

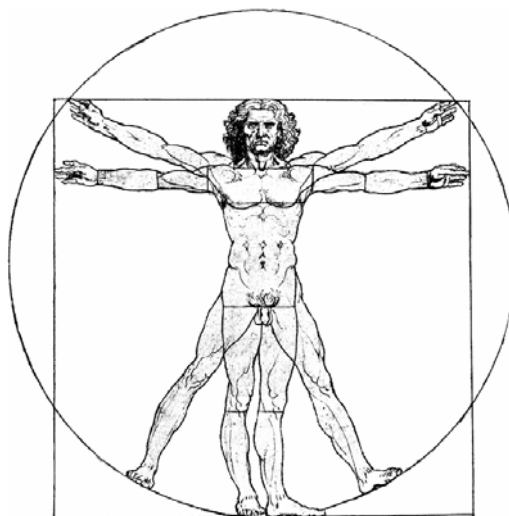
Datensicherheit und Datenschutz im Nationalen Register und Kompetenznetz Angeborene Herzfehler

Version 1.24
06. März 2006

Dr. Peter Debold

Debold & Lux
Beratungsgesellschaft für Informationssysteme
und Organisation im Gesundheitswesen mbH
Hamburg

In Kooperation mit
CIOOffice, Universität Göttingen



Inhalt:

1	Einführung	4
1.1	Vernetzte Forschung braucht eine neue Qualität des Persönlichkeitsschutzes	4
1.2	Datenorganisation im Nationalen Register (NR) und im Kompetenznetz Angeborene Herzfehler - Überblick.....	6
2	Aufgabenstellung	8
2.1	Sammlung von patientenbezogenen Daten	8
2.2	Rechtssichere Einbindung von Maßnahmen für den Datenschutz.....	9
3	Leistungsmodule des Nationalen Registers und des Kompetenznetzes zur Datenbereitstellung	11
3.1	Organisationsmodul (NR)	11
3.1.1	Status quo der Verfahren zur Datenerhebung	12
3.1.2	Weiterentwicklung der Aufgaben des Organisationsmoduls	12
3.1.3	Weiterentwicklung der instrumentell und datenschutzrechtlich relevanten Maßnahmen	13
3.2	Modul zur Prävalenzerhebung	14
3.2.1	Aufgaben	15
3.2.2	Datenschutzrechtlich relevante Maßnahmen.....	15
3.3	Versorgungsmodul	15
3.3.1	Aufgaben	16
3.3.2	Datenschutzrechtlich relevante Maßnahmen.....	16
3.4	Studienmodul - Datenbereitstellung für Forschungsprojekte (KN)	17
3.4.1	Aufgaben	18
4	Prozesse der Datenerhebung und -bereitstellung	18
4.1	Allgemeines Ablaufmodell	19
4.1.1	Aufnahme von Patienten – Rechte des Patienten	19
4.1.2	Identifikation des Patienten, Generierung des PID	21
4.1.2.1	Patientenliste und PID-Generator.....	21
4.1.2.2	Identifikationsdaten (IDAT).....	22
4.1.2.3	Weitere Prozessdaten.....	23
4.1.2.4	Notwendigkeit einer zentralen Patientenliste für die Leistungsmodule.....	23
4.1.2.5	Arztliste	23
4.1.2.6	Prozessablauf.....	24
4.1.3	Erfassung der medizinischen Daten	26

4.1.4	Qualitätssicherung	27
4.1.5	Freigabe der Daten für die Forschungsdatenbank.....	28
4.1.6	Korrektur von Daten in der Forschungsdatenbank.....	30
4.1.7	Zugriff der Forschung auf die Forschungsdatenbank.....	30
4.1.8	Depseudonymisierung von Patientendaten.....	31
4.2	Daten im Organisationsmodul.....	33
4.2.1	Aufbereitung der Altdaten.....	33
4.2.2	Aufnahme eines neuen Patienten in das System	34
4.2.3	Liste der Identifikationsdaten	34
4.2.4	Minimal Data Set.....	41
4.2.5	Meldung der Studienteilnehmer an das Organisationsmodul.....	44
4.2.5.1	Vorgehen beim Update der Registerdatenbank.....	45
4.2.5.2	Rekrutierung von Patienten für neue Studien.....	46
4.2.5.3	Datenpflege im Organisationsmodul	46
4.2.5.4	Pflege der Daten der Patientenliste.....	46
4.2.5.5	Pflege der Registerdatenbank	46
4.3	Text- und Messdaten für die Forschungsdatenbank – Zusammenfassung.....	47
4.4	Bilddaten für die Forschungsdatenbank.....	48
4.4.1	Erfassung und Auswertung der Bilddaten.....	49
4.4.1.1	MRT-Projekt	49
4.4.1.2	Tissue-Doppler-Projekt	49
4.4.2	Qualitätssicherung und Datenfreigabe	49
4.5	Daten im Modul zur Prävalenzerhebung.....	50
4.6	Daten im Versorgungsmodul	50
5	Zentrale Dienste.....	50
5.1	Patientenliste und PID-Generator.....	51
5.2	Qualitätssicherung	51
5.3	Pseudonymisierungsdienst	51
5.4	Führung der Forschungsdatenbank	51
5.5	Teilnehmerservice für die Verwaltung von Zugriffsrechten.....	51
6	Datenschutzrechtlich relevante Regel- und Vertragswerke.....	52
	Abkürzungsverzeichnis	54
	Hinweise zur Version	55

1 Einführung

1.1 Vernetzte Forschung braucht eine neue Qualität des Persönlichkeitsschutzes

Mit der Vernetzung der Forschung werden neue Anforderungen an den Schutz der Persönlichkeit vor Verletzungen des Selbstbestimmungsrechts gestellt. „Die Selbstbestimmung beinhaltet das Recht, über die Verwendung der eigenen persönlichen Daten zu entscheiden (informationelle Selbstbestimmung).¹“ Einschränkungen des Selbstbestimmungsrechts bedürfen stets einer gesetzlichen Begründung, die aber für die Forschung grundsätzlich nicht gegeben ist: Jede Verwendung von personenbeziehbaren Daten für die Forschung setzt die freiwillige und informierte Einwilligung des Patienten voraus.

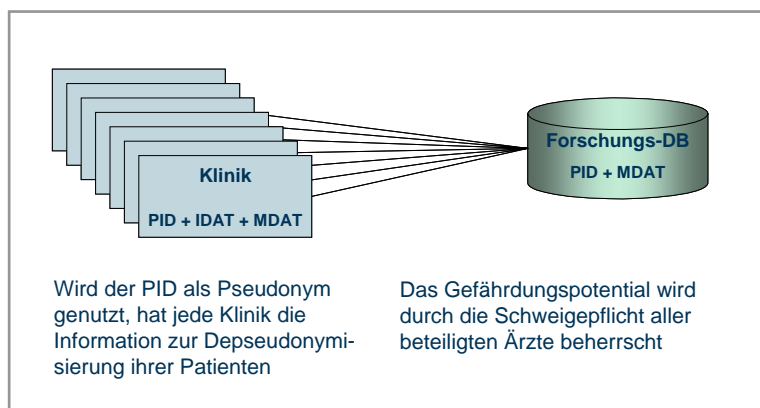


Abb. 1: Pseudonymisierung in traditionellen klinischen Studien

Patienten identifizieren (IDAT), verbleiben bei den Kliniken; die Verknüpfung erfolgt über einen Patientenidentifikator (PID), der sowohl in den Kliniken als auch in der Studiendatenbank gespeichert ist. In der Regel werden in den Kliniken die IDAT getrennt von den MDAT gespeichert. Das Verfahren gilt als Pseudonymisierung der medizinischen Daten, wobei der PID als Pseudonym bezeichnet wird.

Aus der Sicht der Studiendatenbank ist es korrekt, von Pseudonymisierung zu sprechen: Nur mit Hilfe eines Dritten, hier der Klinik, ist es möglich, Patienten zu depseudonymisieren, was die Schweigepflicht der Ärzte verbietet, sofern nicht wichtige und zulässige Gründe für eine Depseudonymisierung vorliegen. Aus der Sicht der Klinik ist es dagegen nicht korrekt, von Pseudonymisierung zu sprechen, da dort der Personenbezug jederzeit hergestellt werden kann: Aus der Sicht der Klinik handelt es sich deshalb um *personenbezogene* Daten, auch dann, wenn IDAT und MDAT technisch getrennt sind.

Die Daten traditioneller klinischer Forschung werden für definierte Studien gesammelt und haben daher sowohl von der Zweckbestimmung wie zeitlich einen klar begrenzten

Bei den traditionellen klinischen Forschungsprojekten beruht der Persönlichkeitsschutz letztendlich auf der Schweigepflicht der Ärzte: Die medizinischen Daten (MDAT) für eine Studie werden in der Regel aus mehreren Kliniken gesammelt und in einer Studiendatenbank gespeichert; die Daten, welche den

¹ Nationaler Ethikrat, Stellungnahme zu Biobanken für die Forschung, S. 29
knahf_datenschutzkonzept_ver_1_24.doc Debold & Lux / CIOffice

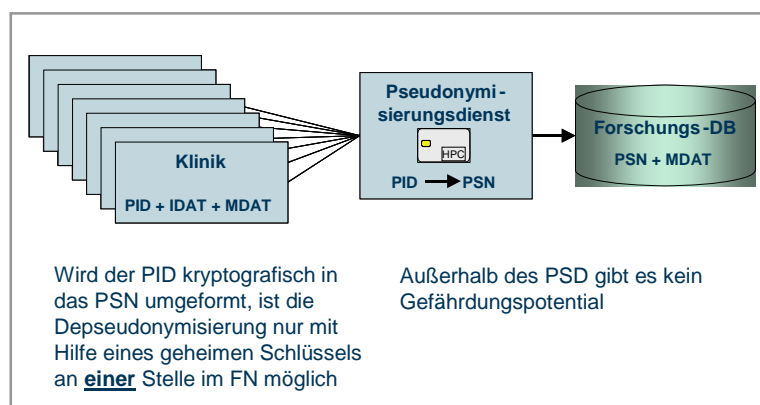
Horizont der Nutzung, der durch die informierte Einwilligung des Patienten legitimiert ist. In diesem Zusammenhang ist die beschriebene Form der Pseudonymisierung in der Studiendatenbank in Verbindung mit der Schweigepflicht des Klinikarztes ein ausreichendes Instrument zur Sicherung der Patientenrechte.

Anders verhält es sich damit im Rahmen der vernetzten Forschung; die Sammlung von Daten folgt einer deutlich weiter gespannten Zielsetzung:

- Um auch seltene Krankheiten und Therapieformen beforschen zu können, sollen medizinische Daten deutschlandweit gesammelt werden; entsprechend ist die Organisation der Forschungsnetze ausgebildet.
- Die Zweckbestimmung der Datenerhebung ist weiter gefasst, zum einen dadurch, dass die Daten für mehrere aktuelle Studien in *einer* Forschungsdatenbank vereint gespeichert werden, zum anderen dadurch, dass die Daten auch für künftige, heute noch nicht definierte Forschungsaufgaben zur Verfügung stehen sollen. Neben einem nationalen Datenaustausch zwischen Forschungsinstitutionen wird auch ein internationaler Austausch von Daten angestrebt, wodurch die Zwecksetzung noch mehr erweitert wird.
- Auch die zeitliche Perspektive für die Nutzung der Daten ist sehr viel weiter gespannt und zielt letztlich darauf, dass die Daten zeitlich unbegrenzt für die Forschung verfügbar sind.

Die vernetzte Forschung erweitert damit die Nutzung medizinischer Daten gegenüber der traditionellen klinischen in drei Dimensionen in ganz erheblichem Maße: den Dimensionen der Menge, der Zeit und der Zweckbestimmung. Derzeit sind es über 40 medizinische Forschungsnetze, die, vom BMBF gefördert, ihren Informationsbedarf in der beschriebenen Weise organisieren; jedes der Netze speichert pro Jahr eine Menge von Datensätzen, die im 5-stelligen Bereich liegt.

Aus der ethischen Bewertung der Sensitivität der medizinischen Daten und der Notwendigkeit, dass sich Patienten auch unter den künftigen Bedingungen bereit finden, ihre Daten für die Forschung zur Verfügung zu stellen, ist die Forderung abgeleitet, den Schutz des Patienten vor einer nicht legitimierten Re-Identifikation auf eine neue Qualitäts- und Sicherheitsstufe zu heben.



Dazu hat die TMF bereits zu Beginn des Jahres 2003 ein Verfahren entwickelt, das mit dem Arbeitskreis Wissenschaft der Konferenz der Bundes- und Landesbeauftragten für den Datenschutz konsentiert werden konnte und seither als verbindlich für die ver-

Abb. 2: Pseudonymisierung für die vernetzte Forschung

06. März 2006

netzte Forschung gilt². Das zentrale Instrument zur Verbesserung des Persönlichkeitsschutzes ist eine mehrstufige Pseudonymisierung, wobei die erste Stufe diejenige darstellt, die auch traditionell verwendet wird. In der zweiten Stufe wird der PID mithilfe eines zentralen Pseudonymisierungsdienstes durch ein Pseudonym (PSN) ersetzt, das nur innerhalb der Forschungsdatenbank verwendet wird und für die Außenwelt ein Geheimnis darstellt. Bei der Weitergabe von Forschungsdaten an Forschungsinstitutionen wird eine dritte Stufe der Pseudonymisierung wirksam, bei der das Pseudonym der Forschungsdatenbank erneut kryptografisch transformiert wird. Durch die Summe dieser Maßnahmen wird das Potential zur Re-Identifikation, das in Form der IDAT in den Kliniken und in der zentralen Patientenliste verfügbar ist, sozusagen neutralisiert, da keine Verknüpfung zur Forschungsdatenbank hergestellt werden kann. Während im traditionellen Verfahren der Persönlichkeitsschutz auf der Schweigepflicht der Ärzte beruht, verwaltet im modernisierten Verfahren eine zentrale Stelle den Schlüssel zu Re-Identifikation, dessen Nutzung exakten und überprüfbaren Regeln unterworfen ist.

Es ist nicht zu vermeiden, dass die mehrstufige Pseudonymisierung Anforderungen an die Geschäftsprozesse stellt, die dadurch komplexer zu gestalten sind, als dies unter traditionellen Bedingungen der Fall ist. Dies hat teilweise zu einer Kritik der auf dem Papier entworfenen Lösungen geführt. Der Hinweis auf „zu komplizierte Prozesse, welche die Arbeit des Forschers behindern“ war in Einzelfällen zum Anlass genommen worden, die Sinnhaftigkeit eines verbesserten Persönlichkeitsschutzes überhaupt in Frage zu stellen.

Diese Kritik wählt ein falsches Objekt. Es war immer das Bemühen der konzeptionellen Entwicklung, einerseits ein möglichst hohes Maß an Persönlichkeitsschutz zu gewährleisten, andererseits die Forschung in keiner Weise zu behindern. Es wurde angestrebt, in der Entwicklungsarbeit den gleichen Prinzipien zu folgen, an denen die Datenschutzbeauftragten ihre Beratungstätigkeit ausrichten. Das falsche Objekt wählt die Kritik, weil sie die Beschreibung der Geschäftsprozesse zum Ziel nimmt, nicht ihre Realisierung. Die Beschreibungen sind notwendig detailreich und manchmal auch komplex, weil sie darstellen, was durch die Programmierung umgesetzt werden soll. Aber es ist grundsätzlich die Aufgabe einer intelligenten Software, die Komplexität zu beherrschen und sie für die Forscher transparent zu halten. Insofern sollte sich das System erst dann der Kritik stellen, wenn die Umsetzung bewertet werden kann.

1.2 Datenorganisation im Nationalen Register (NR) und im Kompetenznetz Angeborene Herzfehler - Überblick

Forschungsnetze sind komplexe Gebilde mit verschiedenen Studienzentren und Diensten und einer Vielzahl von Mitarbeitern. Deshalb ist die Organisation des Workflows, der IT-Dienste und der Datenverwaltung so zu gestalten, dass auch innerhalb des Netzes der Persönlichkeitsschutz auf hohem Niveau gesichert ist. Zu den Sicherheitsmaßnahmen gehört, dass die den Patienten identifizierenden Daten (IDAT) grundsätzlich getrennt von den medizinischen Daten (MDAT) gespeichert und unter getrennter Verant-

² Generische Lösungen der TMF zum Datenschutz für die Forschungsnetze der Medizin, Version 1.10 vom Juli 2003

wortung verwaltet werden. Im Folgenden werden die Grundzüge dieser Datenorganisation dargestellt, aus der hervorgeht, wie innerhalb des Netzes die Bedingungen für den Zugriff auf die verschiedenen Datenkomplexe gestaltet sind.

1. Studien- bzw. Forschungsdaten

- a) Die für Studien erhobenen MDAT werden beim *CIOffice der Universität Göttingen* in der sogenannten Studiendatenbank gespeichert. Diese Daten enthalten den PID, der einen Bezug zu den IDAT ermöglicht. Zugriff zu diesen Daten haben neben der Administration ausschließlich die Personen, die mit der Qualitätssicherung dieser Daten beschäftigt sind und dabei auch die Verbindung mit den Daten-erhebenden Stellen benötigen.
- b) Nach Abschluss der Qualitätssicherung werden diese Daten in der oben beschriebenen Weise pseudonymisiert und in die Forschungsdatenbank übertragen, die ebenfalls vom *CIOffice der Universität Göttingen* verwaltet wird. Die übertragenen Daten werden in der Studiendatenbank gelöscht. Damit kann ein Bezug zum Patienten nur durch eine Depseudonymisierung hergestellt werden, wofür ein spezifisches Regelwerk gilt.
- c) Zugang zu den Forschungsdaten haben die Forscher der jeweiligen Studien und Forscher, die einen Antrag beim Ausschuss Datenschutz stellen und bewilligt erhalten. Für den technischen Zugriff bestehen zwei Optionen: Entweder erhält der Forscher Zugriff auf die Forschungsdatenbank, und zwar indem seine Studie betreffenden Ausschnitt, oder die Daten werden exportiert und dem Forscher zur eigenen Verfügung und sicheren Verwahrung überstellt.

2. Registerdaten, minimal data set

Als Registerdaten werden diejenigen soziodemografischen und medizinischen Daten der AHF-Patienten bezeichnet, die bisher vom NR AHF erhoben worden sind. Die Meldung beruht auf der freiwilligen Beteiligung von Herzzentren und niedergelassenen Kinderkardiologen und der ausdrücklichen Zustimmung der Patienten zur Aufnahme ihrer Daten in das NR. Sie sollen dem Organisationsmodul ermöglichen, die Teilnahme der Patienten an Studien in der für ihre Gesundheitsprobleme optimalen Weise zu steuern. Der Datensatz wurde im Februar 2005 überarbeitet und als „minimal data set“ definiert. Diese Daten werden vom *Organisationsmodul des NR AHF* verwaltet.

3. Identifikationsdaten

Die einen Patienten identifizierenden Daten werden nach der Aufnahme eines Patienten in eine Studie an die Patientenliste übertragen und dort gespeichert. Der Patient erhält einen Patientenidentifikator (PID), der in den meldenden Einrichtungen gespeichert und bei der Erfassung und Übermittlung von Forschungsdaten und Registerdaten verwendet wird. Die Patientenliste wird ebenfalls vom *Organisationsmodul des NR AHF* verwaltet.

Die Daten nach Ziffer 2 und 3 werden auf zwei getrennten, für diesen Zweck dedizierten Rechnern mit unterschiedlichen Zugriffsrechten gespeichert. Ausschließlich

das Personal des Organisationsmoduls verfügt – in getrennten Rollen - über diese Zugriffsrechte.

