Software Design Specification

„RADAR-Software“

Routine Anonymized Data for
Advanced Health Services Research

Routine Anonymized Data for
Advanced Health Services Research

<intern>

1 Inhalt

2 Introduction

2.1 Purpose

Im Projekt RADAR (Routine Anonymized Data for Advanced Health Services Research) und im Nachfolgeprojekt RADARplus wird in der Zusammenarbeit des Instituts für Allgemeinmedizin, des Instituts für Medizinische Informatik der Universitätsmedizin Göttingen, der Gesellschaft für Wissenschaftliche Datenverarbeitung Göttingen, des Instituts für Community Medicine der Universität Greifswald sowie der Technologie- und Methodenplattform für die vernetzte medizinische Forschung e.V. Berlin erforscht, wie Routinedaten aus der ambulanten medizinischen Versorgung zu gewinnen und für Forschungszwecke zu nutzen sind. Dazu wird untersucht, inwiefern Gesundheitsdaten aus dem Praxisverwaltungssysteme (PVS) exportierten Behandlungsdatentransfer-Dateien (BDT-Dateien) für die Forschung nutzbar gemacht werden können.
Dieses Dokument beschreibt die Architektur einer Software, die innerhalb einer Arztpraxis eingesetzt werden soll, um BDT-Dateien unter den Anforderungen des Datenschutzes in eine Forschungsdatenplattform zu übertragen. Es dient als Anforderungsspezifikation und beschreibt, wie die Anforderungen in konkreter Form umzusetzen sind.

2.2 Scope

Implementiert wird eine Software in der Programmiersprache Java, die gestartet von einem USB-Stick in der Lage ist, mehrere BDT-Dateien einzulesen, auf Fehler zu untersuchen, auf die Regeln der BDT-Spezifikation zu prüfen und anschließend weiter zu verarbeiten. Verarbeitungsschritte sind die Filterung auf bestimmte Inhalte (RADAR-Datensatz), die Pseudonymisierung von patientenidentifizierenden Daten unter Anbindung eines Pseudonymisierungsdienstes sowie dem Versand der Daten an eine Datenannahmestelle.

2.3 Definitions, Acronyms, and Abbreviations

ASCII American Standard Code for Information Interchange
BDT Behandlungsdatentransfer (-Schnittstelle/-Datei/-Daten)
PDF Portable Document Format
PVS Praxisverwaltungssystem
SFTP SSH File Transfer Protocol bzw. Secure File Transfer Protocol
THS Treuhandstelle
USB Universal Serial Bus

3 Design

3.1 Black Box View

Dieser Abschnitt beschreibt die Gestaltung der Software, ohne die technische Funktionsweise zu erläutern, um die Komplexität der Beschreibung zu reduzieren. Eine technische Betrachtung wird in Kapitel 3.2 Development View beschrieben.

Arztpraxen, die eingewilligt haben, am RADAR Projekt teilzunehmen, erhalten eine Anleitung zum Verfahren der Datenerfassung und zwei USB-Sticks zur Datenverarbeitung. Einer der USB-Sticks dient als sicherer Zwischenspeicher der Daten innerhalb der Praxis und ist verschlüsselt, der zweite USB-Stick enthält eine Software zur datenschutzkonformen

Verarbeitung und dem sicheren Versand der Daten. Bei Bedarf kann nach Terminvereinbarung ein RADAR-Projekt-Mitarbeiter zur technischen Unterstützung in die Arztpraxis eingeladen werden.

Die in der Arztpraxis durchzuführenden Arbeitsschritte sind im Folgenden genauer erläutert und umfassen den BDT-Datenexport aus dem Praxisverwaltungssystem, die datenschutzkonforme Verarbeitung und den sicheren Versand der Daten.

