**Epilepsiedatenbank zur Integration von Forschungsprojekten epilepsiechirurgisch tätiger Zentren und zur multizentrischen Beforschung der Wirksamkeit der epilepsiechirurgischen Therapie insbesondere bei seltenen Syndromen (EpiSurgeDat)**

# Datenschutzkonzept

## 1. Aufgaben, Ziele:

Erstellung einer Internet-basierten Datenbank mit folgenden Zielen:

- standardisierte Erfassung von Epilepsiediagnosen zur Charakterisierung homogener Patientengruppen
- Erfassung von Patientenkollektiven mit seltenen Syndromen
- zentrale und standardisierte Dokumentation der Wirkungen und Nebenwirkungen der Epilepsiechirurgie zur Verbesserung der Bewertung dieses Therapieansatzes
- Koordination von Forschungsprojekten in der prächirurgischen Epilepsiediagnostik und in der Epilepsiechirurgie
- Verbesserung des Zugangs von Epilepsiepatienten zu Forschungsprojekten

## 2. Kurzdarstellung des Vorhabens

Zur Verbesserung der Patientensicherheit und Schaffung eines Qualitätsstandards plant die Arbeitsgemeinschaft für prächirurgische Epilepsiediagnostik und operative Epilepsietherapie gem. e.V. (vgl. Ethikantrag, Version vom 13.10.10 S. 2ff) eine multizentrische internetbasierte Datenbank zur pseudonymisierten Erfassung der epilepsiechirurgisch behandelten Patienten.

Die epilepsiechirurgische Therapie ist ein etabliertes Verfahren zur Behandlung medikamentös therapierefraktärer Epilepsien. Syndromabhängig können suffiziente Anfallsfreiheitsraten von über 60% erreicht werden, was zu einer signifikanten Verbesserung der Lebensqualität der Patienten und zu einer erheblichen Senkung der Krankheitskosten beiträgt.

Die präoperative Diagnostik wie auch die chirurgische Therapie der Epilepsien fordert einen interdisziplinäreren (Epileptologie, Chirurgie, Psychiatrie,

Neuropsychologie etc.) Ansatz und ist mit einer sehr heterogenen Patientengruppe mit z.T. sehr seltenen Syndromen befasst. Die Beforschung solcher Erkrankungen ist nur multizentrisch sinnvoll. Aber auch für häufiger vorliegende Syndrome erscheint eine multizentrische Beforschung mit größeren Stichproben als in den aktuell publizierten Studien wünschenswert.
Die Datenerfassung soll standardisiert über eine internetbasierte Datenbank erfolgen, die in Kooperation mit der Expertise des Kompetenznetz Parkinson e.V. erstellt wird. Es sollen systematisch demographische Daten (u.a. Geschlecht, Alter, sozio-ökonomische Daten), klinische Charakteristika (u.a. Syndrom, aktuelle Therapie, Bildgebungsbefunde) als wesentliche Ergebnisse der präoperativen Abklärung und der Behandlungsverlauf standardisiert erfasst werden (Anhang 1, „Minimal-Dataset“). Hierbei soll a) die Wirksamkeit der epilepsiechirurgischen Therapie im Langzeitverlauf multizentrisch bewertet werden und b) Patienten zentrumsübergreifend der Zugang zu Forschungsprojekten ermöglicht werden.

## 3. Ethische Aspekte

3.1 Gewinnung der Registerdaten

Die Sammlung der Daten und der Umgang mit ihnen erfolgt unter Einhaltung der ethischen Grundsätze in Übereinstimmung mit der Deklaration von Helsinki/Tokio/Venedig/Hongkong.
Es handelt sich nicht um ein experimentelles Design; vielmehr werden Daten aus klinischen Untersuchungen, die im Rahmen der prächirurgischen Abklärung und im Verlauf der chirurgischen Therapie sowie bei Verlaufsuntersuchungen ohnehin anfallen, zentral dokumentiert. Hiermit soll eine standardisierte Erhebung, Speicherung und Auswertung größerer Patientenpopulationen ermöglicht werden. Die Auswertung eines multizentrischen Kollektivs sowie die Möglichkeit, größere Patientenpopulationen im Rahmen von Forschungsprojekten untersuchen zu können, erscheint vor dem Hintergrund der Fülle von Syndromen, mit denen die Epilepsiechirurgie befasst ist, unbedingt wünschenswert, da monozentrisch in einem übersehbaren Zeitraum keine ausreichenden Patientenkollektive gewonnen werden können. Somit würden sich auch Möglichkeiten zur Beforschung seltener Syndrome eröffnen. Dies stellt einen indirekten Nutzen für diese Patienten dar. Darüber hinaus soll Patienten der Zugang zu

Forschungsprojekten erleichtert werden, woraus sich ein direkter Nutzen für die Patienten ergibt.

Die Information und das schriftliche Einverständnis der Patienten zur zentralen pseudonymisierten Datenerfassung und -speicherung erfolgt vor Aufnahme in das Register (Anhang 2, „Patienteninformation“).
Die Schlüsselliste zur Re-Identifikation wird im behandelnden Zentrum durch den leitenden Prüfarzt geführt (Identifikationsdaten und Pseudonymisierungs-nummer). Die Pseudonymisierung soll zum einen der Sicherung der Datenqualität dienen, sodass bei widersprüchlichen Angaben eine Re-Identifikation durch den leitenden Prüfarzt eines Zentrums und ein Abgleich mit den in der Patientenakte dokumentierten Daten erfolgen kann. Die mit Pseudonymisierung und Identifikationsdaten gekennzeichneten Datensätze existieren ausschließlich als Papierausdruck des Datenbankformulars und werden getrennt unter Verschluss vom leitenden Prüfarzt aufbewahrt (siehe 6. Besondere Datenschutzvorkeh-rungen, S.15ff).
Die Re-Identifikation soll auch dann genutzt werden können, wenn Patienten an Studien anderer Zentren teilnehmen, für welche die Registerdaten zur Entlastung des Patienten und zur Vermeidung von Doppeluntersuchungen genutzt werden können.
Die Voraussetzungen und das Procedere für eine pseudonymisierte Datenübermittlung ist unter 3.2 „Gewinnung potenzieller Studienteilnehmer“ beschrieben.
Die Daten der durch ein Zentrum aufgenommenen Patienten sollen zunächst nur diesem Zentrum zugänglich sein. Die Übermittlung der Daten zur Auswertung an andere Zentren soll anonymisiert erfolgen, wenn für ein Forschungsprojekt ein positives Votum der lokalen Ethikkommission vorliegt und das Projekt auch von einem internen gewählten wissenschaftlichen Gremium (Forschungsbeirat) und der Datenschutzkommission der AG Prächirurgie nach schriftlichem Antrag **(Welche Form? Z.B. analog zu lokalen Ethikanträgen?)** befürwortet wurde. Die Gremien bestehen aus je 3 gewählten Mitgliedern der AG Prächirurgie, die sich durch hohe Expertise in der klinisch-epileptologischen Forschung ausweisen.

