert für k .
10. Übermittle die indirekt personenbezogenen Daten an den sekundären Datennutzer. Protokolliere den Transferzeitpunkt. Zur Gewährleistung der Datensicherheit (Datenintegrität, Ursprungsnachweis) chiffriere und signiere man die zu übertragenden Daten.

Ist die Frage der k -Anonymität aus Schritt 7 nicht beantwortbar beziehungsweise kann diese nicht erzielt werden, so ist alternativ wie folgt vorzugehen (personenbezogene Übermittlung von Daten):

1. Kontrolliere die ausreichende gesetzliche Zuständigkeit oder rechtliche Befugnis des Empfängers im Hinblick auf den Übermittlungszweck. Protokolliere die getroffene Entscheidung.
2. Überprüfe das Vorliegen einer schriftlichen Vereinbarung über die implementierten Datensicherheitsmaßnahmen inklusive Datengeheimnis im Organisationsbereich des Empfängers bzw. dessen MAGDA-LENA-Konformitätserklärung. Die Dokumente sind Teil des Übermittlungsprotokolls.
3. Definiere die zu übermittelnden Daten.
4. Beantrage die personenbezogene Übermittlung der Daten bei der lokalen Ethikkommission.
5. Erfülle mögliche Auflagen und Bedingungen der lokalen Ethikkommission. Protokolliere die durchgeführten Maßnahmen.
6. Schaffe bzw. verifiziere die rechtliche Zulässigkeit der Datenübermittlung:
 - a. Ausdrückliche Zustimmung aller Betroffenen vorhanden?
Führe die entsprechende Meldung an das Datenverarbeitungsregister durch.

- b. Alternativ ist die Genehmigung der Datenschutzkommission einzuholen.
- 7. Erfülle mögliche Auflagen und Bedingungen der Datenschutzkommission. Protokolliere die durchgeführten Maßnahmen.
- 8. Übermittle die personenbezogenen Daten an den sekundären Datennutzer. Protokolliere die Daten und den Transferzeitpunkt. Zur Gewährleistung der Datensicherheit (Vertraulichkeit, Datenintegrität, Ursprungsnachweis) chiffriere und signiere man die zu übertragenden Daten.

4.3. Vorschläge für weitere Entwicklungen

Zur Vereinfachung von einigen, in der vorliegenden Datenschutz-Policy empfohlenen Aktivitäten sei abschließend eine Liste von nutzbringenden weiteren Entwicklungen zusammengestellt.

Die Praxis zeigt, dass ein Großteil der im Rahmen von wissenschaftlichen Untersuchungen erhobenen Daten in Form von Spreadsheets, insbesondere in Microsoft Excel, verwaltet und übermittelt wird.¹⁵ Durch die Programmierung von Makros können eine Reihe von Verarbeitungsschritten automatisiert werden, nämlich

1. die Kennzeichnung von Datensätzen mittels Distinguished Names zur Simplifizierung der reversiblen Anonymisierung,
2. die spaltenweise Verschlüsselung von Attributwerten zur Elimination des Personenbezugs,
3. die Bestimmung der Dimension von k für eine Auswahl von Attributen, sowie
4. die Anwendung von Transformationen für eine beschränkte Übermittlung von Daten entsprechend der Definition in 2.2.4.

Es empfiehlt sich weiters, für gängige Kombinationen sekundärer Identifikationsdaten, im Datenbestand großer Anwender Richtwerte für k zu bestimmen und innerhalb der wissenschaftlichen Gemeinde bekannt zu geben.

¹⁵ Häufig wird der In- und Export von Daten auch über Dateien mit „Comma Separated Values“ durchgeführt.

5. Health Level 7

5.1. HL7 Nachrichtenaufbau

Eine Nachricht ist die kleinste übertragbare Protokolleinheit in HL7 und wird getreu einem Kommunikationsstandard auf Applikationsebene in abstrakter Form spezifiziert (Abstract Message Definition). Demgemäß setzt sich eine Nachricht aus einer Folge von logisch gruppierten Datenfeldern, sogenannten Segmenten, zusammen, die mit Hilfe der Abstract Message Syntax beschrieben werden. Für den allgemeinen Aufbau einer Nachricht gilt:

```
Nachricht ::= <Segment> { <CR> <Segment> } *
Segment ::= <Element> { "|" <Element> } *
Element ::= [ <Komponente> { "^" <Komponente> } * ]
Komponente ::= [ <SubKomponente> { "&" <SubKomponente> } * ]
```

Die Semantik der Segmente wird, ergänzt von sprachlichen Erläuterungen, durch die inkludierten Datenfelder festgelegt. Jedes Element hat einen bestimmten Datentyp und besteht i. Allg. aus einer Reihe von Komponenten. Die Bindung einzelner Komponenten zu einer gemeinsamen Struktur – basierend auf deren Beziehungen zueinander – spiegelt die tägliche Erfahrung im Umgang mit diesen Daten wider und liefert somit den entscheidenden Beitrag zur Abstraktion der realen Welt. Eine explizite Wertemenge wird in der Praxis nur bei Aufzählungstypen in tabellarischer Form vorgeschrieben.

In den folgenden Abschnitten werden jene Segmente angeführt, die primäre oder sekundäre Identifikationsdaten enthalten.

5.2. Segmente mit demographischen Patientendaten

5.2.1. ACC – Accident Segment

Das ACC Segment beinhaltet Unfalldaten relativ zum involvierten Patienten.

SEQ#	LÄNGE	HL7-DATENTYP	HL7-TBL#	ELEMENTNAME
1	26	TS		Accident Date/Time
2	60	CE	0050	Accident Code
3	25	ST		Accident Location
4	60	CE	0347	Auto Accident State
5	1	ID	0136	Accident Job Related Indicator
6	12	ID	0136	Accident Death Indicator

Sekundäre Identifikationsdaten

```
TimeStamp ::= YYYY [ MM [ DD [ <Time> ] ] ] "^" <Degree of Precision>
Time ::= HH [ MM [ SS [ "." SSSS ] ] ] [ <Time Zone> ]
Timezone ::= "+" HHMM | "-" HHMM
```

```
ACC#1-Accident Date/Time ::= [ <TimeStamp> ]
```

Der Zeitpunkt des Unfalls in strukturierter Form mit entsprechender Generalisierungsmöglichkeit.

```
CodedElement ::= <Identifer> "^"
                <Text> "^"
                <Name of Coding System> "^"
                <Alternate Identifier> "^"
                <Alternate Text> "^"
                <Name of Alternate Coding System>
```

ACC#2-Accident Code ::= [<CodedElement>]
 ACC#3-Accident Location ::= [<String>]
 ACC#5-Accident Job Related Indicator ::= [<Coded Value (user-defined)>]
 ACC#6-Accident Death Indicator ::= [<Coded Value (user-defined)>]

5.2.2. AL1 – Patient Allergy Information Segment

Das AL1 Segment enthält Informationen über diverse Allergien eines Patienten, wobei für jede Form der Überempfindlichkeit ein eigenes Segment verwendet wird.

SEQ#	LÄNGE	HL7-DATENTYP	HL7-TBL#	ELEMENTNAME
1	4	SI		Set ID – AL1
2	2	IS	0127	Allergy Type
3	60	CE		Allergy Code/Description
4	2	IS	0128	Allergy Severity
5	15	ST		Allergy Reaction
6	8	DT		Identification Date

Sekundäre Identifikationsdaten

AL1#2-Allergy Type ::= [<Coded Value (user-defined)>]

Beschreibt die allgemeine Kategorie einer Allergie (Medikamente, Nahrungsmittel, etc.).

```
CodedElement ::= <Identifer> "^"
  <Text> "^"
  <Name of Coding System> "^"
  <Alternate Identifier> "^"
  <Alternate Text> "^"
  <Name of Alternate Coding System>
```

AL1#3-Allergy Code/Description ::= <CodedElement>

AL1#4-Allergy Severity ::= [<Coded Value (user-defined)>]

Feld AL1#3 enthält die diagnostische Information der Allergie.

AL1#5-Allergy Reaction ::= [<String>]

Textuelle Kurzbeschreibung der spezifischen allergischen Reaktion (Krämpfe, Niesen, Ausschläge usw.).

5.2.3. DB1 – Disability Segment

Körperbeschädigung, Arbeits- und Erwerbsunfähigkeit sowie Invalidität und Behinderungen eines Betroffenen werden im Disability Segment übermittelt.

SEQ#	LÄNGE	HL7-DATENTYP	HL7-TBL#	ELEMENTNAME
1	4	SI		Set ID - DB1
2	2	IS	0334	Disabled Person Code
3	32	CX		Disabled Person Identifier
4	1	ID	0136	Disabled Indicator
5	8	DT		Disability Start Date
6	8	DT		Disability End Date
7	8	DT		Disability Return to Work Date
8	8	DT		Disability Unable to Work Date

Patientenbezug

```

CompositeID ::= <ID> "^"
               <Check Digit> ""
               <Code Identifying the Check Digit Scheme> ""
               <Assigning Authority> ""
               <Identifier Type Code> ""
               <Assigning Facility>
Assigning Authority ::= <Namespace ID> "&"
                       <Universal ID> "&"
                       <Universal ID Type>
Assigning Facility ::= <Namespace ID> "&"
                      <Universal ID> "&"
                      <Universal ID Type>

DB1#3-Disabled Person Identifier ::= [ <CompositeID>]
DB1#2-Disabled Person Code ::= [ <Coded Value (user-defined)>]

```

„Disabled Person Code“ und „-Identifier“ referenziert den Betroffenen bezüglich der im Segment enthaltenen Information. Attributkombination zur primären Identifikation eines Betroffenen.