Die an der Studie teilnehmende Arztpraxis rekrutiert Patienten und dokumentiert ihre Bereitschaft an der Studienteilnahme in einer Einwilligungserklärung auf Papier. Die Einwilligungserklärung wird modular aufgebaut sein, um eine Abstufung der Datenverarbeitung und der Teilnahme am RADAR-Projekt zu ermöglichen. Um später bei der Verarbeitung der BDT-Daten nur diejenigen Daten der Patienten zu verarbeiten die eingewilligt haben, wird mithilfe der RADAR-Software auf dem Software-USB-Stick eine Patienten-Einwilligungsliste erstellt. Das Verarbeitungsprogramm erfasst dazu die in der Einwilligungserklärung gewählten Optionen zusammen mit der praxisinternen Identifikationsnummer, Vorname und Nachname des Patienten. Die Angaben sind alle der Einwilligungserklärung auf Papier zu entnehmen. Die daraus erstellte Patienten-Einwilligungsliste speichert jedoch nicht die vollen Angaben, sondern generiert lediglich eine Kennung aus den identifizierenden Daten, um den Patienten im BDT-Datensatz eindeutig identifizieren zu können. Obwohl die praxisinterne Identifikationsnummer zum eindeutigen identifizieren im BDT-Datensatz ausreichen würde, wird zur Vermeidung von Zahlendrehern bei der Identifikationsnummer der erste Buchstabe des Vornamens und der erste Buchstabe des Nachnamens bei der Identifizierung abgeglichen. Das Erstellen der Einwilligungsliste soll die Arbeitsschritte in der Arztpraxis erleichtern; die elektronische Erfassung der Einwilligungserklärung kann in einem getrennten Arbeitsschritt vom BDT-Export und dem Versand der Daten erfolgen.
Im RADARplus-Projekt wird alternativ zur papierbasierten Einwilligung die Erfassung der Einwilligung mit Tablets erprobt. Anstelle der zuvor beschriebenen Übertrag der Einwilligungsinformationen vom Papier in die RADAR-Software wird eine Liste der Einwilligungen über einen Datei-Import in die RADAR-Software übertragen. Das Importverfahren dient als Übergangslösung zur Erprobung. Zu einem späteren Zeitpunkt ist eine automatische Übertragung per Datenschnittstelle angedacht.

Sind ausreichend Patienten rekrutiert ist im Arztpraxisinformationssystem ein BDT-Daten-Export durchzuführen. Ergebnis eines Exports sind BDT-Dateien, die anschließend in einem Verzeichnis auf einem Rechner der Praxis abgerufen werden können. Zur weiteren Verarbeitung werden die exportierten BDT-Dateien auf den sicheren USB-Speicherstick übertragen. Wird der sichere USB-Stick an einen PC angeschlossen, ist zum Öffnen des Inhalts ein Passwort zur Verschlüsselung anzugeben. Das Passwort kann frei gewählt werden und wird ab diesem Zeitpunkt für den Zugriff auf die gespeicherten Daten notwendig. Der verschlüsselte USB-Stick gewährleistet den sicheren Transport der Daten innerhalb der Arztpraxis.

Die Verarbeitung der Daten muss an einem PC durchgeführt werden, der mit dem Internet verbunden ist; zur Pseudonymisierung muss mit der Treuhandstelle und zur Datenübermittlung mit Datenannahmestelle über eine gesicherte Internetverbindung kommunizierte werden. An diesen PC wird der verschlüsselte USB-Stick mit den BDT-Daten und zusätzlich der zweite USB-Stick mit der RADAR-Software angeschlossen. Die RADAR-

Software prüft die Exportdateien und listet alle Patienten anhand der erstellten Patienten-Einwilligungsliste auf, für die eine Verarbeitung geplant ist. Nach einer Bestätigung der Verarbeitung durch den Benutzer wird aus dem gesamten BDT-Exportdateien ein gefilterter Datensatz erzeugt, in dem patientenidentifizierende Daten entfernt und mit einem Pseudonym versehen werden. Außerdem wird der gesamte Datensatz mit einem Pseudonym, welches die Arztpraxis identifiziert, versehen.

Nach der Verarbeitung wird dem Nutzer eine Übersicht der zu versendenden Daten angezeigt. Bestätigt er den Versand der Daten, werden die Daten über eine verschlüsselte Verbindung in die Studiendatenbank übertragen.