### 3.2 Gewinnung potenzieller Studienteilnehmer

Das generelle Interesse des Patienten an Informationen über laufende Forschungsprojekte, die über die Daten im Register hinausgehend weitere Selbstauskunft oder die Durchführung von Studienhandlungen am Patienten erfordern, soll unter ausführlicher schriftlicher Aufklärung mit schriftlicher Einwilligung des Patienten dokumentiert werden (*vgl. Anhang 5*).
Patienten, die ihr generelles Interesse an Forschungsprojekten teilzunehmen schriftlich bekundet haben, sollen auf entsprechende für sie geeignete Forschungsprojekte aufmerksam gemacht werden, insofern für das Projekt ein positives Votum der lokalen Ethikkommission vorliegt und das Projekt auch von einem internen gewählten wissenschaftlichen Gremium der AG Prächirurgie nach schriftlichem Antrag befürwortet wurde.
Erste Informationen über eine laufende Studie sollen hierbei durch den behandelnden Arzt am jeweiligen Zentrum durch Übersendung / Übergabe der am projektdurchführenden Zentrum gültigen Patienteninformation erfolgen. Der behandelnde Arzt soll auch für Rückfragen zur Verfügung stehen.
Die Übermittlung der entsprechenden Daten muss für das Forschungsvorhaben notwendig sein. Über die Sinnhaftigkeit des Forschungsvorhabens entscheidet das **3-köpfige** wissenschaftliche Gremium (Der Forschungsbeirat) der AG Epilepsiechirurgie. Die **3-köpfige** Datenschutzkommission der AG Epilepsiechirurgie entscheidet über Art und Ausmaß der Datenübermittlung. Nur insofern für ein Forschungsvorhaben eine Zuordnung zu den zusätzlich erhobenen Daten erforderlich ist, kann die Übermittlung pseudonymisiert erfolgen, insofern der Patient hierzu sein schriftliches Einverständnis gibt.
Nach entsprechender Genehmigung erfolgt die Re-Identifikation durch den leitenden Prüfarzt des behandelnden Zentrums, der die entsprechenden Pseudonymisierungsnummern an das zentrale Daten-Mangement **(Wer? Abhängig von zu Verfügung stehenden Mitteln)** übermittelt. Dieses sendet wiederum die entsprechenden Datensätze an das studiendurchführende Zentrum.
Das Pseudonym der Datenbank wird hierbei nicht versendet, sondern es wird dem Patienten eine Studiennummer für die konkrete Studie, an der er teilnimmt zugeordnet.

## 4. Datenschutzkonforme IT-Infrastruktur

Kernstück der IT-Infrastruktur der AG Epilepsiechirurgie ist ein zentrales Datenbankregister für medizinische Daten. Das System ist mit Hilfe der Secutrial 2.x RDE-Software des Kompetenznetz Parkinson e.V. realisiert. Es handelt sich um ein internet-basiertes System mit Anbindung an eine relationale Oracle-Datenbank.
Die datenschutzkonforme Kompatibilität des RDE-Systems entsprechend den Anforderungen nach GCP, AMG und FDA (21 CRF Part 11) und GCP wurde zuletzt im April 2007 positiv begutachtet (s. Anhang 3, „Gutachten“). Darüber hinaus erfüllt das System bereits jetzt die strengen Anforderungen an eine Systemvalidierung von EDV-Systemen für klinische Studien nach AMG 12. Weiterhin ist der gesamte Softwareentwicklungsprozess von der ABB Eutech validiert.
Das System dient dazu, pseudonymisierte Erhebungsdaten über Patienten zu erfassen. Es enthält Funktionen zur Eingabe von Daten über Formulare, sowie zur Ansicht und zur Auswertung dieser Daten.
Die Erhebungsdaten sind organisiert als Gruppen von Formularen, die zusammen einen vollständigen Erhebungssatz bilden. Patienten können mit diesen Formularen über eine Zeitreihe von mehreren Untersuchungen erfasst werden, wobei die Folge der Formulareingaben pro Patient als Historie (=Audit Trail) dieses Patienten dargestellt wird.
Für eingabeberechtigte Personen existiert ein Benutzer-, Rechte- und Rollenkonzept, das diese definiert und authentifiziert. Alle Eingaben berechtigter Personen werden in einer Historie geloggt.
Wichtigste Funktionen des RDE-Systems:

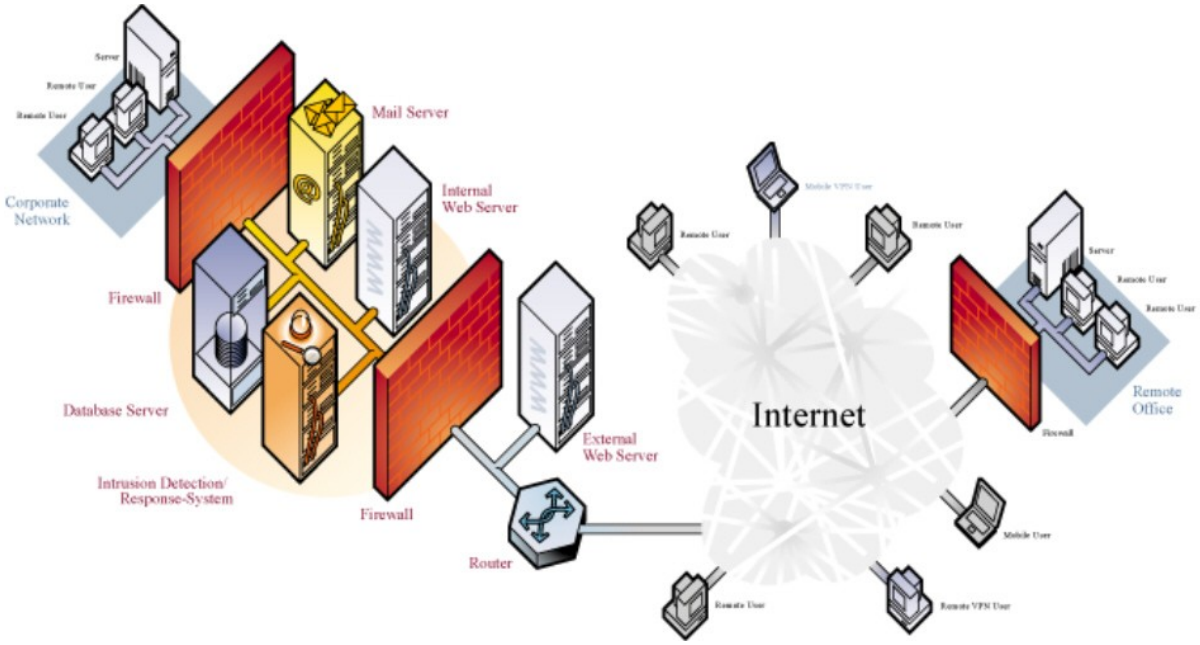
- Abbildung von Studienprotokollen und Registerdesigns in Internetformulare, wahlweise mit festen oder flexiblen Visitplänen
- Integration von Hilfetexten, internen Plausibilitäts- und Vollständigkeitschecks zur Gewährleistung einer hohen Datenqualität
- Funktionen für den Export und Import von Daten
- selektiver und kombinierter Datenexport
- integriertes Messaging-System
- integriertes Query-System für internetbasiertes Monitoring
- flexibles Rechte- und Rollensystem für unterschiedliche Benutzergruppen
- automatisierte Reports und Statistiken (als Tabelle oder Grafik)
- integriertes AE/SAE Management

- mit dem Produktivsystem identisches Trainingssystem für Schulungs- und Präsentationszwecke