Sekundäre Identifikationsdaten

```

TimeStamp ::= YYYY [ MM [ DD [ <Time>]]] "" <Degree of Precision>
Time ::= HH [ MM [ SS [ "." SSSS]]] [ <Time Zone>]
Timezone ::= "+" HHMM | "-" HHMM

DB1#5-Disability Start Date ::= [ <TimeStamp>]
DB1#6-Disability End Date ::= [ <TimeStamp>]
DB1#7-Disability Return to Work Date ::= [ <TimeStamp>]
DB1#8-Disability Unable to Work Date ::= [ <TimeStamp>]

```

Beginn und Ende einer Behinderung/Invalidität bzw. einer Erwerbseinschränkung oder Arbeitsunfähigkeit. Sekundäre Identifikationsattribute mit entsprechender Generalisierungsmöglichkeit.

5.2.4. NK1 – Next of Kin, Associated Parties Segment

Das NK1 Segment enthält Informationen über, mit dem Patienten assoziierte, natürliche oder juristische Personen sowie die Art der Beziehung, in der diese Person zum Betroffenen steht. Darüber hinaus verwendet HL7 dieses Segment auch zur Beschreibung von Geschäftskontakten des Auftraggebers selbst. Jede Relation wird durch ein eigenes Segment repräsentiert, das gilt auch dann, wenn eine Person in unterschiedlichen Rollen auftritt.

SEQ#	LÄNGE	HL7-DATENTYP	HL7-TBL#	ELEMENTNAME
1	4	SI		Set ID - NK1
2	48	XPN		Name
3	60	CE	0063	Relationship
4	106	XAD		Address
5	40	XTN		Phone Number
6	40	XTN		Business Phone Number
7	60	CE	0131	Contact Role
8	8	DT		Start Date
9	8	DT		End Date
10	60	ST		Next of Kin / Associated Parties Job Title
11	20	JCC	0327/0328	Next of Kin / Associated Parties Job Code/Class
12	20	CX		Next of Kin / Associated Parties Employee Number
13	90	XON		Organization Name - NK1
14	80	CE	0002	Marital Status
15	1	IS	0001	Sex
16	26	TS		Date/Time of Birth

SEQ#	LÄNGE	HL7-DATENTYP	HL7-TBL#	ELEMENTNAME
17	2	IS	0223	Living Dependency
18	2	IS	0009	Ambulatory Status
19	80	CE	0171	Citizenship
20	60	CE	0296	Primary Language
21	2	IS	0220	Living Arrangement
22	80	CE	0215	Publicity Code
23	1	ID	0136	Protection Indicator
24	2	IS	0231	Student Indicator
25	80	CE	0006	Religion
26	48	XPN		Mother's Maiden Name
27	80	CE	0212	Nationality
28	80	CE	0189	Ethnic Group
29	80	CE	0222	Contact Reason
30	48	XPN		Contact Person's Name
31	40	XTN		Contact Person's Telephone Number
32	106	XAD		Contact Person's Address
33	32	CX		Next of Kin/Associated Party's Identifiers
34	2	IS	0311	Job Status
35	80	CE	0005	Race
36	2	IS	0295	Handicap
37	16	ST		Contact Person SSN

Vorgehensmodell

Die Felder NK1#3 „Relationship“ und NK1#7 „Contact Role“ spezifizieren die Beziehung zwischen dem Patienten und einer im Segment charakterisierten dritten Person sowie die Rolle respektive die Sachlage, aus der heraus diese zu kontaktieren ist. Beispiele für Dritte sind nächste Angehörige wie allgemein Lebenspartner, Kinder, Eltern, Geschwister, weitere Personen, Firmen und Organisationen. Mögliche Rollen bzw. Situationen sind der Notfallskontakt, Versicherer, Bürge, Zuweiser, Arbeitgeber und dergleichen mehr. Alle, vermöge der im Segment inkludierten Elemente, identifizierbaren Personen sind Betroffene im Sinne des DSG 2000, wobei einzelne Attribute sensible Informationen beinhalten können. Aus Sicht der wissenschaftlichen Forschung und Statistik sind diese Personen und Organisationen i. Allg. nicht Teil der Beobachtung und so wird nachdrücklich empfohlen, keine NK1 Segmente zu übermitteln.

Sollen effektiv Beziehungen zwischen Personen untersucht werden, etwa von Mutter und Kind oder unter Geschwistern, so wird angeregt, für jeden Betroffenen einen eigenen Datensatz zu verwenden und die entsprechenden Daten im PID Segment zu übermitteln. Zur Beschreibung der Beziehungsinformation ist dann ein nur aus „Relationship“ (#3) und „Next of Kin/Associated Party's Identifiers“ (#33) bestehendes NK1 Segment ausreichend. Als Identifier soll der in 4.1.1. beschriebene Distinguished Name des korrespondierenden Datensatzes zur Anwendung kommen; auf diese Weise ist die Verknüpfung relativ bezüglich der transferierten Daten.

5.2.5. PD1 – Patient Additional Demographic Segment

Das Patient Additional Demographic Segment enthält veränderliche demographische Daten des Patienten.

SEQ#	LÄNGE	HL7-DATENTYP	HL7-TBL#	ELEMENTNAME
1	2	IS	0223	Living Dependency
2	2	IS	0220	Living Arrangement
3	90	XON		Patient Primary Facility
4	90	XCN		Patient Primary Care Provider Name & ID No.
5	2	IS	0231	Student Indicator
6	2	IS	0295	Handicap
7	2	IS	0315	Living Will
8	2	IS	0316	Organ Donor
9	1	ID	0136	Separate Bill
10	20	CX		Duplicate Patient
11	80	CE	0215	Publicity Code
12	1	ID	0136	Protection Indicator

Sekundäre Identifikationsdaten

```
PD1#1-Living Dependency ::= [ <Coded Value (user-defined)>
    { "~" [ <Coded Value (user-defined)>] *}
PD1#2-Living Arrangement ::= [ <Coded Value (user-defined)>
```

Informationen über dritte Personen

```
CompositeName ::= <Organization Name> "^"
    <Organization Name Type Code> "^"
    <ID Number> "^"
    <Check Digit> "^"
    <Check Digit Scheme> "^"
    <Assigning Authority> "^"
    <Identifier Type Code> "^"
    <Assigning Facility> "^"
    <Name Representation Code>
Assigning Authority ::= <Namespace ID> "&"
    <Universal ID> "&"
    <Universal ID Type>
Assigning Facility ::= <Namespace ID> "&"
    <Universal ID> "&"
    <Universal ID Type>
```

```
PD1#3-Patient Primary Facility ::= [ <CompositeName> { "~" <CompositeName> } *]
```

Die Praxis des niedergelassenen Arztes. In ruralen Gebieten auch eine Krankenschwester oder Hebamme als primäre Ansprechpartner des Patienten.

```
CompositeID&Name ::= <ID Number>
    <Family Name> "&" <Last Name Prefix> "^"
    <Given Name> "^"
    <Middle Initial or Name> "^"
    <Suffix> "^"
    <Prefix> "^"
    <Degree> "^"
    <Source Table> "^"
    <Assigning Authority> "^"
    <Name Type Code> "^"
    <Identifier Check Digit> "^"
    <Code Identifying the Check Digit Scheme> "^"
    <Identifier Type Code> "^"
    <Assigning Facility> "^"
    <Name Representation Code>
```

```
PD1#4-Patient Primary Care Provider Name & ID ::= [ <CompositeID&Name>
    { "~" <CompositeID&Name> } *]
```

Im Sinne des DSG sind der Name und die Kassenummer des Hausarztes als primäre Identifikationsdaten einzustufen.

Weitere sekundäre Identifikationsdaten

PD1#5-Student Indicator ::= [<Coded Value (user-defined)>]
 PD1#6-Handicap ::= [<Coded Value (user-defined)>]
 PD1#8-Organ Donator ::= [<Coded Value (user-defined)>]

5.2.6. PID – Patient Identification Segment

Das PID Segment wird von allen HL7-Nachrichten als das primäre Objekt zur Übertragung von Patienten-Identifikationsdaten verwendet. Der Datensatz enthält die permanenten Informationen zur Patientenidentifikation sowie demographische Daten mit geringer Änderungswahrscheinlichkeit.

SEQ#	LÄNGE	HL7-DATENTYP	HL7-TBL#	ELEMENTNAME
1	4	SI		Set ID – PID
2	20	CX		Patient ID
3	20	CX		Patient Identifier List
4	20	CX		Alternate Patient ID - PID
5	48	XPN		Patient Name
6	48	XPN		Mother's Maiden Name
7	26	TS		Date/Time of Birth
8	1	IS	0001	Sex
9	48	XPN		Patient Alias
10	80	CE	0005	Race
11	106	XAD		Patient Address
12	4	IS	0289	County Code
13	40	XTN		Phone Number - Home
14	40	XTN		Phone Number - Business
15	60	CE	0296	Primary Language
16	80	CE	0002	Marital Status
17	80	CE	0006	Religion
18	20	CX		Patient Account Number
19	16	ST		SSN Number - Patient
20	25	DLN		Driver's License Number - Patient
21	20	CX		Mother's Identifier
22	80	CE	0189	Ethnic Group
23	60	ST		Birth Place
24	1	ID	0136	Multiple Birth Indicator
25	2	NM		Birth Order
26	80	CE	0171	Citizenship
27	60	CE	0172	Veterans Military Status
28	80	CE	0212	Nationality
29	26	TS		Patient Death Date and Time
30	1	ID	0136	Patient Death Indicator

Attribute basierend auf „Person ID“

```
CompositeID ::= <ID> "^"
               <Check Digit> ""
               <Code Identifying the Check Digit Scheme> ""
               <Assigning Authority> ""
               <Identifier Type Code> ""
               <Assigning Facility>
```

```

Assigning Authority ::= <Namespace ID> "&"
                    <Universal ID> "&"
                    <Universal ID Type>
Assigning Facility ::= <Namespace ID> "&"
                    <Universal ID> "&"
                    <Universal ID Type>

```

```

PID#2-Patient ID ::= [<CompositeID>]
PID#3-Patient Identification List ::= <CompositeID> {"~" <CompositeID>} *
PID#4-Alternate Patient ID ::= [<CompositeID> {"~" <CompositeID>} *]
PID#18-Patient Account Number ::= [<CompositeID>]
PID#21-Mother's Identifier ::= [<CompositeID> {"~" <CompositeID>} *]

```

PID#3-„Patient Identifier List“ enthält eine Aufzählung primärer Identifikationsdaten. Ab HL7 Version 2.3.1 wird von einer organisationsübergreifenden Patienten-ID ausgegangen, die Felder PID#2 (external ID) und PID#4 (alternativer, temporärer oder detaillierender Patienten-Identifizierer) aus Gründen der Kompatibilität zu älteren Versionen des Standards aber belassen. PID#3 beschreibt in Versionen vor 2.3.1 die innerhalb einer Organisation verwendete PID. Falls vorhanden wird empfohlen „Mother's Identifier“ zu löschen.