3.2 Development View

Nachdem im Kapitel 3.1 Black Box View der Ablauf der Datenverarbeitung ohne Kenntnisse über die innere Funktionsweise gegeben wurde, folgt in diesem Kapitel eine detaillierte technische Beschreibung der Datenverarbeitung. Abbildung 1 zeigt den bereits beschriebenen Ablauf als Übersicht in einer Grafik. In den folgenden Unterkapiteln wird der BDT-Datenexport, die Verarbeitung der BDT-Daten, die Pseudonymisierung und der Transport der Daten an die Datenannahmestelle genauer erläutert.

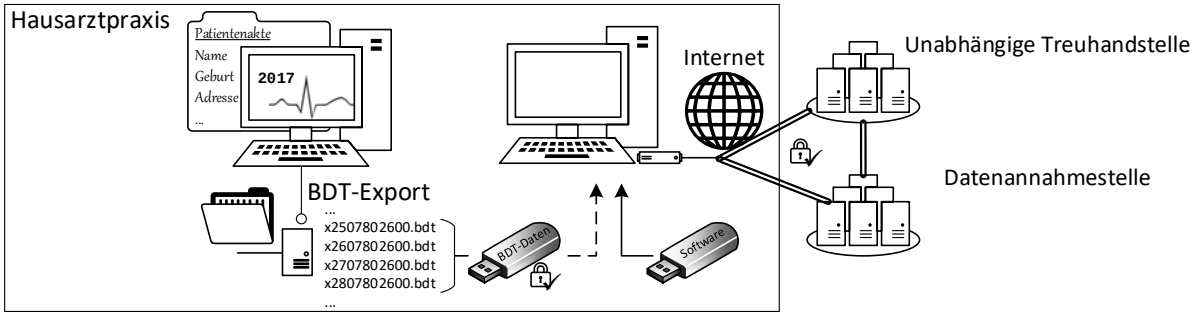

Abbildung 1: Übersicht über den Ablauf der Datenverarbeitung im RADAR-Projekt. Innerhalb einer Arztpraxis wird aus dem Praxisverwaltungssystem ein BDT-Export erzeugt, der auf einen verschlüsselten USB-Stick gespeichert wird. Dieser USB-Stick wird an einen internetfähigen PC zusammen mit dem Software-UBS-Stick angeschlossen und die Software gestartet. Die Software öffnet die Daten vom verschlüsselten USB-Stick, verarbeitet die BDT-Daten, führt eine Pseudonymisierung durch und versendet die pseudonymen Daten an die Datenannahmestelle.

3.2.1 BDT-Datenexport

Die Historie der BDT-Schnittstelle[1] und die BDT-Satzbeschreibung sind der Spezifikation zu entnehmen [1]. Notwendige Voraussetzung für alle weiteren Schritte ist eine zugängliche BDT-Datenexport-Schnittstelle und daher als technische Voraussetzung (4 Preconditions) gelistet. Hintergrund ist, dass einige Softwareanbieter in ihren Praxisverwaltungsprogrammen die BDT-Datenexport-Schnittstelle dem Arzt nicht mehr zugänglich ist oder abgeschafft wurde[2]. Teilweise wird je nach Wartungsvertrag der Zugang entweder kostenlos oder kostenpflichtig zur Verfügung gestellt[3].
Bei BDT-Exporten handelt es sich um eine oder mehrere zusammenhängende Textdateien im ASCII-Format, vorwiegend mit den Dateiendungen „.bdt“ oder „.xdt“. Die Art der Durchführung des BDT-Exports in den Praxen ist abhängig vom jeweiligen Praxisverwaltungsprogramm und mithilfe einer Anleitung durchzuführen. Dabei kann der

[1] https://de.wikipedia.org/wiki/XDT#Behandlungsdatentransfer_.28BDT.29
[2] http://www.aerzteblatt.de/archiv/50761
[3] http://www.med7.de/bdt.html

