Cloudi/o

Ein Ansatz für Cloud-basiertes Datenmanagement in klinischen Studien

Andres, N. (1), Lemberg, B. (2), Gövercin, M. (1)

(1) Forschungsgruppe Geriatrie
Charité – Universitätsmedizin Berlin
Reinickendorfer Straße 61
13347 Berlin
Natascha.Andres@charite.de

(2) Tele-Consulting GmbH
Siedlerstraße 22-24
71126 Gäufelden
BLemberg@tele-consulting.com

Abstract: Mit diesem Beitrag wird das sich in der Entwicklung befindliche Framework zum Cloud-basierten Datenmanagement im klinischen Umfeld – Cloudi/o[1] – umrissen. Im Fokus des Projekts steht ein flexibles, anwenderorientiertes und zugleich sicheres System zur Datenerhebung mittels Tablet-PC, Datenspeicherung in der Cloud sowie der Möglichkeit des Datenimports von medizinischen Drittgeräten für den speziellen Anwendungsfall im Rahmen klinischer Studien. Es kommt zu einer Beschreibung verschiedener auf das Framework wirkenden Standards und Applikationen, einer differenzierten Darstellung der Framework-Komponenten sowie der Beschreibung des Validationsszenarios.

1 Einleitung

In klinischen Studien kommt es immer wieder zu einer Anhäufung von großen Datenmengen, die strukturiert und sicher abgelegt und gespeichert werden müssen. Darüber hinaus stammen die erhobenen Daten aus verschiedenen Datenquellen wie beispielsweise einer Probandenbefragung, Messergebnisse aus verschiedensten diagnostischen Verfahren und Geräten oder der klassischen ärztlichen Anamnese. Durch die Vielzahl von Datenquellen kommt es trotz zunehmender Digitalisierung im medizinischen Umfeld oftmals zu einer Datenerhebung mittels Papier [Co06]. Dies lässt sich unter anderem auf das Vorliegen bereits validierter Fragebögen in Papierform zurückführen. Die so erfassten Daten werden im Nachgang digitalisiert. Dieser Prozess bietet eine relativ hohe Angriffsfläche für Datenverluste und/oder negative Auswirkungen auf die Datenkonsistenz durch die Möglichkeit von Fehleinträgen. Dies gilt es auf Grund der Datensicherheit und Datenintegrität in klinischen Studien zu verhindern. Daraus resultiert das gesteigerte Interesse der Forschenden an digitalen Möglichkeiten der Studiendokumentation [Pa11].

[1] www.cloudi-o.de

Dieser Beitrag stellt den Rahmen des vom Bundesministeriums für Bildung und Forschung geförderten Projektvorhabens Cloudi/o vor. Dieses will im Vergleich zu anderen Digitalisierungsansätzen wie digitalen Stiften, Nutzung von Standalone Personal Digital Assistants (PDA), Hybrid PDAs oder verschiedenster Scanner-Lösungen im Bereich der digitalen Datenmanagementstrukturen in medizinischen Kontext den Fokus auf eine digitale Dokumentation mittels Tablet-PC auf Android-Basis setzen. Hierbei sollen die erhobenen Daten sicher in einer Private Cloud gespeichert werden. Es kommt dabei zu einer vollständigen Darstellung der Studiendaten auf einer Weboberfläche sowie der Möglichkeit der vereinfachten Datenerhebung mittels Tablet-PC ohne das Risiko von Datenverlusten durch Minimierung der Prozessschritte im Bereich der Dateneingabe [Sc07].

Ziel des Projektes ist die Entwicklung eines Frameworks, welches Softwareentwicklern durch die Berücksichtigung von regulatorischen Anforderungen und unter Einbeziehung der sich derzeit auf dem Markt befindlichen Softwarelösungen ein Werkzeug zur Entwicklung themenspezifischer Anwendungen liefert. Die derzeit vorherrschenden Individuallösungen, vor allem im Bereich der Unternehmen mit kleiner oder mittlerer Größe, bergen das Risiko für eine Nichteinhaltung der strengen Regularien im Bereich des Datenschutzes und der Datensicherheit im Umgang mit hoch schützenswerten Daten wie bspw. personenbezogenen Daten. Dem gilt es entgegenzuwirken.

Durch die modulare Anordnung der einzelnen Komponenten des Cloudi/o-Frameworks und dem verfolgten Open-Source-Ansatz bezieht sich das Framework auf eine breite Zielgruppe im Bereich der Speicherung von hoch schützenswerten Daten. Besonders der Umgang mit dieser Art von Daten. Einer Ablage dieser in der Cloud und den damit verbundenen datenschutzrechtlichen Anforderungen sind als Kernaspekt des Frameworks zu verstehen.

2 Umgang mit personenbezogenen Daten in der Cloud

Daten, unabhängig von ihrer Art und Herkunft, bilden die Grundlage jeder wissenschaftlichen Aussage in der klinischen Forschung. Ihre Qualität ist entscheidend für die Belastbarkeit eines nach wissenschaftlichen Kriterien erarbeiteten Ergebnisses [De98]. Entsprechend hoch sind die Ansprüche an Integrität, Revisionssicherheit und Authentizität des Datenbestandes.