Reversible Anonymisierung

Ein Distinguished Name gemäß den Ausführungen in 4.1.1. ist als weiterer Eintrag in PID#3 „Patient Identification List“ zu speichern. Dabei entspricht die „AuthorityID“ des Distinguished Name der „Assigning Authority“ in PID#3, d.h.

```

Assigning Authority.Name Space ::= <RegistrationAuthority>
Assigning Authority.Universal ID ::= <NamingEntity>

```

Der „LocalName“ wird in der Komponente „ID“ gespeichert:

```

ID ::= <TransferID> "/" <SetID>
Check Digit ::= ""

```

Zusätzlich kann als „Assigning Facility“ die Organisationseinheit bzw. Person spezifiziert werden, welche den „LocalName“ vergeben hat.

Attribute basierend auf „Person Name“

```

PersonName ::= <Family Name> "&" <Last Name Prefix> "^"
              <Given Name> "^"
              <Middle Initial or Name> "^"
              <Suffix> "^"
              <Prefix> "^"
              <Degree> "^"
              <Name Type Code> "^"
              <Name Representation Code>

```

```

PID#5-Patient Name ::= <PersonName> {"~" <PersonName>} *
PID#6-Mother's Maiden Name ::= [<PersonName> {"~" [<PersonName>]} *]
PID#9-Patient Alias ::= [<PersonName> {"~" <PersonName>} *]

```

Das Feld PID#3 enthält den offiziellen Patientennamen. Alle anderen Namen (Alias) werden im Feld PID#9 übertragen. Falls vorhanden wird empfohlen „Mother's Maiden Name“ zu löschen. Alle aufgezählten Elemente sind primäre Identifikationsdaten.

Geographische Informationen

„Patient Address“ ist eine strukturierte Adresse und kann, als primäres Identifikationsmerkmal, durch komponentenweise Generalisierung in ein sekundäres Identifikationsdatum umgewandelt werden. Es wird allerdings empfohlen, PID#11 zuverlässig zu eliminieren und stattdessen das Feld PID#12 „County Code“ zur Übermittlung von geographischen Informationen zu verwenden.

```

PersonAddress ::= <Street Address> "^"
                <Other Designation> "^"
                <City> "^"
                <State or Province> "^"
                <Zip or Postal Code> "^"
                <Country> "^"
                <Address Type> "^"
                <Other Geographic Designation> "^"
                <County/Parish Code> "^"
                <Census Tract> "^"
                <Address Representation Code>

PID#11-Patient Address ::= [ <PersonAddress> { "~" <PersonAddress> } * ]
PID#12-County Code ::= [ <Coded Value (user-defined)> ]
PID#23-Birth Place ::= [ <String> ]

```

Weitere primäre Identifikationsdaten

```

PhoneNumber ::= [ NNN [ (999) 999-9999
                 [ "X" 99999 [ "B" 99999 [ "C" <any Text> ] "^"
                 <Telecommunication Use Code> "^"
                 <Telecommunication Equipment Type> "^"
                 <Email Address> "^"
                 <Country Code> "^"
                 <Area/City Code> "^"
                 <Phone Number> "^"
                 <Extension> "^"
                 <any Text>

PID#13-Phone Number Home ::= [ <PhoneNumber> { "~" <PhoneNumber> } * ]
PID#14-Phone Number Business ::= [ <PhoneNumber> { "~" <PhoneNumber> } * ]

PID#19-SSN Number Patient ::= [ <String> ]

LicenseNumber ::= <License Number> "^"
                 <Issuing State, Province, Country> "^"
                 <Expiration Date>

PID#20-Driver's License Number ::= [ <LicenseNumber> ]

```

Sekundäre Identifikationsdaten

```

TimeStamp ::= YYYY [ MM [ DD [ <Time> ] ] ] "^" <Degree of Precision>
Time ::= HH [ MM [ SS [ "." SSSS ] ] ] [ <Time Zone> ]
Timezone ::= "+" HHMM | "-" HHMM

PID#7-Date/Time of Birth ::= [ TimeStamp ]
PID#29-Date/Time of Death ::= [ <TimeStamp> ]

```

Geburts- und Todeszeitpunkt des Betroffenen in strukturierter Form; sekundäres Identifikationsdatum mit entsprechender Generalisierungsmöglichkeit.

Weitere sekundäre Identifikationsdaten

```

CodedElement ::= <Identifier> "^"
                <Text> "^"
                <Name of Coding System> "^"
                <Alternate Identifier> "^"
                <Alternate Text> "^"
                <Name of Alternate Coding System>

PID#8-Sex ::= [ <Coded Value (user-defined)> ]
PID#10-Race ::= [ <CodedElement> { "~" <CodedElement> } * ]
PID#15-Primary Language ::= [ <CodedElement> ]
PID#15-Martial Status ::= [ <CodedElement> ]
PID#17-Religion ::= [ <CodedElement> ]
PID#22-Ethnic Group ::= [ <CodedElement> { "~" <CodedElement> } * ]
PID#26-Citizenship ::= [ <CodedElement> { "~" <CodedElement> } * ]
PID#27-Veterans Military Status ::= [ <CodedElement> ]
PID#28-Nationality ::= [ <CodedElement> ]

PID#24-Multiple Birth Indicator ::= [ <Coded Value (user-defined)> ]
PID#25-Birth Order ::= [ <Numeric> ]
PID#30-Patient Death Indicator ::= [ <Coded Value (user-defined)> ]

```

5.3. Weitere Segmente mit primären und/oder sekundären Identifikationsdaten

Die folgenden, zur Übermittlung von Verwaltungs- und Verrechnungsdaten bestimmten Segmente enthalten primäre und/oder sekundäre Identifikationsdaten, sind aber aus Sicht der wissenschaftlichen Forschung und Statistik ohne Bedeutung:

1. BLG – Billing Segment
2. FT1 – Financial Transaction Segment
3. GT1 – Guarantor Segment
4. IN1 – Insurance Segment
5. IN2 – Insurance Additional Information Segment
6. IN3 – Insurance Additional Information, Certification Segment

Die aufgezählten Segmente sind in den entsprechenden HL7 Nachrichten zu löschen.

5.4. Spezielle HL7 Segmente

5.4.1. NTE – Notes and Comments Segment

NTE ist das allgemeine HL7 Segment zur Übermittlung von textbasierten Anmerkungen und Kommentaren.

SEQ#	LÄNGE	HL7-DATENTYP	HL7-TBL#	ELEMENTNAME
1	4	SI		Set ID - NTE
2	8	ID	0105	Source of Comment
3	64k	FT		Comment
4	60	CE		Comment Type

Das Kommentarfeld NTE#3 hat eine zulässige Textlänge von 64k Zeichen. Es ist darauf zu achten, dass die im Kontext enthaltene Information keine Identifikation des Betroffenen ermöglicht. Da eine maschinelle Auswertung von unstrukturiertem Text i. Allg. nur bedingt Erfolg verspricht, ist zu überlegen, ob dieses Attribut für die wissenschaftliche Forschung und Statistik benötigt wird.

5.4.2. Z-Segmente

HL7 ist ein (internationaler) Standard des American National Standards Institute (ANSI) und Teil der von den Vereinten Nationen verwalteten ISO-Standardisierung. Ziel der Normung ist die größtmögliche Vereinheitlichung der Kommunikation, ohne dabei länderspezifische Varianten oder lokale Ausprägungen zu unterbinden. Es ist die Aufgabe von nationalen Benutzergruppen bzw. von lokalen Vereinbarungen, zusätzlich zu den in der Standardfassung vorgegebenen Nachrichtentypen und Segmenten eigene Erweiterungen zu definieren, die auf die jeweiligen Detailprobleme eingehen. Diese Erweiterungen werden in Form von Z-Segmenten spezifiziert.

Es kommt nicht selten vor, dass große, international durchgeführte Studien Z-Segmente für den Datenaustausch verwenden. Aus der Sicht des Datenschutzes ist zu prüfen, ob allenfalls eingesetzte Z-Segmente primäre oder sekundäre Identifikationsdaten beinhalten und abhängig vom Ergebnis sind, analog zu der in diesem Kapitel applizierten Prozedur, entsprechende Vorgaben zur Wahrung der schutzwürdigen Geheimhaltungsinteressen von Betroffenen zu definieren.

