Fraunhofer

Leitprojekt MED²ICIN

Sichere Konnektoren: Kontrollierbare und sichere Datenübertragung durch den Medical Data Space

Mehrwerte:

- Sichere Datenübertragung zwischen verschiedenen Endpunkten
- Nutzungskontrolle der Daten vor der Übertragung und auch im fremden Datenraum nach der Übertragung
- Verwendung standardisierter Schnittstellen (REST, FHIR)

Hintergrund

Die sichere Übertragung von Daten spielt auch im Leitprojekt MED²ICIN eine große Rolle, da verschiedene klinische Partner und deren Daten an das System angebunden werden. Neben der Notwendigkeit einer abgesicherten Datenübertragung stellen sich bei medizinischen Daten auch die besonderen Fragen hinsichtlich des Datenschutzes. Hierfür bietet die Technologie des Medical Data Spaces (MedDS) diverse Lösungsansätze. Im Rahmen des Leitprojekts MED²ICIN wird ein MedDS aufgespannt, um eine sichere Datennutzung in einem verteilten, dezentralen System zu gewährleisten.

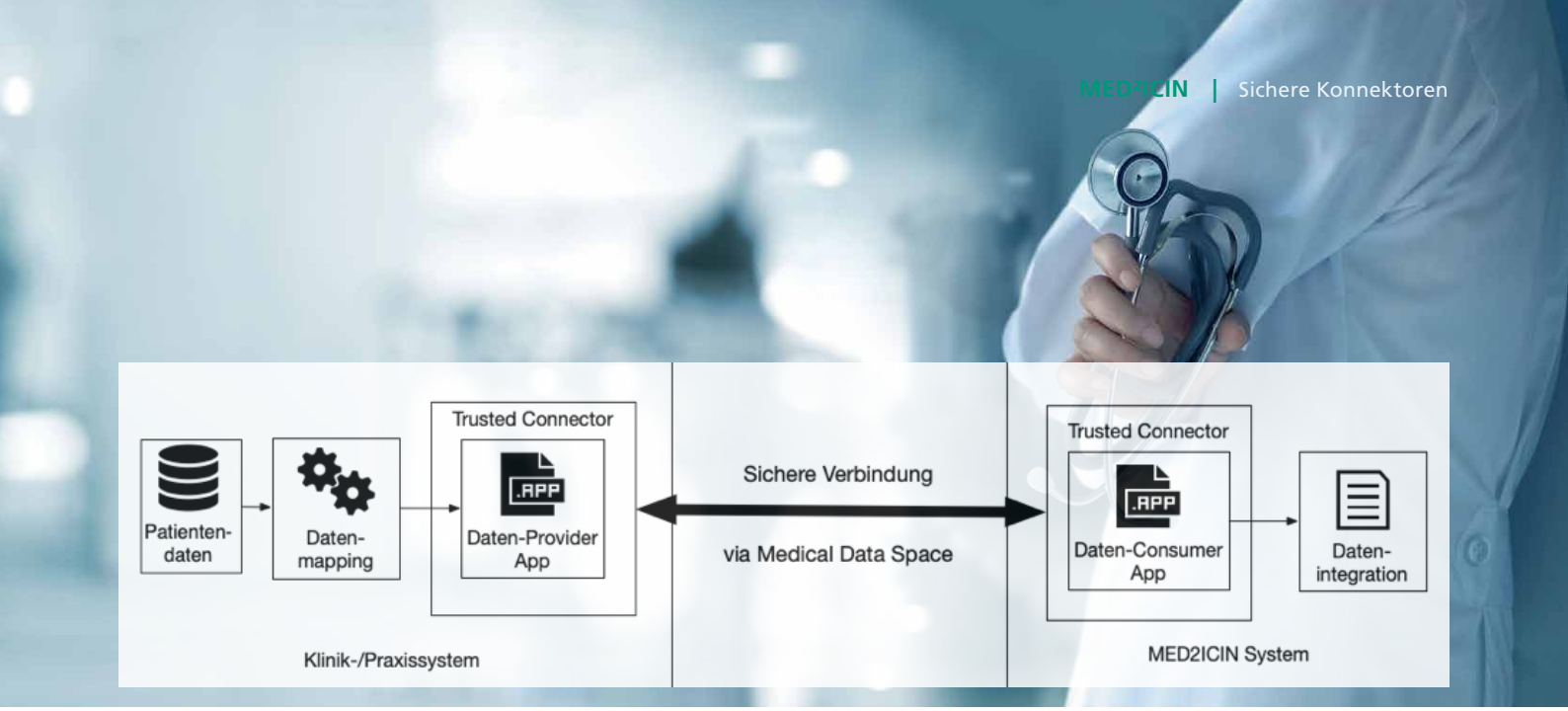
Der Medical Data Space

Dieser MedDS basiert auf Elementen des International Data Space (IDS). Im IDS, der ursprünglich auf die Anforderungen der industriellen Produktion ausgelegt war, wurden Bausteine und Vorgehensweisen entwickelt, um Datenräume für eine vertrauenswürdige gemeinsame Datennutzung zu schaffen. Dabei wird eine Reihe unterschiedlicher Anwendungsdomänen betrachtet, die sich aus der industriellen Basis entwickelt und von einer europäisch aufgestellten Community vorangetrieben werden. Als domänenspezifische Umsetzung soll dieser MedDS von den bisherigen Lösungen hinsichtlich Sicherheit, Datenschutz und Datensouveränität profitieren und gleichzeitig auf die Besonderheiten der medizinischen Anforderungen eingehen. Eine große zusätzliche Herausforderung ist hierbei, dass gegenüber den bisherigen Domänen im MedDS zusätzlich die Patientinnen und Patienten als direkte Betroffene in den Prozess der Transparenz und Datenkontrolle zu involvieren sind. Dies muss zu jeder Zeit sichergestellt werden, um die strengen Vorgaben bezüglich der sensiblen Gesundheitsdaten zu erfüllen, wie sie beispielsweise die Datenschutzgrundverordnung (DSGVO) fordert.

Im Unterschied zu bestehenden Methoden zur sicheren Datenübertragung wie einem Virtual Privat Network (VPN) bietet der MedDS nicht nur die Möglichkeit, die Daten sicher zu übertragen, sondern auch die Möglichkeit, die Nutzung der Daten über die eigentlichen Systemgrenzen hinaus zu kontrollieren.

Sichere Datenräume durch die Trusted Connector Technologie

Der sogenannte Trusted Connector (TC) ist eine standardisierte Komponente des IDS. Der Datenaustausch wird über