Export gegebenenfalls eingeschränkt werden, beispielsweise auf einen bestimmten Zeitraum oder bestimmte Patientennummern. Ergebnis eines Exports sind die BDT-Dateien, die anschließend in einem Verzeichnis auf einem Rechner der Praxis abgerufen werden können. Zur weiteren Verarbeitung werden die exportierten BDT-Dateien auf einen sicheren USB-Speicherstick übertragen. Dieser USB-Stick wird vom RADAR-Projekt den rekrutierten Arztpraxen zur Verfügung gestellt. Der Betrieb des USB-Sticks erfordert keine Administratorrechte, besitzt eine hardwarebasierte Verschlüsselung, und bietet einen Kennwortschutz durch eine vorinstallierte intuitive Sicherheitsanwendung, die beim Anschließen automatisch gestartet wird. Solche USB-Sticks mit integrierter Verschlüsselung sind am Markt für ca. 15,00 € verfügbar[4]. Da die von den Herstellern der USB-Sticks mitgelieferte Sicherheitsanwendung häufig nur für das Betriebssystem Windows ausgeliefert wird, ist Windows als Betriebssystems für den Rechner des Praxisverwaltungssystems eine technische Voraussetzung (siehe Kapitel 4 Preconditions). Die Verwendung des verschlüsselten USB-Sticks gewährleisten den sicheren Transport der Daten innerhalb der Arztpraxis. Somit erfolgt kein direkter Zugriff auf das Arztpraxisinformationssystem, weder durch Software noch durch Projektmitarbeiter.

3.2.2 Verarbeitung der BDT-Daten

Auf einem weiteren USB-Stick wird der am Projekt teilnehmenden Arztpraxis eine Software zur Verfügung gestellt, die die Verarbeitung, Pseudonymisierung und den Versand der BDT-Dateien ermöglicht. Da zur Pseudonymisierung die Treuhandstelle in Greifswald kontaktiert werden muss, muss der PC, an dem der Software-USB-Stick betrieben wird, internetfähig sein, eine weitere technische Voraussetzung (siehe Kapitel 4 Preconditions).
An diesem Rechner wird nun zusätzlich zum USB-Stick mit der RADAR-Software der verschlüsselte USB-Stick mit den BDT-Dateien angeschlossen. Nach Eingabe des Passwortes zur Entschlüsselung der BDT-Dateien kann die RADAR-Software gestartet und die BDT-Dateien eingelesen werden.
Die Verarbeitungssoftware wird direkt vom USB-Stick gestartet. Es muss keine Software installiert werden und es werden keine Dateien auf dem Rechner gespeichert. Es öffnet sich eine grafische Benutzeroberfläche, die den Benutzer durch die verschiedenen Verarbeitungsschritte leitet.

1. Willkommensbildschirm
2. Verwaltung von Einwilligungserklärungen
3. Einlesen der BDT-Daten
4. Pseudonymabfrage
5. Ergebnis der Verarbeitung
6. Versand der Daten

Nach einem Willkommensbildschirm mit einer Beschreibung des weiteren Vorgehens gelangt der Benutzer zur Oberfläche des Schrittes „Verwaltung von Einwilligungserklärungen“. Dort werden wie beschrieben vom Benutzer die auf Papier erfassten Daten der Einwilligungserklärungen in die RADAR-Software übertragen. Beim nächsten Schritt „Einlesen der BDT-Daten“ prüft die Software zunächst, ob der verschlüsselte USB-Stick bereits angeschlossen ist. Des Weiteren wird geprüft, ob der der USB-Stick durch die Verschlüsselungssoftware bereits entschlüsselt wurde. Der dritte Punkt der Liste ist die Pfadeingabe. Sie ist standardmäßig bereits mit dem Laufwerk des verschlüsselten USB-Sticks

[4] z.B.: https://www.reichelt.de/?ARTICLE=150949 (Verbatim Secure Pro 8GB)

vorbelegt, jedoch abänderbar, da eventuell auf dem verschlüsselten Laufwerk Unterordner angelegt wurden, in dem die einzelnen BDT-Dateien abgelegt sind. Eine harte Prüfung auf eine Schaltfläche „Einlesen“, besteht nicht, da der Betrieb (nicht empfohlen), auch ohne das Vorhandensein des verschlüsselten USB-Sticks durchgeführt werden kann. Durch Drücken der Schaltfläche „Einlesen“ wird geprüft ob im gewählten Pfad BDT-Dateien zu finden sind, andernfalls wird eine Fehlermeldung ausgegeben.