2 Aufgabenstellung

Der Zweck des Vereins Nationales Register für angeborene Herzfehler e.V. besteht – nach Zitat seiner Satzung – darin, „Daten von Patienten mit angeborenen Herzfehlern zu erfassen und für medizinische und sozialmedizinische Studien zur Verfügung zu stellen“³. Unter den Zielen des Kompetenznetzes Angeborene Herzfehler ist als erstes genannt, die „Versorgung und Lebensqualität von Patienten mit angeborenen Herzfehlern“ ... „mittels des Nationalen Registers für Patienten mit angeborenen Herzfehlern als Kern einer leistungsfähigen Telematik-Infrastruktur“ zu verbessern⁴.

Dieser Bezug des KN auf das NR bedeutet nicht, dass Forschungsinteressen der Projekte des KN auf Bereiche beschränkt sein sollen, für die das NR die Datenbasis zu liefern in der Lage ist. Vielmehr werden in den Projekten eigene Datenbasen aufgebaut, indem Patientendaten bundesweit erhoben und in einer für das KN gemeinsamen pseudonymisierten Datenbank zusammengeführt werden.

2.1 Sammlung von patientenbezogenen Daten

Die Sammlung der Patientendaten ist mit widerstreitenden Interessen verbunden. An erster Stelle steht der Wunsch jedes Patienten, seine individuelle Gesundheit wiederherzustellen bzw. zu erhalten und hierfür eine optimale Behandlung zu bekommen. Dies ist mit dem Wunsch jedes Patienten verbunden, so wenig wie möglich durch den Behandlungs- und Heilungsprozess beeinträchtigt zu werden. Dazu kommen die spezifischen Bedürfnisse der Forschungsnetze, über Behandlungsdaten und biologische Proben von Patienten zu verfügen, daraus epidemiologische Informationen zu generieren, Untersuchungsergebnisse an biologischen Proben mit den Verlaufsdaten der Erkrankungen zu korrelieren und als Ergebnis der Forschung im besten Fall sogar einen unmittelbaren Vorteil an den individuellen Patienten zurückzugeben.

Der Datenschutz hat für die Bereitstellung der Wissensbasis eine herausragende Bedeutung. Solange die medizinischen Daten im Behandlungszusammenhang gewonnen und genutzt werden, ist dies durch den Behandlungsvertrag gedeckt, ohne dass es besonderer Vereinbarungen bedarf. Sollen Daten aber speziell für die Forschung erhoben werden, ist eine informierte Einwilligung des Patienten unbedingte Voraussetzung.

Es ist im gemeinsamen Interesse von Patienten, behandelnden Ärzten und Wissenschaftlern, alle Gefährdungen des informationellen Selbstbestimmungsrechts des Patienten, die mit der Behandlung und Datenerhebung im Rahmen eines Forschungsnetzes verbunden sind, so gering wie möglich zu halten. Selbst ein unfreiwilliger, potenzieller oder latenter Bruch der ärztlichen Schweigepflicht bzw. die Missachtung von Daten-

³ Satzung Nationales Register für angeborene Herzfehler e.V. <www.kompetenznetz-ahf.de>

⁴ Satzung Kompetenznetz Angeborene Herzfehler <www.kompetenznetz-angeboreneherzfehler.de/kn_ahf_satzung.pdf>

schutzbestimmungen stört das Vertrauensverhältnis zwischen Patient und Arzt und gefährdet die Ziele sowohl der medizinischen Versorgung als auch der Forschung.

Das NR hat bereits eine datenschutzrechtlich akzeptierte Lösung für die Sammlung, Verarbeitung und Speicherung von Daten seiner Zielgruppe gefunden, die für die aktuellen Aktivitäten gilt; sie ist allerdings als Übergangslösung charakterisiert, die es, zusammen mit der Datenlogistik für das KN, weiterzuentwickeln gilt.

Der Grundsatz der Trennung von identifizierenden Daten (IDAT) und medizinischen Daten (MDAT) ist sowohl technisch (durch zwei getrennte Datenbanken auf getrennten Systemen) als auch organisatorisch (durch zwei verschiedene Datenmanager) gewährleistet.

Insbesondere ist die Trennung von IDAT und MDAT gegenüber dem Studienzentrum und dem behandelnden Arzt zu jeder Zeit gewährleistet.

Die Telematikplattform für Medizinische Forschungsnetze hat im Jahr 2003 eine generische Lösung für die Pseudonymisierung von Forschungsdaten in medizinischen Forschungsnetzen entwickelt⁵, die verbindliche Grundlage für die technische und organisatorische Konzeption der datenschutzrechtlich relevanten Maßnahmen im KN ist. Entsprechend dieser generischen Lösung sind auch die Maßnahmen für das NR anzupassen, so dass sie für beide Einrichtungen ein gemeinsames Ganzes bilden.

Die generische Lösung ist Richtschnur für die Datenflussmodelle im NR und KN, nicht aber sklavisch zu befolgendes Vorbild: Im Einzelnen müssen die logistischen und technischen Konzepte den verschiedenen Aufgaben entsprechend formuliert und Abweichungen von der generischen Lösung dargestellt und begründet werden.

2.2 Rechtssichere Einbindung von Maßnahmen für den Datenschutz

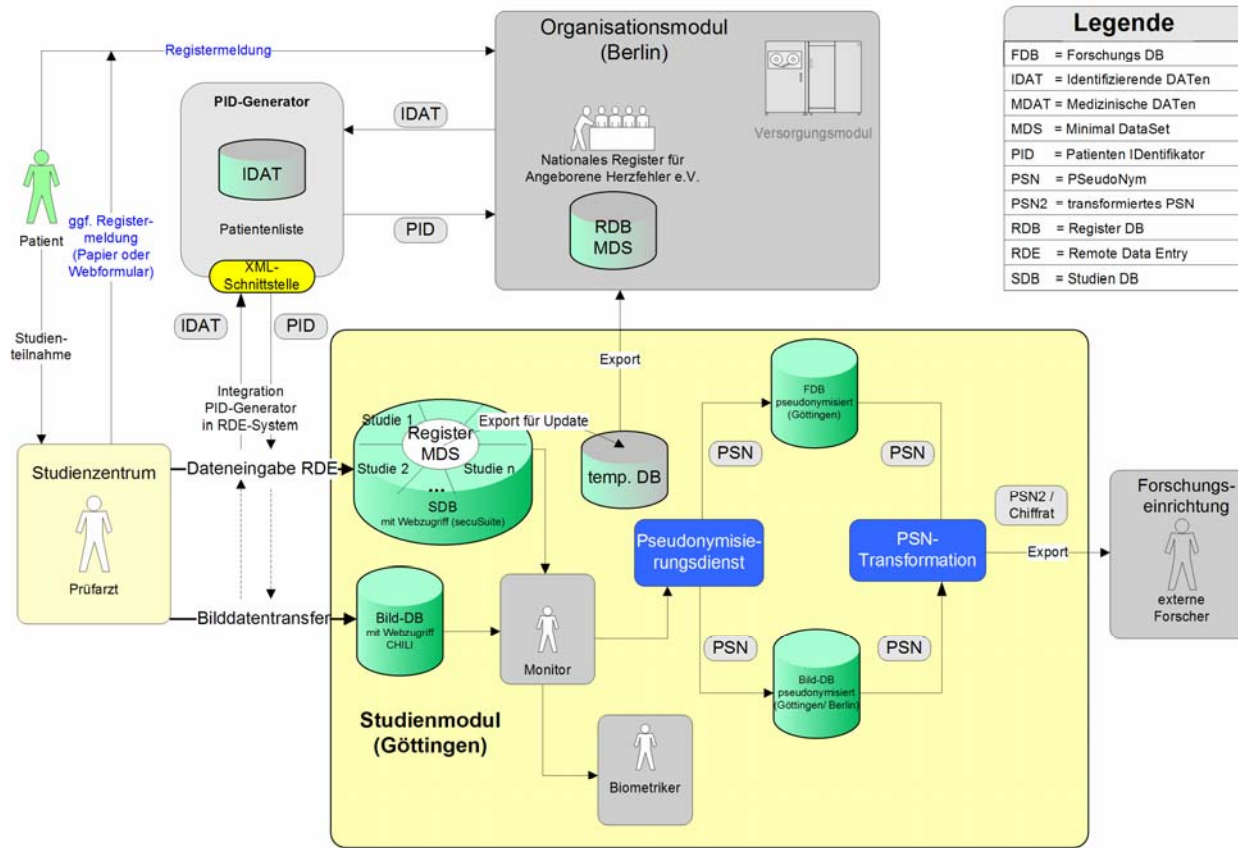
Für eine rechtssichere Umsetzung der Regeln für Datenschutz und Datensicherheit ist es unerlässlich, dass die Verantwortung für die Bereitstellung von Daten an eine juristische Person gebunden ist. Das NR wurde als eingetragener Verein konstituiert, der diese Verantwortung für die Tätigkeit des NR übernimmt.

Die Patientenliste mit den identifizierenden Daten befindet sich in disziplinarischer Verantwortung des DHZB. Da das Nationale Register für angeborenen Herzfehler e.V. auch Daten von Patienten des Deutschen Herzzentrums Berlin enthält, ist durch den Behandlungszusammenhang mit dem DHZB eine hinreichende Beschlagnahmefestigkeit gegeben.

Das Kompetenznetz bildet als Verbund von Einheiten aus verschiedenen Forschungsinstituten und Einrichtungen der medizinischen Behandlung keine juristische Person; deshalb wird auch hier die Gründung eines eingetragenen Vereins vorbereitet.

⁵ Modell B aus: Generische Lösungen der TMF zum Datenschutz für die Forschungsnetze der Medizin, Berlin, Juli 2003

Funktionsübersicht



CIOffice, M. Beckmann 26.08.2005 (Ver 1.1)

Abb. 3: Leistungsmodule und ihre Standorte; Überblick über die Prozesse. (Anmerkung: Ohne Kontaktaufnahme für Epidemiologische und klinische Studien; s. 4.2.5.2)

3 Leistungsmodule des Nationalen Registers und des Kompetenznetzes zur Datenbereitstellung

Die IT-Strategie für NR und KN geht von drei Modulen aus, für die das NR die Verantwortung für die Datenbereitstellung übernimmt:

1. das Organisationsmodul, das im Wesentlichen den Leistungen entspricht, die das NR seit seiner Gründung verfolgt;
2. das Modul zur Prävalenzerhebung, das Daten für die epidemiologische Forschung bereitstellt;
3. das Versorgungsmodul, das die Bereitstellung und Pflege von Daten der Krankheits- und Behandlungsgeschichte von AHF-Patienten anbietet.

Abbildung 3 gibt einen Überblick über die im Kompetenznetz handelnden Akteure (Personen und Einrichtungen), die Struktur der beteiligten Datenbanken und die wesentlichen Prozesse in deren Zusammenspiel.

Die drei Leistungsmodule (*Organisations-, Prävalenz- und Versorgungsmodul*) werden in den folgenden Kapiteln näher erläutert und sind in Berlin angesiedelt (grauer Kasten). In Berlin wird auch die Patientenliste/PID-Generator angesiedelt. Das *Studienmodul* ist mehrteilig: Die *Zentrale* hat ihren Sitz in Berlin und ist für die Organisation der Datenerhebung und für das Monitoring verantwortlich. Die einzelnen *Studienzentren* sind auf verschiedene Forschungseinrichtungen in Deutschland verteilt. Die Datenbanken des Studienmoduls (gelber Kasten) sind in Göttingen stationiert und werden vom CIOOffice betrieben. Sie dienen der Speicherung und Bereitstellung der erhobenen Forschungsdaten und umfassen die Studiendatenbank für Text- und Messdaten, in der die Daten gesammelt und qualitätsgesichert werden, und die Forschungsdatenbanken für Text- und Messdaten sowie für Bilddaten. Der Pseudonymisierungsdienst, der die Pseudonymisierung der Datensätze nach Abschluss der Qualitätssicherung durch den Monitor besorgt, wird ebenfalls in Göttingen vorgehalten.

3.1 Organisationsmodul (NR)

Das Organisationsmodul bildet im Wesentlichen die bisherige Aufgabe des NR ab, Basisdaten für Patienten mit angeborenen Herzfehlern zur Verfügung zu stellen. Neben der Erfassung der Patienten soll im Rahmen von epidemiologischen Studien (s. Kapitel 3.2) der Krankheits- und Behandlungsverlauf unter medizinischen Gesichtspunkten ebenso dokumentiert werden wie die soziale Lebensgeschichte der gesellschaftlichen und beruflichen Orientierung.

Zur Erfassung der Patienten wird das so genannte „minimal data set“ (MDS) von KN und NR definiert, das personenbeziehbar realisiert wird. Dabei werden die medizinischen Daten MDAT in der Registerdatenbank (RDB) und die Identifikationsdaten IDAT in der Patientenliste auf zwei getrennten Rechnern mit unterschiedlichen Zugriffsrechten gespeichert.

Die Meldung der Patientendaten beruht seit Beginn der Tätigkeit des NR auf der freiwilligen Beteiligung von Herzzentren und niedergelassenen Kinderkardiologen und der ausdrücklichen Zustimmung der Patienten zur Aufnahme ihrer Daten in das NR. Sie sollen dem Organisationsmodul ermöglichen, die Teilnahme der Patienten an Studien in der für ihre Gesundheitsprobleme optimalen Weise zu steuern.

3.1.1 Status quo der Verfahren zur Datenerhebung

Gegenwärtig werden die Daten von Papierbelegen erfasst, die von den Patienten bzw. den Eltern der Patienten ausgefüllt worden sind. Zu den Identifikationsdaten wird dabei durch einen Zufallszahlengenerator eine sogenannte Register-ID als Ordnungskriterium erzeugt, die in eindimensionalem Barcode auf Etiketten gedruckt auch zur Verwaltung von Papierbelegen dient. Mit Hilfe der Register-ID werden auch Erhebungsbögen verwaltet, von denen die IDAT abgetrennt werden.

Dieses Verfahren ist besonders geeignet, wenn für jeden Probanden genau ein Erfassungsbogen vorliegt. Bei einer dauerhaften Bestandsführung, bei der Meldungen ggf. auch wiederholt und/oder von verschiedenen Institutionen geliefert werden, tritt das Problem auf, wie die Vergabe von Synonymen für einen Patienten verhindert werden kann, insbesondere dann, wenn Abweichungen in den IDAT durch Schreibfehler, Namens- oder Adressänderungen auftreten.

Gegenwärtig sind bereits etwa 20.000 Datensätze für Patienten erfasst worden, die laufend durch Informationen neuer Patienten erweitert werden. Die Nutzung erfolgt bisher ausschließlich durch Personal des Organisationsmoduls selbst. Eine Verwendung in Forschungsprojekten ist vorgesehen.

Dieser Meldeweg ist historisch gewachsen, in Zukunft wird ein Großteil der Patienten über den qualitätsgescherten Weg gemeldet werden. (s. Kapitel 4.2.5 und 3.2)

3.1.2 Weiterentwicklung der Aufgaben des Organisationsmoduls

Das Organisationsmodul soll Aufgaben im Sinne von Dienstleistungen gegenüber den Patienten und der Forschung übernehmen: Projekte und Patienten sollen gegenseitig vermittelt werden, aus der Sicht des Patienten entsprechend seinem medizinischen Problem, aus der Sicht jedes der Projekte entsprechend ihren Forschungszielen.

Im Modell B der generischen Lösungen ist festgelegt, dass ein Patient grundsätzlich nur durch seinen behandelnden Arzt angesprochen werden darf, wenn es darum geht, ihn zur Teilnahme an einem Forschungsprojekt zu gewinnen oder ihn über Forschungsergebnisse zu informieren. Im hier vorliegenden Fall kann dies auch – das Einverständnis der behandelnden Einrichtung vorausgesetzt - direkt durch das Organisationsmodul selbst erfolgen, da dies Gegenstand der Einwilligungserklärung des Patienten ist.

Bei der Wahl des Informationsweges ist zu berücksichtigen, dass der behandelnde Arzt in der Regel über den Gesundheitszustand des Patienten informiert ist, so dass er besser die Entscheidung fällen kann, ob eine Kontaktierung des Patienten bzw. seiner Eltern möglich und angemessen ist. Als Kompromiss bietet sich an, dass das Organisations-

modul die entsprechende Information für den Patienten aufbereitet, diese aber in kritischen Fällen, die noch zu definieren sind, dem Patienten durch den behandelnden Arzt übermittelt wird.

Die Verwendung der Daten des Organisationsmoduls für die Forschung ist gegenwärtig nicht geplant. Sofern dies später erwogen werden sollte, muss berücksichtigt werden, dass die Daten, so, wie der Meldeweg organisiert ist, nicht qualitätsgesichert sind. Sollten sie tatsächlich für die Forschung verfügbar gemacht werden, fordert die Systematik der Sicherheitspolicy, dass diese Daten, ggf. nach entsprechender inhaltlicher Selektion, pseudonymisiert und in die FDB übertragen werden.

Die Aufgabe, das minimal data set (MDS) zu definieren, wurde im Dezember 2005 abgeschlossen (zur Dokumentation vgl. Kapitel 4.2.4). Für die im Antrag genannte Absicht, in den minimal data set auch Pointer zu weiteren medizinischen Daten aufzunehmen, muss ein Verfahren spezifiziert werden, das zwingend vermeidet, das Ordnungskriterium „Pseudonym“, unter dem die MDAT in den Forschungsdatenbanken abgespeichert sind, zu offenbaren.

3.1.3 Weiterentwicklung der instrumentell und datenschutzrechtlich relevanten Maßnahmen

1. Das bisherige Verfahren der elektronischen Erfassung der IDAT eines Patienten im Register und die zufällige Generierung der Register-ID wird dadurch ersetzt, dass vom Organisationsmodul das Instrument Patientenliste mit PID-Generator genutzt wird. Dieses Instrument wird als zentraler Dienst für das NR und das KN eingerichtet. (vgl. Kapitel 5.1). Das Instrument dient zur sicheren Identifikation eines Patienten⁶ unter Vermeidung von Synonymen. Die bereits erfassten 20.000 Patientendatensätze sollen über das neue Identifikationsverfahren einen neuen Patientenidentifikator (PID) erhalten, der künftig als Ordnungskriterium zu führen ist.
2. *Optional*: Das heute papiergebundene Meldeverfahren soll durch web-basierte Formulare mit integrierter Plausibilitätsprüfung ergänzt werden. Dieses Verfahren kann allerdings nur für Ärzte zugänglich gemacht werden, da aus verfahrensrechtlichen und –technischen Gründen elektronische Meldungen von nicht autorisierten Personen, also von Patienten und ihren Eltern, nicht akzeptiert werden können. Die Datenübermittlung erfolgt über SSL mit Serverzertifikaten. Die Authentifizierung der Nutzer (Prüfarzt oder behandelnder Arzt) erfolgt zunächst mit Benutzername/Passwort; der Übergang zu einer Chipkarten-gebundenen Authentifizierung kann sinnvoll erst dann eingeführt werden, wenn die zugehörigen Instrumente mit der bundesweiten Einführung der elektronischen Gesundheitskarte und des elektronischen Heilberufsausweises flächendeckend verfügbar sein werden.

⁶ Der PID-Generator des Instituts für Medizinische Biometrie, Epidemiologie und Informatik (IMBEI) der Universität Mainz enthält Algorithmen zur Kompensation von Differenzen in der Schreibweise und unterschiedlichen Angaben in bestimmten Datenfeldern. Die Verfahren reduzieren die Gefahr der Vergabe von Synonymen bei Abweichungen in den IDAT (vgl. Kapitel 4.1.2).