Zusätzlich gilt es, ethische Grundsätze zu beachten. In der Datenverarbeitung vor allem dann, wenn personenbezogene Daten, zum Beispiel medizinische Einzelangaben zu Probanden, genutzt werden. Nicht zuletzt durch die rechtlich privilegierte Stellung der wissenschaftlichen Forschung bei der Erhebung personenbezogener Daten [§ 13 Absatz 2 Satz 7 BDSG] kommt hier allen Beteiligten eine besondere Verantwortung zu. Das Grundrecht auf informationelle Selbstbestimmung der Betroffenen muss bei Erhebung, Verarbeitung oder Nutzung ihrer Daten unbedingt gewährleistet bleiben [Bu03].

Das Bundesdatenschutzgesetz (BDSG) nennt in der Anlage zu § 9 Satz 1 beispielhaft acht Maßnahmen, die bei der automatisierten Erhebung, Verarbeitung oder Nutzung

personenbezogener Daten umzusetzen sind, um den besonderen Anforderungen des Datenschutzes gerecht zu werden. Dabei handelt es sich um Maßnahmen zur Zutrittskontrolle, Zugangskontrolle, Zugriffskontrolle, Weitergabekontrolle, Eingabekontrolle, Auftragskontrolle, Verfügbarkeitskontrolle und der Gewährleistung der Trennung von Daten. Ausdrücklich wird hierbei der Einsatz kryptografischer Verfahren zur Umsetzung der Zugangs- und Weitergabekontrolle gefordert. Die Maßnahmen können sich im Einzelnen in den Datenschutzgesetzen der Länder unterscheiden, im Ergebnis sind aber stets Vorkehrungen zu treffen, um eine sichere Datenverarbeitung unter Beachtung des besonderen Schutzbedarfs personenbezogener Daten in Hinblick auf die klassischen Schutzziele der Informations- und Datensicherheit Vertraulichkeit, Integrität, Verfügbarkeit, sowie Authentizität, Revisionssicherheit und Transparenz zu gewährleisten.

Die Sicherheitsanforderungen aus wissenschaftlicher Sicht sind in jenen des Datenschutzes inbegriffen. Letztere sind jedoch durch ihren Zweck, den Schutz eines verfassungsmäßigen Grundrechts, stärker ausgeprägt und bestimmen somit den Schutzbedarf einer Anwendung zum Management personenbezogener Daten.

In der Praxis haben sich zur Umsetzung Standards wie ISO 27001 oder die IT-Grundschutz Vorgehensweise des Bundesamtes für Sicherheit in der Informationstechnik (BSI) etabliert.

Im Grundsatz ist es für eine sichere Informationsverarbeitung nicht entscheidend, ob die Informationsverarbeitung innerhalb einer internen IT-Infrastruktur stattfindet oder durch Auftragnehmer innerhalb externen Strukturen vorgenommen wird, wie dies beim Cloud-Computing der Fall ist. Jedoch treten sowohl bei der Auftragsdatenverarbeitung, als auch bei der Verarbeitung in verteilten Infrastrukturen spezifische Gefährdungen und Bedrohungen auf, denen mit entsprechenden Maßnahmen entgegengewirkt werden muss.

Cloud-Computing wird heute vielfach als Inbegriff für maximale, globale Verteilung von Informationen bei gleichzeitig minimaler Transparenz der Datenverarbeitung angesehen. Dieser Umstand ist bedingt durch eine Vielzahl, in der Regel an Endkunden gerichteter, oft kostenloser, Public-Cloud-Anwendungen, die den Ansprüchen an eine sichere und valide Datenverarbeitung nicht genügen. Hinzu kommt, dass sich bislang keine einheitlichen und verbindlichen Standards bezüglich der Ausgestaltung sicherer Cloud-Dienstleistungen etabliert haben.

Will man die Möglichkeiten des Cloud-Computings, wie zum Beispiel flexible und kosteneffiziente Nutzungsmodelle oder die hohe Skalierbarkeit, für Anwendungsfälle wie dem Datenmanagement im Bereich der klinischen Forschung erschließen, müssen Dienstleistungen und Konzepte entwickelt werden, die zusätzlichen, Cloud-spezifischen Gefährdungen entgegenwirken. Diese entstehen unter anderem dadurch, dass der Cloud-Anwender keinen direkten Einfluss auf die Datenverarbeitung und der hierfür genutzten Systeme hat, die er mit anderen Anwendern teilt. Hierzu zählen vor allem die Kontrolle der endgültigen und vollständigen Löschung von Daten, die Kontrolle der Transparenz und Nachvollziehbarkeit durch Protokollierung und Dokumentation, sowie die Kontrolle

der Vervielfältigung und Verteilung von Daten [Ar11]. Weitere Gefahren bestehen bei der Datenübertragung, da Cloud-Dienste in der Regel außerhalb des internen, gesicherten Netzwerkes ausgeführt werden. Werden Daten, die zu unterschiedlichen Zwecken von unterschiedlichen Stellen erhoben wurden, innerhalb der gleichen Infrastruktur verarbeitet, müssen Maßnahmen umgesetzt werden, die unberechtigten Zugriffen Dritter oder einer unzulässigen Zusammenführung von Daten (z.B. auch durch zu weitgehende Zugriffsmöglichkeiten) entgegenwirken. Gefährdungen für die Verfügbarkeit des Datenbestandes entstehen durch eine mögliche Abhängigkeit vom Cloud-Anbieter und der von ihn angebotenen Dienstleistungen, wenn keine ausreichenden Möglichkeiten zum Export vorgesehen sind. In der Praxis kann zum Beispiel der Zugriff auf einen Datenbestand im Falle der Insolvenz des Cloud-Anbieters nahezu unmöglich werden.

