Datenschutzkonzept des Deutschen NET-Registers

Version 2.1, Juli 2021

Inhaltsverzeichnis

Grundsätzliches

Das „Deutsche Register Neuroendokrine Tumore“ (NET-Register) ist ein Projekt der Arbeitsgemeinschaft Endokrine und Neuroendokrine Onkologie (AG-ENEO) in der Deutschen Gesellschaft für Endokrinologie (DGE) e.V.. Das Register verpflichtet sich zur Einhaltung des Datenschutzes und der Datensicherheit gemäß den Regelungen der Europäischen Datenschutzgrundverordnung (DSGVO) insbesondere Artikel 9 (Verarbeitung besonderer Kategorien personenbezogener Daten) und des Bundesdatenschutzgesetzes sowie sonstiger anwendbaren datenschutzrechtlichen Regelungen.
Es werden die technisch-organisatorischen Maßnahmen zur Gewährleistung des Datenschutzes und der Datensicherheit bei der Erhebung, Verarbeitung und Nutzung der Daten des deutschen NET-Registers angewandt. Die DGE hat die volle Verantwortung für die Daten. Die Einhaltung der datenschutzrechtlichen Regelungen wird durch den Datenschutzbeauftragten der DGE überprüft.

Hintergrund der Studie

Das „Deutsche Register Neuroendokrine Tumore“ (NET-Register) untersucht wissenschaftlich die Langzeitmorbidität und Mortalität neuroendokriner Neoplasien (NEN) und fördert die Qualitätskontrolle in Diagnostik und Therapie.
Neuroendokrine Neoplasien sind Tumore, die aus den Zellen des disseminierten neuroendokrinen Systems entstehen. Am häufigsten treten sie im Gastrointestinaltrakt einschließlich der Bauchspeicheldrüse (gastroenteropankreatisch) und in der Lunge auf. Die neuroendokrinen Neoplasien zählen zu den seltenen Tumoren. Doch zeigt sich in mehreren Studien ein enormer Anstieg der Inzidenz (Anzahl der Neuerkrankungen) in den letzten Jahrzehnten. Neuroendokrine Neoplasien können in jedem Alter auftreten, wobei das mittlere Diagnosealter des Gesamtkollektivs in den meisten epidemiologischen Studien um die 60 Jahre liegt.
Patienten, die neuroendokrine Tumore im Rahmen des genetisch bedingten MEN-1-Syndromes (Multiple Endokrine Neoplasie) entwickeln, aber auch Patienten mit Neuroendokrinen Tumoren der Appendix, sind bei Erstdiagnose durchschnittlich deutlich jünger.

Ziele der Studie

• Erfassung und Dokumentation von Patientendaten aus der NET-Routinebehandlung in spezialisierten Zentren in Deutschland

• Analyse der Qualität der Behandlung und Betreuung von NET-Patienten in Deutschland

• Dokumentation und Auswertung von Langzeitverläufen der NET-Behandlung

• Analyse des Stellenwertes unterschiedlicher Therapieverfahren in der Routineversorgung von NET-Patienten in Deutschland

• Auswertung der Behandlungsresultate und Langzeitergebnisse unterschiedlicher Therapieverfahren in der Routinebehandlung der NET-Behandlung

Ziele der technisch-organisatorischen Maßnahmen des Datenschutzes und der Datensicherheit

Die Ziele sind ausgerichtet an Artikel 5 der DSGVO (Grundsätze für die Verarbeitung personenbezogener Daten) sowie Kapitel 2und §§ 47 und 64 des BDSG und Artikel 9 der DSGVO (Verarbeitung besonderer Kategorien personenbezogener Daten):

• Datenminimierung und Speicherbegrenzung / Berücksichtigung von Datensparsamkeit und Erforderlichkeit

• Rechtmäßigkeit und Richtigkeit / Strikte Zweckbindung der erhobenen Daten für die angegebenen Zwecke und Überprüfung der sachlichen Richtigkeit

• Vertraulichkeit / Der Zutritt und Zugang zum Datenbank-Server durch unbefugte Personen sind zu verhindern. Der Zugriff auf die Daten der Registerdatenbank durch unbefugte Personen bzw. automatisierte Verfahren ist zu verhindern. Zugriff auf die Daten wird nur denjenigen Personen erteilt, die eine Datenschutz- und Verschwiegenheitserklärung gemäß den Regelungen der DSGVO unterzeichnet haben.

• Vertraulichkeit und Integrität / Die Auswertung der Daten der Register-Datenbank ist zentrumsbezogen nur für die jeweiligen Zentren und registerbezogen nur für den Vorstand bzw. die durch Vorstand und DGE beauftragte Firma zulässig. Eine Weitergabe der Daten der Registerdatenbank ohne vorausgegangene Abstimmung mit dem Registervorstand ist nicht zulässig. Eine automatisierte Weitergabe der Daten ist technisch zu verhindern.

• Transparenz / Jegliche Form von Datenverlust, -manipulation, -missbrauch und -diebstahl ist zu vermeiden.