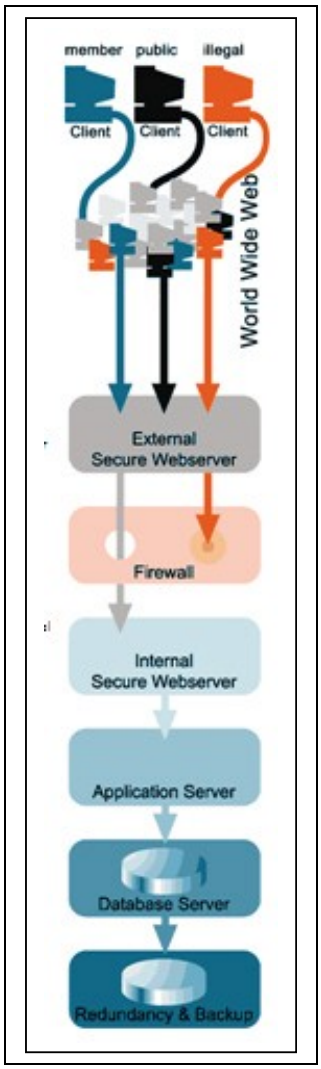
### 4.1. Interne Architektur des Systems

Die Anwendung ist in Java 2 SE und auf den WebObjects-Application Server hin programmiert. Dabei werden zwei Frameworks aus diesem Produkt verwendet: die WOComponents, die serverseitig Webseiten generieren, und das EOFramework, das die objekt-relationale Darstellung von Datenbanktabellen repräsentiert und die Datenhaltung steuert.
Die Anwendungslogik ist einer Web-Sitzung zugeordnet, die durch eine von WOSession abgeleitete Klasse repräsentiert wird. Die GUI-Schicht besteht aus von WOComponent abgeleiteten Klassen, die jeweils HTML-Seiten mit dynamischen Datenbindungen repräsentieren (bzw. auch Teile von Framesets).
Eine zentrale Komponente ist der Formular-Generator, der auf dem WOComponents-Framework basiert. Dieser generiert die anwendungsspezifischen Formulare aus Datenbankabfragen. Aufbau und Aussehen der Formulare sind ebenso wie die dargestellten Inhalte parametrisiert und in der Datenbank definiert. Die Definitionen sind in einem separaten Framework, den IASComponents, organisiert.
Das Datenmodell ist in einem separaten Framework (SRTEnterpriseObjects) zusammen gefasst, das Java-Abbildungen der Datenbank-Tabellen enthält.
Die Benutzerverwaltung ist im Framework IASUsermanagement zusammengefasst. Die zugrundeliegende Datenbank ist in SQL mit Oracle-Erweiterungen erstellt. Sie enthält auf Datenbankebene einen Oracle-spezifischen Primärschlüssel-Generator.

### 4.2. Sicheres Hosting




Das Hosting des RDE-Systems erfolgt in den Räumen des Rechenzentrums der Semgine GmbH, Berlin. Semgine (und sein Vorgänger interActive Systems) hostet in seinem hoch gesicherten Rechenzentrum schon seit vielen Jahren zentrale medizinische Datensammlungen medizinischer Kompetenznetze und verfügt über die dafür erforderliche datenschutzrechtliche Expertise. Das Serversystem, auf dem Secutrial 2.x betrieben wird, besteht aus fünf Servern (Applikation, Datenbank, Backup und zwei Firewalls) allerneuester Bauart. Es wird in einem mit Alarmanlagen gesicherten, klimatisierten Serverraum betrieben. Die Betreuung aller Systeme erfolgt ausschließlich durch qualifiziertes Fachpersonal (Fachrichtungen IT-Security, Netzwerk-, Datenbank- und Systemadministration).
Das Sicherheitskonzept besitzt die Zertifizierung „trusted site“ der TÜV-IT GmbH. Diese beinhaltet die Konzeption und Implementierung der Sicherheitssysteme, die Begleitung der formalen Prozesse der Zertifizierung und die kontinuierliche Wartung durch kompetentes Personal.
Das zweistufige Firewall-System besteht aus zwei Paketfiltern, die die Datenbank- und Applikationsserver vor unberechtigten Zugriffen schützen. Die Paketfilter werden mit dem Linux Kernel-Modul Netfilter realisiert.




Zusätzlich wird der gesamte Netzwerkverkehr zwischen Internet, Firewall-Systemen und den Applikationsservern mit dem netzwerkbasierten Intrusion Detection System Snort überwacht. Auf den externen Paketfiltern wird der Datenaustausch mit dem Internet, auf den internen Paketfiltern der Netzwerkverkehr mit den Sicherheitssystemen sowie mit den Applikations- und Datenbankservern überwacht. Alle von Snort erzeugten Meldungen und Warnungen werden in einer speziellen Datenbank gespeichert, die permanent über auf den Firewallsystemen installierte Auswertungswerkzeuge analysiert werden.

Die hohe Verfügbarkeit der medizinischen Daten auf den Datenbankservern wird durch redundante Festplattenverbünde (RAID) und eine generationsbasierte Datensicherungsstrategie gewährleistet.

Alle medizinischen Daten der Datenbankserver sowie alle Logfiles der Firewallsysteme werden täglich gesichert. Diese Datensicherung folgt einem 3-Wochen-Turnus mit 3 Band-Generationen. Eine Bandgeneration dient der Datensicherung in der laufenden Woche. Eine Bandgeneration hält die Datensicherungen der vergangenen Woche. Beide werden im Rechenzentrum gelagert. Die dritte Bandgeneration hält die Datensicherungen der vorvergangenen Woche. Sie wird aus Sicherheitsgründen im Safe einer Bank aufbewahrt, die sich an einem anderen Ort als das Rechenzentrum befindet. Der Austausch zwischen Rechenzentrum und Bank erfolgt einmal wöchentlich.

Alle Systeme sind vor Stromausfällen durch unterbrechungsfreie Stromversorgungen (USV) geschützt.

### 4.3. Dem System zugrundeliegendes Datenschutzkonzept

Medizinische Daten, die über das Internet übertragen werden, unterliegen allerstrengsten Restriktionen der Datenschutzbehörden. Das Datenschutz- und Sicherheitskonzept des Kompetenznetz Parkinson, das dem hier beschriebenen

Datenschutzkonzept zugrunde liegt, entspricht in allen Teilen den strengsten Sicherheitsanforderungen und wurde bereits 2002 von allen Datenschutzbeauftragten der Länder und des Bundes konsentiert. Seit Juli 2004 ist auch das Datenschutzkonzept für die Einbindung einer Genbank (der Genbank Parkinson'sche Krankheit Deutschland, GEPARD) konsentiert.

### 4.4. Technisch-organisatorische Maßnahmen

1. Rechenzentrum

Die Serversysteme der bei der Semgine GmbH (Nachfolger von iAS GmbH, aber gleiches Personal) gehosteten Projekte werden in einem mit Alarmanlagen gesicherten klimatisierten Serverraum betrieben. Der Serverraum ist mit Brandschutztür gesichert. Der Zugang erfolgt über ein elektronisches Schloss-System, zu dem nur die System-Administratoren der Semgine GmbH Zugang haben.

2. Systemadministration

Bei den Systemadministratoren der Semgine GmbH handelt es sich ausschließlich um qualifiziertes Fachpersonal (Fachrichtungen IT-Security, Netzwerk-, Datenbank- und Systemadministration), die über umfangreiche jahrelange Erfahrung im Umgang mit diesen Technologien verfügen.

3. Trusted Site zertifiziert

Für die Server des Kompetenznetzes Parkinson, auf dem auch das Register der AG Epilepsiechirurgie gehostet wird, wurde darüber hinaus die Zertifizierung „trusted site" durch die TÜV IT GmbH erreicht. Dies beinhaltet die Konzeption und Implementierung der Sicherheitssysteme, die Begleitung der formalen Prozesse der Zertifizierung und die kontinuierliche Wartung durch kompetentes Personal.