Als Framework muss Cloudi/o den technischen Anforderungen an eine sichere Datenverarbeitung gerecht werden, kann aber keine organisatorischen Maßnahmen zur Aufrechterhaltung von Datenschutz und Datensicherheit umsetzen. Es darf diesen Maßnahmen aber auch keinesfalls entgegenwirken und muss die Umsetzung organisatorischer Maßnahmen auf technischer Seite aufnehmen und unterstützen. Zusätzlich sind weite Teile der technischen Sicherheit, wie zum Beispiel die der IT-Infrastruktur, innerhalb welcher eine auf Cloudi/o basierende Anwendung ausgeführt wird, von Cloudi/o selbst nicht beeinflussbar. Dies gilt im Besonderen für Cloud-Infrastrukturen. Hier muss Cloudi/o bestehende Risiken des Cloud-Computings berücksichtigen und möglichen Gefährdungen außerhalb seines direkten Einflussbereichs durch entsprechend zugeschnittene Maßnahmen innerhalb seines Einflussbereichs entgegenwirken.

Die Notwendigkeit und Angemessenheit von Maßnahmen richtet sich dabei nach dem einzelnen Anwendungsfall und der Art der Datenerhebung. Als Framework kann Cloudi/o daher keine allgemeingültigen Lösungen für jede denkbare Anwendung bereitstellen. Es muss aber jene Anforderungen erfüllen, die grundsätzlich für ein rechtkonformes und sicheres Management personenbezogener Daten einzuhalten sind, und zusätzliche Maßnahmen, die sich aus speziellen Anwendungsfällen ergeben können, ermöglichen. In der Gesamtheit muss ein Sicherheitspaket entstehen, welches den Gefährdungen in und durch eine Cloud-Infrastruktur in den Bereichen entgegenwirkt, auf die der Auftraggeber keinen direkten Einfluss nehmen kann. Notwendige Abgrenzungen von Informationen innerhalb unterschiedlicher Nutzer eines Anwendungsfalls müssen ebenso technisch unterstützt werden.

Von grundsätzlichem Charakter sind dabei vor allem Vorkehrungen zur Aufrechterhaltung der Vertraulichkeit durch einen angemessen Zugangskontrolle, einen restriktiven und differenzierbaren Zugriffsschutz sowie verschlüsselte Datenübertragung und –speicherung. Funktionalitäten zum Datenexport in allgemein lesbare Formate wirken der Abhängigkeit des Anwenders gegenüber dem Cloud-Anbieter und den von ihn erbrachten Dienstleistungen entgegen. Die Integrität des Datenbestandes kann durch kryptografische Signatur-Verfahren kontrolliert werden. Zum Zweck der Nachvollziehbarkeit und Revisionssicherheit der Datenverarbeitung stellt das Cloudi/o-Framework umfangreiche Möglichkeiten zur Protokollierung zur Verfügung.

Letztlich soll so die Möglichkeit zur Entwicklung von Dienstleistungen geschaffen werden, die durch die Kombination einer sicheren Anwendung und einer kontrollierbar sicheren Cloud-Infrastruktur, ein Datenmanagement ermöglicht, dass in Fragen des Datenschutzes und der Datensicherheit konventionellen Verfahren nicht nur ebenbürtig ist, sondern auch kleinen und mittleren Unternehmen (KMU) einen Zugang zu Werkzeugen für ein valides, sicheres und zeitgemäßes Datenmanagement ermöglicht.

3 Thematischer Hintergrund

Das vom Bundesministerium für Bildung und Forschung (BMBF) geförderte Projekt Cloudi/o - Sicheres Cloud-basiertes Datenmanagement im Umfeld der klinischen Forschung – basiert auf dem BMBF-Projekt SAMBA[2].

Das Ziel des Verbundvorhabens ist, die bisher im Gesundheitswesen vorherrschende ineffiziente Herangehensweise im Bereich der Datenerhebung sowie des Datenmanagements aufzubrechen und ein modernes, den heutigen Ansprüchen entsprechendes Datenmanagementsystem im Umfeld der klinischen Forschung zu schaffen.

Im Rahmen des Arbeitspakets der Marktumfeldanalyse wurden das thematische Umfeld des Projektvorhabens sowie bestehende IT-Standards, Frameworks und IT-Lösungen für die medizinische Anwendung sowie Referenzarchitekturen beleuchtet.