3.2.2.1 Vorverarbeitung und Syntaxprüfung der BDT-Daten

Der Dateiname von BDT-Dateien setzt sich aus dem Buchstaben x, einer zweistelligen laufenden Nummer des Datenträgers und der Arztnummer zusammen:

```
x<LfdNrDT><Arztnummer>.bdt => z.B. x01999999999.bdt
```

Das Einlesen der BDT-Dateien erfolgt in geordneter Reihenfolge anhand der im Verzeichnis befindlichen BDT-Dateien anhand der laufenden Nummer des Datenträgers. Nachdem alle Dateien zeilenweise als Text in den Speicher eingelesen wurden, erfolgt die logisch-strukturelle Abbildung der BDT-Struktur in Objekte. Die BDT-Objekt-Struktur besteht jeweils aus einer Klasse für Feld, Satz und Datenpaket, analog zur BDT-Struktur der Spezifikation [1].

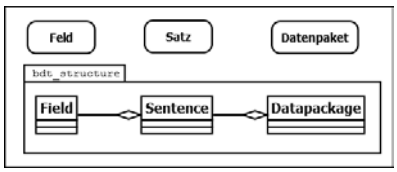

Abbildung 2: BDT-Objekt-Struktur

Beim Abbilden der BDT-Zeilen in die BDT-Objekt-Struktur erfolgt eine Überprüfung der Struktur der BDT-Datenfelder, sowie des Datenpaket Satzaufbaus.

Feldteil	Länge	Bedeutung
Länge	3 Bytes	Feldlänge in Bytes (Inhalt + 9)
Kennung	4 Bytes	Feldkennung
Inhalt	variabel	Information
Ende	2 Bytes	ASCII-Wert 13 = CR (Wagenrücklauf) + ASCII-Wert 10 = LF (Zeilenvorschub

Abbildung 3: Struktur eines BDT-Datenfeldes

Grundlage für die Überprüfung der Datenpakete, des Satzaufbaus und der vorkommenden Felder sind die in der Spezifikation [1] beschriebene Satz- und Feldtabellen. Dazu müssen die leider nur im PDF-Format vorliegenden Formulare in ein geeignetes Format transformiert werden.

3.2.2.2 Regelprüfung der BDT-Daten

Ebenfalls Teil der Spezifikation ist eine Regeltabelle die Formatprüfungen, Inhaltsprüfungen, Existenzprüfungen und Kontextprüfungen vorgibt. Die Spezifikation umfasst 45 Regeln. Abgebildet auf die einzelnen BDT-Felder kann so eine inhaltliche Prüfung vorgenommen werden.

3.2.2.3 Logdatei

Während der Verarbeitung der BDT-Dateien können Fehler unterschiedlicher Schwere auftreten. So können BDT-Zeilen nicht dem Feldaufbau entsprechen, Feldkennungen enthalten sein die nicht Bestandteil der Spezifikation sind, ein falscher Satzaufbau vorliegen

oder BDT-Regelverstöße festgestellt werden. Dabei werden lediglich die Regelverstöße und Fehler geloggt, niemals jedoch ein Feldinhalt aus dem BDT-Datensatz.
Außerdem wird die Logdatei um einige weitere Informationen zur Verarbeitung ergänzt:

- Dauer und Zeitpunkt der Verarbeitung
- Anzahl der verarbeiteten BDT-Zeilen
- Inhalt der BDT-Felder:

Nr.	Feldcode	Bezeichnung
1	9103	Datum der Erstellung
2	9106	Zeichencode
3	9210	Version ADT-Satzbeschreibung
4	9213	Version BDT
5	9600	Archivierungsart
6	9601	Zeitraum der Speicherung
7	9602	Beginn der Übertragung
8	0101	KBV-Prüfnummer
9	0102	Softwareverantwortlicher
10	0103	Software
11	0104	Hardware

Diese Fehlermeldungen, Regelverstöße und Verarbeitungsdaten werden in einer Logdatei festgehalten und beim Versand der pseudonymisierten Daten an die Datenannahmestelle mitübertragen.

3.2.2.4 Filterung der BDT-Daten

Die Auswertung der BDT-Exporte erfolgt für den Zeitraum zwischen dem ersten Quartal 2012 bis einschließlich dem ersten Quartal 2019 (Q1/2012 - Q1/2019).