3. Falls erforderlich, soll die Definition der Plausibilitätsprüfung und einer kontextbezogenen Qualitätssicherung erweitert werden⁷.
4. Die bestehenden Vorgaben für die getrennte Speicherung von IDAT und MDAT und die jeweiligen Zugangsregelungen sind zu prüfen und ggf. zu ergänzen.
 - Die Patientenliste: Sie enthält die IDAT und den PID des jeweiligen Patienten. Zudem enthält sie die Information, ob der Patient damit einverstanden ist, dass seine medizinischen Basisdaten in das NR aufgenommen werden und in welcher Institution der zuletzt behandelnde Arzt, der zum Patienten Kontakt aufnehmen kann, seinen Sitz hat.
 - Die Register-Datenbank: Sie ist über den PID mit der Patientenliste verknüpft und enthält soziodemografische und medizinische Daten des Patienten in Form eines schlanken Datensatzes, des minimal data sets. Zudem enthält sie Informationen über die Studienteilnahme.

Patientenliste und Registerdatenbank sind nur in einem ersten Schritt durch den PID pseudonymisiert⁸, da es ihr expliziter Zweck ist, dass das Organisationsmodul direkt oder – über den behandelnden Arzt – indirekt mit dem Patienten Kontakt aufnehmen kann. Dies ist durch die Einwilligungserklärung des Patienten abgedeckt.

Die Patientenliste enthält auch Daten von Patienten, die nicht in das Register aufgenommen werden. In diesem Fall ist der Zugang zu den IDAT durch den Auftrag zur Verwaltung der Patientenliste abgedeckt. Es ist dem Organisationsmodul aber verwehrt, selbst Kontakt zu diesen Patienten aufzunehmen.

5. Ausarbeitung einer Nutzungsordnung für das Modul und seine Datenbanken als Bestandteil einer Policy für das NR.

3.2 Modul zur Prävalenzerhebung

Die Einrichtung eines Moduls zur Prävalenzerhebung wird über die in Abbildung 3 aufgezeigte Infrastruktur abgewickelt. Hier soll die Basis für die epidemiologische Forschung aufgebaut werden.

Diese Prävalenzerhebung für Neugeborene hat den Charakter einer epidemiologischen Studie und nutzt den qualitätsgesicherten Meldeweg. Die gemeldeten Daten werden ab dem Jahr 2006 im Modul zur Prävalenzerhebung gespeichert.

⁷ Modell B der Generischen Lösungen für den Datenschutz in medizinischen Forschungsnetzen enthält eine Lösung für den Fall, dass für die Qualitätsprüfung eines aktuellen Datensatzes auch auf die Kontextdaten, die als früher gemeldete Daten verfügbar sind, zugegriffen werden muss. Das Verfahren muss dann in die Policy beschreibend aufgenommen werden.

⁸ Der PID stellt bereits ein Pseudonym dar, was allerdings erst der erste Schritt einer mehrstufigen Pseudonymisierung darstellt.

3.2.1 Aufgaben

Das Modul zur Prävalenzerhebung sammelt den für die Erforschung der Prävalenz der angeborenen Herzfehler erforderlichen Datenbestand und führt die Untersuchungen durch. Hierfür ist es erforderlich, dass die betreffenden Patienten bei der Geburt bzw. in den ersten Lebensjahren möglichst vollständig erfasst werden⁹. Da angeborene Herzfehler in den ersten Lebensjahren nur dann sicher erkannt werden, wenn es sich um mittelschwere und schwere Fälle handelt, muss die Prävalenzforschung zunächst auf diesen Bereich beschränkt bleiben. Mit den Jahren sollen Datenbasis und Untersuchungsansätze erweitert werden.

Die Vollständigkeit der Erfassung hat sehr hohe Bedeutung für die Prävalenzforschung. Es soll deshalb ein Instrument entwickelt werden, das es den Ärzten auch dann erlaubt, Meldungen abzugeben, wenn die Eltern eines Patienten seiner Aufnahme in das NR nicht zustimmen. Das Instrument muss deshalb den Bedingungen entsprechen, die für die *Meldepflicht* zu medizinischen Registern gelten¹⁰: Die Meldung muss in den Fällen, in denen die Teilnahme am NR abgelehnt wird, anonym erfolgen. Die notwendige Meldung von Patienten, die anonym bleiben wollen, wird ohne identifizierende Angaben auf Papier erfasst und nicht in die Datenbank übernommen.

3.2.2 Datenschutzrechtlich relevante Maßnahmen

1. Das Meldeverfahren soll für patientenbezogene Meldungen definiert werden; neben den Erhebungsbögen soll auch ein web-basiertes Formular mit integrierter Plausibilitätsprüfung verfügbar sein. Die Datenübermittlung erfolgt über SSL mit Serverzertifikaten, die Authentifizierung der meldenden Ärzte über Benutzername und Passwort. Hierzu soll für die Datenerfassung das RDE-System von iAS genutzt werden. Der Ausbau zu chipkartenbasierten Nutzerzertifikaten soll grundsätzlich ermöglicht werden, sobald die Infrastruktur mit der bundesweiten Einführung der elektronischen Gesundheitskarte bereitsteht.
2. Definition der Maßnahmen zur Qualitätssicherung.
3. Definition der Zugangsbedingungen der Forschung zur Datenbasis.
4. Ausarbeitung einer Nutzungsordnung für das Modul als Bestandteil einer Policy für das NR.

3.3 Versorgungsmodul

Auch das Versorgungsmodul ist ein aktueller Vorschlag zur Ausweitung des Wirkungskreises und der Dienstleistungen des NR.

⁹ Der pränatale Bereich bleibt zunächst wegen der großen Schwierigkeiten seiner Erfassung ausgeklammert.

¹⁰ Das heißt nicht, dass die Gesetzgebung für die Prävalenzforschung bemüht werden soll; es geht darum, den Ärzten ein Meldeinstrument an die Hand zu geben, mit dem das informationelle Selbstbestimmungsrecht des Patienten in keinem Fall verletzt wird.

3.3.1 Aufgaben

Im Versorgungsmodul werden einrichtungsübergreifende Patientenakten gespeichert, die im Rahmen der medizinischen Versorgung von den behandelnden Ärzten eingesehen werden können. Es handelt sich dabei um Daten zum Krankheits- und Behandlungsverlauf in patientenbezogener Form, die dem Begriff der elektronischen Patientenakte nach SGB V § 291 a Abs. 3 Ziff 4 entsprechen.

Wie in 3.3.2 dargestellt, werden die IDAT und die MDAT getrennt gespeichert. Sowohl der behandelnde Arzt als auch der Patient kennen den PID und müssen nicht auf die IDAT zugreifen. Dies wäre beispielsweise der Fall, wenn ein behandelnder Arzt auf MRT-Bilder seines Patienten zugreifen möchte.

Das Ziel ist aber nicht die Bereitstellung der vollständigen, in einem Patientenleben angesammelten Daten; vielmehr sollen diese auf den Bestand reduziert werden, der für die jeweils aktuelle Bewertung des Gesundheitszustandes und des Therapiebedarfs des Patienten relevant ist. Das setzt voraus, dass die Daten der einzelnen Behandlungsepisoden, die zunächst vollständig dokumentiert sind, periodisch so selektiert und komprimiert werden, dass die jeweils kurz-, mittel- und langfristig relevanten Informationen unmittelbar zur Verfügung stehen.

Das Versorgungsmodul stellt damit ein Dienstleistungsangebot an den Patienten dar, eine elektronische Patientenakte bereitzustellen und so zu pflegen, dass sie dem Arzt, der sie konsultiert, als klinischer Metadatensatz eine optimale Informationsgrundlage bietet.

Die Daten des Versorgungsmoduls sind nicht für die Forschung bestimmt. Die Datenbank ist deshalb nur für den Zugriff eines autorisierten Arztes auf den Datenbestand jeweils eines Patienten eingerichtet. Es ist nicht möglich, von außen merkmalsgesteuerte Anfragen an die Datenbank zu stellen oder andere Auswertungen zu machen.

3.3.2 Datenschutzrechtlich relevante Maßnahmen

1. Definition des Anmeldeverfahrens: die Daten der Patienten, die bereits im NR gemeldet sind, können nach entsprechender Einwilligung ins Versorgungsmodul übertragen werden. Die Datenübermittlung erfolgt über SSL mit Serverzertifikaten, die Authentifizierung der meldenden Ärzte über Benutzername und Passwort. Der Ausbau zu Chipkarten-basierten Nutzerzertifikaten soll grundsätzlich ermöglicht werden, sobald die Infrastruktur mit der bundesweiten Einführung der elektronischen Gesundheitskarte bereit steht.
2. Ergänzende Maßnahmen: Die Freigabe der Daten für die Patientenakte des NR muss durch eine Erklärung des Patienten dokumentiert sein. Nach Einführung der eGK kann dies vorbehaltlich einer klaren Regelung zwischen Sorgeberechtigten und minderjährigem Kind z. B. mittels der auf der eGK digital signierten Einwilligungserklärung erfolgen.
3. Identifikation des Patienten über den PID-Generator und die Patientenliste, Vergabe einer eindeutigen PID,

4. Getrennte Speicherung der IDAT in der Patientenliste und der MDAT mit Verknüpfungsmöglichkeit über den PID,
5. Maßnahmen der Qualitätssicherung,
6. Überführung der qualitätsgesicherten Daten in die Versorgungsdatenbank. Die Daten werden dort in verschlüsselter Form in der Weise gespeichert, dass nur der Patient selbst Dritten den Zugang zu den Daten gewähren kann. Daneben haben ausschließlich die Personen, die im NR die Pflege der Daten im Versorgungsmodul übernehmen, Zugriff auf die MDAT, nicht notwendigerweise aber auf die IDAT.¹¹
7. Speicherung der Pointer und der Zugriffsschlüssel auf die eGK des Patienten durch das NR,
8. Abruf der Daten durch einen behandelnden Arzt: Ein Arzt erhält Zugriff auf den Datenbestand eines Patienten nur dann, wenn seine Anforderung eine signierte Zustimmungserklärung des Patienten enthält. Eine Änderung und Ergänzung der Daten ist nicht bei Abruf möglich, sondern nur über das Meldeverfahren nach Ziff 1ff.
9. Ausarbeitung einer Nutzungsordnung für das Modul als Bestandteil einer Policy für das NR.

3.4 Studienmodul - Datenbereitstellung für Forschungsprojekte (KN)

Die Studiengruppen des KN AHF bauen eine Datenbasis auf, die auf die spezifischen Forschungsaufgaben zugeschnitten sind. Vordergründig wird es als Aufgabe der einzelnen Studiengruppe verstanden, die erforderlichen Daten zu erheben und in einer für wissenschaftliche Untersuchungen geeigneten Form bereitzustellen. In Kapitel 2.2 wurde bereits darauf hingewiesen, dass die rechtssichere Einbindung von datenschutzrechtlich relevanten Maßnahmen und Regelwerken in diesem Prozess nur von einer Institution übernommen werden kann, die sich als juristische Person konstituiert. Die Studiengruppen im Forschungsverbund des KN haben diese Eigenschaft einer juristischen Person nicht. Deshalb muss die rechtliche Verantwortung für die Erhebung und Bereitstellung der Datenbasis dem KN AHF e. V. übertragen werden, ohne dass die inhaltlich-methodische Verantwortung des einzelnen Projektes selbst angetastet wird. Der KN AHF e. V. ist in Gründung.

Es ist zweckmäßig, die Erhebung für verschiedene Studien zu bündeln und die zentralen technischen Services wie die Patientenliste, den Pseudonymisierungsdienst und die Führung der Forschungsdatenbank, gemeinsam durch die Projekte und das NR zu nutzen. Der wesentliche Vorteil für die Forschungsprojekte bestünde darin, dass einheitliche Meldewege (Datenflüsse) zwischen den Einrichtungen der medizinischen Behandlung einerseits und dem NR und KN andererseits zusammen mit den datenschutzrechtlich abgesicherten technischen und organisatorischen Verfahren für jede Studie genutzt wer-

¹¹ Das Verfahren soll dem entsprechen, das für die Patientenakte im Zusammenhang mit der eGK entwickelt werden wird. Dies gilt auch für die folgenden Punkte 7 und 8. Eine eigenständige dv-technische Lösung ist nur dann erforderlich, wenn das NR mit seinen Aktivitäten eher auf den Markt treten will, als die Selbstverwaltung der Krankenkassen und der Ärzteschaft.

den können. Damit kann der Aufwand sowohl bei den dokumentierenden Stellen wie auch bei der die Daten verarbeitenden Stelle rationalisiert werden.

3.4.1 Aufgaben

Die Aufgaben, die sich daraus für die Erhebung und Bereitstellung von Forschungsdaten ergeben, sind im generischen Modell B¹² erschöpfend beschrieben. Folgende Einzelschritte sind relevant:

1. Die Bereitstellung der Erhebungsgrundlagen in Form von Erhebungsbögen und über ein web-basiertes Formular-Set, das vom KN-Server mit integrierter Plausibilitätsprüfung angeboten wird. Als Sicherheitsmaßnahmen werden diejenigen genutzt, die im RDE-System von iAS integriert sind: Datenübermittlung über SSL mit Serverzertifikaten, Authentifizierung der Nutzer über Benutzerkennung und Passwort.
2. Identifikation des Patienten über die Patientenliste/den PID-Generator, Vergabe einer eindeutigen PID. Das Instrument PL/PID-Generator wird dabei über eine Schnittstelle des RDE-Systems angesprochen.
3. Getrennte Speicherung der IDAT in der Patientenliste und der MDAT mit dem PID in der Studiendatenbank (SDB), mit deren Hilfe auch die Qualitätssicherung durchgeführt wird.
4. Maßnahmen der Qualitätssicherung.
5. Überführung der qualitätsgesicherten Daten aus der Studiendatenbank in die Forschungsdatenbank (FDB). Bei der Überführung werden die Daten pseudonymisiert, indem der PID kryptografisch transformiert wird.
6. Regelung des Zugangs für externe Forscher zu den Daten durch Export der Daten oder selektiven Direktzugriff zur Datenbank.

Die mit der Datenerhebung und -bereitstellung der Daten verbundenen Aufgaben werden im Detail in Kapitel 4 beschrieben.

4 Prozesse der Datenerhebung und -bereitstellung

In diesem Kapitel werden die Abläufe der Datenerhebung und -bereitstellung in einer allgemeinen Ausprägung beschrieben, die – ggf. mit geringfügigen Varianten – in allen Leistungsmodulen des KN AHF eingesetzt werden sollen. Auf diese Darstellung wird in den anderen Kapiteln referenziert, um Redundanzen möglichst zu vermeiden.

¹² Modell B aus: Generische Lösungen der TMF zum Datenschutz für die Forschungsnetze der Medizin, Berlin, Juli 2003

4.1 Allgemeines Ablaufmodell

Das allgemeine Ablaufmodell bezieht sich auf die Erhebung und Bereitstellung von medizinischen und ggf. sozialen Daten im Studienmodul, und zwar von Text- und Messdaten, die zur Pseudonymisierung nicht gesonderter Maßnahmen, wie z. B. die Bilddaten, bedürfen. Sie werden in einer pseudonymisierten Datenbank für die Forschung bereitgehalten.

4.1.1 Aufnahme von Patienten – Rechte des Patienten

Die Aufnahme eines Patienten in die Patientenliste, in das Register des Organisationsmoduls und/oder in eine Studie ist Gegenstand der Patienteninformation und der Einwilligung, die der Aufnahme des Patienten in eine Datenbank vorausgeht. Wünscht ein Patient nicht teilzunehmen, dürfen ihm daraus in der Behandlung keine Nachteile erwachsen; dies gilt auch bei späterer Rücknahme der Einwilligung.

Der Patient hat das Recht, Auskunft über die Daten zu verlangen, die über ihn in allen betroffenen Dateien gespeichert werden. Das Auskunftsrecht ist Gegenstand der Patienteninformation. In der Regel wendet er sich dazu an den aktuell behandelnden Arzt, der mit dem Forschungsnetz in Verbindung steht.

Wünscht der Patient Auskunft über seine IDAT, so sendet der Arzt Name und Geburtsdatum sowie den PID des Patienten an die Patientenliste, die daraufhin ein gedrucktes – oder druckfähiges – Dokument zur Verfügung stellt, das die gespeicherten Daten in einer für den Patienten verständlichen Form enthält. Der Prozess kann automatisiert ablaufen. Wünscht der Patient Auskunft über die MDAT, sendet der Arzt den PID an den Pseudonymisierungsdienst, der seinerseits das PSN an die Forschungsdatenbank weiterreicht. Dort werden die Daten selektiert und über den PSD zurück an den behandelnden Arzt gesandt, der seinerseits das gedruckte Dokument dem Patienten aushändigt und es, wenn nötig, erläutert (vgl. Abbildung 4).

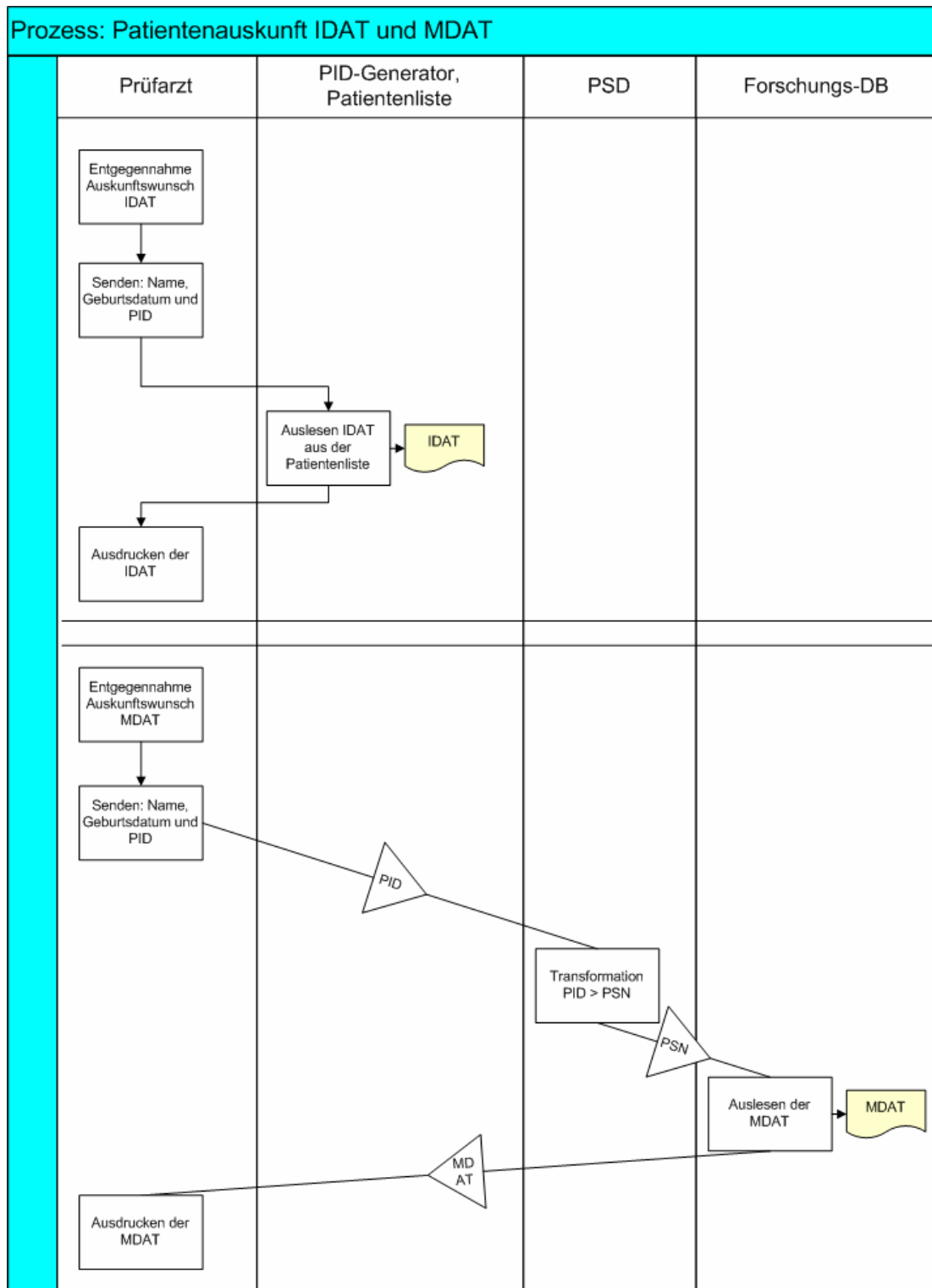


Abbildung 4: Ablaufdiagramm für den Prozess Patientenauskunft IDAT und MDAT

Die Dauer der Speicherung der Daten eines Patienten in pseudonymisierter Form¹³ muss im Einzelnen aus den Forschungszielen abgeleitet werden. Als allgemeine Regel soll gelten, dass die Speicherung für die Dauer von sechs Jahren nach der letzten Behandlung im Forschungsnetz als notwendig angesehen wird, um ggf. Forschungsergebnisse für den Patienten direkt nutzbar zu machen. Gibt es Gründe, die Daten für eine Frist pseudonymisiert verfügbar zu halten, die sechs Jahre überschreitet, ist dies möglich, wenn es in der Einwilligungserklärung entsprechend formuliert ist. Nach Ablauf der Frist sind Forschungsdaten nur noch anonymisiert zu verwenden: Dazu müssen die Daten in der Patientenliste gelöscht und das Pseudonym als Ordnungskriterium in der Forschungsdatenbank durch eine Zufallszahl oder ein nicht rückrechenbares Chiffprat ersetzt werden. Unberührt davon ist die bisherige Regelung des NR, dass Patienten beim Erreichen des 18. Lebensjahres mit der Bitte um Einwilligung zur weiteren Speicherung ihrer Daten im NR angeschrieben werden.