5.5. HL7 Nachrichten für klinische Studien

Obwohl nicht Teil der vorliegenden Datenschutz-Policy sei angemerkt, dass HL7 spezielle Nachrichten für den elektronischen Austausch von Daten im Rahmen klinischer Studien bereitstellt.

5.5.1. CRM – Clinical Study Registration Message

Das Ziel des CRM Nachrichtentyps ist die Identifikation jener Patienten, die

1. in eine klinische Studie eingeschleust werden oder
2. sich in einer bestimmten Studienphase befinden und folglich eine Reihe von Tests bzw. Behandlungen durchzuführen sind oder
3. eine Testphase abgeschlossen haben und entsprechende Daten zur Auswertung bereitstehen.

Der Aufbau der CRM Nachricht ist wie folgt:

CRM	Clinical Study Registration Message
MSH	Message Header
{ PID	Patient Identification
[PV1]	Patient Visit
CSR	Clinical Study Registration
{{ CSP}}	Clinical Study Phase
}	

Als Ereignisse der realen Welt, die einen Datenaustausch bedingen (Trigger Events), sind für die Clinical Study Registration Message definiert:

EVENT	BESCHREIBUNG
C01	Register a patient on a clinical trial.
C02	Cancel a patient registration on clinical trial (for clerical mistakes since an intended registration should not be canceled).
C03	Correct/update registration information.
C04	Patient has gone off a clinical trial.
C05	Patient enters phase of clinical trial.
C06	Cancel patient entering a phase (clerical mistake).
C07	Correct/update phase information.
C08	Patient has gone off phase of clinical trial.

5.5.2. SCU – Unsolicited Study Data Message

Studiendaten können entweder zentral in einem Studiencenter gesammelt oder verteilt in klinischen Subsystemen (Labor-, Pathologie-, Radiologisches Informationssystem etc.) verwaltet werden. Unabhängig von der implementierten Informationsarchitektur wird ein Großteil der klinischen Daten, nämlich Beobachtungen und Studienparameter, mittels OBR und OBX Segmenten (entweder umgehend nach der Freigabe der Daten oder nach Bedarf) ausgetauscht; die CSR, CSP und CSS Segmente verknüpfen diese Informationen mit der korrespondierenden wissenschaftlichen Studie.

CSU	Unsolicited Study Data Message
MSH	Message Header
{ PID	Patient Identification
[PD1]	Additional Demographics
[{NTE}]	Notes and comments
[PV1	Patient Visit
[PV2]	Patient Visit - Additional Info
]	

```

CSR
{ [ CSP]
  { [ CSS]
    { [ ORC]
      OBR
      { OBX}
    }
    { [ ORC]
      { RXA
        RXR
      }
    }
  }
}
}

```

Clinical Study Registration
Clinical Study Phase
Clinical Study Data Schedule
Common Order
Observation Battery
Observation Results

Common Order
Pharmacy Administration
Pharmacy Route

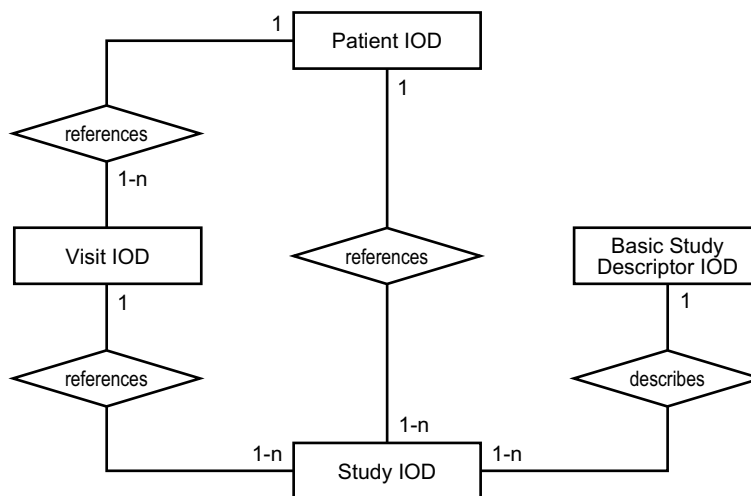
Als Trigger Events für die Unsolicited Study Data Message sind definiert:

EVENT	BESCHREIBUNG
C09	Automated time intervals for reporting, like monthly.
C10	Patient completes the clinical trial.
C11	Patient completes a phase of the clinical trial.
C12	Update/correction of patient order/result information.

6. DICOM

6.1. Information Object Definition

Eine Information Object Definition (IOD) ist ein abstraktes, objekt-orientiertes Datenmodell zur Beschreibung von Entitäten der realen Welt, mit dem Ziel, eine einheitliche Sichtweise auf die zwischen Anwendungen auszutauschenden Informationen zu erzeugen. Dabei charakterisiert eine IOD nicht eine spezifische Instanzierung eines Objekts, sondern vielmehr eine ganze Klasse von solchen Objekten mit gleichen Eigenschaften.



6.1.1. Composite IOD

Eine Information Object Definition bestehend aus Teilen mehrerer Entitäten des DICOM Modells wird „composite IOD“ genannt. Composite IODs beschreiben einen Datenaustausch in einem gesamtheitlichen Kontext, d.h. die Beziehungen zwischen den Entitäten bleiben erhalten.

Die in DICOM definierten Composite IODs findet man in Teil 3, Annex A des Standards.

6.1.2. Normalized IOD

Eine Information Object Definition wird als normalisiert bezeichnet, wenn diese eine singuläre Entität des DICOM Modells beschreibt, d.h. die Attribute innerhalb einer IOD sind spezifisch für das entsprechende Objekt der realen Welt. Man beachte, dass bei der Übermittlung einer normalisierten IOD – genauer einer Instanzierung der IOD – nicht das Objekt selbst, sondern nur eine Referenz übertragen wird. Die tatsächlichen Daten sind über den Verweis zugänglich. Das bedeutet aber auch, dass wenn über die Grenzen eines PACS hinaus kommuniziert werden soll (z.B. Teleradiologie), diese Referenzen durch die tatsächlichen Objekte ersetzt werden müssen.

Die normalisierten IODs sind in Teil 3, Annex B des DICOM Standards spezifiziert.

6.1.3. Attributes

Die Eigenschaften der DICOM Objekte werden durch die Attribute der IOD charakterisiert, wobei verwandte Attribute zu Gruppen, sogenannte Module zusammengefasst sind. Diese Attribute werden als Datenelemente gemäß den Regeln in Teil 5 des Standards kodiert. Schließlich sind die einzelnen Datenelemente in Teil 6 – Data Dictionary – spezifiziert.

6.2. Common Composite Image IOD

6.2.1. Patient Module

„Patient Module“ spezifiziert die zur Identifikation bzw. zur Beschreibung des Patienten erforderlichen Attribute, insbesondere jene, die in der täglichen Routine zur Befundung der medizinischen Bilddaten notwendig sind. Dementsprechend ist das „Patient Module“ teil aller Image Information Object Definitionen.

ATTRIBUT-NAME	TAG	ATTRIBUT-BESCHREIBUNG
Patient's Name	(0010,0010)	Patient's full legal name.
Patient ID	(0010,0020)	Primary hospital identification number or code for the patient.
Patient's Birth Date	(0010,0030)	Birth date of the patient.
Patient's Sex	(0010,0040)	Sex of the named patient.
Referenced Patient Sequence	(0008,1120)	A sequence which provides reference to a Patient SOP Class/Instance pair.
>Referenced SOP Class UID	(0008,1150)	Uniquely identifies the referenced SOP Class.
>Referenced SOP Instance UID	(0008,1155)	Uniquely identifies the referenced SOP Instance.
Patient's Birth Time	(0010,0032)	Birth time of the Patient.
Other Patient IDs	(0010,1000)	Other identification numbers or codes used to identify the patient.
Other Patient Names	(0010,1001)	Other names used to identify the patient.
Ethnic Group	(0010,2160)	Ethnic group or race of the patient.
Patient Comments	(0010,4000)	User-defined additional information about the patient.

Attribute basierend auf „Person Name“

```
PersonName ::= <family name> "^"
             <given name> "^"
             <middle name> "^"
             <name prefix> "^"
             <name suffix>
```

```
Patient's Name ::= [ <PersonName> ]
Other Patient Names ::= [ <PersonName> { "\" <PersonName> } * ]
```

Primäre Identifikationsdaten in strukturierter Form.

Attribute basierend auf „Patient ID“

```
Patient ID ::= [ <String64> ]
Other Patient ID ::= [ <String64> { "\" <String64> } * ]
```

„Patient ID“ und „Other Patient ID“ sind primäre Identifikationsdaten.

Reversible Anonymisierung

Im Falle einer Composite Image IOD wird ein Distinguished Name gemäß den Ausführungen in 4.1.1. im Tag (0010,1000) „Other Patient IDs“ des Patient Module gespeichert.

Geburtsdatum

```
TimeStamp ::= YYYY [ MM [ DD [ <Time> ] ] ]
Time ::= HH [ MM [ SS [ "." SSSS ] ] ] [ <Time Zone> ]
Timezone ::= "+" HHMM | "-" HHMM
```

```
Patient's Birth Date ::= [ <TimeStamp> ]
```

Das Geburtsdatum des Betroffenen in strukturierter Form; sekundäres Identifikationsdatum mit entsprechender Generalisierungsmöglichkeit.

Sekundäre Identifikationsdaten

Die folgenden Attribute sind sekundäre Identifikationsdaten:

```
Patient's Sex ::= [ <CodeString>
Ethnic Group ::= [ <String16>
```

Bemerkung

```
Patient Comments ::= [ <Text10k>
```

Das Kommentarfeld hat eine zulässige Textlänge von 10240 Zeichen. Hier ist darauf zu achten, dass die im Kontext enthaltene Information keine Identifikation des Betroffenen ermöglicht. Da eine maschinelle Auswertung von unstrukturiertem Text i. Allg. nur bedingt Erfolg verspricht, ist zu überlegen, ob dieses Attribut für die wissenschaftliche Forschung und Statistik benötigt wird.