Organisatorische Struktur des deutschen NET-Registers

Das deutsche NET- Register untersucht wissenschaftlich die Langzeitmorbidität und Mortalität neuroendokriner Neoplasien (NEN) und fördert die Qualitätskontrolle in Diagnostik und Therapie.
Es wurde 2004 gegründet, hat zum gegenwärtigen Zeitpunkt über 60 aktive Mitglieder (Zentren). In den zurückliegenden Jahren wurden über 4000 Patienten in pseudonymisierter Form in das Register aufgenommen.
Das Register wird geführt von der AG ENEO der Deutschen Gesellschaft für Endokrinologie (DGE). Der Vorstand besteht aus acht Mitgliedern und dem Sekretär. Die Mitglieder des Vorstandes müssen volle oder assoziierte Mitglieder der DGE sein.

Die Teilnahme am NET-Register steht allen in der Betreuung von NEN-Patienten tätigen Einrichtungen (Kliniken und Praxen) in Deutschland durch einfache Absichtserklärung gegenüber dem Vorstand offen. Voraussetzung ist die Anerkennung der Satzung. Die Mitgliedschaft wird vom Vorstand schriftlich bestätigt.
Von einem Mitglied wird die Einholung und Vorlage eines Ethikvotums der zuständigen Ethikkommission zum pseudonymisierten Einschluss von Patienten in das NET-Register erwartet.
Eine kontinuierliche Dateneingabe von jährlich mindestens zwei Fällen soll erfolgen.
Zunächst wurden die Daten retrospektiv und prospektiv erhoben. Aktuell erfolgt eine prospektive Datenerhebung. Des Weiteren ist jedes Zentrum verpflichtet, sich um die Vollständigkeit der

abzufragenden Daten aller betreuten Patienten zu bemühen, um so die angestrebte Datenqualität des Registers zu gewährleisten.
Jedes Zentrum hat unbeschränkten Zugriff auf seine eigenen Daten.

Datenerhebung

Die Datenerfassung erfolgt durch die behandelnden Ärzte in den beteiligten Zentren oder durch von Ihnen beauftragte, der ärztlichen Schweigepflicht unterliegende Personen unter Berücksichtigung beiliegender Erfassungsinhalte. Die Dateneingabe erfolgt durch die behandelnden Ärzte oder ihre Beauftragten in den beteiligten Zentren über einen passwort-geschützten und personengebundenen Zugang zur Datenbank. Voraussetzung für die Erfassung der Daten eines Patienten mit nachfolgender Eingabe in die Registerdatenbank ist das Vorliegen einer unterschriebenen Einverständniserklärung durch den betreffenden Patienten. Der Patient ist im Vorfeld der Erteilung der Einverständniserklärung durch einen Arzt zu den im Zusammenhang mit einer Aufnahme in das Register bestehenden Details aufzuklären. Sollte ein Patient ein bereits erteiltes Einverständnis widerrufen, so sind seine Daten zu löschen, wenn dies gewünscht wird.

Datenmanagement

Die Datenverarbeitung, Speicherung und Gewährleistung der Wahrung der datenschutzrechtlichen Bestimmungen (DSGVO und Datenschutzgesetz) sowie die gesamte technische Leitung erfolgt durch den Kooperationspartner (Firma Lohmann & Birkner, Health Care Consulting GmbH, Berlin) oder die von ihr beauftragten Firmen.
Es handelt sich dabei um eine Auftragsdatenverarbeitung, die vertraglich geregelt ist. Eine Beauftragung von Firmen in sogenannten Drittstaaten ist per Auftragsverarbeitungsvertrag ausgeschlossen.

Pseudonymisierung / Anonymisierung

Die Patientendaten werden im Zentrum durch den Zentrumsleiter für das NET-Register oder einen durch ihn beauftragten Mitarbeiter pseudonymisiert in die webbasierte Datenbank eingespeist. Das bedeutet, dass in der Datenbank keine personenbezogenen Daten wie Name, Vorname und Anschrift des Patienten erscheinen, sondern lediglich sein Geburtsjahr, das Geschlecht und eine ID-Nummer.
Eine automatisierte Datenverarbeitung personenbezogener Daten findet im Rahmen der webbasierten Datenerhebung auf Grund der Pseudonymisierung nicht statt.
Im Zentrum selbst wird durch die dort zuständigen Mitarbeiter eine ID-Liste geführt, die die ID-Nummer dem konkreten Patienten mit Namen, Vornamen und Geburtsjahr zuordnet. Auf diese Weise ist die Nachverfolgung des Patienten im zuständigen Zentrum bei den behandelnden Ärzten, und ausschließlich dort, sichergestellt. Die Mitarbeiter, die diese Liste erstellen, die Daten erheben und diese in die webbasierte Datenbank eingeben, sind zur Beachtung aller relevanten datenschutzrechtlichen Regelungen verpflichtet. Diese Verpflichtung wird in schriftlicher Form mit Unterschrift des Mitarbeiters dokumentiert (siehe Anhang).
Verantwortliche Personen in den teilnehmenden Zentren sind alle Mitarbeiter, die mit der Datenerhebung betraut wurden und über einen persönlichen Zugang zur webbasierten Datenbank verfügen.