Sofern ein Patient seine Einwilligung nicht nur für künftige, sondern auch für bereits aufgenommene Daten zurückzieht, müssen seine Daten in der Patientenliste gelöscht und in der Forschungsdatenbank anonymisiert werden. Auf zurückliegende Auswertungen hat ein Rückzug des Patienten dagegen keine Auswirkungen.

4.1.2 Identifikation des Patienten, Generierung des PID

4.1.2.1 Patientenliste und PID-Generator

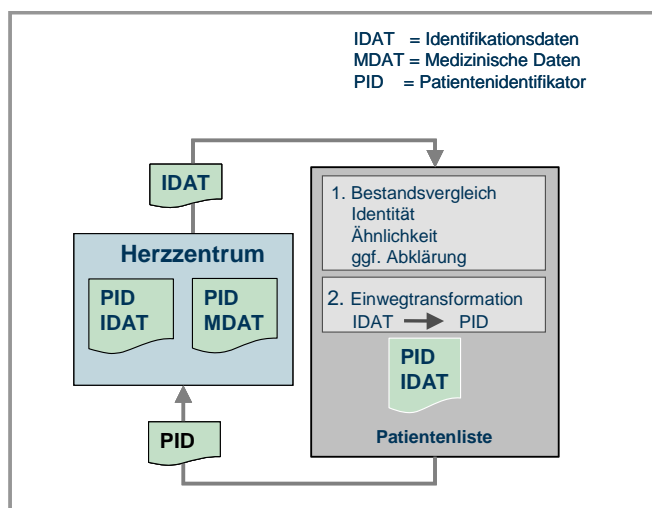


Abb. 5: Identifikation und Anmeldung eines Patienten in der Patientenliste

Die eindeutige Identifikation des Patienten wird als ein Mittel der Qualitätssicherung verstanden. Zugrunde liegt ein Szenario, in dem Patienten mit einer chronischen Erkrankung über einen längeren Zeitraum von unterschiedlichen Einrichtungen der Regelversorgung und spezialisierten klinischen Zentren behandelt bzw. beobachtet werden. Von Ärzten erhobene Daten und Daten aus Patientenfragebögen bilden die Grundlagen für eine oder mehrere Studien in einem Forschungsnetz.

Ein Patient kann von verschiedenen Einrichtungen zu unterschiedlichen Zeitpunkten für eine Studie angemeldet werden. Es ist auch möglich,

¹³ Die pseudonymisierte Form beinhaltet, dass die Möglichkeit besteht, den Patienten zu re-identifizieren.

dass eine Einrichtung den PID eines Patienten mehr als einmal abfragt. Durch die Arbeitsweise der Patientenliste wird mit hoher Sicherheit erreicht, dass ein einmal angemeldeter Patient bei einer späteren Meldung wiedererkannt wird, und zwar auch dann, wenn die Stammdaten durch Modifikation oder durch unterschiedliche Schreibweise voneinander abweichen.

Jeder Patient erhält einen sogenannten Patientenidentifikator PID, eine nicht sprechende Zeichenkette, die vom PID-Generator den Stammdaten zugeordnet wird. Der Algorithmus für die Erzeugung des PID ist so gewählt, dass es nicht möglich ist, aus dem PID allein durch „Rückrechnen“ identifizierende Merkmale des Patienten zu generieren.

Die Identifikation eines Patienten geschieht über die Stammdaten, welche den Patienten im Klartext identifizieren (IDAT). Dazu wird eine Patientenliste aufgebaut. Über die IDAT ist im Bestand dieser Liste zu prüfen, ob der Patient bereits erfasst und ein PID vergeben ist. Im negativen Fall ist ein neuer PID zu erzeugen und mit den IDAT in den Bestand der Patientenliste zu übernehmen.

Abbildung 5 zeigt schematisch den Vorgang: Sobald der Patient seine Einwilligung zur Aufnahme in eine Studie oder in die Registerdatenbank erklärt hat, kann er in der Patientenliste durch die Übermittlung der IDAT angemeldet werden. Die Patientenliste prüft zunächst im Bestand, ob ein Patient mit gleicher oder ähnlicher Schreibweise der IDAT bereits aufgenommen ist und übermittelt die IDAT, zusammen mit dem im Bestand gefundenen oder neu erzeugten PID, zurück an die meldende Stelle¹⁴.

Das Problem der Identifikation besteht darin, sicherzustellen, dass auch bei sehr großen Patientenlisten die Vergabe von PID als Synonyme¹⁵ und Homonyme¹⁶ mit möglichst hoher Sicherheit vermieden wird. Dies wird durch Qualitätssicherung für die Arbeitsweise des Matchalgorithmus sichergestellt¹⁷.

4.1.2.2 Identifikationsdaten (IDAT)

Die Erhebung der IDAT muss möglichst einheitlich sein. Als Basis der IDAT wird der Datensatz der Versichertenkarte (VK) empfohlen, da hiermit das größtmögliche Maß an Normierung erreicht wird und durch elektronische Übernahme der Daten fehlerhafte Eingaben vermieden werden können. Zusätzlich soll der Geburtsname oder ein anderer früherer Name erfasst werden, wenn ein Patient während seiner Verweilzeit im Forschungsnetz den Namen wechselt, um so die Zusammenführung der Daten unter einem PID zu ermöglichen.

Für die Erhebung der Identifikationsdaten soll sowohl die Option bestehen, die Daten aus dem Klinik- oder Praxisverwaltungssystem zu übernehmen, als auch, sie aus der Versichertenkarte direkt einzulesen. Hat ein Patient keine Versichertenkarte, müssen die

¹⁴ Siehe auch Fußnote 4. Dokumentation: <PID Manual.pdf>

¹⁵ ein Patient hat mehrere PID

¹⁶ zwei oder mehr Patienten haben einen identischen PID

¹⁷ Aus der Sicht der Biometriker ist in den Studien des AHF-Netzes der Fehler Synonyme eher zu tolerieren als der Fehler Homonyme. Im Rahmen der Qualitätssicherung kann die Arbeitsweise des Matchalgorithmus in der Weise kalibriert werden, dass er den Anforderungen entsprechend arbeitet.

verfügbaren Daten mit Hilfe einer einheitlichen Maske manuell mit integrierten Checks auf Vollständigkeit und (formale) Plausibilität erhoben werden.

Das RDE-System von iAS kennt derartige Schnittstellen nicht. Ein wesentlicher Vorteil des RDE-Systems ist die Tatsache, dass lokale Installationen beim Anwender zur Datenerfassung nicht notwendig sind. Es würde aber einen erheblichen Verlust der Qualität der IDATs nach sich ziehen, wollte man auf die elektronische Übermittlung verzichten. Die Aufgabe soll in Kürze einer Lösung zugeführt werden.

Anmerkung: Durch die bevorstehende Ausgabe der neuen eGK wurde eine Anbindung der alten Krankenversichertenkarte im KN AHF nicht realisiert.

4.1.2.3 Weitere Prozessdaten

Bei der Anmeldung eines Patienten bei der Patientenliste werden das Kennzeichen der meldenden Klinik oder Praxis und das Datum der Meldung übertragen und in der Liste gespeichert. Dies gilt auch dann, wenn einem Patienten bereits ein PID zugewiesen wurde und dieser einer neu meldenden Klinik übermittelt wird.

Kennzeichen und Datum werden grundsätzlich nicht als Historie geführt sondern durch die jeweils aktuelle Meldung überschrieben. Die Daten werden benötigt, damit die Stelle, welche die Patientenliste führt, erkennen kann, welche Klinik informiert werden muss, wenn ein Patient depseudonymisiert und angesprochen werden soll. In Sonderfällen, z. B. wenn ein Patient gleichzeitig in mehr als einer Studie geführt wird, wird eine Mehrfachspeicherung vorgesehen.

4.1.2.4 Notwendigkeit einer zentralen Patientenliste für die Leistungsmodule

Mit der zentralen Einrichtung der Patientenliste wird angestrebt, dass die Kranken- und Behandlungsgeschichten von Patienten mit einer chronischen oder rezidivierenden Erkrankung möglichst langfristig verfolgt werden können. Der Wechsel von Behandlungseinrichtungen und hohe räumliche Mobilität der Patienten führen dazu, dass Patienten im Laufe der Zeit von verschiedenen Einrichtungen an die Patientenliste gemeldet werden. Wie unter Kapitel 4.1.2.1 erwähnt, soll auch bei modifizierter Eingabe der IDAT (z. B. durch Schreibfehler bei manueller Erfassung oder Adressänderung) sichergestellt werden, dass der Patient im Bestand identifiziert und ihm der identische PID zugewiesen wird.

4.1.2.5 Arztliste

Über das Administrationswerkzeug für das RDE-System wird die Liste der zugangsberechtigten Prüfarzte geführt. Sie enthält die Kontaktdaten aller dokumentierenden Stellen und ihrer für die Dokumentation verantwortlichen Ärzte.

Diese Codes sind in SDB und FDB zu führen. Im AHF-Netz wird kongruent zu den mit den Ärzten zu schließenden Verträgen die Pseudonymisierung der Arzt-ID nicht vorgesehen.

4.1.2.6 Prozessablauf

Beim Aufbau des vom Organisationsmodul verwalteten Registers wird der Patient vom Personal des Organisationsmoduls bei der Patientenliste angemeldet. Die Daten kommen in der geltenden Anordnung von den Patienten bzw. ihren Eltern selbst auf Papierbelegen. Die Rechtschreibung von Namen dürfte hier korrekt sein. Bei der elektronischen Erfassung sollte aber auf jeden Fall eine doppelte Eingabe mit Ergebnisvergleich – wie bei der Eingabe von Passworten – eingerichtet werden. Eine web-Meldung von Patienten soll dagegen nicht eingerichtet bzw. keinesfalls automatisch verarbeitet werden, da es bei unbekanntenen Personen nicht möglich ist, ein Authentifizierungsverfahren vorzuschalten.

Werden Patienten für das Register von Ärzten gemeldet, sollten sie eine Schnittstelle, wie in Kapitel 4.1.2.2 beschrieben, nutzen.

Bei der Datenerhebung für Studien werden die IDAT durch die Prüfärzte bzw. deren Dokumentationsassistenten auf dem Web-Formular-Set erfasst. Auch hier ist die Schnittstelle zu den Daten aus PVS und KIS unverzichtbar (vgl. Abbildungen 6 und 7).

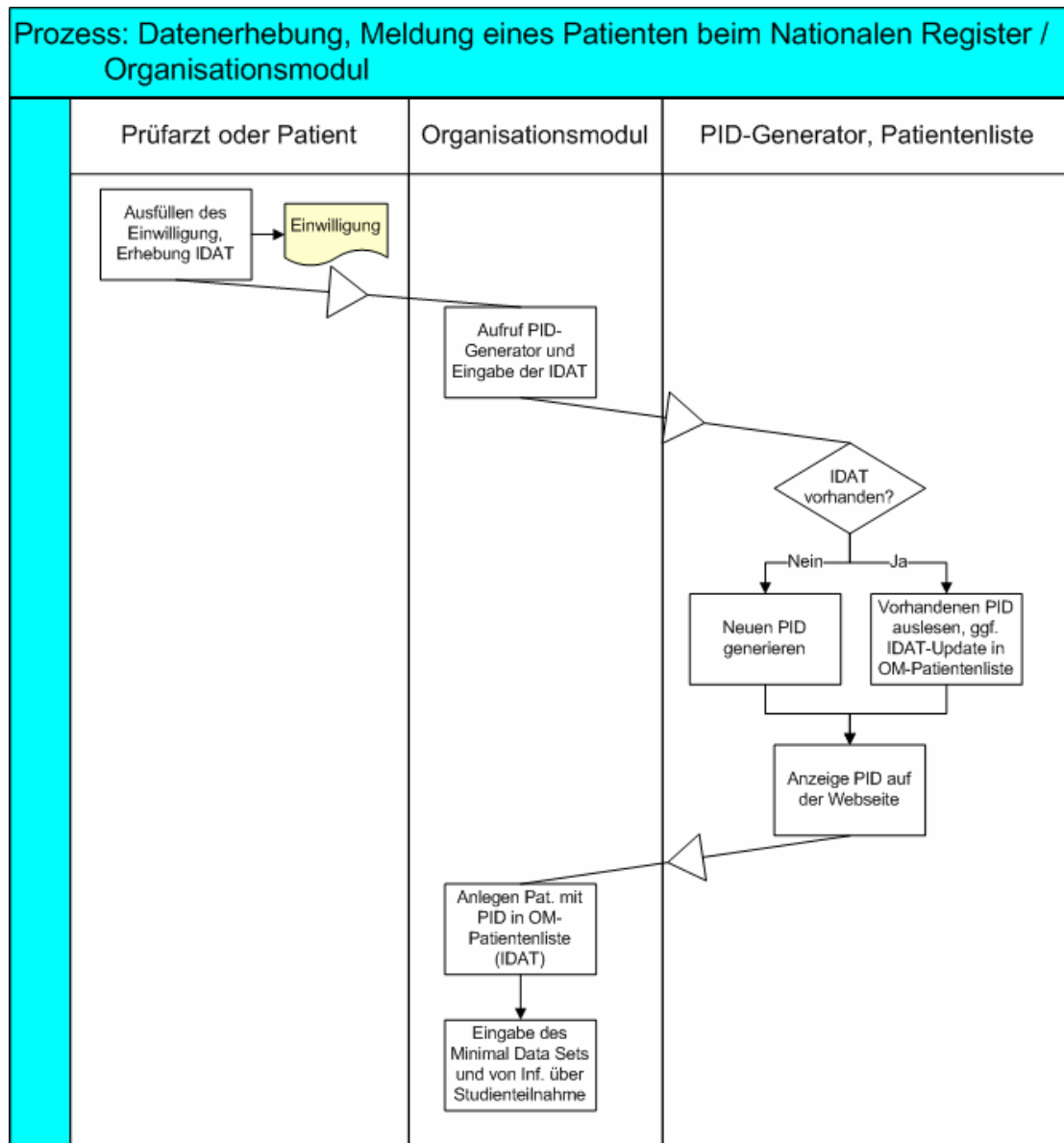


Abbildung 6: Ablaufdiagramm für den Prozess Datenerhebung bzw. Registermeldung

Alle auf elektronischem Weg meldenden Personen müssen durch ihre eigene Anmeldung autorisiert sein. Der Meldeweg selbst wird durch das RDE-System hergestellt. Der Datenverkehr der Meldung zum Register und zur SDB erfolgt über SSL mit Benutzererkennung und Passwort für die Nutzer und Authentifizierung der Server mit x501.v3-Zertifikaten. Der Datenverkehr zwischen Organisationsmodul und PL bzw. zwischen RDE-System und PL soll über Server mit x501.v3-Zertifikaten abgesichert sein.

4.1.3 Erfassung der medizinischen Daten

Die Erfassung medizinischer Daten, ohne Bilddaten, kann auf verschiedenen Wegen erfolgen:

- Vom Arzt erhobene Daten werden in der Regel aus behandlungsnaher Dokumentation entnommen und nach den Vorschriften der Studienprotokolle in web-basierte Formulare des RDE-Systems manuell übertragen.
- Daten aus Analysegeräten, z. B. Labor, Spiroergometrie, Bilddaten aus Echokardiografie und MRT werden in den von den Geräten vorgegebenen Formaten übertragen und gespeichert. Eine Übernahme von Biosignaldaten im Original ist im ersten Schritt nicht vorgesehen.