6.2.2. Patient Study Module

Das Patient Study Module beinhaltet Informationen über den Patienten zum Untersuchungszeitpunkt.

ATTRIBUT-NAME	TAG	ATTRIBUT-BESCHREIBUNG
Admitting Diagnoses Description	(0008,1080)	Description of the admitting diagnosis (diagnoses).
Patient's Age	(0010,1010)	Age of the Patient.
Patient's Size	(0010,1020)	Length or size of the Patient, in meters.
Patient's Weight	(0010,1030)	Weight of the Patient, in kilograms.
Occupation	(0010,2180)	Occupation of the Patient.
Additional Patient's History	(0010,21B0)	Additional information about the Patient's medical history.

Sekundäre Identifikationsdaten

Die folgenden Attribute sind sekundäre Identifikationsdaten:

```
Patient's Age ::= [ <DecimalString>
Patient's Size ::= [ <DecimalString>
Patient's Weight ::= [ <DecimalString>
Occupation ::= [ <String16>
```

Bemerkung

```
Additional Patient History ::= [ <Text10k>
```

„Additional Patient History“ hat eine zulässige Textlänge von 10240 Zeichen. Hier ist darauf zu achten, dass die im Kontext enthaltene Information keine Identifikation des Betroffenen ermöglicht. Da eine maschinelle Auswertung von unstrukturiertem Text i. Allg. nur bedingt Erfolg verspricht, ist zu überlegen, ob dieses Attribut für die wissenschaftliche Forschung und Statistik benötigt wird.

6.3. Basic Study Descriptor IOD

Ein „Basic Study Descriptor IOD“ ist die Abstraktion eines Basisdatensatzes für den Austausch zwischen DICOM-konformen Geräten, und ist konzeptionell von einer Modalität unabhängig. Praktisch implementiert der Basic Study Descriptor eine einfache Verzeichnisstruktur und übermittelt auf diese Weise explizit den Kontext der Untersuchung.

MODULE	MODULE-BESCHREIBUNG
Patient Summary	Provides summary Information about the Patient.
Study Content	Study content information.
SOP Common	Contains SOP common information.

6.3.1. Patient Summary Module

Definiert die wichtigsten Attribute zur Patientenidentifikation.

ATTRIBUT-NAME	TAG	ATTRIBUT-BESCHREIBUNG
Patient's Name	(0010,0010)	Patient's full legal name.
Patient ID	(0010,0020)	Primary hospital identification number or code for the patient.

Primäre Identifikationsdaten

Die folgenden Attribute sind primäre Identifikationsdaten:

```

PersonName ::= <family name> "^"
              <given name>  "^"
              <middle name> "^"
              <name prefix>  "^"
              <name suffix>

Patient's Name ::= [<PersonName>]
Patient ID ::= [<String64>]

```

Reversible Anonymisierung

Bei Verwendung eines Basic Study Descriptors wird ein Distinguished Name gemäß den Ausführungen im 4.1.1. in Tag (0010,0020) „Patient ID“ des Patient Summary Module gespeichert.

6.4. Patient Information Object Definition

„Patient Information Object Definition“ ist die DICOM Abstraktion eines Patienten. Dazu wird die Patient IOD von einer Reihe von Service Class Definitions verwendet, mit deren Hilfe der Austausch von patientenbezogenen Informationen zwischen DICOM Application Entities realisiert wird. Eine Patient SOP Instance verwendet die Patient IOD zur Beschreibung des realen Patienten; darüberhinaus referenziert jede Patient SOP Instance die zugehörigen Visit SOP Instances und Study SOP Instances.

MODULE	MODULE-BESCHREIBUNG
SOP Common	Contains SOP common information.
Patient Relationship	References to related SOPs.
Patient Identification	Identifies the real world patient.
Patient Demographic	Describes the patient.
Patient Medical	Medical information about patient.

6.4.1. Patient Identification Module

Das Patient Identification Module beschreibt die zur Identifikation eines Patienten notwendigen Attribute.

ATTRIBUT-NAME	TAG	ATTRIBUT-BESCHREIBUNG
Patient's Name	(0010,0010)	Patient's full legal name.
Patient ID	(0010,0020)	Primary hospital identification number or code for the patient.
Issuer of Patient ID	(0010,0021)	Name of healthcare provider which issued the Patient ID.
Other Patient IDs	(0010,1000)	Other identification numbers or codes used to identify the patient.
Other Patient Names	(0010,1001)	Other names used to identify the patient.
Patient's Birth Name	(0010,1005)	Patient's birth name.
Patient's Mother's Birth Name	(0010,1060)	Birth name of patient's mother.
Medical Record Locator	(0010,1090)	An identifier used to find the patient's existing medical record.

Attribute basierend auf „Person Name“

```

PersonName ::= <family name> "^"
              <given name> "^"
              <middle name> "^"
              <name prefix> "^"
              <name suffix>

```

```

Patient's Name ::= [ <PersonName> ]
Other Patient Names ::= [ <PersonName> { "\" <PersonName> } * ]
Patient's Birth Name ::= [ <PersonName> ]
Patient's Mother's Birth Name ::= [ <PersonName> ]

```

„Patient's Name“, „Other Patient Name“, „Patient's Birth Name“ sind, falls vorhanden, primäre Identifikationsdaten. Falls vorhanden wird empfohlen „Patient's Mother's Birth Name“ zu löschen.

Attribute basierend auf „Patient ID“

```

Patient ID ::= [ <String64> ]
Other Patient IDs ::= [ <String64> { "\" <String64> } * ]

```

„Patient ID“ und „Other Patient IDs“ sind primäre Identifikationsdaten.

Reversible Anonymisierung

Bei DICOM Implementierungen mit Normalized IODs wird ein Distinguished Name gemäß den Ausführungen in 4.1.1. im Tag (0010,1000) „Other Patient IDs“ des Patient Identification Module gespeichert.

Medical Record Locator

```

Medical Record Locator ::= [ <String64> ]

```

„Medical Record Locator“ ist ein primäres Identifikationsdatum.

6.4.2. Patient Demographic Module

Das Patient Demographic Module enthält allgemeine Attribute zur Beschreibung eines Patienten.

ATTRIBUT-NAME	TAG	ATTRIBUT-BESCHREIBUNG
Patient's Address	(0010,1040)	Legal address of the named patient.
Region of Residence	(0010,2152)	Region within patient's country of residence.
Country of Residence	(0010,2150)	Country in which patient currently resides.
Patient's Telephone Numbers	(0010,2154)	Telephone numbers at which the patient can be reached.
Patient's Birth Date	(0010,0030)	Date of birth of the named patient.
Patient's Birth Time	(0010,0032)	Time of birth of the named patient.
Ethnic Group	(0010,2160)	Ethnic group or race of patient.

ATTRIBUT-NAME	TAG	ATTRIBUT-BESCHREIBUNG
Patient's Sex	(0010,0040)	Sex of the named patient.
Patient's Size	(0010,1020)	Patient's height or length in meters.
Patient's Weight	(0010,1030)	Weight of the patient in kilograms.
Military Rank	(0010,1080)	Military rank of patient.
Branch of Service	(0010,1081)	Branch of the military.
Patient's Insurance Plan Code Sequence	(0010,0050)	A sequence that conveys the patient's insurance plan.
>Code Value	(0008,0100)	The code value (defined by the coding scheme) that represents the patient's insurance plan name.
>Coding Scheme Designator	(0008,0102)	The code from designating the coding scheme which maps the Code Value (0008,0100) onto the Code Meaning (0008,0104).
>Code Meaning	(0008,0104)	The patient's insurance plan name that is represented by the Code Value (0008,0100).
Patient's Religious Preference	(0010,21F0)	The religious preference of the patient.
Patient Comments	(0010,4000)	User-defined comments about the patient.

Primäre Identifikationsdaten

```
Patient's Address ::= [ <String64>
Region of Residence ::= [ String64>
Country of Residence ::= [ <String64>
```

„Patient's Address“ ist eine unstrukturierte Adresse und daher ein primäres Identifikationsdatum. Die restlichen geographischen Attribute sind sekundäre Identifikationsdaten.

```
Patient's Telephone Numbers ::= [ <String16> { "\" <String16>}*
Patient's Insurance Plan Code Sequence ::= { <Item>>*
```

Geburtsdatum

```
TimeStamp ::= YYYY [ MM [ DD [ <Time>]]]
Time ::= HH [ MM [ SS [ "." SSSS]]] [ <Time Zone>
Timezone ::= "+" HHMM | "-" HHMM
```

```
Patient's Birth Date ::= [ <TimeStamp>
```

Das Geburtsdatum des Betroffenen in strukturierter Form; sekundäres Identifikationsdatum mit entsprechender Generalisierungsmöglichkeit.

Sekundäre Identifikationsdaten

Die folgenden Attribute sind sekundäre Identifikationsdaten:

```
Ethnic Group ::= [ <String16>
Patient's Sex ::= [ <CodeString>
Patient's Size ::= [ <DecimalString>
Patient's Weight ::= [ <DecimalString>
Military Rank ::= [ <String64>
Branch of Service ::= [ <String64>
Patient's Religious Preference ::= [ <String64>
```

Bemerkung

```
Patient Comments ::= [ <Text10k>
```

Das Kommentarfeld hat eine zulässige Textlänge von 10240 Zeichen. Hier ist darauf zu achten, dass die im Kontext enthaltene Information keine Identifikation des Betroffenen ermöglicht. Da eine maschinelle Auswertung von unstrukturiertem Text i. Allg. nur bedingt Erfolg verspricht, ist zu überlegen, ob dieses Attribut für die wissenschaftliche Forschung und Statistik benötigt wird.