Die Validierung der Daten erfolgt datenbankseitig in pseudonymisierter Form. Die Informationen bezüglich der Datenqualität werden anhand der ID-Nummern mit den zuständigen Mitarbeitern in den jeweiligen Zentren kommuniziert.
Im Rahmen des Monitorings vor Ort wird anhand der dort hinterlegten ID-Listen sowie der bereitgestellten klinischen Dokumentationsmaterialien eine Überprüfung der Datenqualität vorgenommen. Die Kenntnis der Namen ist den Monitoren nur im Rahmen dieses Besuches gegeben. Die Monitore, die durch den Vorstand des Registers mit dieser Aufgabe beauftragt werden, sind zur Beachtung aller relevanten datenschutzrechtlichen Regelungen verpflichtet. Diese Verpflichtung erfolgt durch Setzen der Unterschrift des Mitarbeiters unter das entsprechende Dokument.

Die Anonymisierung von Daten erfolgt entweder, wenn ein Zentrum nicht mehr aktiv an der Dateneingabe beteiligt ist oder ein Patient sein Einverständnis zur weiteren Dateneingabe entzieht. Wenn ein Zentrum nicht mehr aktiv an der Dateneingabe beteiligt ist, erfolgt durch die IT / Administratoren bei Lohmann&Birkner die manuelle Bearbeitung der Datensatz-ID. Hierbei wird das zentrumsbezogene Präfix durch ein neutrales Präfix ersetzt.

Bei Widerruf der Einwilligung zur Datenerhebung durch einen Patienten (ohne Wunsch zur Löschung) wird der Datensatz des Patienten anonymisiert (die Zuordnung zum Behandlungszentrum wird gelöscht – der Datensatz bleibt für Auswertungen erhalten). Diese Anonymisierung kann nur datenbankseitig (durch Beauftragung von IT-Mitarbeitern der Firma L&B) erfolgen. Bei Widerruf der Einwilligung verbunden mit der Forderung zur Löschung aller bisher erhobenen Daten wird der gesamte Datensatz des Patienten gelöscht. Dafür gibt es einen entsprechenden „Löschen"-Button auf der Startseite der Dateneingabe, der von jedem User bedient werden kann.

Datenbankstruktur

Angaben zum Server:

Web Server:	Glassfish 3
IP-Adresse:	85.214.27.136
Hosting:	STRATO AG, Pascalstr. 10, 10587 Berlin (strato.de)
Housing:	STRATO AG, Pascalstr. 10, 10587 Berlin
Windows-Server:	Windows Server 2012 R2
Zugang:	Remote

Die STRATO AG kann per Zertifikat (DIN EN 27001) höchste Anforderungen an Zutritts-, Zugangs- und Zugriffskontrolle sicherstellen.
Die vertragliche Verantwortung gegenüber der Lohmann & Birkner Health Care Consulting GmbH und damit gegenüber dem Deutschen NET-Register der DGE obliegt der Firma STRATO. Sie stellt sicher, dass die Internet-Anbindung des Servers hinter einer sicheren Firewall platziert ist und die Datenübertragung den Anforderungen, die an eine webbasierte Datenbank dieser Größenordnung gestellt werden, entspricht.
Die Firma STRATO ist zur Beachtung aller relevanten datenschutzrechtlichen Regelungen verpflichtet.
Der Server selbst ist Eigentum der Deutschen Gesellschaft für Endokrinologie (DGE) e.V.. Er steht lediglich im Auftrag der Lohmann & Birkner Health Care Consulting GmbH in den Räumen der STRATO AG.
Die Pflege der erforderlichen Server-, Datenbank- und Internet-Software obliegt der technischen Projektleitung des Registers, in diesem Fall der Lohmann & Birkner Health Care Consulting GmbH.

Dazu gehören alle Tätigkeiten, die mit der Pflege der Server-Software im Zusammenhang stehen sowie die wöchentlichen und monatlichen Datensicherungen.

Angaben zur Datenbank:

Name:	oracle
Version:	11 XE
Lizensiert:	unbegrenzt

Angaben zur Domain:

Name:	dge-register.de
URL:	https://www.dge-register.de/netregister/
Hosting:	DomainFactory GmbH, Oskar-Messter-Str. 33, 85737 Ismaning (df.eu)

Angaben zum Sicherheitszertifikat:

Name:	SSL Encryption (128Bit) TLS1.0 (Version 3)
Lizensiert:	für jeweils 1 Jahr

Angaben zur Firewall:

Name:	Windows-Firewall (Domainprofil) Symantec Endpoint Protection

Angaben zur Datensicherung:

lokal:	2x wöchentlich und 1x monatlich via DB-Dump
Sicherungskopie:	jährliche CD: Daten-Dump im CSV-Format und Software als WAR-Datei Per Kurier an die DGE-Geschäftsstelle

Angaben zur Technischen Ausstattung:
Verwendete Software:
- Java 7, inkl. JavaServer Faces JSF-API
- PrimeFaces JSF-Komponenten- framework
- Hibernate-ORM-framework
- erforderliche Systemprogramme

Zugang zur webbasierten Registerdatenbank:
- an jedem PC mit Internetanschluss,
- unter Nutzung einer Browsersoftware und
- unter Benutzung eines Passwortes, zugehörig zu einem Benutzernamen

sind ausreichende Sicherheitsmaßnahmen zu ergreifen, die einen unautorisierten, unerlaubten Zugriff zu den Daten der webbasierten Datenbank verhindern.