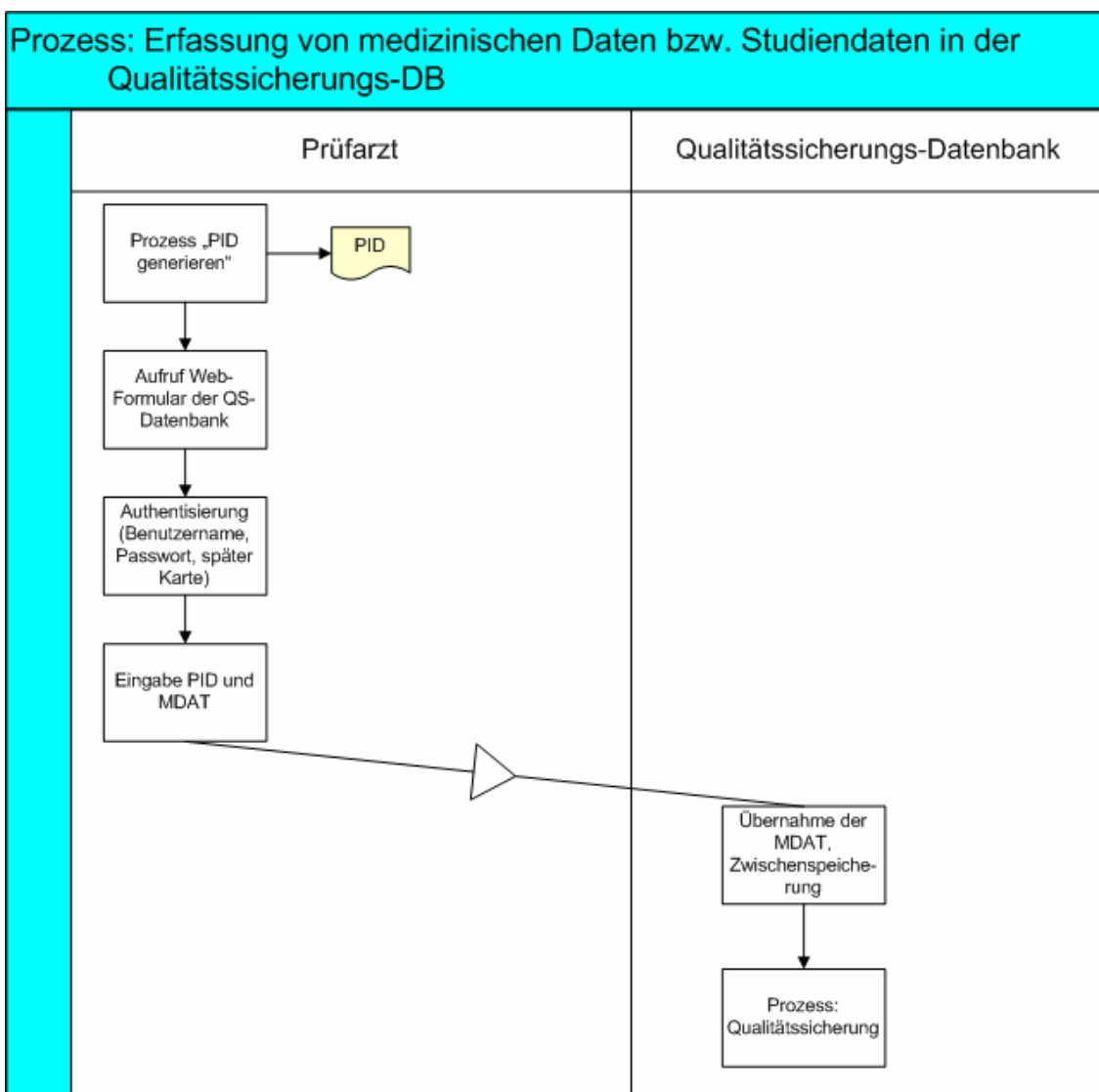


Abbildung 7: Ablaufdiagramm für den Prozess der Eingabe von Studiendaten in die SDB über ein RDE-System.

Diese Daten werden ohne IDAT und mit dem PID als Ordnungskennzeichen an die Datenbank übertragen, auf der die Daten einer Qualitätskontrolle unterzogen (QS-DB) und dafür temporär gespeichert werden (vgl. Abbildungen 6 und 7).

Berechtigt sind dazu Prüfarzte und von Prüfarzten angeleitete Dokumentationskräfte für die vom Arzt erhobenen Daten und Prüfarzte und Assistenten für die Selektion von Maschinendaten.

Instrumente des Datenverkehrs mit der QS-DB ist SSL mit X.509.v3-Serverzertifikaten; für den Nutzer wird die Authentifizierung mit Benutzername/Passwort durchgeführt.

4.1.4 Qualitätssicherung

Die Prozesse sind bisher allgemein formuliert und mit Fachleuten der Biometrie abgestimmt. Bei der Anpassung an die realen Gegebenheiten des NR und KN AHF sind ggf. Modifikationen einzuarbeiten.

Bei den generischen Lösungen Modell B ist vorgesehen, dass für die Qualitätssicherung eine Datenbank eingerichtet wird, auf der die Erhebungsdaten unter dem Ordnungskriterium PID bis zum Abschluss der Qualitätssicherung temporär gespeichert und danach über den Pseudonymisierungsdienst (PSD) mit Transformation des PID gegen das PSN an die FDB übermittelt werden. Im KN AHF wird die Qualitätssicherung mit Hilfe der SDB durchgeführt, Änderungen durch das Audit Trail protokolliert, so dass hier die Führung einer eigenen QS-DB entfällt.

Die Qualitätssicherung wird von sog. Monitoren übernommen; sie wird grundsätzlich in zwei Prozessen durchgeführt:

- a) Prüfung der Vollständigkeit und Plausibilität der von den dokumentierenden Stellen übernommenen Daten, in Ergänzung der automatischen, mit den web-Formularen verbundenen Prüfungen;
- b) Prüfung der Übereinstimmung zwischen der lokalen Dokumentation und den Daten, die an die SDB übermittelt worden sind, sowie der Prüfung, dass die gemeldeten Patienten tatsächlich in der Klinik behandelt bzw. beobachtet werden. Diese Form der Qualitätssicherung wird in den dokumentierenden Stellen selbst durchgeführt.

Für die Qualitätssicherung wird im KN AHF eine Fachkraft angestellt, der es, neben der eigenen Prüftätigkeit, vor allem obliegt, den Qualitätssicherungsprozess zu organisieren. Das KN AHF wird sich dazu qualifizierter Einrichtungen, wie etwa der KKS, bedienen, deren Personal im Auftrag des KN vor allem die Prüfungen vor Ort in ihrer Region übernehmen wird.

Es wird also eine Reihe von Monitoren für mehrere Studien gleichzeitig die Prüfaufgaben übernehmen. Für alle Monitore müssen die besonderen Rechte, die ihnen eingeräumt werden, in einer Rollen- und Berechtigungs-Datenbank eingerichtet werden. Die genaue Form und die Verwaltung dieser Datenbank ist mit iAS abgestimmt zu definieren, da dies ggf. auch im Rahmen des RDE-Systems geleistet werden kann.

Nach Abschluss der QS durch Freigabe der entsprechenden Datensätze werden die Daten über den PSD zur FDB übermittelt und dort gespeichert, während in der SDB die qualitätsgesicherten Daten gelöscht werden (vgl. Abbildung 8).

Die von iAS im Auftrag des ISST erstellte PSD-Software soll (nach Auftrag) diese Leistungen enthalten. Diese Software muss ggf. für die Aufgaben „revitalisiert“ und eingesetzt werden, die zur Datenverwaltung nach der Datenerfassung im RDE-System erforderlich sind.

Alternativ dazu – und wahrscheinlich mit geringerem Aufwand, kann anstelle der Übertragung der Kontextdaten in die SDB dem Monitor eine selektive Sicht auf die Daten der von ihm ausgewählten PID's in der FDB geöffnet werden.

Für die Bilddatenbank ergeben sich bei Übernahme der Lösung für die Mess- und Textdaten allerdings Probleme: Es muss geprüft werden, ob ein Im- und Export von Datensätzen in einer Größe von bis zu 250MB je Bilddatensatz für den Pseudonymisierungsdienst leistbar ist und ob nicht zudem eine zweite Instanz der Serversoftware lizenziert werden müsste.

4.1.5 Freigabe der Daten für die Forschungsdatenbank

Die Freigabe der Daten erfolgt nach Abschluss der Qualitätssicherung durch den Monitor. Mit der Freigabe sollen die MDAT mit dem öffentlichen Schlüssel der FDB verschlüsselt und dem nicht verschlüsselten PID zum PSD übermittelt werden, wo der PID durch ein PSN ersetzt wird. Die Daten werden nach Transformation des PID an die FDB übertragen, dort mit dem privaten Schlüssel der FDB entschlüsselt und mit dem PSN als Ordnungskriterium in die FDB eingestellt. Gleichzeitig werden die Kontextdaten in der SDB gelöscht bzw. die Sicht des Monitors auf die Kontextdaten in der FDB wieder aufgehoben. Nach Rückmeldung der erfolgreichen Übermittlung und Eintragung in die FDB werden die übertragenen Daten in der SDB gelöscht.

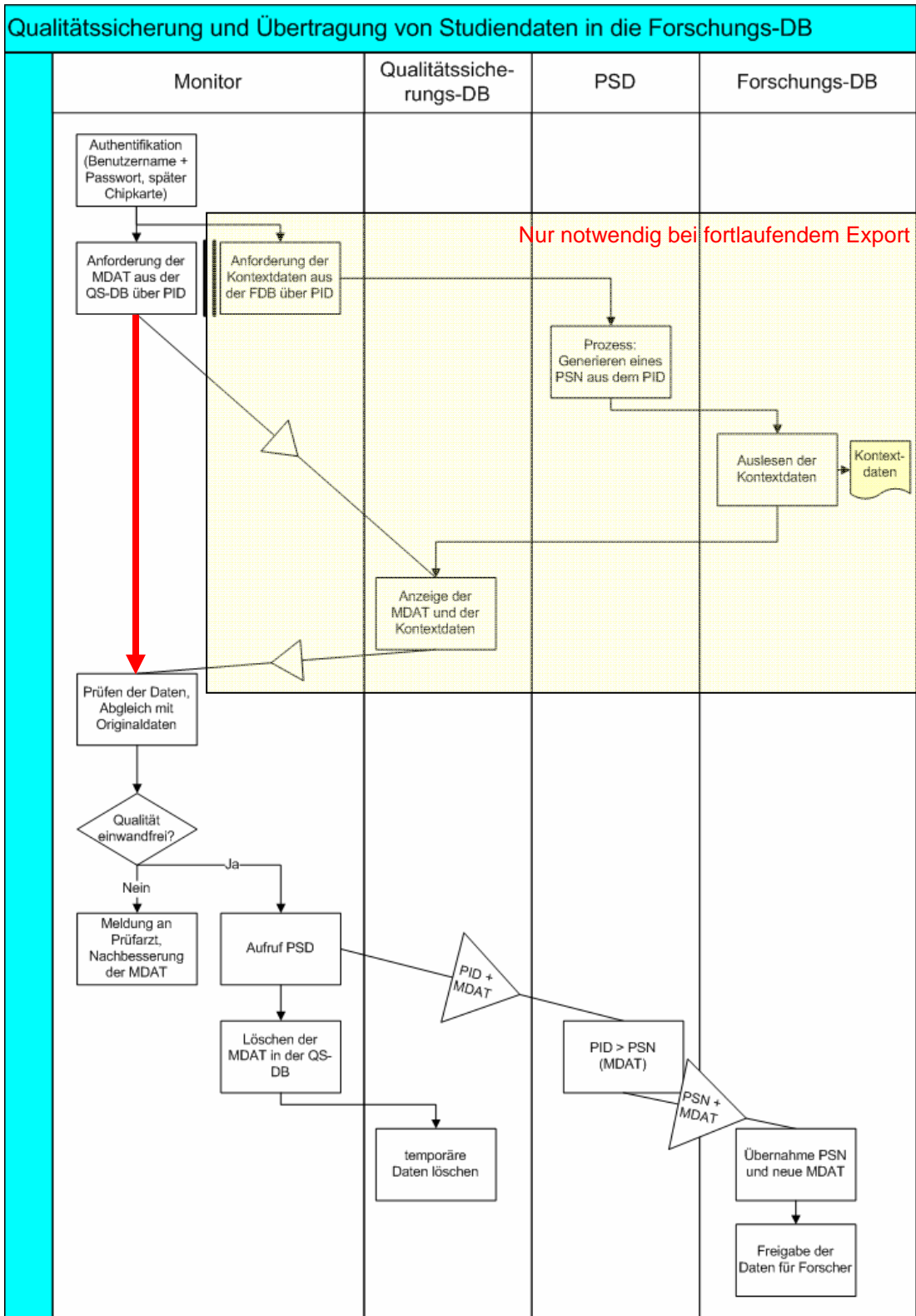


Abbildung 8: Ablaufdiagramm für den Prozess Qualitätssicherung. In dieser Darstellung wird ein fortlaufender Export in die Forschungsdatenbank vorgesehen (gelber Kasten). Dies ist beim Kompetenznetz AHF nicht notwendig – die Daten werden einmalig qualitätsgesichert nach Studienabschluss und dann in die FDB exportiert (= roter Weg).

4.1.6 Korrektur von Daten in der Forschungsdatenbank

Eine Korrektur der Daten in der Forschungsdatenbank ist im Kompetenznetz AHF nicht notwendig, da der Export der Daten in die FDB erst nach Abschluss der Studie nach Qualitätskontrolle durch den Monitor erfolgt (s. Abbildung 9, roter Pfeil).

Dennoch soll der ursprünglich vorgesehene Weg eines fortlaufenden Exports beschrieben werden (Abb. 9, gelber Kasten).

Im Rahmen der Analysen und statistischen Auswertungen der FDB kann bei einem Modell mit fortlaufendem Export erneut Korrekturbedarf sichtbar werden. Zur Bearbeitung wird folgendes Verfahren eingerichtet, das – abgesehen von den Tätigkeiten des Monitors – automatisiert ist und das einzige Verfahren darstellt, mit dem Korrekturen in der FDB vorgenommen werden können:

1. Die FDB hält ein web-Formular bereit, auf dem der Forscher den Datensatz mit seiner Korrekturanforderung hinterlegt. Die FDB ersetzt auf diesem Formular die $PSN_{Patient}^{18}$ durch die $PSN_{Patient}$ und ergänzt den Datensatz mit dem Code der dokumentierenden Stelle. Ist diese Stelle pseudonymisiert, wird auch hier die PSN_{Arzt} gegen die PSN_{Arzt} ausgetauscht.
2. Der Datensatz wird über den PSD an den Monitor übermittelt; der PSD transformiert das $PSN_{Patient}$ in den $PID_{Patient}$.
3. Der Monitor holt sich die Kontaktdaten der dokumentierenden Stelle von der Prüfartzliste (vgl. Ziff. 4.1.2.5).
4. Der Monitor klärt mit der dokumentierenden Stelle den Korrekturbedarf und erstellt auf einem web-Formular den Korrekturauftrag.
5. Der Korrekturauftrag wird über den PSD an die FDB gesandt und dort eingetragen. Die Korrektur wird durch das Audit Trail, das auch den Code des Monitors übernimmt, dokumentiert.

4.1.7 Zugriff der Forschung auf die Forschungsdatenbank

Forscher erhalten ein Zugriffsrecht auf die Daten, wenn ihr Forschungsansatz mit Definition der dafür benötigten Daten vom Ausschuss Datenschutz des KN bewilligt ist. Der Ausschuss Datenschutz leitet die Bewilligung an den Administrator der FDB weiter, der die Daten entsprechend der genehmigten Anforderung des Wissenschaftlers aus der FDB selektiert und exportiert. Ggf. kann dem Forscher über eine spezifische Datenbanksicht auch ein direkter Zugriff auf die Forschungsdatenbank ermöglicht werden.

¹⁸ Werden Daten aus der FDB dem Forscher überlassen, wird das PSN, das der FDB als Ordnungskriterium dient, kryptografisch in ein PSN2 transformiert. Vgl. Ziff. 4.1.7

Das PSN wird dabei erneut transformiert, wozu zwei verschiedene Verfahren eingesetzt werden:

- Ist im Forschungsantrag begründet, dass die Daten zu einem späteren Zeitpunkt eventuell depseudonymisiert werden sollen, um ausgewählte Patienten für eine neue Studie zu gewinnen, oder um sie über Forschungsergebnisse zu informieren, so wird das PSN mit einem symmetrischen Schlüssel, aber einem anderen als dem für die Pseudonymisierung verwendeten, oder mit anderem Startwert, in ein PSN2 chiffriert. Dieses Verfahren ist umkehrbar.
- Ist für später keine Depseudonymisierung geplant, wird das PSN für den Export in einem Einwegverfahren chiffriert oder durch eine Zufallszahl ersetzt.

Diese Leistung der Pseudonymisierung in der dritten Stufe kann von der FDB im Rahmen des Exports selbst geleistet werden. Es ist nicht erforderlich, dafür den Pseudonymisierungsdienst als unabhängigen Dritten einzuschalten, wie dies für die zweite Stufe entsprechend dem generischen Konzept festgelegt ist. Die gleiche Behandlung gilt für das PSN des Arztes.

4.1.8 Depseudonymisierung von Patientendaten

Die Depseudonymisierung ist zweistufig angelegt: Die erste Stufe wird - technisch gesehen - auf dem inversen Weg der Pseudonymisierung geleistet, durch die Transformation eines PSN_{Patient} in einen PID_{Patient} . In der zweiten Stufe werden die PID an die Patientenliste übersandt, um sie dort um die Identifikationsdaten zu ergänzen. Alternativ können sie auch den jeweils zuletzt behandelnden Kliniken zur Re-Identifikation des Patienten übersandt werden.

Beide Stufen können nur von autorisierten Personen nach einem strengen Regelwerk und nach Genehmigung eines Antrags durch den Ausschuss Datenschutz durchgeführt werden (s. Abbildung 9).

Bei der Depseudonymisierung sind drei Fälle zu unterscheiden:

1. Bei der Freigabe von Kontextdaten zur Qualitätssicherung für den Monitor (siehe Kapitel 4.1.4) wird nur die erste Stufe der Depseudonymisierung genutzt; sie ist als reine Maschinenfunktion ausgeprägt, die nur vom Monitor selbst oder besonders autorisierten Mitarbeitern der Forschungsdatenbank (z. B. Systembetreuer) angestoßen werden kann. Voraussetzung für die Bereitstellung von Kontextdaten ist die einmalige Genehmigung des Verfahrens der Qualitätssicherung durch den Ausschuss Datenschutz des KN AHF.
2. Wünscht ein Patient Auskunft über die in der Forschungsdatenbank über ihn gespeicherten Daten, so wendet er sich an den behandelnden Arzt oder eine andere Vertrauensperson. Dieser sendet die Anforderung an die Patientenliste. Diese sendet die Anweisung um Auskunftserteilung an den Pseudonymisierungsdienst. Die Anweisung wird dort in geeigneter Form geprüft und nach Transformation des PID in das PSN an die Forschungsdatenbank weitergeleitet.

Auf dem Rückweg erhält der Pseudonymisierungsdienst verschlüsselte medizinische Daten mit dem PSN, die er nach Transformation des PSN in den PID dem anfragenden Arzt übermittelt. Für den Arzt muss die Möglichkeit geschaffen werden, diese Daten zu entschlüsseln; dies setzt die Installation des Proxy von SIT, der Bestandteil der vom iAS im Auftrag des ISST geschaffenen Software für den PSD ist, voraus. Hierfür muss zumindest ein Softwarezertifikat nach X509.v3 zur Verfügung stehen.