Für das RADAR-Projekt werden die folgenden BDT-Felder verarbeitet:

Nr.	Feldcode	Bezeichnung	Verarbeitung
1	0202	Praxistyp	
2	0204	Arztgruppe verbal	
3	0206	PLZ Ort der Praxis	
4	0225	Anzahl Ärzte	
5	3103	Geburtsdatum des Patienten	Geburtsjahr des Patienten
6	3110	Geschlecht des Patienten	
7	3649	Dauerdiagnosen ab Datum	
8	3650	Dauerdiagnosen	
9	3651	Dauermedikamente ab Datum	
10	3652	Dauermedikamente	
11	3656	Allergien	
12	4101	Quartal der Abrechnung	
13	4105	Geschäftsstelle	
14	4107	Abrechnungsart (Schein)	
15	4121	Gebührenordnung	
16	5000	Leistungstag	
17	5001	GNR/GNR-Ident	

18	6000	Abrechnungsdiagnose	
19	6001	ICD-Schlüssel	
20	6200	Tag der Speicherung von Behandlungsdaten	
21	6205	Aktuelle Diagnose	
22	6210	Medikament verordnet auf Rezept	
23	6211	Außerhalb Rezept verordnetes Medikament	
24	6215	Ärztemuster	
25	6220	Befund	
26	6221	Fremdbefund	
27	6222	Laborbefund	
28	6225	Röntgenbefund	
29	6260	Therapie	
30	6265	Physikalische Therapie	
31	6280	Überweisung Inhalt	
32	6285	AU Dauer	
33	6286	AU wegen	
34	6290	Krankenhauseinweisung, Krankenhaus	
35	6291	Krankenhauseinweisung wegen	
36	8401	Befundart	
37	8410	Test-Ident	
38	8411	Testbezeichnung	
39	8420	Ergebnis-Wert	
40	8421	Einheit	

3.2.3 Pseudonymisierung

Anonymisierung oder Pseudonymisierung sowie ein erfolgreicher Ethikantrag bilden die Basis für datenschutzkonforme Forschungsprojekte mit Gesundheitsdaten. In beiden Fällen müssen die Identitätsmerkmale von natürlichen Personen aus den Datensätzen entfernt werden. Dies gilt für Patientendaten sowie in der Regel für alle anderen personenbezogenen Daten, etwa die des Arztes. Dies sind z.B. Vorname, Nachname, Geburtsdatum, Wohnort mit Straße und Hausnummer des Patienten. Die reine Anonymisierung mittels der RADAR-Software wird zum aktuellen Zeitpunkt nicht weiter spezifiziert. Da man Routinedaten in der Regel personenbezogen verknüpfen will, ist eine eindeutige Kennzeichnung der Patienten und Ärzte nötig. Bei der Pseudonymisierung wird eine Kennung generiert, der Datensätze zugeordnet werden können, nur diese Kennung wird mit den restlichen Daten des RADAR-Datensatzes gespeichert. Die Vergabe der Pseudonyme und Speicherung der identifizierenden Daten erfolgt über die Treuhandstelle in Greifswald.

Zunächst überprüft die RADAR-Software die Internetverbindung und die Erreichbarkeit der Treuhandstelle (THS) in Greifswald. Bei fehlerhafter Konnektivität wird eine Fehlermeldung ausgegeben, bei Erfolg die Erreichbarkeit angezeigt. Anschließend wird der Benutzer um die Eingabe des „THS-Kennwortes“ gebeten, dass er mit der Anleitung und den USB-Sticks erhalten hat. Nach Eingabe aller Daten wird die sichere Verbindung überprüft und angezeigt. Die Interaktion mit der Treuhandstelle wird im Kapitel 3.3.13.3 detailliert beschrieben.

Für die Pseudonymisierung wird aus dem BDT-Export die Betriebsstättennummer, Feldkennung 0201, extrahiert und durch die Treuhandstelle in das Arztpraxispseudonym

umgewandelt. (Anmerkung: Laut Spezifikation ist die Feldinhaltbeschreibung der Feldkennung 0201 „Arztnummer“, dennoch wird in diesem Feld die Betriebsstättennummer (BSNR) übertragen). Dem Benutzer wird das Pseudonym der Arztpraxis angezeigt, die für die Übermittlung der Daten verwendet wird.