Technisch-organisatorische Schutzmaßnahmen

Die Dokumentation der technisch-organisatorischen Schutzmaßnahmen werden der DGE im Rahmen des Auftragsverarbeitungsvertrages bei Bedarf aktualisiert mitgeteilt.

Zutrittskontrolle (betrifft ausschließlich den Server als Gerät)
Ziel der Zutrittskontrolle ist es, mit Hilfe geeigneter baulicher, technischer, organisatorischer und personeller Maßnahmen zu verhindern, dass Unbefugte Zutritt zu Datenverarbeitungsanlagen haben:

Sicherstellung durch folgende Maßnahmen:

- Sichere Aufstellung des Servers in den Räumen der „STRATO AG“
- Sicherstellung der Zutrittskontrolle zur Verhinderung des Zutritts durch unbefugte Personen.

Zugangskontrolle

Ziel der Zugangskontrolle ist es, mit Hilfe geeigneter Maßnahmen das Eindringen in Datenverarbeitungssysteme und deren Nutzung seitens Unbefugter im arbeitstäglichen Gebrauch auszuschließen.

Sicherstellung durch folgende Maßnahmen:

- Personengebundenes Passwort, es wird offiziell auf Antrag vergeben und gilt ausschließlich für den User, der den Antrag gestellt hat. Es ist an den jeweiligen Usernamen gebunden.
- Die Bekanntgabe und Weitergabe des Passwortes ist untersagt.
- Abschottung gegen Zugriffe von extern durch Nutzung einer Firewall sowie eines kryptografischen Protokolls bei der Datenübertragung im Internet.
- Die Adresse der Website, von der aus der Zugriff zur Register-Datenbank erfolgt, ist nur den gelisteten Usern, die über ein Passwort verfügen, bekannt. Eine Verlinkung von anderen Webseiten sowie die Mitteilung der Webseiten-Adresse an nichtgelistete User ist nicht zulässig.
- Die STRATO AG hat keinen Zugang zu den Daten des Servers, der sich in Ihren Räumen befindet. Ihre Aufgabe ist es lediglich, den Server in seiner Internet-Anbindung hinter einer sicheren Firewall zu platzieren und die erforderliche Datenübertragungsrate sicherzustellen.

Zugriffskontrolle

Ziel der Zugriffskontrolle ist zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten – unabhängig vom Speichermedium - bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Sicherstellung durch folgende Maßnahmen:

- Autorisierte Vergabe, Änderung und Entzug von Zugriffsberechtigungen
- Funktionelle und/oder zeitlich beschränkte Nutzung
- Automatische Sperrung bei Nichtnutzung der Eingabemaske nach 15 Minuten
- Automatische Sperrung von Zugangsberechtigungen bei dreimaliger Falscheingabe in Folge
- Verwaltung, Lagerung und Vernichtung von Datenträgern (Datensicherung)
- Zugriff auf die Daten wird nur denjenigen Personen erteilt, die eine Datenschutz- und Verschwiegenheitserklärung gemäß den Regelungen der DSGVO unterzeichnet haben.
- Nur die Daten des eigenen Zentrums des jeweiligen Users sind einsehbar.
- Zugangsberechtigungen konkret (betrifft Lesen, Bearbeiten, Löschen, Auswerten=Abfragen)
    - jeder User hat Zugriff zu den Daten aller erfassten Patienten seines Zentrums,
    - Vorstand und Mitarbeiter der technischen Projektleitung der Lohmann & Birkner Health Care Consulting GmbH haben Zugriff zu den Daten aller erfassten Patienten aller Zentren

Weitergabekontrolle

Ziel der Weitergabekontrolle ist es, mit Hilfe geeigneter Maßnahmen zu gewährleisten, dass personenbezogene Daten / Sozialdaten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass im Bedarfsfall überprüft und festgestellt werden kann, an welchen Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

Sicherstellung durch folgende Maßnahmen:

- SSL-Standard der Datenübertragung
- Eine erste Weitergabe von Daten erfolgt bereits im Prozess der webbasierten Dateneingabe am PC unter Nutzung eines Internet-Browsers und in die webbasierte Datenbank.
- Grundlage für die gesicherte Übermittlung dieser Daten ist der SSL-Standard. SSL (= Secure Sockets Layer) ist ein kryptografisches Protokoll zur sicheren Datenübertragung im Internet. Es wird für Browser, Email-Programme, Internet-Fax und andere Datenübertragungen genutzt.
- Das SSL Record Protocol dient zur Absicherung der Verbindung durch End-zu-End-Verschlüsselung mittels symmetrischer Algorithmen. Der verwendete Schlüssel wird dabei im Voraus über ein weiteres Protokoll (zum Beispiel das SSL Handshake Protocol) ausgehandelt und kann nur einmal für die jeweilige Verbindung verwendet werden. Zu sichernde Daten werden in Blöcke von maximal 65.536 (2_{16}) Byte fragmentiert und beim Empfänger wieder zusammengesetzt.
- Das SSL Handshake Protocol baut auf dem SSL Record Protocol auf und erfüllt die folgenden Funktionen, noch bevor die ersten Bits des Anwendungsdatenstromes ausgetauscht wurden:
    - Identifikation und Authentifizierung der Kommunikationspartner auf Basis asymmetrischer Verschlüsselungsverfahren und Public-Key-Kryptografie. Im Normalfall authentifiziert sich zumindest der Server gegenüber dem Client.
    - Aushandeln zu benutzender kryptografischer Algorithmen und Schlüssel.
- Die Weitergabe umfangreicher Datensätze aus der webbasierten Datenbank darf nur in Abstimmung mit dem Vorstand des NET-Registers erfolgen, z.B. im Rahmen von regulären Auswertungen für Vollversammlungen und Jahresberichte sowie für die Bereitstellung ausgewählter Daten für die Durchführung von wissenschaftlichen Auswertungen. Das Format und Umfang des zu verschickenden Datensatzes werden durch den Registervorstand festgelegt und sind bei der Weitergabe einzuhalten.
- Der jeweilige Datensatz ist mit einem Kennwort zu versehen. Entsprechend Umfang bzw. Brisanz des Datensatzes ist der Zustellungsweg zu wählen (z.B. Datenträger mit verschlüsselten Daten auf dem Postweg verschicken). Die beteiligten Projektmitglieder sind in diesem Zusammenhang auf mögliche Sicherheitslücken, die sich bei der Versendung als Email ergeben könnten, hinzuweisen.

Eingabekontrolle

Ziel der Eingabekontrolle ist es, mit Hilfe geeigneter Maßnahmen sicherzustellen, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten / Sozialdaten in Datenverarbeitungssysteme/n eingegeben, verändert oder entfernt worden sind.

Sicherstellung durch folgende Maßnahmen:

- Protokollierung der Zugriffsberechtigungen (Beginn, Ende, Rechte)
- Eine Protokollierung aller Eingaben, Änderungen und Löschungen und Zuordnung zu den jeweiligen Nutzern erfolgt nicht
- Der Benutzer, der die Dateneingabe in einem Zentrum vornimmt, hat nur Zugriff auf die Daten der für dieses Zentrum erfassten Fälle. Er sieht in der ebenfalls für die webbasierte Datenbank geplanten Business-Intelligence-Anwendung nur die für das jeweilige Zentrum zutreffenden automatisierten Auswertungen.
- Die Vorstandsmitglieder sowie die mit der Erstellung und Pflege der webbasierten Datenbank beauftragte Dienstleistungsfirma sind berechtigt, auf den kompletten Datensatz zuzugreifen.

Verfügbarkeitskontrolle

Ziel der Verfügbarkeitskontrolle ist es zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind. Schutz vor zufälliger Zerstörung oder Verlust meint beispielsweise Schutz vor Wasserschäden, Blitzschlag oder Stromausfall.

Sicherstellung durch folgende Maßnahmen:

- Datensicherungen, Backup-Routine, Recovery-Verfahren,
- Erstellung von Sicherungskopien der Daten und Datenbankstruktur für die DGE. Die Sicherungskopien werden durch einen Kurier an die DGE-Geschäftsstelle geliefert und der Empfang quittiert.
- Unterbrechungsfreie Stromversorgung (USV)
- Erfüllung aller brandschutz- und sicherheitstechnischen Auflagen durch die Lohmann & Birkner Health Care Consulting GmbH sowie der beauftragten STRATO AG.

Sicherheits-Infrastruktur der webbasierten Datenbank des Deutschen NET-Registers

- Windows Server 2012 R2 security features
- Oracle 11 XE security features
- SSL Encryption (128Bit) für sichere Kommunikation zwischen User und Datenbank
- Separate Firewall mit nur zwei offenen Ports (1) für https Kommunikation – 2) für einen Terminal Server mit Zugriff zur Pflege der Server-Software durch Lohmann & Birkner)
- Symantec Endpoint Protection

