RHÖN-KLINIKUM
AKTIENGESELLSCHAFT

EHEALTHCOM
Magazin für Health-IT, vernetzte Medizintechnik und Telemedizin

CLOUD UND DATENSCHUTZ – EIN WIDERSPRUCH?

Aspekte einer datenschutzkonformen Nutzung von Cloud-Technologien zur nachhaltigen Wissensgenerierung in der Medizin aus Sicht eines Gesundheitsdienstleisters

Julian LAUFER[1], Marina WEFER[1], Philipp Daumke[2]
[1]*RHÖN-KLINIKUM AG, 97616 Bad Neustadt / Saale*
[2]*Averbis GmbH, 79106 Freiburg*

EINLEITUNG:

Im Umfeld der Informationstechnologie werden auch im Gesundheitswesen der Einsatz des Cloud-Computing und die Erschließung vorhandener Datenmengen als entscheidende Faktoren für die nachhaltige Gestaltung der IT-Strategie angesehen und diskutiert. Die perspektivische Nutzung einer sicheren und datenschutzkonformen Cloud Technologie kann hierbei neue Möglichkeiten der Wissensgenerierung durch Nutzbarmachung von Daten für unterschiedlichste Zwecke eröffnen.

In der medizinischen Versorgung von Patienten vor Allem in Gesundheitskonzernen und Krankenhäusern wie z.B. der RHÖN-KLINIKUM AG entstehen im Rahmen des Behandlungsprozesses und der Organisation im Behandlungsumfeld täglich erhebliche Mengen an Datensätzen. Doch wie kann man diese Daten datenschutzkonform auch neben der klinischen Routine zum Wohle der Patienten einsetzen? Welche organisatorischen,

datenschutzrechtlichen und technischen Herausforderungen treten in diesem Zusammenhang auf und welche Lösungen sind denkbar?

Frau Marina Wefer (Konzerndatenschutzbeauftragte der RHÖN-KLINIKUM AG) und Herr Julian Laufer (Projektleiter Cloud4Health der RHÖN-KLINIKUM AG) stellen im nachfolgenden Text mögliche Antworten auf obenstehende Fragen im Kontext des Forschungsprojektes Cloud4Health dar.

Das vom Bundesministerium für Wirtschaft und Technologie (BMWi) geförderte Projekt Cloud4Health, in dem die RHÖN-KLINIKUM AG als klinischer Projektpartner agiert, zeigt einen flexiblen, generischen und cloudbasierten Lösungsansatz zur Sekundärnutzung medizinischer Routinedaten auf. In diesem werden wichtige Informationen und Merkmale datenschutzkonform aus strukturierten und freitextlichen Daten erhoben, zusammengefasst und zur Wissensgenerierung erschlossen.

DATENSCHUTZRECHTLICHE RISIKEN UND HERAUSFORDERUNGEN

Bei der Erhebung, Verarbeitung und Nutzung personenbezogener Daten sind, unabhängig vom Einsatz von Cloud Technologien, die Vorschriften der einschlägigen Datenschutzgesetze sowie der vorrangigen Spezialnormen einzuhalten. Dies gilt in besonderem Maße für die Verarbeitung besonders sensibler Arten personenbezogener Daten, zu denen auch Angaben zur Gesundheit gehören. In diesem Rahmen sind bei der Abwägung datenschutzrechtlicher Risiken für den Betroffenen, in diesem Fall für Patienten, besonders strenge Maßstäbe anzusetzen, um deren Grundrecht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 GG in Verbindung mit Art. 1 Abs. 1 GG) nicht zu verletzen.

Sollen medizinische Daten der Patienten über den Behandlungszusammenhang hinaus für andere Zwecke, etwa der medizinischen Forschung, genutzt werden, steht dem Recht auf informationelle Selbstbestimmung beispielsweise die ebenfalls im Grundgesetz (Art.5 Abs. 3 GG) verankerte Freiheit der Forschung gegenüber. Sind personenbezogene Daten für ein Forschungsvorhaben erforderlich, ist hierfür in der Regel vorab eine informierte Einwilligung des Betroffenen einzuholen. Die Umsetzung dieser Anforderung gestaltet sich in der Praxis aber oft schwierig bis organisatorisch unlösbar.

Des Weiteren bestimmt das datenschutzrechtliche Prinzip der Datenvermeidung und Datensparsamkeit, so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen und diese Daten zu anonymisieren oder zu pseudonymisieren, sofern dem im Verhältnis zum angestrebten Schutzzweck, der bei besonders sensiblen Daten als besonders hoch einzuordnen ist, kein unverhältnismäßiger Aufwand entgegensteht. Jedenfalls muss für eine Sekundärnutzung medizinischer Daten das Risiko der Re-Identifizierung des Betroffenen minimiert werden.
In diesen Zusammenhang sind Lösungen für eine technische Umsetzung der Anonymisierung oder Pseudonymisierung zu finden, da die Durchführung insbesondere bei unstrukturierten Dokumenten deutlich schwieriger als bei definierten Datensätzen mit festgelegtem Format ist.