6.4.3. Patient Medical Module

Das Patient Medical Module definiert die Attribute zum medizinischen Status des Patienten.

ATTRIBUT-NAME	TAG	ATTRIBUT-BESCHREIBUNG
Patient State	(0038,0500)	Description of patient state.
Pregnancy Status	(0010,21C0)	Describes pregnancy state of patient.
Medical Alerts	(0010,2000)	Conditions to which medical staff should be alerted.
Contrast Allergies	(0010,2110)	Description of prior reaction to contrast agents.
Special Needs	(0038,0050)	Medical and social needs.
Last Menstrual Date	(0010,21D0)	Date of onset of last menstrual period.
Smoking Status	(0010,21A0)	Indicates whether patient smokes.
Additional Patient History	(0010,21B0)	Additional information about the patient's medical history.

Sekundäre Identifikationsdaten

Die folgenden Attribute sind sekundäre Identifikationsdaten:

```
Medical Alerts ::= [ <String64> { "\" <String64> } * ]
Contrast Allergies ::= [ <String64> { "\" <String64> } * ]
Special Needs ::= [ <String64> ]
Smoking Status ::= [ <CodeString> ]
```

Bemerkung

```
Additional Patient History ::= [ <Text10k> ]
```

„Additional Patient History“ hat eine zulässige Textlänge von 10240 Zeichen. Hier ist darauf zu achten, dass die im Kontext enthaltene Information keine Identifikation des Betroffenen ermöglicht. Da eine maschinelle Auswertung von unstrukturiertem Text i. Allg. nur bedingt Erfolg verspricht, ist zu überlegen, ob dieses Attribut für die wissenschaftliche Forschung und Statistik benötigt wird.

6.5. Anmerkungen

Man beachte, dass bei medizinischen Bildern häufig die Identifikationsdaten des Patienten „einbelichtet“ werden. Dieses in der täglichen Routine vielfach bewährte Verfahren bedingt, aus der Sicht des Datenschutzes, ein „retouchieren“ der Bilddaten vor der Übermittlung. In der Regel sind dazu entsprechende Programme notwendig, die vom jeweiligen PACS-Hersteller zu beziehen sind. Sofern nicht bereits vorhanden wird empfohlen, bei zukünftigen Beschaffungen von PACS-Modalitäten, insbesondere bei Befundkonsolen, Software für die Anonymisierung von DICOM-Studies in die Anforderungsliste der Produkte aufzunehmen.

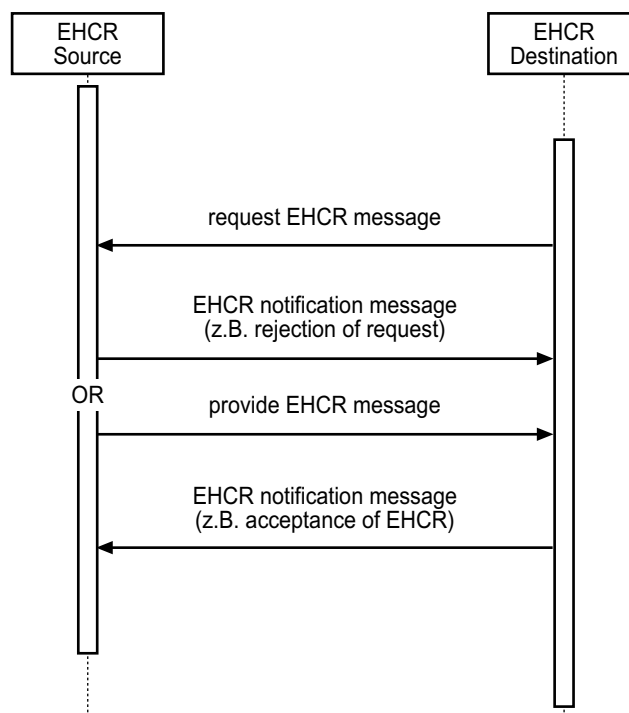
7. CEN/TC 251 Electronic Healthcare Communication

7.1. Informationsmodell

Die Electronic Healthcare Record Message, definiert in ENV 13606-1 und ENV 13606-4, ist ein abstraktes Modell (Domain Information Model) für den Austausch von elektronischen Krankengeschichten. Die Norm beinhaltet die General Message Descriptions – also die allgemeinen Teile (Komponenten) – von drei Nachrichten als da sind:

1. request EHCR message,
2. provide EHCR message und
3. EHCR notification message.

Dabei ist der allgemeine Kommunikationsablauf wie folgt skizzierbar:



Ohne Beschränkung der Allgemeinheit ist für die vorliegende Datenschutz-Policy eine Diskussion der „provide EHCR message“ hinreichend.

7.2. EHCR Nachrichten

Die in diesem Abschnitt gegebene Beschreibung von Komponenten einer EHCR Nachricht mit inhärenten Identifikationsdaten erfolgt in Form von XML Document Type Definitions (DTDs). Es ist anzumerken, dass die Definitionen nur soweit ausgeführt wurden, wie dies für ein Verständnis notwendig erscheint bzw. die Standardspezifikation vorgibt. Für detaillierte Informationen sei auf die entsprechende Norm verwiesen.

Den Aufbau einer provideEHCR Nachricht zeigt das folgende Codefragment:

```

<!ELEMENT provideEhcr (
  ..., <!-- Datum, Sender, Empfänger, ... -->
  PatientMatchingInfo,
  ..., <!-- Sprache, Distributionsregeln, ... -->
  EhcrExtract)>
<!ATTLIST ProvideEhcr RcptAckRequest (NEVER | ALWAYS | ON_ERROR) #REQUIRED
  Urgency (LOW | NORMAL | HIGH | IMMEDIATE) #REQUIRED>

```

7.2.1. Patient Matching Information

Die Klasse Patient Matching Information definiert einen „Filter“ zur eindeutigen Identifikation des Patienten und soll nicht mit demographischen Informationen verwechselt werden. Die eigentliche Beschreibung eines Patienten erfolgt in den entsprechenden Data Item (siehe 7.2.3.).

```

<!ELEMENT PatientMatchingInfo (
  ((PatientId, PersonName?, BirthDate?)|(PersonName, BirthDate?)|BirthDate),
  AlternativePersonName*,
  PersonAdministrativeSex?,
  Address*)>

```

Patienten ID

PatientId ist ein primäres Identifikationsmerkmal. Im Falle einer reversiblen Anonymisierung kann der Distinguished Name gemäß den Ausführungen in 4.1.1. als weitere Id zugegeben werden.

```

<!ELEMENT PatientId (Id+)>
<!ELEMENT Id (
  IdType?,
  IdScheme?,
  IdValue)>
<!ELEMENT IdType (#PCDATA)>
<!ATTLIST IdType ICSI CDATA #IMPLIED>
<!ELEMENT IdScheme (#PCDATA)>
<!ATTLIST IdScheme ICSI CDATA #IMPLIED>
<!ELEMENT IdValue (#PCDATA)>

```

Primäre Identifikationsdaten basierend auf Person Name

Der Name eines Betroffenen in strukturierter und unstrukturierter Form. Werden kryptographische Methoden zur Elimination des Personenbezugs angewendet, ist der Name als String zu übermitteln. Mögliche Namenstypen sind: „Alias“, „Maiden Name“, „Former Name“, „Mother’s Maiden Name“ sowie „Preferred Name“.

```

<!ELEMENT PersonName (
  PersonNameType?,
  Period?,
  (StructPersonName|String))>
<!ELEMENT PersonNameType (#PCDATA)>
<!ELEMENT StructPersonName (
  FamilyName,
  GivenName?,
  MiddleName?,
  Title?,
  GenerationQualifier?)>
<!ELEMENT AlternativePersonName (
  PersonNameType?,
  Period?,
  (StructPersonName|String))>

```

Sekundäre Identifikationsdaten

```

<!ELEMENT BirthDate (#PCDATA)>
<!ATTLIST BirthDate Cen251:Type CDATA #FIXED "TOCD">
<!ELEMENT PersonAdministrativeSex (#PCDATA)>

```

Adressen von Betroffenen

Wie bereits in den vorangegangenen Kapiteln mehrfach ausgeführt, stellt eine vollständige Adresse ein primäres Identifikationsdatum dar. Man beachte insbesondere, dass die Spezifikation Adressdaten sowohl strukturiert wie auch in unstrukturierter Form zulässt. Werden kryptographische Methoden zur Elimination des Personenbezugs angewendet, soll die vollständige

Adresse im Tag <UnstructAddress> übermittelt werden; Adressteile in <StructAddress> bieten die Möglichkeit einer Generalisierung.

```
<!ELEMENT Address (
    Period?,
    PostCode?,
    CountryOrCountyArea?,
    (StructAddress | UnstructAddress))>
<!ATTLIST Address AddrType (HOME|WORK|...|UNSPECIFIED) #REQUIRED>
<!ELEMENT PostCode (#PCDATA)>
<!ELEMENT CountryOrCountyArea (CodedElement|String)>
<!ELEMENT StructAddress (
    HouseNumOrName?,
    PoBox?,
    ApartmentNum?,
    StreetName?,
    District?,
    CityOrTown?,
    Country)>
<!ELEMENT HouseNumOrName (#PCDATA)>
<!ELEMENT PoBox (#PCDATA)>
<!ELEMENT ApartmentNum (#PCDATA)>
<!ELEMENT StreetName (#PCDATA)>
<!ELEMENT District (#PCDATA)>
<!ELEMENT CityOrTown (#PCDATA)>
<!ATTLIST CityOrTown CE ICSI CDATA #IMPLIED>
<!ELEMENT Country (CodedElement|String)>
<!ELEMENT UnstructAddress (UnstructAddressLine+)>
<!ELEMENT UnstructAddressLine (#PCDATA)>
```

7.2.2. EHCR Extract

Jede EHCR Nachricht enthält genau einen EHCRExtract Component Complex, der sowohl eine gesamte elektronische Krankengeschichte wie auch Teile dieser umfassen kann; RcStatus= SUPERSEDED spezifiziert einen Update. Die einfachste Form einer Übermittlung besteht aus einem simplen „Text Data Item“, mit der Krankengeschichte in textueller Form. Alternative Recordkomponenten sind Folder, Composition, Selected Component Complex, Link Set Item und eine Empty Record Component zum Löschen eines Datensatzes.