Es soll geprüft werden, ob diese Aufgabe auch an einer Stelle, z. B. beim NR konzentriert werden kann – zumindest für die in das Register aufgenommenen Patienten – um die Zahl der Installationen solcher Features im Vorfeld der Einführung der eGK in Deutschland möglichst gering zu halten

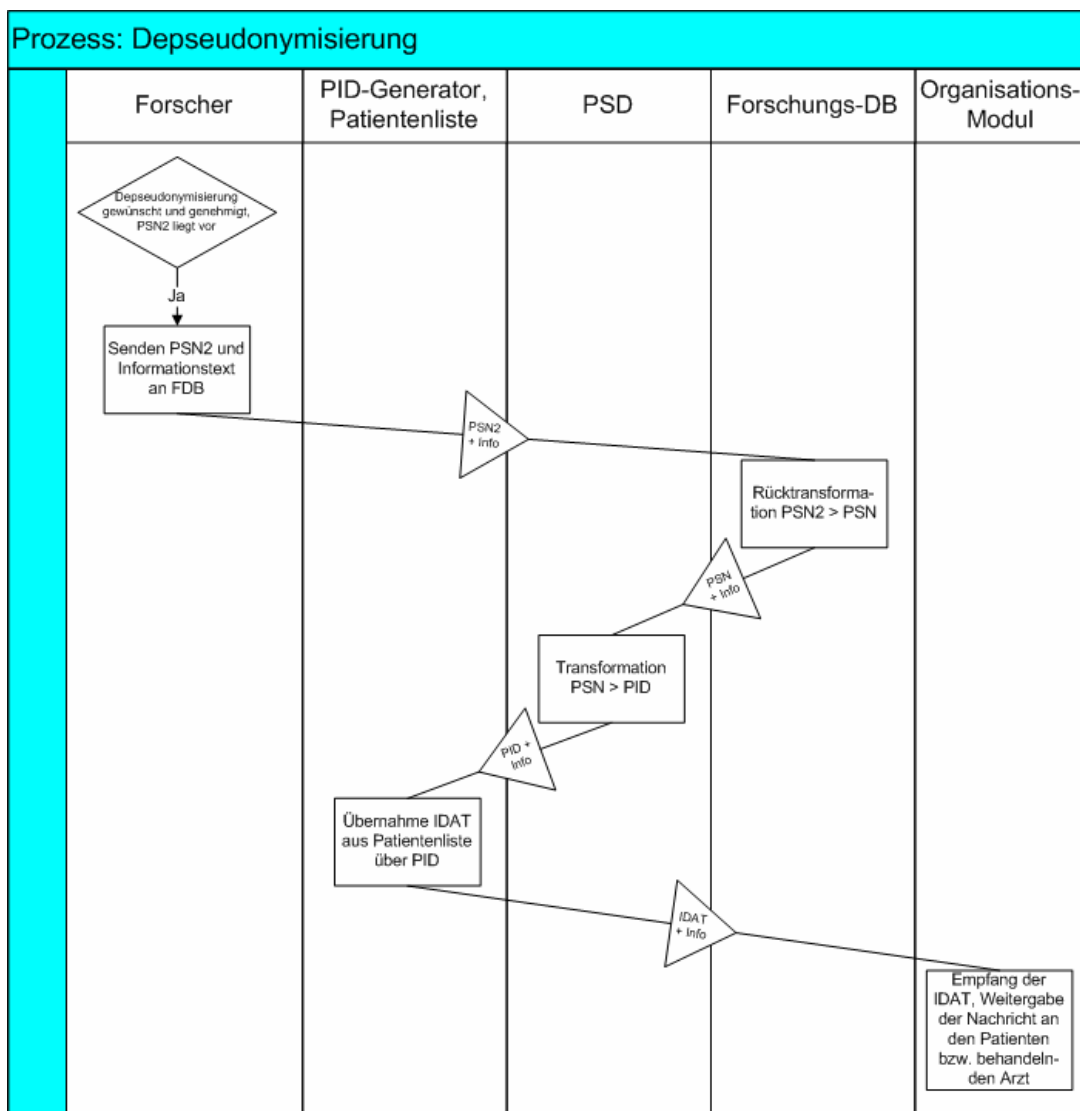


Abbildung 9: Ablaufdiagramm für den Prozess Depseudonymisierung. Es wird davon ausgegangen, dass der Forscher einen Patienten gefunden hat, der auf Grund seines Merkmalprofils von einer neuen Erkenntnis oder Behandlung profitieren könnte bzw. an einer neuen Studie teilnehmen soll und deshalb

mit einer entsprechenden Nachricht durch das Organisationsmodul oder durch den behandelnden Arzt angeschrieben wird (vgl. Fall 3).

3. Für jeden anderen Zweck, wie die Information eines Patienten über Forschungsergebnisse oder die Werbung für die Beteiligung an einer neuen Studie, ist die Depseudonymisierung in jedem Einzelfall von Antrag und Bewilligung durch den Ausschuss Datenschutz des KN AHF abhängig. Das Verfahren ist so einzurichten, dass es erst nach aktueller Prüfung der Genehmigung durch den Verantwortlichen manuell gestartet werden kann. Folgende Prozesse sind dafür möglich:
 - a) Der Forscher liefert eine Liste von $PSN_{Patient}$, die von der FDB in eine Liste von $PSN_{Patient}$ transformiert wird. Über den PSD wird sie in eine Liste von $PID_{Patient}$ transformiert. In dieser Form wird sie entweder an die Patientenliste übermittelt, welche die Kontaktdaten zusteuert und – entsprechend selektiert – an die zuständigen Prüfärzte weiterreicht, die ihrerseits die Patienten kontaktieren.
 - b) Die Patienten werden nach definierter Merkmalskombination, die vom Forscher vorgegeben wird, in der FDB ermittelt. Der weitere Weg entspricht Buchstabe a).

Szenarien, die eine **Depseudonymisierung** für die Zwecke der Forschung oder die Anwendung ihrer Ergebnisse begründen, sind für das KN AHF nach den spezifischen Aufgaben zu entwickeln und durch Regelwerke abzusichern.

4.2 Daten im Organisationsmodul

Im Folgenden werden die besonderen Bedingungen dargestellt, die für die Registerdatenbank des Organisationsmoduls gelten. Die hier beschriebenen Prozesse müssen überprüft werden, sobald die im Register zu speichernden Datensätze in ihrer Struktur definiert sind.

4.2.1 Aufbereitung der Altdaten

Im Dezember 2005 sind Datensätze von etwa 20.000 Patienten in der Personendatenbank des Registers gespeichert, für ca. 60 % der Patienten bestehen auch Diagnosen und/oder Leistungen beschreibende Datensätze in der Registerdatenbank¹⁹ Unter Ziffer 3.1.3 wurde darauf hingewiesen, dass hier an die Stelle der bisherigen Register-ID der Patientenidentifikator PID treten soll, der vom PID-Generator der Patientenliste erzeugt wird. Dazu werden die Identifikationsdaten der Patientendatenbank in einem Batchverfahren der Patientenliste zugeführt.

¹⁹ Die hier gewählten Bezeichnungen der Datenbanken entsprechen der Begriffswahl im Dokument „Führung der Datenbanken des Nationalen Registers für angeborene Herzfehler e.V.“. Die Personendatenbank des Registers soll künftig durch die der generischen Lösung entsprechende Patientenliste abgelöst werden, während in der Registerdatenbank die Register-ID gegen den vom PID-Generator der Patientenliste erzeugten Patientenidentifikator PID ausgetauscht wird. Der Inhalt der Registerdatenbank wird neu definiert.

Im Rahmen der Umstellung muss eine Konkordanzliste der Register-ID (alt) und der PID (neu) erstellt werden. Die Konkordanzliste wird zur Umstellung der Registerdatenbank genutzt, wo die Register-ID gegen den PID auszutauschen ist. Mit der Übernahme der Patienten des Bestandes in die neue Patientenliste wird die ursprüngliche Patientendatenbank des Registers gelöscht.

Die Patientenliste enthält den PID und ist so mit den Daten der Registerdatenbank verknüpfbar, wie es dem Dienstleistungsauftrag des Organisationsmoduls entspricht. Dagegen besteht keine Verknüpfbarkeit zu den Daten des KN in der FDB, wo die Daten unter dem Ordnungskriterium PSN organisiert sind.

Es ist vorgesehen, dass die Aufbereitung der Altdaten durch das Personal des Organisationsmoduls besorgt wird. Gegenwärtig fehlt die Analyse, inwieweit die Struktur der Altdaten mit den IDAT der Patientenliste und mit dem minimal data set (MDS) kompatibel ist. Nach der analytischen Aufarbeitung der Struktur der Altdaten wird empfohlen, den Datenbestand auch darauf hin zu überprüfen, welche Felder tatsächlich und mit welcher Häufigkeit besetzt sind. Auf der Basis dieser Kenntnisse ist die Strategie für die Aufarbeitung der Altdaten abschließend zu definieren.

4.2.2 Aufnahme eines neuen Patienten in das System

Patienten, die neu in das Register und/oder Studien aufgenommen werden, sollen nach Möglichkeit zuerst an das Organisationsmodul gemeldet und dort nach Plausibilitätsprüfung der Daten durch das Personal in die Patientenliste übernommen werden. Dieser Weg entspricht der aktuellen Übung bei der Meldung eines Patienten durch seine Eltern bzw. durch die eigene Meldung erwachsener Patienten, und wird auch künftig unter der Annahme empfohlen, dass so die Qualität der IDAT am besten gewährleistet wird.

Es besteht aber auch die Möglichkeit, dass die erste Meldung durch einen Prüfarzt bei der Erhebung von Studiendaten erfolgt.

Die telematische Lösung kann auf keinen Fall für Meldungen durch die Patienten bzw. ihre Eltern zugänglich gemacht werden, da Personen ohne Berechtigungsnachweis grundsätzlich kein Zugriff zum Server gestattet werden kann. Bei freiem Zugang zum Verfahren bestehen hohe Risiken, dass Daten auch in destruktiver Absicht eingegeben werden.

Die telematische Lösung wird, bezogen allein auf die IDAT, nach der Erstmeldung grundsätzlich für jede weitere Patientenidentifikation genutzt, die entweder über das RDE-System oder auch direkt zwischen den dokumentierenden Stellen, den Herzzentren und Kinderkardiologen, und der Patientenliste im Dialog erfolgt.

4.2.3 Liste der Identifikationsdaten

Die Tabelle zeigt die verwendeten Merkmale an. Der Begriff „Verwendung“ betrifft die logische Verknüpfung der Daten einer neuen Meldung mit dem Bestand zur Identifikation bereits erfasster Patientendaten. Die nachfolgende Tabelle zeigt die Klassifizierung der Merkmale (Gruppenbildung) und ihre Ausprägung

Bedeutung der Abkürzungen in der Spalte „Typ“ der nachfolgenden Tabelle		
Erstes Merkmal		
A	Alphanumerisch	
N	Numerisch	
Zweites Merkmal, mit dem vorausgehenden durch „/“ verknüpft		
M	Mandatory	Das Merkmal ist unverzichtbar; der Datensatz ist nur <u>mit</u> diesem Merkmal zulässig
M1	bedingt mandatory	Das Merkmal ist unverzichtbar, wenn ein in diesem Zusammenhang bezeichnetes Feld belegt ist.
O	Optional	freigestellt bei manueller Erfassung
O1	optional_1	freigestellt nur bei manueller Erfassung ohne Versichertenkarte (VK); bei Verwendung der VK oder Übernahme der Daten aus einem PVS- bzw. KIS-System muss dieses Merkmal belegt sein
O2	optional_2	freigestellt; bei Erfassung über die VK ist die in der VK gespeicherte Ausprägung des Merkmals zu übernehmen
Z	Zusatzinformation	Die Daten werden nicht für die Identifikation des Patienten im Bestand verwendet, sie sind in der Datenbank gespeichert, dienen aber ausschließlich zur Aufnahme des Kontakts

Alphanumerische Daten mit dem Kennzeichen mandatory und optional werden von den Algorithmen der Patientenliste in normierter Schreibweise aufbereitet und zusätzlich in zwei Schreibweisen phonetisiert²⁰. Die Regeln dazu sind in der Beschreibung des PID-Generators niedergelegt.

Heißt es bei der Verwendung „Zusatzinfo, keine Prüfung“, werden die Daten so wie eingegeben ohne Prüfung gespeichert.

Nr.	Merkmal	Typ	Länge in Bytes	Quelle / Kommentar zu optional / Verwendung
1.	Informationen zur Krankenversicherung			
1.1	KrankenKassenNummer	N / o1	7	VK // Prüfung auf Identität; fehlende Identität schließt Zuordnung zu Bestand nicht aus (z.B. Kassenwechsel), dann ist auch 1.2 nicht identisch)
1.2	VersichertenNummer	N / o1	6-12	VK // Prüfung auf Identität; fehlende Identität schließt Zuordnung zu Bestand nicht aus (z.B. Kassenwechsel, dann ist auch 1.1 nicht identisch)

²⁰ Kölner und Hannoveraner Phonetik
knahf_datenschutzkonzept_ver_1_24.doc Debold & Lux / CIOffice

Nr.	Merkmal	Typ	Länge in Bytes	Quelle / Kommentar zu optional / Verwendung
1.3	Versicherten-Nummer ²¹	A / o1	10	VK // Prüfung auf Identität; fehlende Identität schließt Zuordnung zu Bestand aus ; dies gilt nicht, wenn das Feld im Bestand leer ist (erste Aufnahme der neuen VNR). Die Felder 1 und 2 werden bei Übernahme der neuen Versichertennummer nicht belegt und können gelöscht werden.
2	Namen, Geburtsdatum, Geschlecht			
2.1	Titel	A / o2	2-15	VK, mehrere Titel sind durch Blank getrennt // Prüfung auf Identität; fehlende Identität nach manueller Erfassung schließt Zuordnung nicht aus
2.2	FamilienName	A / m	2-28	VK // mehrere Namensbestandteile werden bei der Aufbereitung in Einzelfelder gespeichert; Prüfung auf Identität und Ähnlichkeit; mindestens für ein Feld muss Übereinstimmung bestehen
2.3	NamensZusatz/ VorsatzWort	A / o2	2-15	VK / bei Erfassung ohne VK optional / Prüfung auf Identität; fehlende Identität nach manueller Erfassung schließt Zuordnung nicht aus
2.4	Geburtsname	A / M	2-28	
2.5	VorName	A / m	2-28	VK, mehrere Vornamen sind durch Bindestrich oder Blank getrennt // mehrere Vornamen werden bei der Aufbereitung in Einzelfelder gespeichert; Prüfung auf Identität und Ähnlichkeit ²² ; mindestens für ein Feld muss Übereinstimmung bestehen
2.6	GeburtsDatum	N / m	8	// Prüfung auf Identität
2.7	Geschlecht	N / m	1	// Prüfung auf Identität, Codierung 1=männlich, 2=weiblich, 3= nicht bekannt

²¹ mit der Gesundheitskarte wird eine neue Versichertennummer eingeführt. Diese ist lebenslang identisch, ändert sich also nicht bei Kassenwechsel. Die neue Versichertennummer besteht aus 20 oder 30 alphanumerischen und numerischen Zeichen.

Der Versicherte, der **Mitglied** ist, hat im ersten 10er-String die Versichertennummer, im zweiten 10er-String die Kassennummer und eine Prüfziffer. Es ist nur der **erste 10er String** zu übernehmen. Der Versicherte, der **Familienmitglied** ist, hat im ersten 10er String seine Versichertennummer, im zweiten 9er-String die Kassennummer, im dritten 11er-String die Versichertennummer des Mitglieds und eine Prüfziffer. Es ist nur der **erste 10er-String** zu übernehmen.

²² Unter Ähnlichkeit wird verstanden, dass zwischen einem phonetisierten Feld im Bestand und in der Eingabe Gleichheit besteht, während die nicht phonetisierten Felder des gleichen Merkmals Abweichungen aufweisen.

Nr.	Merkmal	Typ	Länge in Bytes	Quelle / Kommentar zu optional / Verwendung
3	Informationen Wohn- und Geburtsort			
3.1	Postleitzahl-WohnOrt	N / o1	4-7	VK // Prüfung auf Identität; fehlende Übereinstimmung schließt Zuordnung nicht aus (z.B. nach Umzug)
3.2	OrtsName-WohnOrt	A / o1	2-22	VK // mehrere Namensbestandteile durch Blank oder Sonderzeichen getrennt; Zusatzinfo, keine Prüfung bei Zuordnung
3.3	StraßenName & HausNummer WohnOrt	A / o1	2-28	VK // StraßenName von HausNummer durch Blank getrennt; Zusatzinfo, keine Prüfung bei Zuordnung
3.4	TelefonNummerWohnOrt	N / o	8-30	Manuelle Erfassung / optional / Zusatzinfo, keine Prüfung bei Zuordnung
3.5	FaxNummerWohnOrt	N / o	8-30	Manuelle Erfassung / optional / Zusatzinfo, keine Prüfung bei Zuordnung
3.6	eMailAdresseWohnOrt	A / o	8-40	Manuelle Erfassung / optional / Zusatzinfo, keine Prüfung bei Zuordnung
3.7	Geburtsland Deutschland	A / o	2-22	Manuelle Erfassung / optional / Zusatzinfo, keine Prüfung bei Zuordnung; wenn ja, dann 3.8-3.9
3.8	PostleitzahlGeburtsOrt	N / o	4-7	Manuelle Erfassung / optional / Prüfung auf Identität und Ähnlichkeit; fehlende Identität nach manueller Erfassung schließt Zuordnung nicht aus
3.9	OrtsNameGeburtsOrt	A / o	2-22	Manuelle Erfassung / optional / mehrere Namensbestandteile durch Blank oder Sonderzeichen getrennt; Prüfung auf Identität und Ähnlichkeit; fehlende Identität nach manueller Erfassung schließt Zuordnung nicht aus
4	Teilnahme an Studien			
4.1	Studie n	A / o	5-40	Manuelle Erfassung / optional / Zusatzinfo, keine Prüfung bei Zuordnung; Merkmal kann mehrfach (maximal vierfach) auftreten.
4.1.1	Art der Studie	A / o	5-40	Manuelle Erfassung / optional / Zusatzinfo, keine Prüfung bei Zuordnung
4.1.2	Beginn- und Endedatum	N / o	16	Manuelle Erfassung / optional / Zusatzinfo, keine Prüfung bei Zuordnung

Nr.	Merkmal	Typ	Länge in Bytes	Quelle / Kommentar zu optional / Verwendung
5.	Kontaktperson für Patienten unter 18 Jahren und entmündigte Patienten			
	Die Besetzung der Merkmalsgruppen 5 und 6 ist optional; wird aber das Feld 5.2 belegt, gilt die Erfassungslogik für alle Felder entsprechend der Beschreibung.			
5.1	KontaktPersonTitel	A / o2	2-15	VK, mehrere Titel sind durch Blank getrennt / bei Erfassung ohne VK optional / Zusatzinformation ohne Prüfung
5.2	KontaktPersonVorName	A / m	1-28	VK, mehrere Vornamen sind durch Bindestrich oder Blank getrennt // Zusatzinformation ohne Prüfung, Feld muss besetzt sein, wenn der Patient <18 Jahre alt ist. In anderen Fällen kann es besetzt sein, wenn der Patient einer Betreuung bedarf (ist nicht Gegenstand einer Prüfung)
5.3	KontaktPersonNamensZusatz/ Vorsatz-Wort	A / o2	1-15	VK / bei Erfassung ohne VK optional / Zusatzinformation ohne Prüfung
5.4	KontaktPersonFamilienName	A / m	2-28	VK // mehrere Namensbestandteile werden bei der Aufbereitung in Einzelfelder gespeichert; Zusatzinformation ohne Prüfung, Feld muss jedoch besetzt sein, wenn Feld 5.2 besetzt
6	KontaktPersonWohnort			
6.1	KontaktPersonPostleitzahlWohnOrt	N / o1	4-7	VK // Zusatzinformation ohne Prüfung
6.2	KontaktPersonOrtsNameWohnOrt	A / o1	2-22	VK // Zusatzinformation ohne Prüfung
6.3	KontaktPersonStraßenName & HausNummerWohnOrt	A / o1	2-28	VK // Zusatzinformation ohne Prüfung
6.4	KontaktPersonTelefonNummerWohnOrt	N / o	8-30	Manuelle Erfassung / optional / Zusatzinformation ohne Prüfung
6.5	KontaktPersonFaxNummerWohnOrt	N / o	8-30	Manuelle Erfassung / optional / Zusatzinformation ohne Prüfung Zusatzinfo,

Nr.	Merkmal	Typ	Länge in Bytes	Quelle / Kommentar zu optional / Verwendung
6.6	KontaktPersonenMailingadresseWohnort	A / o	8-40	Manuelle Erfassung / optional / Zusatzinfo, keine Prüfung bei Zuordnung
7	Datenquelle			
7.1	Sicherheit der Datenquelle	Binär oder num/ m	1	// Nur Versichertenkarte gilt als sicher, jede andere Quelle als unsicher; sichere Daten in Bestand und Eingabe werden nur auf Gleichheit, nicht auf Ähnlichkeit geprüft.
7.2	Prüfarzt-ID ²³ = AID	A / m	8	ID des für die Meldung verantwortlichen Arztes der meldenden Klinik bzw. Arztpraxis // Zusatzinfo, keine Prüfung bei Zuordnung
7.3	Datum/Uhrzeit der Anfrage / Meldung	N / m	12	Wird von der Patientenliste im Prozess generiert/ / Zusatzinfo, keine Prüfung bei Zuordnung
8	PID	A / m	8	Patientenidentifikator, vom PID-Generator der Patientenliste generiert

²³ Logisch parallel zur Patientenliste wird eine Arztliste und eine Liste der medizinischen Einrichtungen geführt. Die Listen enthalten die Kontaktdaten sowie die Kennung der Datenobjekte. Die **Kennung des** Prüfarztes AID als des für die Dokumentation der Daten eines Patienten verantwortlichen Arztes wird von der Arztliste generiert, und zwar in einem Prozess der Anmeldung des Arztes am System.