4. Sicherheitssysteme

Die zweistufigen Firewallsysteme bestehen aus zwei Paketfiltern, die die Datenbank- und Applikationsserver vor unberechtigten Zugriffen schützen. Die Paketfilter sind mit dem Linux Kernel-Modul Netfilter realisiert.

Zusätzlich wird der gesamte Netzwerkverkehr zwischen Internet, Firewallsystem und den Applikationsservern mit dem netzwerkbasierten Intrusion Detection System auf den Netzwerkverkehr nach bekannten Angriffsmustern und/oder Unregelmäßigkeiten untersucht. Auf den externen Paketfiltern wird mit Snort der Datenaustausch mit dem Internet überwacht, auf den internen Paketfiltern der Netzwerkverkehr zwischen den Sicherheitssystemen sowie mit den Datenbank- und Applikationsservern. Die von Snort erzeugten Meldungen und Warnungen werden in einer Datenbank gespeichert. Zur Auswertung ist auf den Firewallsystemen ein webbasiertes Analyse- und Auswertungswerkzeug installiert.

## 5. Applikations- und Datensicherheit

Auf Seiten der Applikations- und Datenbankserver kommt Linux Enterprise zum Einsatz. Als Datenbank ist Oracle in den Versionen 9i und 10i eingesetzt, als Middleware WebObjects und als Webserver Apache. Applikationsseitig wird das auf Java basierende SecuTrial 2.x eingesetzt.
Die Verfügbarkeit der Patientendaten auf den Datenbankservern erfolgt durch redundante Festplattenverbünde (RAID) sowie eine generationsbasierte Datensicherungsstrategie.
Alle Systeme sind zur Absicherung vor Stromausfällen durch unterbrechungsfreie Stromversorgungen (USV) geschützt.

## 6. Besondere Sicherheitsleistungen des Hosters

- Es erfolgt eine zeitnahe, kontinuierliche Überwachung der Funktionalität der Applikationsserver mit Hilfe von Monitoring-Software.
- Es erfolgt eine zeitnahe, kontinuierliche Überwachung der Logfiles der Firewallsysteme sowie der Integrität der Systeme selbst.
- Es erfolgt eine tägliche, gründliche Überprüfung der Sicherheitssysteme.
- Es erfolgt ein tägliches Backup der Datenbanken und der Applikationsserver sowie aller Protokolldateien der Firewallsysteme (alle Logfiles der Firewallsysteme werden dauerhaft archiviert).
- Es erfolgt ein wöchentlicher Austausch der Datensicherungsmedien. Eine Generation der Datensicherungsmedien befindet sich jeweils im Bank-Schließfach.

- Die Systemparameter aller beteiligten Systeme werden kontinuierlich überwacht. Bei Bedarf werden die Oracle-Parameter optimiert.
- Alle relevanten Sicherheitsupdates werden zeitnah eingespielt.
- Der Hoster Semgine GmbH bietet einen werktäglichen telefonischen und Email-Support.

7. Begutachtung des eingesetzten SecuTrial hinsichtlich Compliance zu AMG/GCP und FDA (21 CFR Part 11)

Das eingesetzte System SecuTrial 2.x wurde im April 2007 hinsichtlich seiner Compliance zu AMG, GCP und FDA positiv begutachtet. Das Gutachten konstatiert:

„Abweichungen zu den gesetzlichen Anforderungen aus AMG/GCP und FDA (21 CFR Part 11) wurden bei der Untersuchung der Software SecuTrial 2.1 nicht festgestellt.

Die Systemarchitektur und besonders die Verfahrensweisen, die zur Nachvollziehbarkeit von Änderungen hinsichtlich der gespeicherten Daten aber auch der Studienkonfiguration bzw. der Änderungen in der Systemverwaltung implementiert sind, stellen in den Kernbereichen weit über die geforderten Minimalanforderungen sicher, dass die behördlichen Anforderungen erfüllt sind.

Ansonsten sei hier auf das Gutachten selbst verwiesen (s. Anhang 3, „Gutachten“).

8. Verschlüsselung und Pseudonymisierung

Die Datenübertragung zwischen Webclient und Applikation bzw. Datenbank erfolgt ausnahmslos SSL-128-verschlüsselt.

Es werden prinzipiell keine identifizierenden Daten übertragen. – auch nicht zum Zweck der Generierung von Pseudonymen.

Wie weiter unten beschrieben, sendet das Programm bei Anforderung „neuer Patient“ lediglich ein leeres Formular und ein Pseudonym an den Webclient. Das erzeugte Pseudonym ist, da völlig unabhängig von identifizierenden Daten generiert, darüber hinaus ausprobiersicher (s. auch Grafik Pseudonymisierung im Anhang).

9. Benutzerkennungen

Der Antrag eines Zentrums an der Teilnahme am an der Datenbank verlangt ein unterschriebenes Antragsformular eines zentrumsverantwortlichen Arztes und einen von Seiten des zentrumsverantwortlichen Arztes und der AG Epilepsiechirurgie, vertreten durch den Vorstand, unterschriebenen Prüfarztvertrag. Erst nach Vorliegen dieser Dokumente sendet der Datenschutzbeauftragte der AG Epilepsiechirurgie ein Formular mit den Daten des neuen Teilnehmers an das Datenmanagement **(Wer wird das sein?).**

Zusätzliche Ärzte eines Zentrums, das bereits am Gesamtprojekt teilnimmt, die dem Datenschutzbeauftragten nicht bekannt sind, müssen darüber hinaus eine Authentifizierung durch den leitenden Prüfarzt des Zentrums vorweisen. Das Datenmanagement richtet darüber hinaus den Zugriff für einen neuen Arzt erst dann ein, wenn auf dem Formular bestätigt worden ist, dass der neu aufzunehmende Arzt in der Handhabung der Datenbank und der damit verbundenen besonderen Datenschutzbestimmungen unterrichtet worden ist.
Die Aufnahme eines neuen Zentrums ist nur dann möglich, wenn dem Vorstand der AG Epilepsiechirurgie derjenige Arzt, der die Funktion des leitenden Prüfarztes dieses Zentrums übernehmen soll, persönlich bekannt ist.
Erst nach Erhalt des o.g. Formulars wird für den neuen Teilnehmer eine Benutzer-ID eingerichtet. Das Datenmanagement unterrichtet den Datenschutzbeauftragten durch Rücksendung des unterschriebenen Formulars über die Einrichtung. Dieser wiederum informiert den Teilnehmer. Die Benutzer-ID ist wie unter 10. beschrieben persönlich und nicht übertragbar.

## 10. Passworte

Die Passworte für den Datenbankzugriff sind vom System auf mindestens 8 Zeichen Länge eingestellt. Zusätzlich muss ein Zeichen nicht-alphabetisch sein.
Für einen neuen Teilnehmer wird vom Datenmanagement ein Start-Passwort eingerichtet, das nur einmal verwendet werden kann und sofort bei der ersten Anmeldung an der Datenbank vom neuen Teilnehmer die Erstellung eines eigenen Passworts verlangt.
Bei dreimaliger falscher Passwort-Eingabe wird die Teilnehmer-ID gesperrt. Eine Entsperrung kann nur durch Beauftragung des Datenmanagements durch den Datenschutzbeauftragten erfolgen.