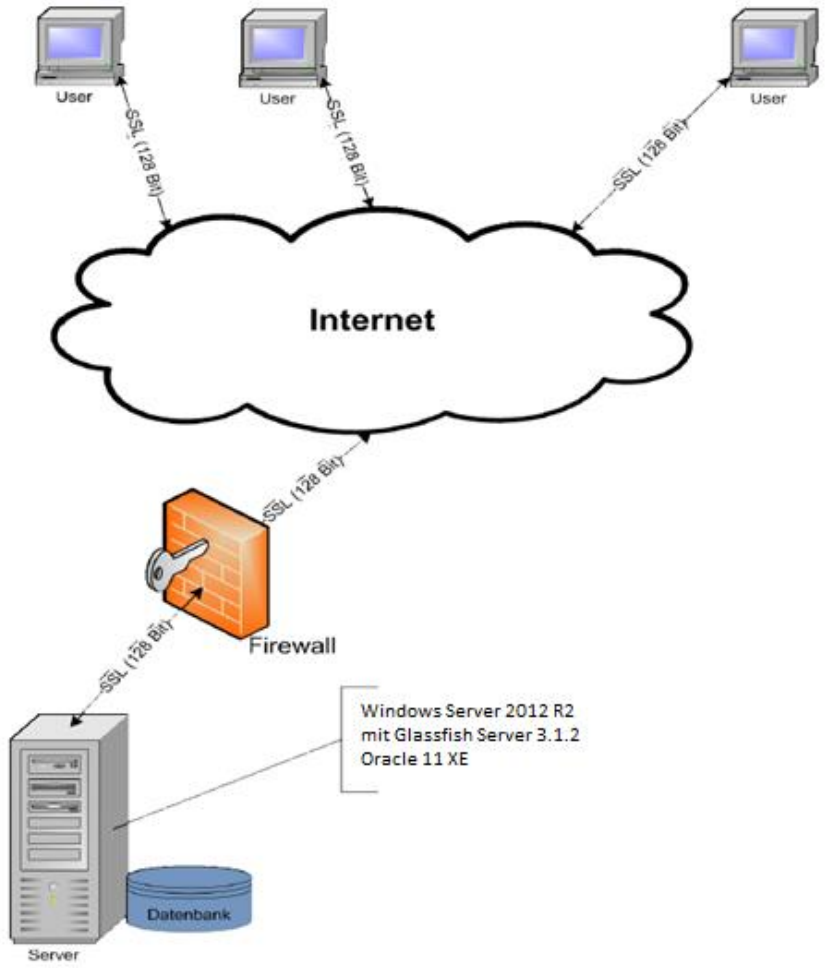

Abbildung 1, Sicherheits-Infrastruktur

Bedrohungs- und Risikoanalyse

Für die Bedrohungs- und Risikoanalyse werden folgende Risikobereiche abgeschätzt:
• Datenbank mit allen Datensätzen
• Hardware (Server)
• Software (Programmierung, Systemsoftware, Backup-Routine...)
• Datenübertragung im Internet
• Datenbankoberfläche im Browser
• Papierdokumentation (betrifft ID-Listen)
• User

1. Datenbank mit allen Datensätzen

1.a Bedrohung:

- Datenverlust
  - durch physikalische Einflüsse, siehe Punkt 2. „Hardware (Server)“
  - durch Löschung
    - mutwillig durch Hacker oder User
    - versehentlich durch User
- Datenmanipulation
  - mutwillig durch Hacker oder User
  - versehentlich durch User
- Datenmissbrauch
  - mutwillig durch Hacker oder User
- Datendiebstahl
  - mutwillig durch Hacker oder User

1.b Wahrscheinlichkeit:

- Grundsätzlich kann ein Hackerangriff auf eine webbasierte Datenbank nie vollständig ausgeschlossen werden.
- Ebenso ist der versehentliche oder mutwillige schädliche Zugriff durch die User nicht auszuschließen.

1.c Maßnahmen:

- Auf Grund der technischen und organisatorischen Maßnahmen ist die Wahrscheinlichkeit eines Datenverlustes und einer schädlichen Datenmanipulation nahezu ausgeschlossen.
  - Der Server befindet sich physisch in den Räumen der STRATO AG. Diese stellt per Zertifikat höchste Anforderungen an Zutritts-, Zugangs- und Zugriffskontrolle sicher.
  - Abschottung gegen Zugriffe von extern durch Nutzung einer Firewall sowie eines kryptografischen Protokolls bei der Datenübertragung im Internet.
  - Grundlage für die gesicherte Übermittlung der Daten ist der SSL-Standard. SSL (= Secure Sockets Layer) ist ein kryptografisches Protokoll zur sicheren Datenübertragung im Internet. Es wird für Browser, Email-Programme, Internet-Fax und andere Datenübertragungen genutzt.
  - Die Adresse der Website, von der aus der Zugriff zur Register-Datenbank erfolgt, ist nur den gelisteten Usern bekannt. Eine Verlinkung von anderen Webseiten sowie die Mitteilung der Webseiten-Adresse an nichtgelistete User sind nicht zulässig.
  - Vergabe und Nutzung von ausschließlich personengebundenen Passwörtern
  - Vorliegen einer Passwortregel einschließlich Verpflichtungserklärung zur entsprechenden Einhaltung durch User
  - Automatische Sperrung bei Nichtnutzung der Eingabemaske nach 15 Minuten

2. Hardware (Server)

2.a Bedrohung:

- Äußere Einflüsse
    - Feuer, Wasser, Explosion, Kälte, Hitze, Stromausfall, Zerstörung u.a.
    - Serverdefekt

2.b Wahrscheinlichkeit:

- sowohl äußere Einflüsse als auch die begrenzte Lebensdauer eines Servers können einen Ausfall des Systems zur Folge haben.