Als **Kennung der medizinischen Einrichtung (EID)** wird das Institutionenkennzeichen (IK) verwendet; es muss in einem Prozess der Anmeldung der Einrichtung im System eingegeben werden.

4.2.4 Minimal Data Set

Das minimal data set basiert auf den soziodemographischen und medizinischen Daten, die vom NR AHF seit Beginn seiner Tätigkeit erhoben worden sind. Im Dezember 2005 wurde der Datensatz überarbeitet und in der im Folgenden dokumentierten Form festgelegt.

Nr.	Merkmal	Typ	Länge in Bytes	Kommentar / Verwendung
1.	Demographische Daten			
1.1	PID	A / M	8	Vergabe durch Patientenliste
1.2	Melddatum	N / O	14	Tag (2).Monat (2).Jahr (4)
1.2	Gesunder Proband	binär/M	1	
1.3	Teilnahme am NR	binär/M	1	
1.4	Geschlecht	N / M	1	Männlich, weiblich, Intersexualität, nicht bekannt
1.5	GeburtsDatum	N/M	6	Monat (2), Jahr (4)
1.6	StaatsAngehörigkeit	binär/M	1	deutsch/sonstige
1.7	GeburtsLand Deutschland	binä/M	1	Ja/nein, wenn ja, dann 1.8-1.10
1.8	GeburtsOrtPLZ	N/O	5	Bei der Auswertung werden Felder mit weniger als drei Betroffenen nicht veröffentlicht (k-Anonymität mit K=3)
1.9	GeburtsOrt	A/O	22	Bei der Auswertung werden Felder mit weniger als drei Betroffenen nicht veröffentlicht (k-Anonymität mit K=3)
1.10	GeburtsBundesland	A/M		nach Auswahlliste

Nr.	Merkmal	Typ	Länge in Bytes	Kommentar / Verwendung
2.	Geburtsdaten (nur ab Geburtsjahr 2006 Pflicht)			
2.1	WohnOrtbeiGeburtPLZ	N/O	5	Bei der Auswertung werden Felder mit weniger als drei Betroffenen nicht veröffentlicht (k-Anonymität mit K=3)
2.2	WohnOrtbeiGeburt	A/O	22	Bei der Auswertung werden Felder mit weniger als drei Betroffenen nicht veröffentlicht (k-Anonymität mit K=3)
2.3	BundeslandbeiGeburt	A/M		nach Auswahlliste
2.4	AlterMutterbeiGeburt	N/M	2	Alter in Jahren / nicht bekannt
2.5	GeburtsGewicht	N/M	4	Gewicht in g / nicht bekannt
2.6	GestationsAlter	N/M	2	Wochen / nicht bekannt
2.7	Mehrlings-Schwangerschaft	N/M	1	ja / nein / unbekannt
2.8	PEKDurchgeführt ?	N/M	1	Ja / nein / unbekannt
2.9	Wenn 2.8= ja: AHF diagnostiziert?	N/M1	1	ja/nein/unbekannt
2.10	Wenn 2.8= ja: Identität Diagnosen prä und post partum	N/M1	1	ja/nein/unbekannt
3.	Medizinische Daten			
3.1	Kardiovaskuläre Diagnosen			
3.2	Hauptdiagnose (angeboren)			
3.3	Diagnose	A/M	?	nach Auswahlliste 1
3.4	EPC-Code	N/M	?	nach Auswahlliste 1
3.5	ICD-10/ICD10-additional		10	Keine Eingabe, nur Datenbankanzeige
3.6	DatumDiagnosestellung	N/M	50	Tag (2).Monat (2).Jahr (4); nicht bekannt
3.7	Nebendiagnosen (angeboren)			
3.8	Diagnose	A/O	?	nach Auswahlliste 1
3.9	EPC-Code	N/M1	?	nach Auswahlliste 1

3.10	ICD-10/ICD10-additional		10	Keine Eingabe, nur Datenbankanzeige
3.11	DatumDiagnosestellung	N/M1	50	Tag (2).Monat (2).Jahr (4); nicht bekannt
3.12	Nebendiagnosen (erworben)			
3.8	Diagnose	A/O	?	nach Auswahlliste 2
3.9	EPC-Code	N/M1	?	nach Auswahlliste 2
3.10	ICD-10/ICD10-additional		10	Keine Eingabe, nur Datenbankanzeige
3.11	DatumDiagnosestellung	N/M1	50	Tag (2).Monat (2).Jahr (4); nicht bekannt
3.12	Hereditäre, fetale, neonatale und extrakardiale Diagnosen			
3.13	Hereditäre, fetale und neonatale Diagnosen			
3.14	Diagnose	A/O	?	nach Auswahlliste 3
3.15	EPC-Code	N/M1	?	nach Auswahlliste 3
3.16	ICD-10/ICD10-additional		10	Keine Eingabe, nur Datenbankanzeige
3.17	DatumDiagnosestellung	N/M1	50	Tag (2).Monat (2).Jahr (4); nicht bekannt
3.18	Extrakardiale Diagnosen			
3.19	Diagnose	A/O	?	nach Auswahlliste 4
3.20	EPC-Code	N/M1	?	nach Auswahlliste 4
3.21	ICD-10/ICD10-additional		10	Keine Eingabe, nur Datenbankanzeige
3.22	DatumDiagnosestellung	N/M1	50	Tag (2).Monat (2).Jahr (4); nicht bekannt
3.23	Kardiale Operationen und Interventionen			
3.24	Kardiale Operationen			
3.25	Operation	A/O	?	nach Auswahlliste 5
3.26	EPC-Code	N/M1	?	nach Auswahlliste 5
3.27	DatumOperation	N/M1	50	Tag (2).Monat (2).Jahr (4); nicht bekannt

3.28	Kardiale Intervention			
3.29	Intervention	A/O	?	nach Auswahlliste 6
3.30	EPC-Code	N/M1	?	nach Auswahlliste 6
3.31	DatumIntervention	N/M1	50	Tag (2).Monat (2).Jahr (4); nicht bekannt
3.32	Symptome, Risikofaktoren, Komplikationen und diagnostische Maßnahmen			
3.33	Symptome und Risikofaktoren			
3.34	Symptom/Risikofaktor	A/O	?	nach Auswahlliste 7
3.35	EPC-Code	N/M1	?	nach Auswahlliste 7
3.36	ICD-10/ICD10-additional		10	Keine Eingabe, nur Datenbankanzeige
3.37	DatumFeststellung	N/M1	50	Tag (2).Monat (2).Jahr (4); nicht bekannt
3.38	Komplikation bei Operation/Intervention			
3.39	Komplikation	A/O	?	nach Auswahlliste 8
3.40	EPC-Code	N/M1	?	nach Auswahlliste 8
3.41	ICD-10/ICD10-additional		10	Keine Eingabe, nur Datenbankanzeige
3.42	DatumFeststellung	N/M1	50	Tag (2).Monat (2).Jahr (4); nicht bekannt
3.43	Diagnostische Maßnahmen			
3.44	Maßnahme	A/O	?	nach Auswahlliste 9
3.45	EPC-Code	N/M1	?	nach Auswahlliste 9
3.46	ICD-10/ICD10-additional		10	Keine Eingabe, nur Datenbankanzeige
3.47	DatumMaßnahme	N/M1	50	Tag (2).Monat (2).Jahr (4); nicht bekannt

4.2.5 Meldung der Studienteilnehmer an das Organisationsmodul

Werden Patienten neu für eine Studie gewonnen und schließlich aufgenommen, soll dies an das Organisationsmodul gemeldet werden. Dies gilt nur für Patienten, die der Aufnahme in das Register früher schon zugestimmt haben oder dies aktuell tun. Für Patienten-

ten, für die dies zutrifft, wird im Rahmen der Meldung an die SDB über das RDE-System die Aufnahme in die PL und in die Studie automatisch besorgt.

4.2.5.1 Vorgehen beim Update der Registerdatenbank

Der Datenmanager des RDE-Systems startet den Update-Prozess durch Zugriff auf das Export-Tool des RDE-Systems. Über das Feld „Teilnahme am Nationalen Register“ im MDS werden nur die Datensätze selektiert, bei denen eine Zustimmung zur Aufnahme im Nationalen Register vorliegt. Das Feld „Teilnahme am Register“ ist ein Pflichtfeld.

Die Exportdaten (nur MDS und PID) werden an den Datenmanager des NR gesendet - dieser erhält eine Nachricht über den erfolgreichen Export. Der Datenmanager des NR prüft die Daten und importiert sie ins NR. Ist der Datensatz bereits im NR vorhanden, wird der alte Datensatz versioniert. Der Prozess wird durch eine Rückmeldung beendet. Abbildung 10 stellt diesen Prozess in Form eines UML Sequenzdiagrammes dar.

Sequenzdiagramm: Datenexport RDE-NR

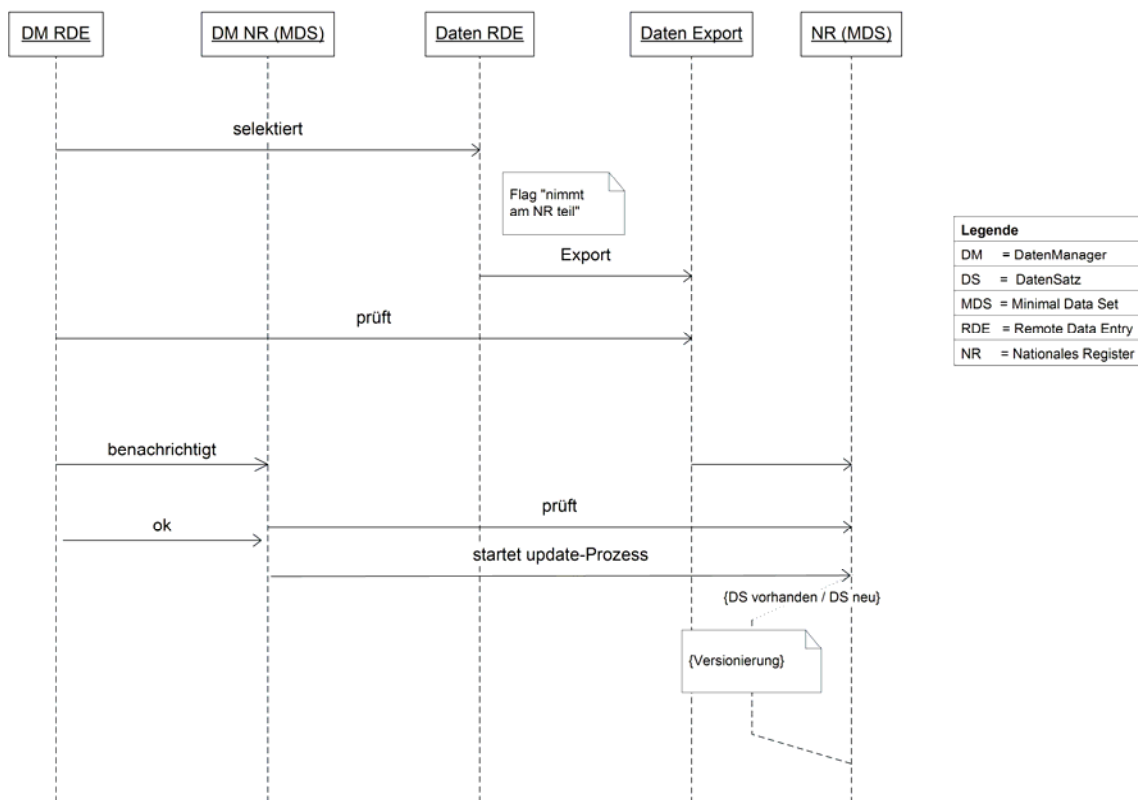


Abbildung 10: Ablaufdiagramm für den Prozess des Datenexports aus der Studiendatenbank (RDE) in das Nationale Register (NR): Über das Feld „Teilnahme“ ist sichergestellt, dass nur Datensätze aus dem RDE exportiert werden, bei dem die Zustimmung zur Teilnahme im NR vorliegt bzw. eine Einverständniserklärung zur Teilnahme an der Prävalenzstudie. Vorhandene Datensätze im Register werden versioniert (nicht gelöscht).

4.2.5.2 Rekrutierung von Patienten für neue Studien

Das Organisationsmodul enthält eine Rekrutierungsfunktion sowohl für Epidemiologische Studien als auch für klinische Studien. Soweit die Zustimmung des Patienten vorliegt, kann er angeschrieben werden, ob er an neue Studien teilnehmen möchte.

Dazu werden im NR interessante Fälle selektiert (MDS). Der zugehörige PID wird an den IDAT-Datenmanager weitergegeben, der für die Anschreiben zur Kontaktaufnahme die Adressdaten der Patienten selektiert und einen Serienbrief erzeugt.

Ansonsten erfolgen anonymisierte statische Auswertungen beispielsweise zur Prävalenz von AHF regionalisiert, jedoch nicht personenbezogen.

4.2.5.3 Datenpflege im Organisationsmodul

Im Organisationsmodul ist die Aktualisierung der Daten in der Patientenliste (Adress- und Namensänderungen) und in der medizinischen Datenbank in der Weise vorgesehen, dass das Organisationsmodul periodisch mit den Eltern der Patienten und später mit den Patienten selbst in Kontakt tritt und um Angaben auf den Erhebungsbögen bittet.

Dies ist ein außerordentlich aufwendiges Verfahren, das deshalb durch teilautomatisierte Prozesse der Datenpflege ergänzt bzw. ersetzt werden soll. Möglich ist dies bei der Aufnahme von Patienten in eine Studie und bei der nachfolgenden Erhebung medizinischer Daten.

4.2.5.4 Pflege der Daten der Patientenliste

Die Speicherung der IDAT in der Patientenliste ist in der Weise organisiert, dass nach der Anmeldung bei späteren Meldungen bzw. Anfragen zur Patientenidentifikation Änderungen des Inhalts einzelner Felder gespeichert werden.

Die Patientenliste ist daher immer auf dem neuesten Stand, ohne dass es dazu gesonderter Maßnahmen bedarf, soweit Patienten in Studien aufgenommen sind und periodisch Meldungen medizinischer Daten erfolgen. Die Kontaktaufnahme ist daher mit allen Patienten möglich, unabhängig davon, ob ihre Daten nur im Register geführt werden oder ob sie an Studien teilnehmen, ohne in der Registerdatenbank verzeichnet zu sein. Für Patienten ohne Studienbeteiligung muss das Register selbst die Aktualisierung der Daten organisieren.

4.2.5.5 Pflege der Registerdatenbank

Die Fortschreibung der Daten des „minimal data set“ der Registerdatenbank (RDB), die zur Kennzeichnung des Gesundheitszustands, der erfolgten Eingriffe und der sozialen Lage des Patienten dienen, soll aus den Erhebungen für die Forschungsdatenbank gewonnen und automatisch in die RDB übertragen werden. Dies gilt nur für Patienten, die an Studien beteiligt sind.

Bei der Strukturierung der Datenerhebung für die Studien werden die Daten, die zur Aktualisierung der Registerdatenbank dienen, in einem gesonderten Abschnitt des web-

Formular-Sets berücksichtigt. Diese Daten werden nach Abschluss der Qualitätssicherung automatisch in die Registerdatenbank übertragen. Die RDB wird in Berlin geführt

Für Patienten ohne Studienbeteiligung muss das Register selbst die Daten zur Aktualisierung der RDB beschaffen.

4.3 Text- und Messdaten für die Forschungsdatenbank – Zusammenfassung

Das allgemeine Ablaufmodell (Kapitel 4.1.1 bis 4.1.8) gilt für die in Texten und Zahlen gefassten Daten über Diagnosen, Befunde und Leistungen. Das Ablaufmodell gilt auch für Bilddaten, für die gesonderte Datenformate gelten. Es berücksichtigt aber nicht die zusätzlichen Maßnahmen, die dort für die Behandlung von Patienten identifizierenden Daten getroffen werden müssen (vgl. Kapitel 4.4). Kurz zusammengefasst gelten folgende Prozessschritte:

1. Identifikation des Patienten in der Patientenliste und Generierung bzw. Übermittlung des PID, ausgeführt vom Personal des Organisationsmoduls im Dialog mit der Patientenliste oder im Rahmen Erhebung von Studiendaten mit Hilfe des RDE-Systems;
2. Erfassung der medizinischen und sonstigen Erhebungsdaten für Studien mit dem PID und Übermittlung an die SDB mit Hilfe des RDE-Systems durch den Prüfarzt;
3. Qualitätssicherung nach den Vorgaben der Studienprotokolle, ausgeführt durch die Monitore, ggf. im Dialog mit dem Prüfarzt;
4. Freigabe der qualitätsgesicherten Daten durch den Monitor, der damit folgende automatisierte Prozesse auslöst:
 - a. Übertragung der für die RDB bestimmten Daten mit dem PID als Ordnungskriterium an diese,
 - b. Verschlüsselung der nach a) verbliebenen MDAT mit dem öffentlichen Schlüssel der FDB und Versand der Nachricht an den PSD,
 - c. Transformation des $PID_{Patient}$ in das $PSN_{Patient}$ und (ggf.) des PID_{Arzt} in das PSN_{Arzt} durch den PSD und Weiterleitung an die FDB,
 - d. Entschlüsselung der MDAT mit dem privaten Schlüssel der FDB und Einstellen der Daten in die FDB.

Nach diesen Prozessschritten stehen die Daten in der FDB durch Pseudonymisierung gesichert für die Nutzung zur Verfügung. Im Einzelfall können in der FDB Daten, durch einen Korrekturauftrag des Monitors und durch das Audit Trial dokumentiert, modifiziert werden.

Es besteht keine Möglichkeit, Daten aus der Forschungsdatenbank auf Patienten zu beziehen, außer durch die Einschaltung des zentralen Pseudonymisierungsdienstes. Zur weiteren Nutzung gelten folgende Prozessschritte:

5. Bereitstellung der Daten für die Forschung nach Antrag und Bewilligung durch selektiven Export der Daten mit kryptografischer Transformation der $PSN_{Patient}$ und PSN_{Arzt} in die $PSN2_{Patient}$ und $PSN2_{Arzt}$, ein automatisierter Prozess beim Export der Daten.
6. Depseudonymisierung ausgewählter Datensätze oder Pseudonyme in einem streng kontrollierten Verfahren nach Antrag und Bewilligung nach Kapitel 4.1.8.