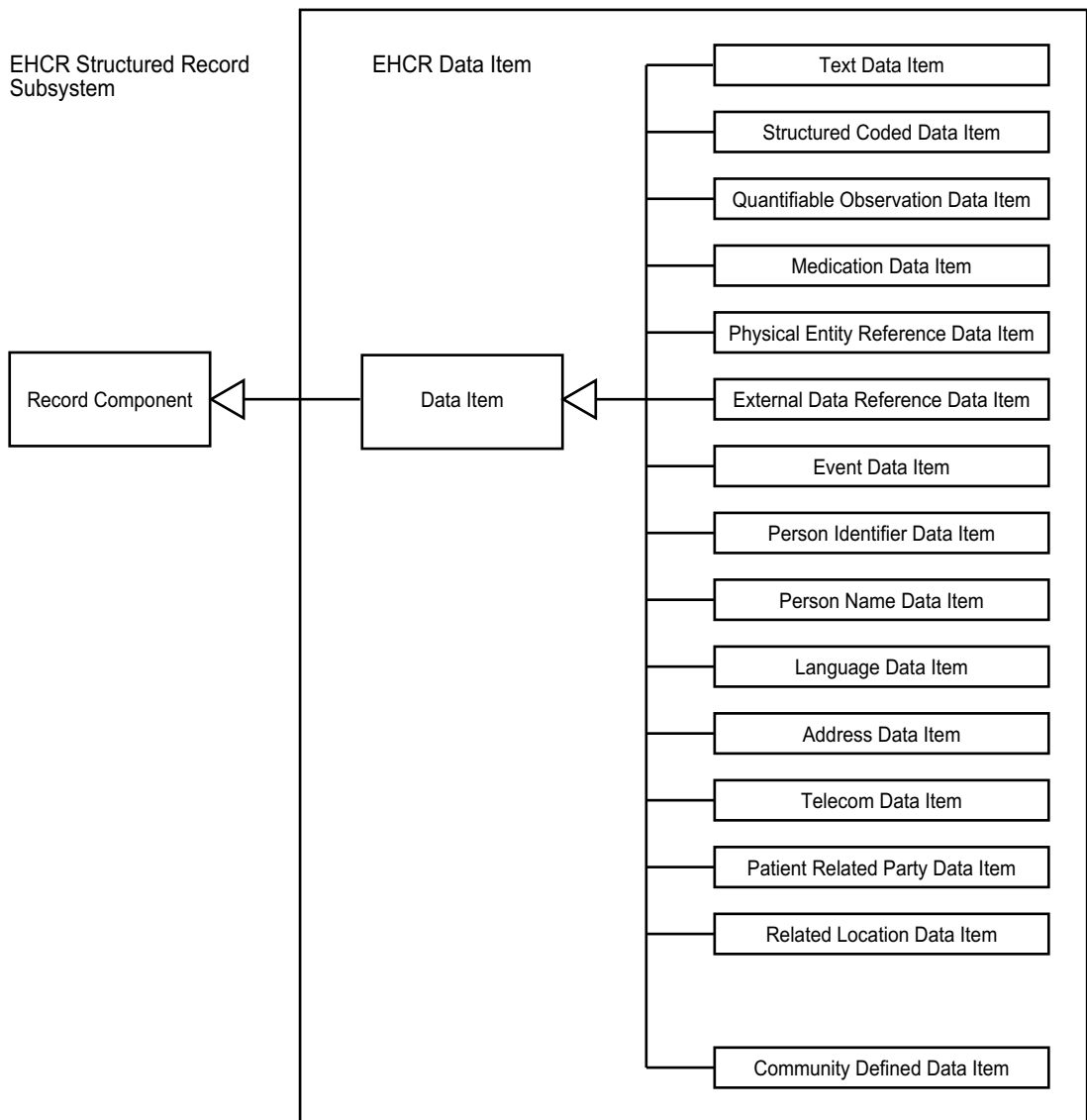
```
<!ELEMENT EhcrExtract (
    ...,
    (Folder|Composition|SelectedRcComplex|LinkSetItem|EmptyRecordRc)+)>
<!ATTLIST EhcrExtract xml:lang CDATA #IMPLIED
    RcStatus (CURRENT | SUPERSEDED) #REQUIRED
    DateValidity (CONFIRMED|PROBABLE|...|COMPILED) #IMPLIED>
```

Die einzelnen Recordkomponenten sind Abstraktionen spezifischer Sichtweisen auf Patientendaten, welche auch für einen Datentransfer zu wissenschaftlichen Zwecken Anwendung finden:

1. Composition: Daten eines Patientenkontakts.
2. Folder: Sequenz mehrerer Patientenkontakte (Messwiederholungen, Zeitreihen etc.).
3. Cluster: Gruppierung von Daten aus logischer oder organisatorischer Sicht, beispielsweise Phasen einer klinischen Studie.
4. Selected Component Complex: Auswahl von Teilen des EHCR, etwa zur Übermittlung an einen sekundären Datennutzer.

Durch rekursive Definition der Komponenten sind entsprechend dem aktuellen Kontext beliebig komplexe Strukturen erzeugbar.

Die grundlegenden Bausteine des EHCR Subsystems sind Data Items, die allgemein zu Recordkomponenten aggregiert werden. Die folgende Abbildung zeigt eine Übersicht der im Standard spezifizierten Data Items.



7.2.3. EHCR Data Items

Text Data Item

Man beachte, dass die im Kontext enthaltene Information eine Identifikation des Betroffenen ermöglichen kann. Da eine maschinelle Auswertung von unstrukturiertem Text i. Allg. nur bedingt Erfolg verspricht, ist zu überlegen, ob dieses Komponente für die wissenschaftliche Forschung und Statistik benötigt wird.

```

<!ELEMENT TextItem (
  .../
  TextBlock)>
<!ATTLIST TextItem NarrativeAccount (TRUE|FALSE) #IMPLIED
  ...>
<!ELEMENT TextBlock (#PCDATA)>
  
```

Person Identifier Data Item

```

<!ELEMENT PersonIdItem (
  .../
  Id)>
<!ATTLIST PersonIdItem ... >
  
```

Person Name Data Item

```
<!ELEMENT PersonNameItem (
    ...,
    PersonName)>
<!ATTLIST PersonNameItem ... >
```

Language Data Item

```
<!ELEMENT LanguageItem (
    ...,
    Language)>
<!ATTLIST LanguageItem ...>
<!ELEMENT Language (#PCDATA)>
<!ATTLIST Language LangAbility (FIRST|PREFERRED|...|NONE) #IMPLIED>
```

Address Data Item

```
<!ELEMENT AddressItem (
    ...,
    Address)>
<!ATTLIST AddressItem ... >
```

Telecom Data Item

```
<!ELEMENT TelecomItem (
    ...,
    Telecom)>
<!ATTLIST TelecomItem ... >
<!ELEMENT Telecom (
    Period?,
    (StructTelecomNum|UnstructTelecomNum))>
<!ATTLIST Telecom AddrType (HOME|WORK|...|UNSPECIFIED) #IMPLIED
    TelecomType (VOICE|MOBILE|...|OTHER) #REQUIRED>
<!ELEMENT StructTelecomNum (
    TelecomCountryCode?,
    TelecomAreaCode?,
    TelecomNum,
    TelecomExtNum?)>
<!ELEMENT TelecomCountryCode (#PCDATA)>
<!ELEMENT TelecomAreaCode (#PCDATA)>
<!ELEMENT TelecomNum (#PCDATA)>
<!ELEMENT TelecomExtNum (#PCDATA)>
<!ELEMENT UnstructTelecomNum (#PCDATA)>
```

7.3. Anmerkungen

Die Spezifikation des CEN/TC 251 definiert den elektronischen Austausch von elektronischen Krankenakten in abstrakter Form, was dazu führt, dass bei der Implementierung eine Fülle von Detailproblemen, insbesondere die rekursive Struktur der Recordkomponenten bzw. deren Zusammensetzung aus Data Items zu lösen sind. Das mag auch einer der Gründe sein, warum die Spezifikation bisher ohne praktische Umsetzung blieb.