Im Falle einer Entsperrung generiert das Datenmanagement ein neues Start-Passwort, das wiederum bei der nächsten Anmeldung des Teilnehmers in ein eigenes Passwort geändert werden muss.
Die Passworte unterliegen einer von Systemseite erzwungenen Änderung nach 6 Monaten.

## 11. Revisionsfähigkeit

Hier verweisen wir auf das ausführliche Gutachten zur Compliance mit AMG, GCP und FDA (21 CFR Part 11) im Anhang.
Das SecuTrial-System verfügt über drei verschiedene Arten des Audit Trails:
a) Die erfassten medizinischen Daten werden mit Zeitstempel, elektronischer Signatur des Eingebenden und Grund der Eingabe (bei Änderung) in der Datenbank erfasst. Bei Änderungen wird immer ein neuer Eintrag in der Datenbank erzeugt. Das heißt, dass bestehende Einträge nicht verändert oder gelöscht werden können. Bei Änderungen wird vielmehr der originale Datensatz in eine Archivtabelle verschoben.
b) Änderungen am Design oder der Konfiguration des Datenregisters werden über freigegebene Versionen nachvollziehbar gespeichert. Vorherige Versionen werden archiviert.
c) Alle Änderungen, die in der Administration gemacht werden, werden als inkrementelle Einträge in eine separate Logtabelle geschrieben. So ist auch die Systemverwaltung jederzeit nachvollziehbar.

## 12. Wartung der Systeme

Die Wartung der Systeme unterliegt verschiedenen Zuständigkeiten:

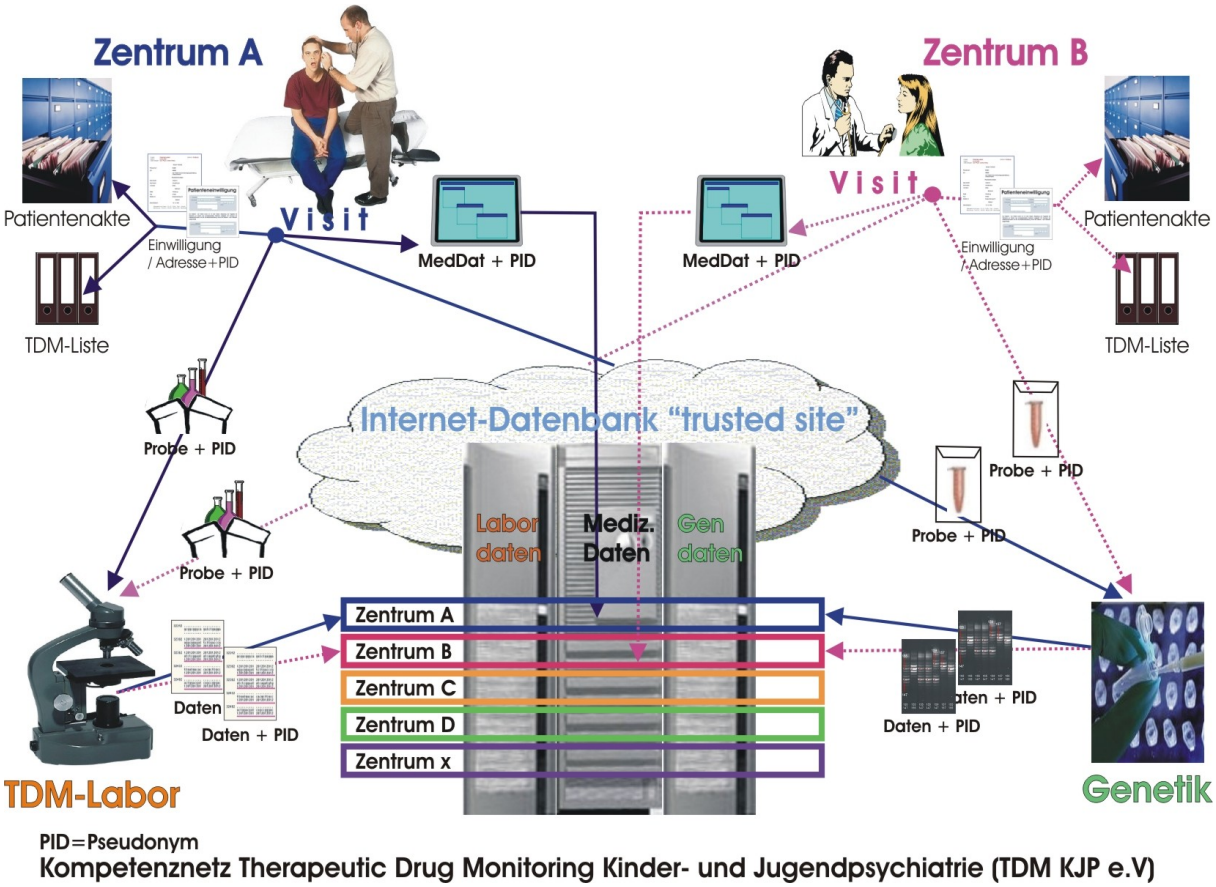
Die Systemadministatoren der Semgine GmbH (Rechenzentrum) haben lediglich physikalischen Zugriff auf die Server und deren Betriebs-, Programm- und Sicherheitssysteme. Sie sind im Auftrag des KN Parkinson (als Besitzer der Server) für die Hardware-Wartung, die Überprüfung der Sicherheitssysteme und die Datensicherung (mittels Backup-Roboter) zuständig. Sie haben keinen Zugriff auf die Datenbanken.

Die Programmierer der interactive Systems sind für die Wartung der Programme zuständig (SecuTrial). Ihnen obliegt die Beauftragung des Einspielens von Updates und evtl. Behebung von Fehlern. Sie haben keinen Zugang zum Rechenzentrum und somit keinen Zugriff auf die Hardware-Systeme, sowie keinen Zugriff auf die Datenbanken.

Das Datenmanagement der AG Prächirurgie ist für das Design des Registers, die Vergabe von Teilnehmerrechten und das Datenmanagement (z.B. Löschen von Patientendaten bei Widerruf) zuständig und verfügt über Zugriff auf die Datenbanken (medizinische Daten und Registerformulare). Das Datenmanagement hat keinen Zugriff auf die Hardwaresysteme und auf die Programme.
Die Semgine GmbH hostet die Server des KN Parkinson, das wiederum seine Server und sein SecuTrial-System der AG Epilepsiechirurgie zur Verfügung stellt. Wenn überhaupt, betreibt demnach das KN Parkinson Auftragsdatenverarbeitung für die AG Epilepsiechirurgie.
**Frau Antony, Central Information Officer des KN Parkinson ist ordentliches (Gründungs-)Mitglied im KN TDM KJP e.V. und hat ordnungsgemäß den Prüfarztvertrag unterschrieben. Frau Antony ist darüber hinaus seit 2002 aktives Mitglied der Arbeitsgruppe Datenschutz der TMF e.V. und bringt die dort erarbeitete Expertise in den Schutz der Daten ein.**
[Anmerkung der Verfasserin: Es sollte ein hier wahrscheinlich ein Datenschutz-beauftragter der AG benannt werden, der Expertise aufweisen kann.]