Die Pseudonymisierung bzw. Anonymisierung ist gerade auch dann relevant, wenn die Nutzung cloudbasierter Dienste vorgesehen ist, die aufgrund ihrer Flexibilität durch

bedarfsgerechten Einsatz, Einsparmöglichkeiten bei Anschaffung und Betrieb von IT Systemen sowie der standortunabhängigen Verfügbarkeit ökonomisch vorteilhaft sein können[1]. Andererseits birgt die Nutzung von Cloud Diensten aufgrund oft fehlender Transparenz bzgl. der Lokationen der Datenverarbeitung und der daran beteiligten Unternehmen sowie mangelnder Kontrollmöglichkeiten besondere datenschutzrechtliche Risiken.[2]
Ist im Falle der Übermittlung bzw. Weitergabe von Daten an einen Cloud Anbieter eine Rückführbarkeit auf eine Person gegeben, sind zuvor die datenschutzrechtliche Zulässigkeit zu prüfen und dann die Vorgehensweisen vertraglich zu regeln, etwa im Rahmen einer Datenverarbeitung im Auftrag[3] mit ihren formalen Voraussetzungen.
Liegen Sitz und Verarbeitungsort des Cloud Anbieters im außereuropäischen Ausland, sind zudem komplexe rechtliche Anforderungen zu beachten, die Privilegierung, die eine Datenverarbeitung im Auftrag nach §11 BDSG ermöglicht (der Auftraggeber bleibt verantwortliche Stelle, der Dienstanbieter wird als „verlängerter Arm“ des Auftraggebers eingeordnet) entfällt. Dies hat zur Konsequenz, dass jede Übermittlung von Daten einer expliziten Rechtsgrundlage auf Basis einer Rechtsvorschrift bzw. einer informierten Einwilligung bedarf, die regelhaft dann unzulässig und auch praxisfern ist, wenn es entweder keine Wahlmöglichkeit für den Betroffenen gibt oder dieser von seinem Recht Gebrauch macht, seine Einwilligung zu widerrufen[4].

GENERISCHES ARCHITEKTURMODELL

Um den datenschutzrechtlichen Risiken und Herausforderungen im Umfeld der Sekundärnutzung von medizinischen Daten in der Kombination mit Cloud-Technologien entgegen zu treten, wurde das Forschungsvorhaben Cloud4Health im Gesundheitswesen platziert. In diesem Vorhaben wird derzeit die Referenzarchitektur zum generischen Ansatz umgesetzt.

Für die Realisierung von cloud4health wurden zunächst vier fachliche Anwendungsfälle spezifiziert, die als Basis für die Implementierung sowohl des Prototypen als auch der cloud4health-Infrastruktur dienen.

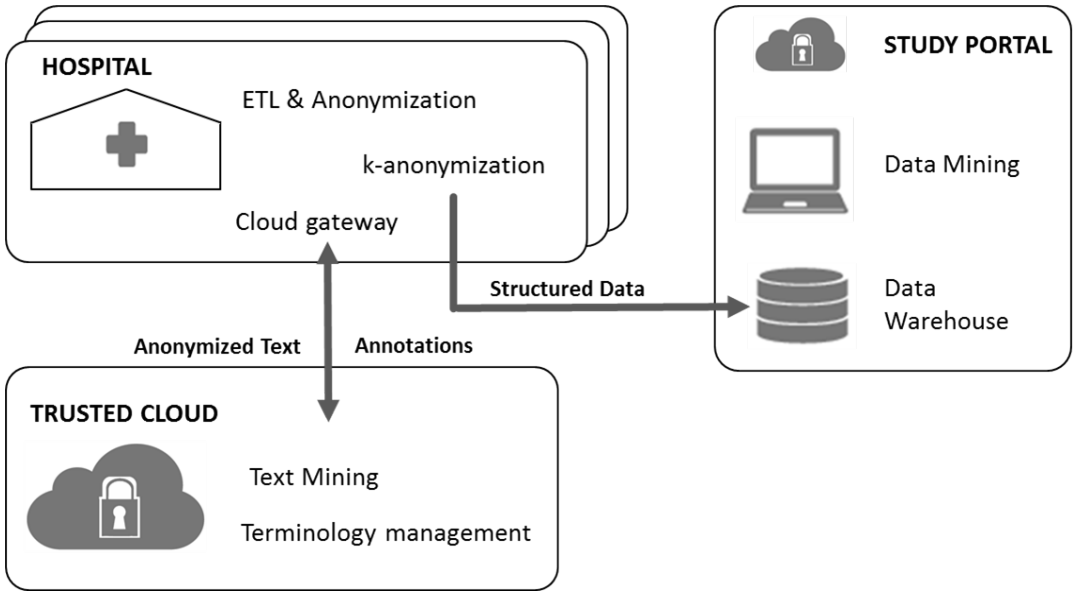
Die cloud4health-Architektur ermöglicht, dass verschiedene Datenlieferanten ihre strukturierten und freitextlichen Daten jeweils lokal aufbereiten und anschließend die für den Anwendungsfall benötigten Daten strukturiert in eine Datenbank liefern. Um das System für die Datenlieferanten kostengünstig anzubieten, wurden für die Implementierung der Architektur frei verfügbare Werkzeuge und Standards verwendet.