Verarbeitete BDT-Felder	Verarbeitung	Treuhandstelle
0201 Betriebsstättennummer	->	-> Arztpraxispseudonym

Durch die RADAR-Software wird eine Liste der Patienten gepflegt, die ihre Zustimmung an der Teilnahme der Studie auf Papier erklärt haben. Die RADAR-Software erfasst dazu die in der Einwilligungserklärung gewählten Optionen zusammen mit der praxisinternen Identifikationsnummer, Vorname und Nachname des Patienten. Die daraus erstellte Patienten-Einwilligungsliste speichert jedoch nicht die vollen Angaben sondern generiert lediglich eine Kennung aus den identifizierenden Daten, um den Patienten im BDT-Datensatz eindeutig identifizieren zu können. So kann die elektronische Erfassung der Einwilligungserklärung in einem getrennten Arbeitsschritt vom BDT-Export und dem Versand der Daten erfolgen. Die Patienten-Einwilligungsliste wird auf dem unverschlüsselten USB-Stick zwischengespeichert, da sie keine identifizierenden Daten enthält. Die Datei enthält eine Liste, bestehend aus der für den Patienten im Arztpraxisinformationssystem interne Nummer und jeweils dem ersten Buchstaben des Vornamens und des Nachnamens, sowie eine Ziffer die die Option der modularen Informierten Einwilligung des Patienten. Die ersten Buchstaben des Namens dienen zum Plausibilitätscheck mit der Patienten-ID, so kann sichergestellte werden, dass nicht versehentlich eine falsche Patienten-ID verwendet wird. Anhand dieser Liste werden die Pseudonyme bei der Treuhandstelle abgefragt indem identifizierende Patientendaten übermittelt werden.

Verarbeitete BDT-Felder	Verarbeitung	Treuhandstelle
	Arztpraxis-Pseudonym	Speicherung für Kontaktierung
3000 Patientennummer	Patientennummer	Speicherung für Kontaktierung
3101 Name des Patienten	->	-> Patientenpseudonym
3102 Vorname des Patienten	->	
3103 Geburtsdatum des Patienten	->	
3110 Geschlecht des Patienten	->	
3106 Wohnort des Patienten	Postleitzahl	Speicherung für Kontaktierung
	Wohnort	Speicherung für Kontaktierung
3107 Straße des Patienten	Straße	Speicherung für Kontaktierung

Genau genommen werden pro Patienten bei der Treuhandstelle zwei Pseudonyme für einen Patienten angefragt. Ein Patienten-Arztpraxisinformationssystem-Pseudonym und einem temporären Pseudonym. Das Patienten-Arztpraxisinformationssystem-Pseudonym wird in der RADAR-Software angezeigt und kann in der Arztpraxis notiert werden und dient zur Kommunikation im Falle einer Kontaktierung. Das Patienten-Arztpraxisinformationssystem-Pseudonym wird nicht mit dem RADAR-Datensatz übermittelt, d.h. es ist nur der Arztpraxis und der Treuhandstelle bekannt. Mit dem RADAR-Datensatz übermittelt wird das temporäre Pseudonym, das bei Erhalt des Datensatzes in der Datenannahmestelle gegen ein Forschungsdatenbank-Pseudonym aufgelöst werden kann. So werden für verschiedene Datenhoheiten verschiedene Pseudonyme verwendet. Die technische Interaktion mit der Treuhandstelle wird in Kapitel 3.3.1 (Software Components Interaction - Treuhandstelle Greifswald) genauer beschrieben.

Eine Übersicht der Patienten, die verarbeitet werden sollen, wird anschließend dem Arzt angezeigt. Dieses Vorgehen stellt sicher, dass keine Daten von Patienten verarbeitet werden, die nicht der Teilnahme an der Studie zugestimmt haben.

Der im Kapitel 3.2.2.4 (Filterung der BDT-Daten) beschriebene RADAR-Datensatz wird zusammen mit dem Arztpraxis-Pseudonym und dem Patientenpseudonym zum Transport vorbereitet.