4.4 Bilddaten für die Forschungsdatenbank

Für die Erhebung und Bereitstellung von Bilddaten im Kompetenznetz gilt, wie oben erwähnt, ebenfalls das allgemeine Ablaufmodell mit nur geringfügigen Modifikationen. Zusätzlich müssen folgende Besonderheiten beachtet werden:

Generell enthalten vor allem Schichtbilddaten Informationen, aus denen mit Hilfe moderner dreidimensionaler Rekonstruktionsverfahren morphologische Informationen über einen Patienten rekonstruiert werden können; so kann z. B. das Gesicht einer Person aus einer Computertomographie des Schädels erzeugt werden. Dies birgt die Gefahr, dass trotz Anonymisierung oder Pseudonymisierung und der Löschung der identifizierenden Daten aus dem DICOM²⁴-Header die Möglichkeit besteht, solche Rekonstruktionen mit biometrischen Daten aus anderen Quellen abzugleichen und so den Patienten zu identifizieren.

In den bisher geplanten Querschnittsprojekten 2 (MRT) und 3 (Tissue Doppler) werden Bilddaten vom Herzen erhoben. Dabei entsteht kein Informationspotential, das eine Re-Identifikation der Patienten unterstützen könnte. Gleichwohl muss dieses Problem, dass derartig informationstragende Daten entstehen können, bei der Beantragung und Genehmigung von Studien geprüft werden.

Eine weitere Besonderheit betrifft das sog. „Einbrennen“ von Patienten identifizierenden Daten in das Bildmaterial selbst. Solche Daten finden sich vor allem auf gescannten Röntgenbildern oder auch in Datensätzen aus Ultraschallgeräten. Hier ist ein nachträgliches Löschen der Daten, z. B. durch eine (semi-)automatisierte „Schwärzung“ der betroffenen Bereiche, erforderlich. Da dieser Vorgang zum Teil sehr kompliziert, in bestimmten Datenformaten sogar kaum zu lösen ist, muss bereits im Vorfeld einer Studie geklärt werden, welche Geräte für die Datenerhebung eingesetzt werden sollen, um ihre spezifischen Eigenschaften prüfen und entsprechende Löschroutinen implementieren zu können. Alternativ muss das Einbrennen der Daten von vornherein verhindert werden, indem die identifizierenden Daten vor der Untersuchung durch einen vom Prüfarzt angeforderten PID ersetzt werden.

²⁴ DICOM: *Digital Imaging and Communications in Medicine*; Format für Schnittbilddaten, welches vom *American College of Radiology (ACR)* und der *National Electrical Manufacturers Association (NEMA)* als Kommunikationsschnittstelle zwischen bildgebenden Systemen entwickelt wurde und seit 1985 in verschiedenen Versionen den de-facto-Standard darstellt. Das Format besteht aus einem Header mit insgesamt 584 Attributen - welche neben Patienten- und Untersuchungsdaten auch Informationen über das verwendete bildgebende Gerät enthalten – und den eigentlichen Bilddaten.

4.4.1 Erfassung und Auswertung der Bilddaten

In Ergänzung zu dem unter Kapitel 4.1 vorgestellten allgemeinen Ablaufmodell werden hier die Erfassungsprozeduren für die Bilddaten in den Querschnittsprojekten QP2 und QP3 erläutert und es wird auf Besonderheiten des Datenmaterials eingegangen.

4.4.1.1 MRT-Projekt

In dem Querschnittsprojekt 2 des Kompetenznetzes werden Magnet-Resonanz-Tomographien (MRT) erstellt. Bei jedem Patienten werden dabei mehrere Untersuchungen in definierten Abständen nach einem definierten Untersuchungsprotokoll durchgeführt. Dabei entstehen relativ große Datensätze mit sehr vielen Einzelbildern, welche selbst jedoch keine Patienten-identifizierenden Daten tragen. Eine selektive Schwärzung bestimmter Bereiche ist in diesen Fällen nicht erforderlich.

Die Auswertung der MRT-Datensätze erfolgt an zwei Studienzentren (Bad Oeynhausen und Berlin) durch die Anwendung einer speziellen Auswertungssoftware. Zur Minimierung der Interobservervariabilität soll die Auswertung von beiden Zentren in einem vorgeschalteten Qualitätssicherungsprozess parallel vorgenommen und später in einer Telekonferenz abgeglichen werden. Dabei entsteht aus den Auswertungsergebnissen (Messdaten) ein weiterer Teildatensatz, der zunächst in die SDB und später in die FDB übertragen wird.

4.4.1.2 Tissue-Doppler-Projekt

Dieses Querschnittsprojekt 3 dient, wie das QP2, der nicht-invasiven Funktionsanalyse. Dazu werden verschiedene Formen der Ultraschalldiagnostik angewandt und kombinierte Datensätze erzeugt (M-Mode- und B-Mode-Bilder, B-Mode-Loops und Tissue-Doppler-Daten). Bisher wird für die Datenerfassung nur ein Gerätetyp eines bestimmten Herstellers eingesetzt. Die generierten Datensätze enthalten dabei im Bildmaterial selbst Daten, welche Patienten, Institutionen und Geräte identifizieren und die für die Aufnahme in die Forschungsdatenbank geschwärzt werden müssten. Falls dies im Nachhinein auf Grund der Komplexität der Datensätze technisch nicht möglich wäre, müsste bei der Untersuchung von vornherein eine PID angefordert und vergeben werden. Mit den Herstellern muss dafür eine Änderung ihrer Software ausgehandelt werden.

4.4.2 Qualitätssicherung und Datenfreigabe

Der Prozess der Qualitätssicherung der Bilddaten durch den Monitor verläuft analog zu 4.1.4. Die technische Qualität der Daten kann vom Monitor nicht geprüft werden, sondern muss vom jeweiligen Projektleiter gewährleistet werden, indem er sie mit den in den Untersuchungsprotokollen definierten Anforderungen abgleicht. Daraufhin kann die Freigabe erfolgen und der Transfer in die Forschungsbilddatenbank ausgelöst werden.

4.5 Daten im Modul zur Prävalenzerhebung

In diesem Abschnitt wird darzulegen sein, welche Prozesse der Erzeugung, Meldung und Weiterverarbeitung der Daten im Modul zur Prävalenzerhebung dem allgemeinen Ablaufmodell nach Kapitel 4.1 folgen, was weit überwiegend der Fall sein wird. Notwendige Abweichungen davon, z. B. die durchgehende Anonymisierung der Daten in der FDB, werden festzustellen und zu begründen sein. Voraussetzung für die Bearbeitung ist die Entwicklung konkreter Ziele und Aufgaben für das Modul und ihre Operationalisierung.

4.6 Daten im Versorgungsmodul

Die Datenspeicherung und –verarbeitung im Versorgungsmodul (VM) unterscheiden sich grundsätzlich von den anderen Leistungsmodulen des NR und des KN AHF: Es werden Patientenakten angelegt, welche mittel- und langfristig die Krankheits- und Behandlungsgeschichte von Patienten mit angeborenen Herzfehlern aufzeigen. Im Prinzip wird dieses Modul die Leistungen liefern, die mit der Einführung der Patientenakte auf der Basis der elektronischen Gesundheitskarte (eGK) geplant werden.

Der wesentliche Unterschied zur allgemeinen Vorstellung von der Patientenakte besteht darin, dass hier nicht auf die (technische) Vollständigkeit der Behandlungsgeschichte abgestellt wird, sondern dass die Daten durch ein periodisches Update so selektiert und transformiert werden sollen, dass sie dem behandelnden Arzt die Informationen bereitstellen, die für eine jeweils aktuelle Beurteilung des Gesundheitszustandes und des Behandlungsbedarfs des Patienten geeignet sind. Das heißt, dass fachärztliche Bearbeitung der angesammelten Informationen die oft geringe Halbwertszeit von Behandlungsdaten berücksichtigt und Redundanzen ausmerzt, um so die Informationsmenge auf ein Maß zu reduzieren, das vom behandelnden Arzt faktisch auch wahrgenommen werden kann.

Dieses Konzept ist durchaus als Gegenmodell zu den überwiegend informationstechnologisch getriggerten Vorstellungen über eine verteilte Patientenakte zu verstehen, die heute die Szene beherrschen, und soll einen Beitrag zu der komplexen Fragestellung liefern, wie die neue Verfügbarkeit von Information auch zu einem faktischen Nutzen für den Medizinbetrieb gebracht werden kann.

Die Erhebung, Bearbeitung und Bereitstellung der Daten des VM unterscheidet sich so erheblich von der Bereitstellung der Forschungsdaten, dass, wenngleich aus der Sicht des Datenschutzes die selben Instrumente eingesetzt werden, der überwiegende Teil der Prozesse ganz neu entwickelt und gestaltet werden muss. Auch hier ist die Voraussetzung für die Bearbeitung die Entwicklung konkreter Ziele und Aufgaben für das Modul und ihre Operationalisierung.

5 Zentrale Dienste

In diesem Kapitel werden die zentralen Dienste aus der Sicht der Projektorganisation und der datenschutzrechtlichen Anforderungen an ihre Verfassung und den Standort dargestellt. Ihre Funktion wurde bereits im Zusammenhang mit dem allgemeinen Ab-

laufmodell in Kapitel 4.1 beschrieben. Diese Kapitel ersetzt nicht die detaillierten Festlegungen zur technisch-organisatorischen Ausgestaltung und zur Nutzung der zentralen Dienste, die im Zusammenhang mit dem Dokument zur Sicherheitspolicy für das NR und das KN AHF in Form von Nutzungsordnungen zu erstellen sind.

5.1 Patientenliste und PID-Generator

Die Patientenliste ist der Ort des Identitäts-Managements und hat damit eine zentrale und besonders schützenswerte Rolle. Den generischen Lösungen der TMF zum Datenschutz in der vernetzten Forschung folgend, wird die Patientenliste örtlich und technisch getrennt von den Forschungsdaten angeordnet und getrennter Verantwortung unterworfen.

In Kapitel 3.1 sind die Funktionen des Organisationsmoduls dargestellt. Es ist durch die Einwilligung der Patienten befugt, die Patientenliste zu führen und zu pflegen, seit das Nationale Register für angeborene Herzfehler seine Geschäfte aufgenommen hat. Diese Funktion soll das Organisationsmodul weiter ausfüllen, auch für die Studien des Kompetenznetzes.

5.2 Qualitätssicherung

Die Methodik der Qualitätssicherung ist in Kapitel 4.1.4 beschrieben: Verschiedene Fachleute, die mit der Aufgabe innerhalb der einzelnen Studien beauftragt sind, brauchen lesenden und schreibenden Zugriff auf die zentrale Studiendatenbank, wobei alle Änderungen durch ein Audit Trial protokolliert werden. Die Verwaltung der zentralen Studiendatenbank wird rechtlich, technisch und örtlich dem CIOffice an der Universität Göttingen zugeordnet, das die IT-Aufgaben im NR und KN AHF betreut.

5.3 Pseudonymisierungsdienst

Der Pseudonymisierungsdienst ist eine reine Maschinenfunktion; lediglich im Falle der Depseudonymisierung zur Information von Patienten ist der Eingriff spezifisch befugter Operatoren erforderlich (vgl. dazu Kapitel 4.1.8). Der Pseudonymisierungsdienst wird der Betriebseinheit Informationstechnologie (BE-IT) zugeordnet und unterliegt damit dessen personeller und dienstrechtlicher Verantwortung, die von der des CIOffice getrennt ist.

5.4 Führung der Forschungsdatenbank

Die Führung der Forschungsdatenbank wird dem CIOffice der Universität Göttingen zugeordnet, unter der selben Verantwortung wie die Führung der Studiendatenbank.

5.5 Teilnehmerservice für die Verwaltung von Zugriffsrechten

Es besteht Einvernehmen, dass bis zu dem Zeitpunkt, an dem die im Zusammenhang mit elektronischen Gesundheitskarte eGK zu schaffende public key infrastructure be-

reitet, für die Daten erhebenden Stellen Authentifikation ohne starke Kryptographie eingesetzt wird. Dagegen sollen die Mitarbeiter der zentralen Funktionen sehr wohl mit einer chipkartenbasierten PKI ausgestattet werden. Dazu muss ein Teilnehmerservice zur Beantragung und Ausgabe der Chipkarten für die Mitarbeiter und der Zertifikate für die Server eingerichtet werden. Dies gehört zum Aufgabenbereich des CIOOffice. Das Regelwerk dafür kann aus dem Dokument „Sicherheitspolicy für das Kompetenznetz Rheuma, Version 1.1, 18.12.2003“ abgeleitet werden.

6 Datenschutzrechtlich relevante Regel- und Vertragswerke

Zur Konkretisierung der datenschutzrechtlichen Vorschriften sowie der Landeskrankenhausgesetze, des Strafgesetzbuches, der Berufsordnung und der sonstigen berufsethischen Normen sind Regelwerke erforderlich, auf die alle Beteiligten vertrauen können, und woran das medizinisch behandelnde und forschende Personal in der Nutzung der Systeme rechtsverbindlich gebunden wird.

1. Für den Patienten geschieht dies im Rahmen des Behandlungsvertrags mit den Ärzten oder der Klinik sowie durch die Aufklärung und eine informierte Einwilligung, Daten für das Forschungsnetz zur Verfügung zu stellen.
2. Für die behandelnden Ärzte und klinisches Personal gelten in erster Linie die Regeln, die von den jeweiligen Kliniken unter der Verantwortung des leitenden Arztes vorgegeben sind. Soweit allerdings Daten erhoben werden, welche den Verfügungsbereich der Klinik verlassen – und dies ist in der vernetzten Forschung regelmäßig der Fall – muss ein Regelwerk bestehen, das die Eigentumsverhältnisse an den Daten definiert und die Lieferung an Verträge mit dem künftigen Eigentümer bindet.
3. Auch das forschende medizinische und nicht-medizinische Personal kann an die Regeln der jeweils verantwortlichen Klinik gebunden werden. Manche der Tätigkeiten, wie der Zugriff zu Forschungsdaten oder die Überlassung für definierte Forschungszwecke, überschreitet die Grenzen der Klinik und muss an Regelwerke gebunden sein, die vom KN AHF verantwortet werden und das forschende Personal über Verträge an die Regelwerke bindet.
4. Für die zentralen Dienste – z. B. Führung der Datenbanken, Patientenliste, Qualitätssicherung und Pseudonymisierungsdienst – sind geeignete Nutzungsordnungen mit den datenschutzrechtlich relevanten Regeln aufzustellen und Verträge zu schließen, welche alle Beteiligten rechtsverbindlich an die Regelwerke binden.

Diese Regelwerke sind nicht im Rahmen der generischen Lösungen der TMF für den Datenschutz erarbeitet worden. Wie unter Kapitel 5.5 bereits erwähnt, sind sie jedoch mit der Bezeichnung „Sicherheitspolicy“ für ein konkretes Vorhaben, nämlich für den Pseudonymisierungsdienst des Kompetenznetzes Rheuma, geschaffen und mit dem Datenschutzbeauftragten für das Land Berlin konsentiert worden.

Dieses Dokument bietet eine detaillierte Grundlage für die Ausarbeitung der Sicherheitspolicy auch für das NR und KN AHF, indem es an die konkreten Bedingungen, die in diesem Forschungsverbund herrschen, angepasst wird.

Abkürzungsverzeichnis

AHF	Angeborene Herzfehler
CIOffice	Chief Information Office, Abt. Med. Informatik, Göttingen
DB	Datenbank
eGK	elektronische Gesundheitskarte nach der für Deutschland laufenden Planung
FDA	Food and Drug Administration <www.fda.gov>
FDB	Forschungsdatenbank (enthält pseudonymisierte Daten)
HPC	Health Professional Card, Heilberufsausweis
iAS	InterActiveSystems GmbH
IDAT	patientenidentifizierende Daten (Name, Vorname, Geb.-Datum, Geschlecht, ...)
ISST	Fraunhofer Institut Software- und Systemtechnik
KIS	Krankenhausinformationssystem
KN	Kompetenznetz
MDAT	medizinische Daten
MDS	minimal data set (Diagnosen, Prozeduren)
MRT	Magnetresonanztomografie
NR	Nationales Register für Angeborene Herzfehler e.V., Berlin
PID	Patientenidentifikator
PKI	Public Key Infrastructure
PL	Patientenliste
PSD	Pseudonymisierungsdienst
PSN	Pseudonym
PSN2	aus dem originären Pseudonym transformiertes Pseudonym
PVS	Patientenverwaltungssystem
QP2	Querschnittsprojekt 2: MRT
QP3	Querschnittsprojekt 3: Tissue Doppler
QS-DB	Qualitätssicherungdatenbank (enthält nicht pseudonymisierte Daten)
RDB	Registerdatenbank

SDB	Studiendatenbank
SSL	Secure Socket Layer (Protokoll)
TMF	Telematikplattform Medizinische Forschungsnetze e.V., Berlin
UML	Unified Modeling Language
VM	Versorgungsmodul, ein Leistungsmodul des Nationalen Registers AHF
VK	Versichertenkarte

Hinweise zur Version

Das vorliegende Papier gibt den Stand eines „work in progress“ wieder. Es beschreibt die Sicherheitsinfrastruktur sowohl für das Nationale Register (NR) als auch für das Kompetenznetz (KN) Angeborene Herzfehler (AHF). In der aktuellen Version liegt der Schwerpunkt auf der Ausarbeitung der datenschutzrelevanten Regelungen für das Studienmodul des Kompetenznetzes. Die entsprechende Ausarbeitung für das NR AHF sind zwar in sich vollständig; jedoch harren die zwei weiteren Leistungsmodul des NR, das Modul zur Prävalenzerhebung und das Versorgungsmodul, noch der Bearbeitung.

Die Versionen 0.1 – 0.3 sind Vorstufen der Version 0.4 (12.11.2004) und sind nur intern verfügbar. Version 0.4 wurde den Auftraggebern und dem Softwarehaus iAS zur Kommentierung übergeben. Die Version 0.5 nimmt die Anregungen daraus auf und berücksichtigt insbesondere eine möglichst weitgehende Annäherung an das nach den Regeln des FDA zertifizierte RDE-System des Softwareherstellers interActiveSystems iAS, das zur Datenerhebung für die Studien des KN AHF eingesetzt werden wird.

Version 0.6 nimmt unter der Ziffer 1 eine Begründung dafür auf, dass in der vernetzten Forschung höhere Anforderungen an den Schutz der Persönlichkeit gestellt werden müssen als in der traditionellen klinischen Forschung. Die übrigen Textteile sind präzisiert und ergänzt, ohne dass wesentlich neue Inhalte aufgenommen wurden. Unter den Ziffern 4.2.3 und 4.2.4 wurden die Daten für die Patientenliste ergänzt und für das minimal data set neu definiert.

Die Versionen >0,9 sind gründlich überarbeitet worden bezüglich geänderter Begrifflichkeiten (z.B. Inzidenzmodul – Modul zur Prävalenzerhebung).

In Version 0.95 wurden die Items des MDS der aktuellen Version der DSTen in iAS Secutrial angepasst.

Die Versionen 1.00 und 1.01 wurden final abgestimmt, Umbruchfehler in den Tabellen beseitigt.

Die Version 1.10 wurde am 19. Oktober 2005 zusammen mit dem Landesbeauftragten für Datenschutz Berlin durchgesprochen.

Die Version 1.24 wurde am 9. Februar 2006 mit dem LfD Berlin aufgrund der Rückmeldungen der anderen LfD präzisiert, Grafiken neu nummeriert und Grafiken ergänzt. Weiterhin wurde der MDS im Text an die überarbeitete Version 1.5 angepasst.