verschiedene Routen zwischen ein- und ausgehenden Daten organisiert. Die vertrauenswürdige Ausführungsumgebung des TC selbst besteht lediglich aus dem Routing und dem Datentransferprotokoll, das durch sogenannte Remote Attestierung abgesichert ist. Hierdurch werden die Sicherheit der Verbindung und die Konformität der Konnektoren selbst dem technischen Gegenüber nachweisbar sichergestellt. Um den TC mit den entsprechenden Daten zu verbinden, wird eine zusätzliche Datenanbindungsanwendung innerhalb des Konnektors benötigt. Dieser wird ein Praxis-/Zielsystem angebunden und kann entsprechend notwendige Datenmappings – beispielsweise um Daten in das gewünschte Format zu überführen – durchführen.

Datensouveränität für Patienten und Ärzte

Die verschiedenen Kontroll- und Durchsetzungsmechanismen ermöglichen Datensouveränität sowohl für Ärzte als auch Patienten. Patienten können zielgerichtete Einwilligungen für ihre Daten erteilen, die bei der Verarbeitung im TC vor der Datenübertragung durchgesetzt werden. So können hier bereits Daten oder spezielle Attribute, für die ein Patient keine Einwilligung erteilt hat, entfernt werden. Zusätzlich können Ärzte bestimmt Richtlinien vor Übertragung der Daten festlegen, wie beispielsweise eine Pseudonymisierung oder komplette Anonymisierung. Eine solche Pipeline kann individuell in den verschiedenen Konnektoren aufgesetzt werden.

Zusätzlich besteht die Möglichkeit, auch im fremden Datenraum der Zielkonnektoren die weitere Benutzung der übertragenen Daten zu kontrollieren. Diese Art der Nutzungskontrolle ermöglicht es beispielsweise, Richtlinien wie die einmalige Nutzung der Daten oder das Löschen der Daten nach 30 Tagen zu forcieren.

Integration des MedDS

Um den MedDS im Rahmen von MED²ICIN zu integrieren wird pro Datenanbieter ein TC aufgesetzt. Der TC ist eine reine Softwarelösung, die in der Regel keine zusätzliche Hardware benötigt. Innerhalb dieses TC wird dann die Anbindung an die entsprechende Datenbank vorgenommen. Je nach Format wird noch ein Mapping benötigt. Ein solches Mapping wird in der IDS-spezifischen Variante eines VoCoReg-Services implementiert und vorgehalten.

Der Zielkonnektor im MED²ICIN-Verbund empfängt diese Daten und integriert sie innerhalb des Gesamtsystems. Die obenstehende Abbildung zeigt die hier beschriebene Architektur.

Der MedDS soll in seiner finalen Form die gängigsten medizinische Datenstandards wie FHIR unterstützen. Dadurch soll eine nahtlose Integration in verschiedene Praxis- und Kliniksysteme ermöglicht werden, ohne dass aufwändige, nachgelagerte Anpassungen oder weitere Integrationsschritte durchgeführt werden müssen.

Fraunhofer-Institut für Optronik, Systemtechnik und Bildauswertung

Ansprechpartner
Dr. Erik Krempel
Gruppenleiter Identitätsmanagement
Tel. +49 721 6091-292
erik.krempel@iosb.fraunhofer.de

Fraunhoferstraße 1
76131 Karlsruhe

s.fhg.de/med2icin