## 5. Zugang zur Datenbank

Voranzustellen ist, dass nur diejenigen Ärzte einen personalisierten Zugang (eigene ID und Passwort) zur Datenbank nutzen können, die einen Vertrag mit der AG Epilepsiechirurgie haben (im folgenden Prüfarzt genannt). Diese Prüfärzte haben sich im Prüfarztvertrag darüber hinaus verpflichtet, Ihre Zugangsdaten (ID und Passwort) sicher aufzubewahren und zu verhindern, dass sie anderen zur Kenntnis gelangen. Andere Ärzte desselben Zentrums (derselben Klinik) können also selbst bei Kenntnis des Pseudonyms die in der Datenbank gespeicherten Daten nicht einsehen. Von einer Schwächung der Pseudonymisierung ist deshalb nicht auszugehen.




Das RDE-System SecuTrial verfügt über ein feinst skalierbares Rechte- und Rollensystem, das die strikte Einhaltung der Zugangsregelungen zu den pseudonymisierten medizinischen Daten technisch unterstützt.

Generell erhalten einen Zugang zur Datenbank nur Mitarbeiter (d.h. Prüfärzte) von Mitgliedszentren, von denen ein Vertreter ordentliches Mitglied des Vereins „Arbeitsgemeinschaft für prächirurgische Epilepsiediagnostik und operative Epilepsietherapie gem. e.V." ist **(einzufügen: Anhang XX, Satzung, Voraussetzungen für Mitgliedschaft?)**, und die zuvor auf die Wahrung des Datengeheimnisses entsprechend § 5 BDSG bzw. den entsprechenden landesrechtlichen Regelungen verpflichtet wurden. Die Pflicht zur strengen Einhaltung aller datenschutzrechtlich gebotenen Regularien bestätigt der einzelne Prüfarzt der AG Epilepsiechirurgie gegenüber in einer schriftlichen Vereinbarung (Anhang 4, „Prüfarztvertrag").

### 5.1. Zugriff nur auf zentrumseigene Daten und Materialien

Weiterhin beschränkt sich der Zugang auf die im zentralen Register gespeicherten Daten generell jeweils auf die Daten derjenigen Institution, an der das Beschäftigungsverhältnis besteht.
Gründungsmitglieder sind die Mitglieder des Vorstandes der AG Epilepsie-chirurgie, soweit diese klinisch tätig sind.
Nach Etablierung der Datenbank und Abschluss der Pilotphase ist eine Erweiterung auf weitere Zentren im europäischen Raum zu erwarten.
Über die Neuaufnahme von Mitgliedern entscheidet der Vorstand des Vereins (vgl. Briefkopf des Anschreibens). Dieser informiert die Mitgliederversammlung jährlich über die aufgenommenen Personen.

### 5.2. Mitglieder mit notwendigerweise erweitertem Zugang:

Der Zugang zu den pseudonymisierten Daten aller Zentren ist an die jeweilige Rolle des Funktionsträgers gebunden und auf wenige Personen begrenzt:

Zentrale IT-Koordination:

- Benutzermanagement, Datenmanagement, Sperren und Löschen von Datensätzen, wenn der Proband seine Einwilligung zurückzieht, Extrakt von Daten nach Anweisung des Ausschusses Datenschutz (s. unten), Auswertungen zur Gewährleistung einer hohen Datenqualität

Mitglieder des Forschungsbeirates der AG Epilepsiechirurgie:

- Datenübersicht zur Ableitung wissenschaftlicher Hypothesen, projektbegleitende Übersicht über die Erhebung von Daten in den einzelnen Zentren für Steuerungszwecke, Controlling, Monitoring

## 6. Besondere Datenschutzvorkehrungen

**(Anmerkung der Verfasserin: Lösung ohne Notar)**

Voranzustellen ist:
Eine zentrale multizentrische Patientenliste gibt es nicht. Darüber hinaus erfolgt die Speicherung der medizinischen Daten in der Datenbank strikt pseudonym. Einzig und allein die der Prüfarzt am behandelnden Zentrum kennt sowohl

Namen und Adresse als auch das Pseudonym, unter dem seine Daten in der Datenbank hinterlegt sind. Nur ihm ist es möglich, den Patienten zu re-identifizieren bzw. seine Daten in der Datenbank einzusehen. Der Prüfarzt ist über seinen Antrag auf Teilnahme am Register der AG Epilepsiechirurgie sowie über den Prüfarztvertrag an die Einhaltung der festgelegten Regeln gebunden.

Die datenschutzrechtliche Verantwortung verteilt sich wie folgt:

- Die Datensicherung innerhalb der Datenbank und Datenverarbeitung/ -auswertung liegt in der Verantwortung der AG Epilepsiechirurgie
- Die Zentrumsliste wird verantwortlich durch den benannten leitenden Prüfarzt verwaltet und sicher aufbewahrt.
- Die Eingabe und Verwaltung der Patientendaten in der Datenbank erfolgt im Behandlungszeitraum verantwortlich durch den behandelnden Prüfarzt.

## 6.1. Generelles Prinzip der Pseudonymisierung von Daten und Proben

### 6.1.1. Pseudonymisierungsverfahren

Das Prinzip der strikten Pseudonymisierung aller Daten gilt generell.
Bei der Aufnahme eines neuen Probanden in das Register werden Name, Adresse, Geburtsdatum und Geschlecht des Probanden in einem vom RDE-System zur Verfügung gestellten Formular erfasst, um das Pseudonym des Probanden zu erzeugen (s. Anhang 5 „Pseudonymisierungsbeschreibung“).
Zu keiner Zeit werden diese personenbezogenen Daten, weder auf dem lokalen Rechner des Prüfarztes noch im zentralen Register, gespeichert. Das RDE-System erzeugt lediglich einen Ausdruck, der diese Daten zusammen mit dem Pseudonym enthält. Der Pseudonymisierungsalgorithmus des SecuTrial-Systems arbeitet völlig unabhängig von personenbezogenen Daten. Bei Sendung der Anforderung „neuer Patient“ an das SecuTrial-System sendet dieses ein leeres Formular und ein Pseudonym an den Browser des Arztes. Das Pseudonym wird dabei über einen mit Huch-Algorithmus versehenen Zufallsgenerator aus den möglichen Pseudonymen aaa000 bis zzz999 erzeugt. Das SecuTrial-System prüft in der Datenbank, ob es dieses Pseudonym schon gibt. Wenn ja, wird diese Pseudonymgenerierung so oft wiederholt, bis ein noch nicht verwendetes Pseudonym generiert ist.