Der Architekturentwurf von cloud4health bildet ein strukturelles Rahmenwerk, um die einzelnen Komponenten mit ihren Verbindungen untereinander gesamtheitlich darzustellen.

---

[1] S.a. Orientierungshilfe Cloud Computing Konferenz der DSB Version 1.0, Stand 26.09.2011 http://www.datenschutz-bayern.de/technik/orient/oh_cloud.pdf, letzter Abruf 10.09.2013
[2] Pressemitteilung des ULD, 13.07.2012 https://www.datenschutzzentrum.de/presse/20120713-datenschutzkonformes-cloud-computing.htm, letzter Aufruf, 08.09.2013
[3] S. §11 BDSG
[4] S.a Eckpunktepapier Sicherheitsempfehlungen für Cloud Computing Anbieter, Bundesamt für Sicherheit in der Informationstechnik 2011, Kapitel 13.1, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindestanforderungen/Eckpunktepapier-Sicherheitsempfehlungen-CloudComputing-Anbieter.pdf, letzter Abruf 08.09.2013

Entscheidend ist hierbei die Trennung der verschiedenen Elemente der Datenverarbeitung. So erfolgt der Extract-Transform-Load (ETL)-Prozess dezentral in der datenliefernden Klinik und die Cloud-Datenpools können bei dem verantwortlichen Betreiber betrieben werden. Dafür wurde die Architektur für cloud4health in drei Bereiche untergliedert:



- Lokale cloud4health-Services: Erschließung und De-Identifizierung (Anonymisierung/Pseudonymisierung) der strukturierten und freitextlichen Rohdaten bei jedem Datenlieferanten vor Ort (ETL-Prozess)

- Textmining-Cloud: Annotation von Freitexten, geschützter Raum für Datenlieferanten als Arbeitsumgebung für studienspezifische Instanziierung, Textmining und Rückgabe strukturierter Ergebnisse an Lieferanten

- Cloud4health-Studienportal: Zusammenführung der Daten mehrerer Lieferanten in einem Studienportal, das neben dem Zugriff auf die Daten auch Services zur Auswertung (z.B. Reporting, Datamining) zur Verfügung stellt

Im Rahmen des Projektes Cloud4Health kommen somit verschiedene Cloudarten zum Einsatz - eine Private Cloud für die lokalen Dienste, die innerhalb der teilnehmenden Klinik verbleiben sowie im Textmining-Bereich eine Community-Cloud.

DATENSCHUTZKONFORMER UMGANG MIT PATIENTENDATEN FÜR DIE SEKUNDÄRNUTZUNG

Die oben dargestellten Herausforderungen erfordern neben diesen technischen Lösungsansätzen auch die Beachtung rechtlicher Rahmenbedingungen auf Basis des BDSG und weiterer Rechtsnormen, bis zu evtl. strafrechtlichen Konsequenzen nach §203 StGB. Für die Sekundärnutzung von Patientendaten ist eine Anonymisierung oder Pseudonymisierung personenbezogener Daten unabdingbar, vor allem, weil eine Einwilligungslösung an den Realitäten oft scheitert.

Auch die Nutzung von Cloud Diensten wird aus datenschutzrechtlicher Sicht dann vereinfacht, wenn keine besonderen personenbezogenen Daten an den Cloudanbieter übertragen werden.

Die Anonymisierung ist von der Pseudonymisierung personenbezogener Daten zu unterscheiden. Anonymisieren[5] bedeutet die Veränderung personenbezogener Daten derart, dass eine Rückführung auf eine Person nicht oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft möglich ist. Sind die Daten hinreichend wirksam „faktisch" anonymisiert, entfällt der Schutz der Datenschutzgesetze, diese sind nicht mehr anwendbar. Die Anonymisierungsprozedur selbst unterliegt den Regelungen des BDSG.