Im Bereich der IT Standards sorgen vor allem Standards wie xDT und HL7 (Health Level Seven) für eine Vereinheitlichung im Bereich der Datenstrukturierung und -Übertragung sowie des Datenaustauschs im Gesundheitswesen [Ka12][Be03]. Weiterhin regelt der DICOM (Digital Imaging and Communications in Medicine) Standard die Speicherung von Daten bildgebender und bildverarbeitender Systeme in der Medizin sowie deren Austausch in Kommunikationsprotokollen. Schwerpunkt ist hierbei die Interoperabilität zwischen medizinischen Endgeräten für bildgebende Verfahren [Na11]. Vereint werden solche Standards beispielweise in IHE (Integrating the Healthcare Enterprise) Profilen, welche domänenspezifische Regeln zur Datenspeicherung und –Verarbeitung beinhalten [Ih12]. Somit können seitens der Anwender Prozesse definiert werden, welche seitens der Softwareentwickler einzuhalten sind. Um die Kommunikation zwischen den sehr spezifischen Fachgebieten zu vereinfachen sorgen LOINC (Logical Observation Identifiers Names and Codes) und SNOMED (Systematized Nomenclature of Human and Veterinary) durch die Sammlung von Begriffen und Begrifflichkeiten für eine einheitliche Nomenklatur [Na09][Re13].

Standards im Bereich des Datenaustauschs zwischen verschiedenen Medien wie SOAP (Simple Object Access Protocol) oder REST (Representational State Transfer) bieten die Möglichkeit des strukturierten und gelenkten Datenaustauschs auf XML- und HTTP-Basis [Ba02][Su03]. Die gesamte Datenübertragung, von Verbindungsaufbau über Verschlüsselung bis hin zur Nachrichtenbestätigung wird in der Standardsammlung EDI

[2] http://www.samba-framework.de/

(Electronic Data Interchange) definiert. Dies dient der Sicherung der Datenübertragung, besonders bei hoch sensiblen Daten wie medizinischen Daten [Nö02].

Als themenrelevante Frameworks wurden das Spring-Framework, Dcm4che sowie Apache Jena identifiziert. Spring, als Open-Source-Framework auf Java-Basis, implementiert technische Lösungen für die Anwendungsentwicklung [Bi08]. Durch die umfängliche Herangehensweise müssen die Spring-Applikationen „Data“, „Security“ und „Integration“ besonders hervorgehoben werden.

Dcm4che dient ebenfalls als Java-Framework zur Erzeugung und Verarbeitung von Daten im DICOM-Format. Darüber hinaus unterstützt dieses Framework auch die Versendung von Dateien über das DICOM-Netzwerkprotokoll [Op13]. Somit stellt Dcm4che einen De-Facto-Standard im Bereich der medizinischen Datenübermittlung dar.

Apache Jena ist das am weitesten verbreitete Semantic-Web-Framework für Java. Es unterstützt das Lesen und Schreiben von Resource Direction Framework-(RDF)-Graphen, wobei verschiedene Datenquellen unterstützt werden, wie z.B. Dateien (XML oder platzsparende Jena-native Formate) oder Datenbanken. Die RDF- Informationen werden intern unabhängig von der Quelle als RDF-„Modelle“ repräsentiert [Ap13].

Im Bereich der Softwarelösungen zur Studiendokumentation stellt sich Oracle mit der Eigenentwicklung Oracle Clinical als Marktführer dar. Hierbei stellt Oracle Clinical ein integriertes Clinical Data Management- sowie ein Remote-Data-Capture-System dar, das nach eigenen Angaben weltweit bei mehr als 200 Unternehmen im Rahmen von klinischen Studien zum Einsatz kommt. Die integrierte Architektur sowie die Integration der Datensammlung, der Lokalisierung und des Reportings, die hohe Skalierbarkeit, die einfache Implementierung, leichte Benutzbarkeit und Erfüllung von regulatorischen Anforderungen hebt Oracle Clinical als größte Stärken des Produkts hervor [Or10].

GoodClinica ist ein Clinical Data Management System (CDMS) zur Erfassung, Strukturierung und Überprüfung von Daten, die im Rahmen klinischer Studien erhoben werden. Die webbasierte Anwendung zeichnet sich durch leicht bedienbare Benutzeroberflächen aus. Der Einstieg erfolgt über auf den Anwender zugeschnittene Sichten bzw. Matrizen, die einen Statusüberblick über die zu erfassenden Daten geben und direkten Zugriff auf die Erfassungsmasken ermöglichen. Alle Daten, die in GoodClinica eingegeben, geändert oder gelöscht werden, werden durch ein Audit Trail regulatorisch konform erfasst [So12].

Die Unternehmenssoftware IMPACT CTMS findet vor allem im Bereich der pharmazeutisch-klinischen Forschung im Rahmen der Planung, Verwaltung und Überwachung von klinischen Studien Anwendung. Auszeichnend für IMPACT CTMS ist die große Bandbreite an Konfigurationsmöglichkeiten in Verbindung mit der einer größtmöglichen Flexibilität. Somit werden hohe Anpassungsmöglichkeiten an Sponsor spezifische Workflows geboten [Pe13].