Aus diesem Grunde ist die Pseudonymisierung des SecuTrial-Systems (im Gegensatz zu Verfahren, die in einigen anderen Systemen verwendet werden) völlig ausprobiersicher. Während es in Programmen, die aus den personenbezogenen Daten des Patienten das Pseudonym generieren, möglich ist, durch probeweise Eingabe von bekannten personenbezogenen Daten eines Patienten ein Pseudonym zu erzeugen und dann in der Datenbank danach zu fahnden – was die Erkenntnis liefern würde, dass die entsprechende Person in der Datenbank vorhanden ist – erzeugt das SecuTrial-System jedes Mal ein neues Pseudonym.
In das gesendete leere Formular (s.o.) kann der Prüfarzt die personenbezogenen Daten des Patienten (abgestimmt mit der wissenschaftlichen Leitung der AG Epilepsiechirurgie) eintragen. Das Formular wird dann mit dem Pseudonym an den lokalen Drucker des Arztes gesendet, so dass ein sauber gedruckter „Merkzettel“ für die Ablage entsteht. Die in dieses Formular eingetragenen personenbezogenen Daten werden weder auf dem lokalen Rechner des Arztes gespeichert, noch an den Server zurück geschickt. Nach Ausdruck des Formulars wird lediglich das Pseudonym zurück mit dem Befehl, einen neuen Datensatz anzulegen, an die Datenbank geschickt (s. grafische Darstellung in der Anlage).
Das ausgedruckte Formular wird in der Patientenakte aufbewahrt, um die Falldokumentation in der Datenbank fortführen und zuordnen zu können. Die Patientenakten per se unterliegen selbst dem Datenschutz und werden stets verschlossen aufbewahrt, so dass andere außer dem behandelnden Arzt (und dessen direkte Vertreter), keinen Zugang zu der Akte im Behandlungsverlauf erhalten. Eine Kopie wird in einer Zentrumsliste abgelegt. Die Verantwortung für diese Zentrumsliste wird pro Zentrum dem Projektverantwortlichen übertragen, der namentlich benannt wird. Seine Rolle besteht darin, die PID-Zentrumsliste zu verwalten und an einem sicheren Ort innerhalb des Zentrums unter Verschluss aufzubewahren. Einen Zugang zu dieser Liste hat nur diese Person. Informationen zu PIDs sind im konkret erforderlichen (s.u.) Fall nur über diese definierte Person zu erhalten. Andere Prüfärzte des Zentrums erhalten keinen Einblick in die Zentrumsliste.

### 6.1.2. Fallgruppen und Abläufe der Re-Identifikation

Eine **Re-Identifikation** von Patienten ist erforderlich

i) innerhalb des Behandlungszentrums

a. bei Auswertung der eigenen, zentrumsinternen Daten, sofern widersprüchliche oder unlogische Angaben in der Datenbank auftreten, die einer Nachprüfung in der Akte bedürfen
b. Wunsch eines Probanden, Einsicht in seine Daten zu nehmen.
c. Bei Interesse des Patienten, an einer Studie eines anderen Zentrums teilzunehmen, die weitere studienbezogene Handlungen am Patienten erfordert, wobei hier vor der Übermittlung des Datensatzes die Pseudonymisierungsnummer durch die lokale Studiennummer ersetzt werden muss.

In diesen Fällen nimmt der leitende Prüfarzt des Zentrums die Re-Identifikation vor.
Bei Wunsch eines Probanden, über wissenschaftliche Ergebnisse informiert zu werden, ist keine Re-Identifikation erforderlich, da die Ergebnisse der Datenanalyse nur anonymisiert dargestellt werden (statistische Werte). Entsprechende Publikationen sind öffentlich und können dem Anfragenden zugestellt werden.

### 6.1.4. Anonymisierung der Daten

Im Falle des Versterbens eines Probanden sowie auf Wunsch des Probanden werden die Daten anonymisiert. Im Falle des Todes eines Patienten werden dessen Daten noch einmal durch den leitenden Prüfarzt des Behandlungszentrums auf Korrektheit überprüft und dann der Datensatz auf „Data Entry complete“ gesetzt. Das sperrt die Datenformulare für weitere Bearbeitungen. Danach setzt der Prüfarzt den Patientenstatus auf „Patient verstorben“. Diese Eingabe löst eine Anonymisierung der Daten aus.

## 6.2. Ausschuss Datenschutz

Der Verein „prächirurgische Epilepsiediagnostik und operative Epilepsietherapie gem. e.V.“ verfügt über eine Datenschutzkommission, die alle Belange hinsichtlich Datenaustausch und -zugang regelt **(vgl. § zur Datensicherheit der Vereinssatzung, Anhang XX, Passus der ergänzt werden sollte?)**.

Dem Ausschuss „Datenschutz“ kommen folgende Aufgaben zu:

- Bewertung und Bewilligung der Anträge von Wissenschaftlern auf die Bereitstellung von Datensätzen. Mit der Bewilligung sind zu definieren:
  - der auf das Forschungsprojekt zugeschnittene Datensatz
  - die anzuwendenden Selektionsfilter
  - der Zugang zu pseudonymisierten oder anonymisierten Daten
- Bewertung und Bewilligung von Anträgen auf Übermittlung von Forschungsergebnissen an Patienten durch die behandelnden Ärzte.
- Die Beauftragung der zentralen Dienste und die Verabschiedung der Nutzungsordnungen für diese zentralen Dienste, welche die für Datenschutz und Datensicherheit relevanten Regeln enthalten.

Die Mitglieder des Ausschusses "Datenschutz" werden von der Mitgliederversammlung gewählt. Der Ausschuss "Datenschutz" wird in Datenschutzfragen von IT-Experten und / oder Rechtsbeiständen beraten.

## 6.3. Streng kontrollierte Weitergabe von Daten und Material für Forschungsfragen

### 6.3.1. Zentrumsinterne Datenauswertung

Prinzipiell kann jedes Zentrum Daten, die es selbst in der klinischen Routine gesammelt hat, auswerten (vgl. 6.1.): Der wissenschaftliche Beirat der Bundesärztekammer hat in seinen „Empfehlungen hinsichtlich der Wahrung der ärztlichen Schweigepflicht und des Datenschutzes in der medizinischen Forschung“ (Deutsches Ärzteblatt 1989) deutlich betont, dass die Doppelrolle Arzt/Forscher vom Arzt ein Handeln verlangt, das sowohl der Wahrung des Patientengeheimnisses als auch der angemessenen Durchführbarkeit der medizinischen Forschung dienen soll und entsprechende Gebote formuliert. Ganz

deutlich ist jedoch auch das Recht des Arztes auf Forschung mit „eigenen Daten“ bestätigt:

„Ärzte dürfen Patientendaten, die innerhalb ihrer Fachabteilung oder bei Hochschulen innerhalb ihrer Klinik oder sonstigen medizinischen Einrichtungen gespeichert sind, für eigene wissenschaftliche Forschungsvorhaben verarbeiten. Dies gilt auch für sonstiges wissenschaftliches Personal, das der Schweigepflicht unterliegt.“

Dementsprechend ermöglich auch die AG Epilepsiechirurgie den Mitgliedszentren die Forschung mit „eigenen Daten“. Die Exportfunktion der medizinischen Datenbank beschränkt die Exportmöglichkeiten für den einzelnen Prüfarzt strikt auf die Daten des eigenen Zentrums. Dabei kann der Prüfarzt wählen, ob die Daten anonymisiert oder pseudonymisiert exportiert werden. Für die meisten Auswertungen (deskriptive Statistiken, Häufigkeitsverteilungen, Korrelationen etc.) ist die Verwendung anonymisierter Daten völlig ausreichend.

Gerade bei Auswertungen im Zusammenhang mit der Qualitätssicherung des ärztlichen Handelns und damit auch mit der Qualitätssicherung der in der medizinischen Datenbank gespeicherten Daten kann es jedoch notwendig werden, unlogische oder unplausible Daten mit der Patientenakte abzugleichen. In diesen Fällen ist die Verwendung von Datenauszügen mit Pseudonym unerlässlich, da sonst ein Rückgriff auf die Patientenakte nicht erfolgen kann.

Dem Prüfarztvertrag wurde eine Empfehlung hinzugefügt, dass Daten des eigenen Zentrums, an deren Auswertung auch Ärzte oder medizinisches Personal beteiligt werden sollen, die keinen Prüfarztvertrag der AG Epilepsiechirurgie haben, ausschließlich in anonymisierter Form an diese „externen“ Ärzte gegeben werden.