2.c Maßnahmen:

- Aufstellung des Servers in Räumlichkeiten, die höchsten Anforderungen an räumliche und Datensicherheit genügen
- Erstellung wöchentlicher und monatlicher Datensicherungen in Bezug auf die Server-Systemsoftware

3. Software (Programmierung, Systemsoftware, Backup-Routine...)

3.a Bedrohung:

- Systemdefekt
    - mutwillig durch Hacker erzeugt
    - Einfluss von Schadsoftware
    - Fehler und Sicherheitslücken in der genutzten Fremdsoftware
    - firmenseitige Fehlprogrammierung
- Verlust der CD mit der Sicherungskopie
    - durch Diebstahl
    - Fahrlässigkeit

3.b Wahrscheinlichkeit:

- Grundsätzlich können sowohl Schadsoftware als auch ein Hackerangriff auf eine Systemsoftware nie vollständig ausgeschlossen werden.
- Fehler und Sicherheitslücken in genutzter Fremdsoftware sind nicht auszuschließen.
- Fehler in Softwarelösungen sind nicht auszuschließen.
- Verlust der Sicherungskopie-CD ist auf Grund der etablierten Logistik nahezu ausgeschlossen.

3.c Maßnahmen:

- regelmäßige Erstellung von Updates der System- und Fremdsoftware mit entsprechender Dokumentation
- regelmäßige und gezielte Schulungen der IT-Mitarbeiter mit entsprechender Dokumentation
- regelmäßige Auswertung der protokollierten Fehler
- Erstellung wöchentlicher und monatlicher Datensicherungen
- Transport und Lagerung der Sicherungs-CD beim Auftraggeber (DGE).
- Eine Wiederherstellung der Daten auf Grundlage der Sicherungs-CD ist nur unter Nutzung der L&B-Hard- und Softwarekonfigurationen möglich.

4. Datenübertragung im Internet

4.a Bedrohung:

- Zugriff auf Daten der Registerdatenbank durch nichtberechtigte Personen bzw. Schadsoftware mit der möglichen Folge von Datenverlust, -manipulation, -missbrauch und -diebstahl

4.b Wahrscheinlichkeit:

- Grundsätzlich kann ein Hackerangriff auf eine webbasierte Datenbank nie vollständig ausgeschlossen werden.

- Bei unsachgemäßem bzw. fahrlässigem Umgang mit Zugangsberechtigungsdaten (Web-Adresse der Datenbank, Benutzername, Passwort) ist eine unerwünschte Weitergabe an Dritte nicht auszuschließen.

4.c Maßnahmen:

- Auf Grund der technischen und organisatorischen Maßnahmen ist die Wahrscheinlichkeit eines unerwünschten Zugriffs auf die Datenbank nahezu ausgeschlossen.
    - Abschottung gegen Zugriffe von extern durch Nutzung einer Firewall sowie eines kryptografischen Protokolls bei der Datenübertragung im Internet.
    - Grundlage für die gesicherte Übermittlung der Daten ist der SSL-Standard. SSL (= Secure Sockets Layer) ist ein kryptografisches Protokoll zur sicheren Datenübertragung im Internet. Es wird für Browser, Email-Programme, Internet-Fax und andere Datenübertragungen genutzt.
    - Das SSL Record Protocol dient zur Absicherung der Verbindung durch End-zu-End-Verschlüsselung mittels symmetrischer Algorithmen. Der verwendete Schlüssel wird dabei im Voraus über ein weiteres Protokoll (zum Beispiel das SSL Handshake Protocol) ausgehandelt und kann nur einmal für die jeweilige Verbindung verwendet werden. Zu sichernde Daten werden in Blöcke von maximal 65.536 (216) Byte fragmentiert und beim Empfänger wieder zusammengesetzt.
    - Die Adresse der Website, von der aus der Zugriff zur Register-Datenbank erfolgt, ist nur den gelisteten Usern bekannt. Eine Verlinkung von anderen Webseiten sowie die Mitteilung der Webseiten-Adresse an nichtgelistete User sind nicht zulässig.
    - Vergabe und Nutzung von ausschließlich personengebundenen Passwörtern
    - Vorliegen einer Passwortregel einschließlich Verpflichtungserklärung zur entsprechenden Einhaltung durch User
    - Automatische Sperrung bei Nichtnutzung der Eingabemaske nach 15 Minuten

5. Datenbankoberfläche im Browser

5.a Bedrohung:

- Versuch des Zugangs zur webbasierten Datenbank über die Browser-Oberfläche
- Manipulation der Masken

5.b Wahrscheinlichkeit:

- Zufälliges Öffnen der Startmaske ist sehr unwahrscheinlich.

5.c Maßnahmen:

- Erreichbarkeit der Startmaske ist über Suchmaschinen-Abfrage nicht möglich
- Es finden sich keine Querverweise auf den Internet-Seiten von DGE, NET-Register und L&B.
- Kenntnis der genauen Adresse ist Voraussetzung für das Öffnen der Startmaske.