Gerade im Bereich der kleinen und mittleren Unternehmen (KMU) kommen die oben genannten Softwarelösungen nur selten zum Einsatz, da diese durch ihren umfänglichen

Charakter hohe Anschaffungs- und Unterhaltungskosten erfordern. Daher greifen diese Einrichtungen oftmals auf anwendungsorientierte Standardlösungen zur Datenbankverwaltung und Tabellenkalkulation zurück. Diese Systeme werden individuell angelegt und gepflegt, eine Übertragbarkeit auf weitere Projekte ist oftmals nicht gegeben. Somit resultiert hieraus ein hoher individueller Anpassungsbedarf. Darüber hinaus werden diese Systeme auf Grund der abweichenden ordinären Aufgabengebiete den speziellen regulatorischen Anforderungen von klinischen Studien nicht gerecht. Dies birgt die Gefahr von Datenverlusten sowie negativen Einflüssen auf die Datenkonsistenz.

Abschließend wird deutlich, dass durch verschiedene Standards und bestehende Lösungen im thematischen Umfeld ein bereits definierter Rahmen für neu zu entwickelnde Frameworks geboten wird. Dennoch bilden die bereits auf dem Markt befindlichen Softwarelösungen die speziellen Bedürfnisse der Zielgruppe kleiner und mittlerer Unternehmen nicht ab. Teilweise erfüllen diese zwar die regulatorischen und systemspezifischen Anforderungen, welche aus der klinischen Sicht hervorgehen, sind aber im Grad der Implementierung in kleineren Betrieben nicht umsetzbar. An diesem Punkt setzt das Projektvorhaben Cloudi/o an. Den bisher vorrangig mit Insellösungen arbeitenden Forschungseinrichtungen soll mit dem Cloudi/o-Framework die Möglichkeit einer Vereinfachung der Datenerfassung, der strukturierten und sicheren Datenspeicherung in der Cloud sowie ein den regulatorischen Anforderungen konformes Datenmanagement dargeboten werden.

4 Komponenten

Die Realisierung von Cloudi/o beinhaltet verschiedene definierte Komponenten, welche die Kernfunktionalitäten des mobilen und Cloud-basierten Datenmanagementansatzes abbilden. Cloudi/o wird dabei folgende sieben Komponenten enthalten.

Cloudi/o Repository: Das Cloudi/o Repository stellt die Schnittstelle zum eigentlichen Datenspeicher zur Verfügung. Dabei basiert das Repository auf Spring Data[3] um eine möglichst hohe Abstraktionsebene zum eigentlichen Speicher bzw. Cloud-Provider anzubieten. Somit erhält der Anwender eine hohe Flexibilität und Erweiterbarkeit, um vorhandene Infrastrukturen nutzen zu können. Gegebenenfalls muss lediglich das zur Verfügung gestellte Repository-Interface für die eingesetzte Speicherlösung implementiert werden, falls bisher noch keine Spring Data Implementierung vorhanden ist. Im Praxisprojekt soll hierfür eine Private-Cloud-Infrastruktur genutzt werden. Diese Lösung wird mit der MongoDB umgesetzt. Dabei handelt es sich um eine sogenannte NoSQL-Datenbank, die Daten dokumentbasiert im BSON Format speichert. Bei BSON (binäres JSON) handelt es sich um JSON mit einigen Erweiterungen. MongoDB kann aber auch nativ mit dem Format JSON umgehen, was auch zum Datenaustausch zwischen den Komponenten verwendet wird. Des Weiteren bietet MongoDB Replica-Sets zur Bildung von Master-Slave-Replikationen an, wodurch die Ausfallsicherheit und Performance bei Bedarf gesteigert werden kann. Ein Dokumentspeicher ist zudem für

[3] http://www.springsource.org/spring-data

Cloudi/o besonders gut geeignet, da bei Cloudi/o in der Regel Formulare gespeichert werden, die eins zu eins auf die Dokumentstruktur abgebildet werden können. Da es sich bei der MongoDB zudem um eine schemalose Datenbank handelt, können die verwendeten Objekte problemlos angepasst werden.

Cloudi/o Security: Cloudi/o Security ist keine in sich geschlossene Komponente. Hierbei handelt es sich sowohl um einen Teil des Frameworks, in denen die Authentifizierung und Autorisierung stattfinden, als auch um konkrete Maßnahmen zum sicheren Betrieb, die die einzelnen Komponenten durchziehen. Die Autorisierung wird dabei anhand einer Access Control List (ACL) implementiert, damit feingranular entschieden und eingestellt werden kann, welcher Nutzer auf welche Daten zugreifen kann. Somit wird technisch gewährleistet, dass ein Nutzer nur die Daten einsehen kann, die er auch wirklich für seine Arbeit benötigt. Um die Rechtevergabe etwas zu vereinfachen, werden Rechte-Templates angeboten, um bestimmte Rechte gruppieren zu können. Dabei handelt es sich um eine Art Schablone mit der automatisch mehrere Rechte zugewiesen werden können. Der Authentifizierungs- und Autorisierungsteil von Cloudi/o Security wird dabei direkt vor das Repository gelagert, um so bei jedem Zugriff eine Rechteprüfung durchzuführen. Somit werden an die anderen Komponenten nur Daten ausgeliefert, auf die der Nutzer Zugriff haben darf. Darüber hinaus wird jegliche Kommunikation zwischen den Komponenten von einem lückenlosen Auditingsystem erfasst.