8. Referenzen

- [1] 165. Bundesgesetz: Datenschutzgesetz 2000 – DSG 2000. Bundesgesetzblatt für die Republik Österreich. Teil I. 1999, S. 1277–1303.
- [2] 190. Bundesgesetz: Signaturgesetz – SigG. Bundesgesetzblatt für die Republik Österreich. Teil I. 1999, S. 1451–1462.
- [3] 201. Verordnung: Standard- und Muster-Verordnung 2000 – StMV. Bundesgesetzblatt für die Republik Österreich. Teil II. 2000, S. 1637–1691.
- [4] 520. Verordnung: Datenverarbeitungsregister-Verordnung 2000 – DVRV. Bundesgesetzblatt für die Republik Österreich. Teil II. 2000, S. 3493–3501.
- [5] Digital Imaging and Communications in Medicine (DICOM). Part 3: Information Object Definition. NEMA Standards Publication PS3.3, 1998.
- [6] Digital Imaging and Communications in Medicine (DICOM). Part 5: Data Structures and Encoding. NEMA Standards Publication PS3.5, 1998.
- [7] Digital Imaging and Communications in Medicine (DICOM). Part 6: Data Dictionary. NEMA Standards Publication PS3.6, 1998.
- [8] Digital Imaging and Communications in Medicine (DICOM). Security Enhancements One. NEMA Standards Publication PS3, Supplement 31, 2000.
- [9] Digital Imaging and Communications in Medicine (DICOM). Security Enhancements Two – Digital Signatures. NEMA Standards Publication PS3, Supplement 41, 2000.
- [10] ENV 12251/1999. Health Informatics – Secure User Identification for Healthcare – Identification and Authentication by Passwords – Management and Security. Comité Européen de Normalisation: 1999.
- [11] ENV 12388/1996. Medical Informatics – Algorithm for Digital Signature Services in Health Care. Comité Européen de Normalisation: 1996.
- [12] ENV 12924/1997. Medical Informatics – Security Categorisation and Protection for Healthcare Information Systems. Comité Européen de Normalisation: 1997.
- [13] ENV 13606-1/1999: Health informatics – Electronic healthcare record communication – Part 1: Extended architecture. Comité Européen de Normalisation: 1999.
- [14] ENV 13606-4/1999: Health informatics - Electronic healthcare record communication - Part 4: Messages for the exchange of information. Comité Européen de Normalisation: 1999.
- [15] ENV 13608-1/1999. Health Informatics – Security for Healthcare Communication Part 1: Concepts and Terminology. Comité Européen de Normalisation: 1999.

- [16] ENV 13608-2/1999. Health Informatics – Security for Healthcare Communication Part 2: Secure data objects. Comité Européen de Normalisation: 1999.
- [17] ENV 13608-3/1999. Health Informatics – Security for Healthcare Communication Part 3: Secure data channels. Comité Européen de Normalisation: 1999.
- [18] Health Level Seven: Application Protocol for Electronic Data Exchange in Healthcare Environments. Version 2.3.1. Health Level Seven, 1999.
- [19] ISO/IEC 8824-1/1998. Information technology – Abstract Syntax Notation One (ASN.1): Specification of basic notation. International Standards Organization: 1998.
- [20] ISO/IEC 9594-1/1998. Information technology – Open Systems Interconnection – The Directory: Overview of concepts, models and services. International Standards Organization: 1998.
- [21] OENORM A 2642: Informationstechnik – Kommunikation Offener Systeme – Verfahren zur Registrierung von Informationsobjekten in Österreich. Österreichisches Normungsinstitut: 1997.
- [22] P. Mockapetris: Domain Names – Concepts and Facilities. RFC 1034. Information Sciences Institute: 1987.
- [23] Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr. Amtsblatt NR. L 281 vom 23. November 1995, S. 0031–0050.
- [24] String-Kommission beim Bundesministerium für soziale Sicherheit und Generationen: Rahmenbedingungen für ein logisches österreichisches Gesundheitsnetzwerk („MAGDALENA“). Version 2.0 v. 21.6.2000.

9. Glossar

Auftraggeber: Natürliche oder juristische Personen, Personengemeinschaften oder Organe einer Gebietskörperschaft beziehungsweise die Geschäftsapparate solcher Organe, wenn sie allein oder gemeinsam mit anderen die Entscheidung getroffen haben, Daten für einen bestimmten Zweck zu verarbeiten, und zwar unabhängig davon, ob sie die Verarbeitung selbst durchführen oder hierzu einen anderen heranziehen. Als Auftraggeber gelten die genannten Personen, Personengemeinschaften und Einrichtungen auch dann, wenn sie einem anderen Daten zur Herstellung eines von ihnen aufgetragenen Werkes überlassen und der Auftragnehmer die Entscheidung trifft, diese Daten zu verarbeiten.

Betroffener: Jede vom Auftraggeber verschiedene natürliche oder juristische Person oder Personengemeinschaft, deren Daten verwendet werden.

CEN/TC 251: Comité Européen de Normalisation – Technical Committee 251. Europäische Normungsbehörde – Ausschuss zuständig für den Bereich medizinische Informatik.

Datei: Strukturierte Sammlung von Daten, die nach mindestens einem Suchkriterium zugänglich ist.

Datenanwendung: Die Summe der in ihrem Ablauf logisch verbundenen Verwendungsschritte, die zur Erreichung eines inhaltlich bestimmten Ergebnisses (des Zwecks der Datenanwendung) geordnet sind und zur Gänze oder auch nur teilweise automationsunterstützt, also maschinell und programmgesteuert, erfolgen (automationsunterstützte Datenanwendung).

Datenschutz-Policy: Rahmenwerk zur Sicherstellung des Datenschutzes bei der Verwendung personenbezogener Daten.

DICOM: „Digital Imaging and Communications in Medicine“. ISO-Standard für den elektronischen Austausch medizinischer Bilddaten.

Dienstleister: Natürliche oder juristische Personen, Personengemeinschaften oder Organe einer Gebietskörperschaft beziehungsweise die Geschäftsapparate solcher Organe, wenn sie Daten, die ihnen zur Herstellung eines aufgetragenen Werkes überlassen wurden, verwenden.

Distinguished Name: Eine Folge von Relative Distinguished Names (RDNs) zur Identifikation von Informationsobjekten innerhalb einer Verzeichnisstruktur.

Elektronische Signatur: Elektronische Daten, die anderen elektronischen Daten beigefügt oder mit diesen logisch verknüpft werden und die der Authentifizierung, also der Feststellung der Identität des Signators, dienen.

Ermitteln von Daten: Das Erheben von Daten in der Absicht, sie in einer Datenanwendung zu verwenden.

HL7 (Health Level Seven): ANSI-Standard für den elektronischen Austausch von textbasierten medizinischen Daten.

Indirekt personenbezogene Daten: Daten für einen Auftraggeber, Dienstleister oder Empfänger einer Übermittlung, wenn der Personenbezug der Daten derart ist, dass dieser Auftraggeber, Dienstleister oder Übermittlungsempfänger die Identität des Betroffenen mit rechtlich zulässigen Mitteln nicht bestimmen kann.

k-Anonymität: Die Eigenschaft eines Datensatzes, bezüglich der sekundären Identifikationsdaten von mindestens k anderen Datensätzen nicht unterscheidbar zu sein.

Personenbezogene Daten: Daten mit Angaben über Betroffene, deren Identität bestimmt oder bestimmbar ist.

Primäre Identifikationsdaten: Attribute oder Attributkombinationen, die von Natur her oder aufgrund ihrer Definition oder Verwendung dazu dienen, einen Betroffenen eindeutig zu identifizieren, auch wenn dazu eine Verknüpfung mit anderen Daten notwendig ist.

Primärer Datennutzer: Der für das Erhebungskonzept und die Erhebungsmethodik verantwortliche Datennutzer (Auftraggeber).

Reversible Anonymisierung: Die Methode der Rückführung von k -anonymen Daten auf den Betroffenen durch und nur durch den Auftraggeber.

Sekundäre Identifikationsdaten: Attribute oder Attributkombinationen einer Person, die aufgrund der möglichen Werte dieser Attribute ein eindeutiges Muster ausprägen können, welches eine Identifikation des Betroffenen durch Verknüpfung mit anderen Daten ermöglicht.

Sekundärer Datennutzer: Datennutzer, wenn dieser Daten durch Übermittlung erhält.

Sensible Daten: („besonders schutzwürdige Daten“) Daten natürlicher Personen über ihre rassische und ethnische Herkunft, politische Meinung, Gewerkschaftszugehörigkeit, religiöse oder philosophische Überzeugung, Gesundheit oder ihr Sexualeben.

Sicherheits-Policy: Die Gesamtheit der organisatorischen und technischen Datensicherheitsmaßnahmen eines Auftraggebers oder Dienstleiters.

Überlassen von Daten: Die Weitergabe von Daten vom Auftraggeber an einen Dienstleister.

Übermitteln von Daten: Die Weitergabe von Daten einer Datenanwendung an andere Empfänger als den Betroffenen, den Auftraggeber oder einen Dienstleister, insbesondere auch das Veröffentlichen solcher Daten; darüber hinaus auch die Verwendung von Daten für ein anderes Aufgabengebiet des Auftraggebers.

Untersuchung: Die Summe der, zur Beantwortung einer wissenschaftlichen Fragestellung, durchzuführenden organisatorischen, technischen und methodischen Handlungen.

Verarbeiten von Daten: Das Ermitteln, Erfassen, Speichern, Aufbewahren, Ordnen, Vergleichen, Verändern, Verknüpfen, Vervielfältigen, Abfragen, Ausgeben, Benützen, Überlassen, Sperren, Löschen, Vernichten oder jede andere Art der Handhabung von Daten einer Datenanwendung durch den Auftraggeber oder Dienstleister mit Ausnahme des Übermittels von Daten.

Verschlüsseln von Daten: Die Kodierung von Daten mittels kryptographischer Methoden.

Verwenden von Daten: Jede Art der Handhabung von Daten einer Datenanwendung, also sowohl das Verarbeiten als auch das Übermitteln von Daten.

Zustimmung: Die gültige, insbesondere ohne Zwang abgegebene Willenserklärung des Betroffenen, dass er in Kenntnis der Sachlage für den konkreten Fall in die Verwendung seiner Daten einwilligt.