6. Papierdokumentation (betrifft ID-Listen)

6.a Bedrohung:

- Verlust der ID-Liste
    - Äußere Einflüsse
        - Feuer, Wasser, Explosion, Zerstörung u.a.
    - Fahrlässigkeit
    - Diebstahl
- Im Zuge von Personalwechsel geht die Information zum Aufbewahrungsort der ID-Liste verloren.

6.b Wahrscheinlichkeit:

- Der Verlust der Information zum Standort der Liste ist möglich
- Je nach Sicherungsmaßnahmen in den Zentren ist der Verlust durch Diebstahl unterschiedlich einzuschätzen.

6.c Maßnahmen:

- standardisierte und sichere Lagerung der ID-Listen
- Bereitstellung eines gesonderten Ordners zur Verwaltung aller relevanten Dokumente des Registers (u.a. ID-Liste) durch die Projektleitung
- Hinwirken auf sorgsamen Umgang mit der ID-Liste, da diese die Grundlage für die Zuordnung von Patient und Datensatz im Zentrum ist, insbesondere im Rahmen eines regelmäßigen Monitorings und in der Bedienungsanleitung

7. User

7.1 Zentrumsmitarbeiter

7.1.a Bedrohung:

- Fahrlässigkeit im Umgang mit Passwort und ID-Liste, Versäumen des Ausloggens aus der Datenbank
- vorsätzlicher Datenmissbrauch jeglicher Art

7.1.b Wahrscheinlichkeit:

- Fahrlässigkeit und Datenmissbrauch im Sinne eines nichtregelhaften Umgangs mit schützenswerten Daten sind auf Grund der geltenden Regelungen für Ärzte und medizinisches Personal (z.B. ärztliche Schweigepflicht, Verschwiegenheitsverpflichtungen) wenig wahrscheinlich.

7.1.c Maßnahmen:

- Aufklärung aller am Projekt beteiligten Zentrumsmitarbeiter
- Unterzeichnung der Verschwiegenheitsverpflichtungen durch alle am Projekt beteiligten Zentrumsmitarbeiter
- Hinweis auf Einhaltung der Passwortregel
- Time-out-Einstellung des Systems, wenn die Dateneingabe zu lange nicht fortgesetzt wird
- Userverwaltung mit namentlicher Nennung aller User des Registers (beim Vorstand und bei L&B)
- Regelmäßige Belehrungen im Rahmen von Rundmails sowie des Monitorings

7.2 Vorstand

7.2.a Bedrohung

- Fahrlässigkeit im Umgang mit Passwort und ID-Liste, Versäumen des Ausloggens aus der Datenbank
- vorsätzlicher Datenmissbrauch jeglicher Art
- Vorstandsmitglieder, die noch keine Mitglieder der DGE sind, haben keine Berechtigung auf die Daten zuzugreifen.

7.2.b Wahrscheinlichkeit:

- Fahrlässigkeit und Datenmissbrauch im Sinne eines nichtregelhaften Umgangs mit schützenswerten Daten sind auf Grund der geltenden Regelungen für Ärzte (z.B. ärztliche Schweigepflicht, Verschwiegenheitsverpflichtungen) wenig wahrscheinlich.

7.2.c Maßnahmen:

- Aufklärung aller am Projekt beteiligten Zentrumsmitarbeiter
- Unterzeichnung der Verschwiegenheitsverpflichtungen durch alle Vorstandsmitarbeiter
- Hinweis auf Einhaltung der Passwortregel
- Userverwaltung (auch Vorstandsmitarbeiter) mit namentlicher Nennung aller User des Registers (beim Vorstand und bei L&B)
- Regelmäßige Belehrungen im Rahmen von Rundmails
- ggf. Ausschluss der Vorstandsmitglieder, falls Mitgliedschaft nicht eingegangen wird.

7.3 Lohmann & Birkner Health Care Consulting GmbH (L&B)

7.3.a Bedrohung:

- Fahrlässigkeit im Umgang mit Passwort und ID-Liste, Versäumen des Ausloggens aus der Datenbank
- vorsätzlicher Datenmissbrauch jeglicher Art

7.3.b Wahrscheinlichkeit:

- Fahrlässigkeit und Datenmissbrauch im Sinne eines nichtregelhaften Umgangs mit schützenswerten Daten sind auf Grund der geltenden Regelungen (z.B. Verschwiegenheitsverpflichtung, Datenschutzvereinbarung) wenig wahrscheinlich.

7.3.c Maßnahmen:

- Unterzeichnung einer Verschwiegenheitsverpflichtung gegenüber der DGE und dem NET-Register
- Unterzeichnung einer Datenschutz-Vereinbarung betreffend die Überlassung von Daten zum Zwecke der Auftragsdatenverarbeitung Sinne von Art. 4 Nr. 2, Nr. 8 und Nr. 15, sowie Art. 28 DSGVO)
- Userverwaltung (auch L&B-Mitarbeiter) mit namentlicher Nennung aller User des Registers (beim Vorstand und bei L&B)