Cloudi/o Studio: Das Studio ist das Verwaltungswerkzeug von Cloudi/o und verfügt über eine grafische Benutzeroberfläche. Es dient geschultem Personal zur Konzeption, Verwaltung und Auswertung von Studien, Erstellung von Workflows und Regeln für die Datenvalidierung, sowie der Erstellung und Verwaltung von Nutzerkonten und –rechten. Trotz ihres Umfangs ist diese Administrationssoftware so zu gestalten, dass die grafische Nutzungsoberfläche das IT-Personal nicht vor neue Probleme stellt. Auch die Darstellung und Auswertung von Daten, sowie der Export der Daten, sollen in Cloudi/o Studio ohne Expertenwissen durchführbar sein. Zusätzlich zum Verwalten von Studien und Studiendaten bietet Cloudi/o Studio eine Ansicht zur Konfiguration von Cloudi/o Security und zum Anzeigen und Auswerten der Auditing Daten. Um einen einfachen Zugang und eine ortsunabhängige Verfügbarkeit zu gewährleisten, wird Cloudi/o Studio wie auch Cloudi/o Care in einer Webanwendung umgesetzt. Es wird mit dem Google Webtool Kit (GWT) realisiert und teilt sich eine Codebasis mit dem Cloudi/o Care. Dabei werden die Daten per REST über Cloudi/o Connect zum jeweiligen Computer übertragen und schließlich per JavaScript im Browser des Nutzers angezeigt.

Cloudi/o Care: Die Komponente Cloudi/o Care dient als grafische Oberfläche für Patienten, Angehörige, Krankenhauspersonal oder wissenschaftliches Personal zur Erfassung von Daten. Cloudi/o Care muss speziell für Anwender ohne technisches Vorwissen konzipiert werden. Die grafischen Benutzungsoberflächen von Cloudi/o sollen selbsterklärend und intuitiv verständlich sein, so dass keine oder nur wenige Ressourcen aufgewendet werden müssen, um ein Cloudi/o System einsatzfähig zu machen. Cloudi/o Care wird dabei ebenso wie Studio als Webanwendung mit dem Google Webtool Kit (GWT) realisiert.

Cloudi/o Mobile Care: Die immer weiter verbreiteten Tablet-PC sind wie Smartphones hochportable Systeme, die sich sehr gut zur Erfassung von klinischen Daten eignen. Im Vergleich zu Cloudi/o Care, welches auch innerhalb eines Browsers auf einem Tablet-PC verwendet werden könnte, bietet Cloudi/o Mobile Care eine optimierte Eingabeoberfläche für das mobile Android und die entsprechenden Bildschirmgrößen und dient damit einer intuitiven Bedienung und einer flexiblen und standortunabhängigen Dateneingabe. Sie bietet die Möglichkeit zum sofortigen Datentransfer, Datenvalidierung und eine generelle Aufwandsreduzierung bei der Dateneingabe, da durch die Erfassung von Daten auf mobilen Endgeräten eine Verbesserung der Automatisierung ermöglicht werden kann. Um eine solche Verbesserung der Workflows zu ermöglichen, muss vor allem auf die Benutzbarkeit der mobilen Oberflächen geachtet werden, da auch diese möglichst ohne Vorwissen einsetzbar sein sollen.

Cloudi/o Connect: Die Konzeption der sicheren Verbindungen innerhalb einer Cloud-Architektur und die Bereitstellung der verschlüsselten Daten für Endgeräte wird in Cloudi/o Connect zusammengefasst. Cloudi/o Connect soll zusätzlich als Schnittstelle zu aktuell eingesetzten Lösungen konzipiert werden, d. h. sowohl zu KIS-Systemen wie auch zu Datenbanken von Speziallösungen, als auch zu ursprünglich auf einem definierten Excel-Schema basierenden Dateien, die importiert werden können. Cloudi/o Connect soll einen graduellen Wechsel zu Cloudi/o ermöglichen, ohne eine sofortige Anpassung aller existierender Workflows während der Einführung des Systems zu erfordern. Neben der Schnittstelle zu externen Systemen bildet Connect auch die Kommunikationsschnittstelle zu Cloudi/o Mobile Care. Realisiert wird Connect als ein REST-Service, der über eine sichere HTTPS-Verbindung angesprochen wird. Für die Umsetzung des REST-Service wird der entsprechende Teil des Spring MVC Frameworks verwendet.

Cloudi/o Bridge: Um Altsysteme anbinden und Daten aus existierenden Systemen importieren zu können, ist eine Komponente zu konzipieren, die eine Brücke zu Cloudi/o Connect darstellt. Diese Cloudi/o Bridge dient dem Import von Daten, die in XML, CVS, XLS oder JSON vorliegen, und deren Modell zuvor durch eine Schablone definiert wurde. Über diese Schablone können die Daten zugeordnet werden und so über die Connect- Schnittstelle in das Cloudi/o Repository importiert werden. Die Software ist so zu konzipieren, dass Soft- und Hardware auf verschiedenen Betriebssystemen angesprochen werden kann.