3.2.4 Transport der verschlüsselten verarbeiteten BDT-Daten

Im letzten Schritt wird die erstellte Transportdatei an die Datenannahmestelle bei der GWDG übertragen. Die Transportdatei beinhaltet den gefilterten und pseudonymisierten RADAR-Datensatz sowie die Log-Datei.

Wie bei der Interaktion mit der Treuhandstell überprüft die RADAR-Software zunächst die Internetverbindung und die Erreichbarkeit der Datenannahmestelle bei der GWDG. Bei fehlerhafter Konnektivität wird eine Fehlermeldung ausgegeben, bei Erfolg die Erreichbarkeit angezeigt. Anschließend wird der Benutzer um die Eingabe des „Datenannahmestelle-Kennwortes“ gebeten, dass er mit der Anleitung und den USB-Sticks erhalten hat. Nach Eingabe aller Daten wird die sichere Verbindung überprüft und angezeigt. Nach Versandaufforderung durch den Benutzer erfolgt die Datenübertragung. Die Interaktion mit der Datenannahmestelle wird im Kapitel 3.3.2 detailliert beschrieben.

3.3 Software Components Interaction

3.3.1 Treuhandstelle Greifswald

Die Treuhandstelle Greifswald stellt zur Übermittlung der identifizierenden Daten und Abfrage der Pseudonyme eine REST-Webservice Schnittstelle zur Verfügung (siehe [2,3]).
Zur Absicherung der Verbindung erstelle die Treuhandstelle Greifswald Clientzertifikate, die für jeden Software-USB-Stick in die Konfiguration übernommen werden. Ebenfalls wird ein Passwort zum Entschlüsseln des Clientzertifikates hinterlegt. Zusätzlich wird ein API-Key als Authentifizierungsschlüssel, der bei jeder Anfrage übertragen wird, hinterlegt. Als weitere Authentifizierung wird jeder Software-USB-Sticks für eine HTTP-Authentifizierung (Basic Authentication) konfiguriert. Die Treuhandstelle übergibt dazu eine Liste mit BasicAuth-Benutzername und BasicAuth-Passwörtern. Bei Konfiguration der Software-USB-Sticks wird in die Konfigurationsdatei der BasicAuth-Benutzername eingetragen. Das zugehörige Passwort auf der Anleitung zum Verfahren der Datenerfassung notiert.
Konfigurierte Parameter sind URL des Webservice, ein API-Key, das Clientzertifikat-Passwort und der BasicAuth-Benutzername.

3.3.2 Datenannahmestelle GWDG

Der Datenversand erfolgt per SFTP an die Datenannahmestelle bei der GWDG. Die GWDG richtet für die Anzahl der teilnehmenden Arztpraxen FTP-Zugänge ein, die auf getrennte FTP-Verzeichnis Zugriff haben ein. Dabei werden die Zugänge lediglich nummeriert, ein Rückschluss auf die Arztpraxis ist nicht möglich. Bei Konfiguration der Software-USB-Sticks wird in die Konfigurationsdatei der FTP-Zugang eingetragen. Das zugehörige Passwort auf der Anleitung zum Verfahren der Datenerfassung notiert.
Konfigurierte Parameter sind die URL des SFTP-Servers, der Port, und der SFTP-User.

4 Preconditions

Voraussetzungen um das beschriebene Szenario auszuführen sind:

- Zugang zur BDT-Datenexport-Schnittstelle im Praxisverwaltungssystem
- Internetfähiger PC Rechner mit zwei freien USB-Anschlüssen
- Betriebssystem Windows auf dem Rechner des Praxisverwaltungssystems und dem Rechner am Internet zum Betrieb der verschlüsselten USB-Sticks und der RADAR-Software

5 References

Number	Filename	Link
1	BDT94 Schnittstellenbeschreibung.pdf	
2	THS-Schnittstellenspezifikation_v1.4.0.pdf	
3	RADAR THS Schnittstellenspezifikation.pdf	

6 Revision History

Version	Date	Author	Description
1	20.01.2017	Johannes Pung	Initiale Version
2	12.07.2017	Johannes Pung	Anforderungen erfasst
3	24.11.2017	Johannes Pung	Software Interaktion mit THS und GWDG erfasst
4	13.01.2020	Johannes Pung	Erweiterung RADARplus