### 6.3.2. Zentrumsübergreifende Datenauswertung

Der Zugriff auf Daten und Material der anderen Zentren wird vom fein skalierten Rollen- und Rechtesystem des zentralen Datenbanksystems von vornherein verhindert.

Die Bereitstellung von Daten und/oder Material für wissenschaftliche Untersuchungen an Forscher und/oder Forschergruppen über diese Zentrumsgrenzen hinaus muss schriftlich beim Forschungsbeirat der AG Epilepsiechirurgie beantragt werden. Wichtigstes Kriterium ist die

wissenschaftliche Qualität der geplanten Studie. Zur Begutachtung der Qualität können Gutachten von auswärtigen Gutachtern eingeholt werden. Stimmt der Forschungsbeirat. Nach mehrheitlicher Befürwortung des Antrags wird der Ausschuss Datenschutz informiert, der die Notwendigkeit der angeforderten Informationen zur Beantwortung der Fragestellung überprüft. Alle Mitglieder des Ausschuss Datenschutz müssen der Weitergabe zustimmen. Der Ausschuss Datenschutz meldet seine Zustimmung dem Forschungsbeirat. Dieser beauftragt das zentrale Data Management, die beantragten Daten aus der Datenbank zu extrahieren und den Antragstellern zur Verfügung zu stellen. Erst nach schriftlicher Genehmigung aller Mitglieder des Ausschuss Datenschutz und dessen schriftlichem Auftrag wird das Datenmanagement der AG Epilepsiechirurgie **(Central Information Office des Kompetenznetz Parkinson, Universität Marburg) [Anmerkung der Verfasserin: Muss ersetzt werden durch eigene Stelle]** tätig und erstellt einen Datenauszug entsprechend dem schriftlichen Auftrag.
Dabei bestimmt der Ausschuss Datenschutz je nach Forschungsfrage, ob den anfragenden Forschern die Daten in anonymisierter oder pseudonymisierter Form zur Verfügung gestellt werden. Wie oben bereits dargestellt, sind die meisten wissenschaftlichen Auswertungen ohne weiteres mit anonymisierten Daten möglich. Dementsprechend wird der Ausschuss Datenschutz auch in aller Regel bestimmen, dass die Daten dem anfragenden Mitglied anonymisiert zur Verfügung gestellt werden.

Die Verwendung pseudonymisierter Daten ist denkbar bei Fragestellungen einer zentrumsübergreifenden Qualitätssicherung (im Sinne eines externen Monitoring) mit anschließendem Abgleich „auffälliger Daten“ über Source Data Verification (Patientenakte).
Ein externes Monitoring soll nur in diesem Fall und stichprobenartig erfolgen um die Integrität der Patientendaten gewährleisten. Die Integrität der Patientendaten ist eines der sieben Grundziele der im BDSG festgelegten Sicherheitsanforderungen, das besagt, dass die personenbezogenen Daten während aller Phasen der Verarbeitung unversehrt, vollständig, gültig und widerspruchsfrei bleiben müssen. Dieses Erfordernis hat im Bereich medizinischer Netze naturgemäß eine besonders große Bedeutung. Sind Patientendaten unvollständig oder verfälscht, kann dies zu falschen

medizinischen Entscheidungen und Empfehlungen führen, verbunden mit haftungsrechtlichen Konsequenzen für den Mediziner.
Aus diesem Grunde ist die Verwendung pseudonymisierter Daten für den beschriebenen Qualitätssicherungszweck auch datenschutzrechtlich nicht nur zu vertreten, sondern sogar geboten.
Eine Weitergabe von Daten an Forscher, die nicht über Prüfarztvertrag an die AG Epilepsiechirurgie gebunden sind, ist nicht vorgesehen. (S. Anhang 6 „Genehmigung an den Ausschuss Datenschutz“).

### 6.4. Prinzip der Datensparsamkeit

Bei der Konzeption der Erfassungsformulare für das zentrale Register der AG Epilepsiechirurgie wurde strikt auf größtmögliche Datensparsamkeit geachtet.
Aufgrund des Forschungszweckes sind folgende personenbezogene Daten unerlässlich: Geburtsmonat, -jahr (nicht: -tag) und Geschlecht sowie Daten zur sozialen Situation des Patienten (z.B. allein lebend, im Pflegeheim lebend). Es werden jedoch keinerlei Angaben über den Wohnort (z.B. Ortsname / PLZ o.ä.) gemacht. Die Patienten, die zur präoperativen Abklärung ein Epilepsiezentrum aufsuchen, kommen aufgrund der großen Einzugsgebiete der Zentren nicht regelhaft aus der Region, sodass auch aus der Zentrumsnummer kein Rückschluss auf den Wohnort möglich ist (s. Anhang 1 „Minimal Dataset“.

### 6.5. Unaufgeforderte Vorlage einer kurzen Patienteninformation und Einholung einer schriftlichen Einwilligung in die elektronische Datenspeicherung.

Die Datengewinnung erfolgt im Rahmen der Routinediagnostik zur Sicherheit des Patienten; es erfolgen keine zusätzlichen Eingriffe, es handelt sich nicht um eine experimentelle Studie. Gemäß den Ethik-Kommissionen sind deshalb für diese reinen Anwendungsbeobachtungen keine Patientenaufklärungen und schriftliche Einwilligungserklärungen zu den Projektinhalten erforderlich. Jedoch wird allen Patienten bzw. ihren Sorgeberechtigten oder gesetzlichen Betreuern der Patienten, eine Information und Einverständniserklärung zur elektronischen Datenspeicherung personenbezogener Daten vorgelegt**.** Das darüber hinausgehende generelle Interesse an einer Studienteilnahme muss von der entsprechenden Person gesondert schriftlich bekundet werden (vgl. Anhang 2 „Patienteninformation“). Die Information und Einverständniserklärung erfolgt im

Falle einer Studienteilnahme gesondert, wobei der behandelnde Arzt die erste Information über die Studie gemäß der für die Studie gültigen Patienten-information übermittelt und für Rückfragen zur Verfügung steht.

### 6.6. Formulare zum Widerruf des Patienten und Vorgehen beim Löschen von Daten im Fall des Widerrufs

Der Patient kann seine Einwilligung zur Speicherung von Daten im Register AG Epilepsiechirurgie jederzeit widerrufen. Dafür werden ihm Formulare zur Verfügung gestellt, mit denen er seinen Widerrufswillen skaliert kundtun kann (s. Anhang 7 „Widerruf“).

Das zentrale Register-System stellt Automatismen bereit, die es den Datenverantwortlichen erlauben, unverzüglich auf den Widerruf eines Patienten zu reagieren.

## 8. Anlagen

1. Protokollauszüge der AG Epilepsiechirurgie (Minimal-Dataset)
2. Patienteninformation und Einwilligungserklärung zur elektronischen Datenverarbeitung (Version vom 13.10.10)
3. Datenschutzgutachten zu SecuTrial 2.1.
4. Prüfarztvereinbarung (Version vom 13.10.10)
5. Pseudonymisierungsbeschreibung
6. Antrag auf Genehmigung an den Ausschuss Datenschutz und Genehmigungsformular der Mitglieder des Ausschuss Datenschutz
7. Widerruf der Einwilligung zur Datenspeicherung im Register der AG Epilepsiechirurgie

**XX:** Zu Ergänzen: Satzung der AG Epilepsiechirurgie (oder gesonderter Satzung für Datenbank) mit entsprechendem Passus über Datensicherheit und Passus über Voraussetzungen für die Mitgliedschaft

**Stand: 14.10.10**