Cloudi/o Core: Bei Cloudi/o Core handelt es sich um eine Programmierbibliothek, die domänenspezifische Klassen enthält, die verteilt in mehreren Komponenten verwendet werden können. Sie enthält zum Beispiel Klassen die benötigt werden, um Formulare abbilden zu können. Diese Klassen werden zur Beschreibung von Formularen benötigt, damit mehrere Komponenten die Formulare anzeigen können. Diese mit Cloudi/o Studio erstellten Definitionen werden zu JSON serialisiert und im Cloudi/o Repository gespeichert oder über Cloudi/o Connect an Cloudi/o Mobile Care übertragen.

5 Cloudi/o Komponenten im Zusammenspiel

Cloudi/o wird als Webanwendung realisiert, wobei die Komponenten Studio, Care, Connect, Bridge und Repository auf dem gleichen Server ausgeführt werden und wie in der Abbildung zu sehen ist, den Kernbereich von Cloudi/o ausmachen. Cloudi/o Security hat eine Sonderstellung, da sie nicht an einer bestimmten Stelle implementiert wird. In der Grafik ist der Einfachheit halber nur die Authentifizierung abgebildet. Die Daten aus dem Repository werden über Cloudi/o Connect an Cloudi/o Studio, Cloudi/o Care und Cloudi/o Mobile Care ausgeliefert. Dieses findet allerdings nur nach einer erfolgreichen Authentifizierung und Autorisierung statt. Bei der Benutzung von Studio und Care werden die Anwendungsdaten in Form von HTML, CSS und JavaScript auf den Browser übertragen. Erst nach erfolgreicher Authentifizierung können die Studiendaten abgefragt werden. Über das Cloudi/o Repository wird der Datenspeicher in Form einer Private oder Public Cloud angebunden. Im Falle der Private Cloud kann die Datenbank-Infrastruktur auf dem gleichen oder einem anderen Server aufgesetzt werden. Cloudi/o Bridge dient als Adapter, der die Daten von externen Systemen wenn nötig in das Cloudi/o Format umwandelt und über Connect in Cloudi/o importiert.

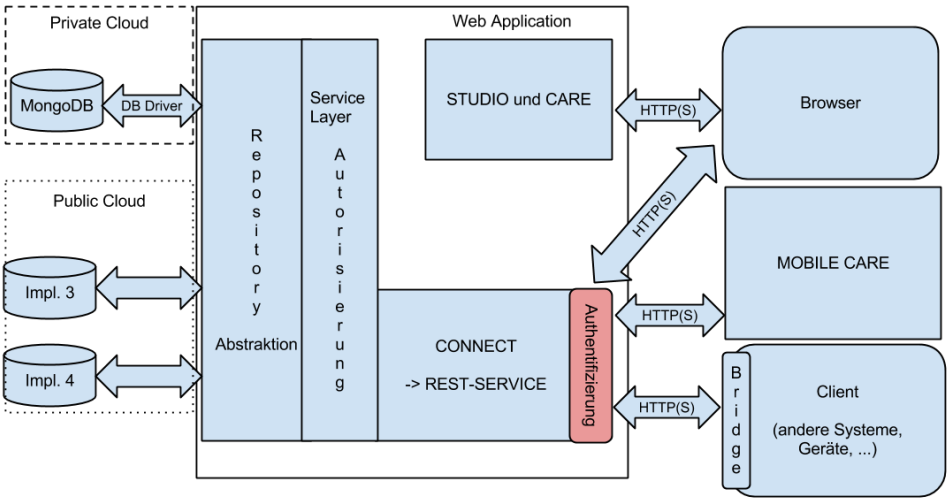

Abbildung 1: Schematische Darstellung des Cloudi/o-Frameworks

6 Evaluationsaufbau

Im Rahmen des Cloudi/o-Projektvorhabens kommt Scrum als Softwareentwicklungsmodell zum Einsatz. Während der Entwicklungsphase von insgesamt acht Monaten werden wiederholt Expertengespräche stattfinden, die eine strukturierte Usability Testung nach dem Modell des User Experience Tests darstellen. Hierbei wird der jeweilige Entwicklungsstand im Echtsystem anhand von differenzierten

Aufgaben getestet. Die Erfahrungen werden sowohl durch einen Fragebogen als auch durch eine abschließende Diskussion zwischen den Experten festgehalten.

Am Ende der ersten Entwicklungsphase steht ein Prä-Pilotmodell des Frameworks. Dieses wird in einem realitätsnahen, klinischen Forschungssetting für vier Wochen getestet. Auf Basis der Ergebnisse des Prä-Piloten wird der Prototyp einer auf dem Cloudi/o-Framework basierenden Anwendung entwickelt. Dieser wird im Rahmen eines Forschungsvorhabens der Charité, Universitätsmedizin Berlin, in einem realen Szenario über einen längeren Zeitraum angewendet. Diese Evaluationsstudie bildet die Basis für die Abschlussevaluation des Cloudi/o-Projektvorhabens. Im Fokus dieser Evaluation stehen die Kernaspekte Usability, Datenschutz- und GCP-Konformität, Skalierbarkeit der Daten, Performance und Datensicherheit.