Damit nicht zu verwechseln ist die Pseudonymisierung[6], die eine gewollte Rückführbarkeit auf eine bestimmte oder bestimmbare natürliche Person ermöglicht, die Daten bleiben personenbeziehbar, ihre Verwendung zu anderen als den ursprünglichen Zwecken wird somit nur mit Einwilligung des Betroffenen erlaubt. Allerdings gelten an einen Dritten weitergegebene Daten dann als für diesen anonym, wenn für ihn keine Rückführbarkeit auf den Betroffenen möglich ist, etwa, weil die Zuordnungsvorschrift oder Zusatzinformationen nicht vorliegen.

Die oben erwähnten lokalen Dienste der C4H Architektur wurden aufgrund der Anforderungen des Datenschutzes (bzw. evtl. strafrechtlicher Konsequenzen nach §203 StGB) implementiert, da personenbezogene Daten nicht ohne Rechtsgrundlage übermittelt werden dürfen, und daher die Anonymisierung bzw. Pseudonymisierung innerhalb der verantwortlichen Stelle erfolgen muss. Zur Sicherstellung der Nachvollziehbarkeit der Vorgänge wurde ein Audit Trail implementiert, der jeden Versand, Zugriffe und Anfragen des Systems protokolliert.

Im Rahmen des Textminings, das außerhalb der teilnehmenden Klinik stattfindet, werden anonymisierte Textdaten verarbeitet, dies wird durch visuelle Prüfungen kontrolliert.

Zur Sicherstellung weiterer technischer und organisatorischer Erfordernisse wurde außerdem ein umfassendes Datenschutz- und Datensicherheitskonzept erstellt, das neben organisatorischen Verantwortlichkeiten, Rollen- und Berechtigungskonzepten und Löschvorgaben auch Schutzbedarfsfeststellungen sowie einzuhaltende Sicherheitsmaßnahmen enthält.

Durch die Schaffung anonymer bzw. pseudonymer Nutzungsmöglichkeiten und die Umsetzung dieser Maßnahmen kann ein besonders hohes Schutzniveau und eine datenschutzkonforme Nutzung medizinischer Sekundärdaten gewährleistet werden.

[5] S. §3 (6) BDSG:

[6] S. §3 (6a) BDSG: Pseudonymisieren ist das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren

DANKSAGUNG:

Das cloud4health-Konsortium besteht aus der Averbis GmbH (Konsortialführer), der RHÖN-KLINIKUM AG, der TMF - Technologie- und Methodenplattform für die vernetzte medizinische Forschung e.V., dem Fraunhofer-Institut SCAI und der Friedrich-Alexander-Universität Erlangen-Nürnberg. Das Projekt wird bis November 2014 vom Bundesministerium für Wirtschaft und Technologie (BMWi) im Förderprogramm Trusted Cloud (FKZ 01MD11009) gefördert.

REFERENZEN:

- Li Z, Wen J, Zhang X, Wu C, Li C, Li Z, Liu L. ClinData Express - A Metadata Driven Clinical Research Data Management System for Secondary Use of Clinical Data. AMIA Annu Symp Proc, 2012: 552-7.
- cloud4health. Online verfügbar unter: http://cloud4health.de/, zuletzt geprüft am 16.09.2013.
- Griebel, L.; Leb, I.; Christoph, J.; Laufer, J.; Marquardt, K.; Prokosch, H.U.; Toddenroth, D.; Sedlmayr, M.: Cloud-Architektur für die datenschutzkonforme Sekundärnutzung strukturierter und freitextlicher Daten, Proceedings of the eHealth2013, 2013,
- Rechtliche Rahmenbedingungen BDSG (Begriffsbestimmungen §3 BDSG - personenbezogene Daten, Anonymisierung / Pseudonymisierung)
- Stellungnahme 4/2007 zum Begriff „personenbezogene Daten“ der EU Article 29 Data Protection Working Party - WP 136 01248/07/DE WP 136 (personenbezogene Daten, Anonymisierung / Pseudonymisierung)
- Eckpunktepapier Sicherheitsempfehlungen für Cloud Computing Anbieter, Bundesamt für Sicherheit in der Informationstechnik 2011 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindestanforderungen/Eckpunktepapier-Sicherheitsempfehlungen-CloudComputing-Anbieter.pdf
- OH Cloud Computing AK Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder V. 1.0 26.09.2011, http://www.datenschutz-bayern.de/technik/orient/oh_cloud.pdf
- Weiterführende Hinweise: EU Article 29 Data Protection Working Party : Opinion 05/2012 on Cloud Computing 01037/12/EN WP 196
- EuroPriSe – Das Europäische Datenschutz-Gütesiegel des ULD Datenschutzrechtliche Anforderungen an Cloud Computing (Cloud Computing FS-201207-DE)
- Weiterführende Literatur: Studie des Europäischen Parlaments zum Cloud Computing, Download unter http://www.europarl.europa.eu/studies http://www.europarl.europa.eu/committees/en/studiesdownload.html?languageDocument=EN&file=73411