Durch die umfängliche entwicklungsbegleitende Evaluation unter Einbeziehung verschiedenster Experten aus dem Feld der potenziellen Anwender des Frameworks wird der Praxisbezug des Cloudi/o-Projektvorhabens deutlich. Somit kann die Anwendbarkeit des generisch angelegten Frameworks mehrfach hinterfragt werden.

7 Weitere Schritte

Derzeit entsteht in sechs Entwicklungsschritten (Sprints) der Prä-Pilot des Systems. Darüber hinaus wird für die Realisierung des Praxisprojekts an einer differenzierten Anwendung auf Basis des Frameworks gearbeitet. Parallel befindet sich die Endevaluation in der detaillierten Planungsphase.

Literaturverzeichnis

[Ap13] Apache Jena. http://jena.apache.org/. - aufgerufen am 04.01.2013.

[Ar11] Arbeitskreise Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder (Hrsg.): Orientierungshilfe – Cloud Computing, Version 1.0, Stand 26.9.2011. http://www.datenschutz-berlin.de/content/technik/ratgeber/technisch-organisatorische-empfehlungen-und-orientierungshilfen/ - aufgerufen am 25.03.2013

[Ba02] Bayer, T.: REST Web Services: Eine Einführung. 2002.http://www.oio.de/public/xml/rest-webservices.pdf. – aufgerufen am 26.11.2012.

[Be03] Becker, P.: Datenkommunikation: Neue Schnittstellengeneration. Köln: Deutsches Ärzteblatt, PraxisComputer, Heft 3/2003.

[Bi08] Biskup, et al.: Spring Praxishandbuch: Integration und Testing. EntwicklerPress, 2008.

[Bu03] Bundesdatenschutzgesetz in der Fassung der Bekanntmachung vom 14. Januar 2003 (BGBl. I S. 66), das zuletzt durch Artikel 1 des Gesetzes vom 14. August 2009 (BGBl. I S. 2814) geändert worden ist. Stand: Neugefasst durch Bek. v. 14.1.2003 I 66; Zuletzt geändert durch Art. 1 G v. 14.8.2009 I 2814.

[Co06] Cole, E. et al.: A comparative study of mobile electronic data entry systems for clinical trials data collection. In: International Journal of Medical Informatics 75, 722-729, 2006. Elsevier Publishing

[De98] Deutsche Forschungsgemeinschaft (Hrsg.): Vorschläge zur Sicherung guter wissenschaftlicher Praxis – Empfehlungen der Kommission „Selbstkontrolle in der Wissenschaft“.Weinheim:Wiley-VCH, 1998

[Ih12] IHE International (Hrsg.): Integrating the Heathcare Enterprise. http://www.ihe.net/Technical_Framework/index.cfm#radiology Radiology Technical Framework. – aufgerufen am 22.11.2012.

[Ka12] Kassenärztliche Bundesvereinigung (Hrsg.): Schnittstellen: Schnittstellen für elektronischen Datenaustausch in der Arztpraxis. http://www.kbv.de/ita/4274.html. - aufgerufen am 16.12.2012.

[Na09] National Center for Biotechnology Information (Hrsg.): Sematik Network. http://www.ncbi.nlm.nih.gov/bookshelf/br.fcgi?book=nlmumls&part=ch05. – aufgerufen am 16.12.2012.

[Na11] National Electrical Manufacturers Association (Hrsg.): The DICOM Standard. http://medical.nema.org/standard.html. - aufgerufen am 16.12.2012.

[Nö02] Nöcker, G: Die beleglose Spedition. Lit Verlag, 2002

[Op13] Open Source Clinical Image and Object Management. http://www.dcm4che.org/ - aufgerufen am 04.01.2013.

[Or10] Oracle Industries. Powering Clinical Studies with Oracle Clinical. www.oracle.com/us/industries/life-sciences/oracle-life-sciences-solutions-br-414127.pdfhttp://www.oracle.com/us/products/applications/health-sciences/e-clinical/clinical/index.html. – aufgerufen am 04.01.2013.

[Pa11] Patapovas, A. et al.: Acceptance and Use of Digital Pen in an Emergency Department, In: Proceedings of the 23rd International Conference of the European Federation for Medical Informatics, User Centred Networked Health Care - A. Moen et al. (Eds.), Oslo, 2011.

[Pe13] Perseptive Informatics. http://www.perceptive.com/ctms/impact/. – aufgerufen am 04.01.2013.

[Re13] Regenstrief Institute, Inc (Hrsg.): RELMA: Regenstrief LOINC Mapping Assistent. http://loinc.org/downloads/files/RELMAManual.pdf. – aufgerufen am 16.12.2012.

[Sc07] Schweiger, A., Sunyaev, A., Leimeister, J. M., Krcmar, H.: Toward Seamless Healthcare with Software Agents. In: Information Systems and Healthcare XX, Communications of the Association for Information Systems, Volume 19, 2007, Berkeley Electronic Press.

[So12] sofd GmbH. http://www.sofd.de/goodclinica/. – aufgerufen am 04.01.2013.

[Su03] Suda, B.: SOAP Web Services, Master Thesis. Edinburgh: University of Edinburgh, 2003.