Helios.bridge: Brücke zum Patienten

Bei der Digitalisierung administrativer und medizinischer Prozesse ist Helios Vorreiter in Europa. Der Krankenhausbetreiber hat eine wegweisende Architektur aufgebaut mit dem Ziel, Patienten aktiv in digitale Behandlungsprozesse einzubinden. Dafür nutzt Helios die Module der ICW eHealth Suite. Datenschutz und -sicherheit spielten bei der Umsetzung eine zentrale Rolle.

Helios ist Europas führender privater Krankenhausbetreiber mit mehr als 111 Akut- und Rehabilitationskliniken, 89 medizinischen Versorgungszentren (MVZ), vier Rehazentren, 17 Präventionszentren und 12 Pflegeeinrichtungen allein in Deutschland.

Als innovatives Unternehmen treibt Helios die Digitalisierung der administrativen und medizinischen Prozesse in allen Einrichtungen voran und stellt einrichtungsübergreifende Mehrwertdienste für Patienten und Ärzte zur Verfügung. Für Mehrwertdienste wie das Helios Patientenportal hello oder integrierte mobile Apps hat Helios in den vergangenen Monaten eine zentrale Infrastruktur namens Helios.bridge aufgebaut. Die Helios.bridge ist in die vorhandene Infrastruktur der Helios Kliniken integrierbar, unterstützt offene Standards für den interoperablen Datenaustausch zwischen den IT-Systemen der Einrichtungen und den Mehrwertdiensten und entspricht aktuellen Datenschutzanforderungen. Die Helios.bridge läuft in der Helios.cloud. Diese Backbone-Infrastruktur verbindet alle Helios Standorte und zentralen Rechenzentren (zertifiziert gemäß Reliable Data Center CAT III). Über diese Infrastruktur werden auch sämtliche institutionsübergreifenden Onlineservices angeboten. Alle Komponenten und Prozesse der Helios.bridge unterliegen daher dem zertifizierten Informationsmanagementsystem gemäß ISO/IEC 27001:2013 und werden somit auch im Rahmen der jährlich stattfindenden Audits durch den TÜV Rheinland sowie unabhängiger externer Pen-Tests geprüft.

Architekturübersicht

Für die Helios.bridge wurde eine zentrale IHE Affinity Domain aus verschiedenen Modulen der ICW eHealth Suite aufgebaut:

In den lokalen Helios Einrichtungen ist das Modul **MESSAGE FILTERING AGENT** installiert, das Patientendaten in die Helios.bridge weiterleitet, sobald eine elektronische Patienteneinwilligung vorliegt. Die Helios.bridge verfügt über einen **MASTER PATIENT INDEX,** der die Patientenidentitäten der lokalen Einrichtungen über HL7-ADT-Nachrichten empfängt

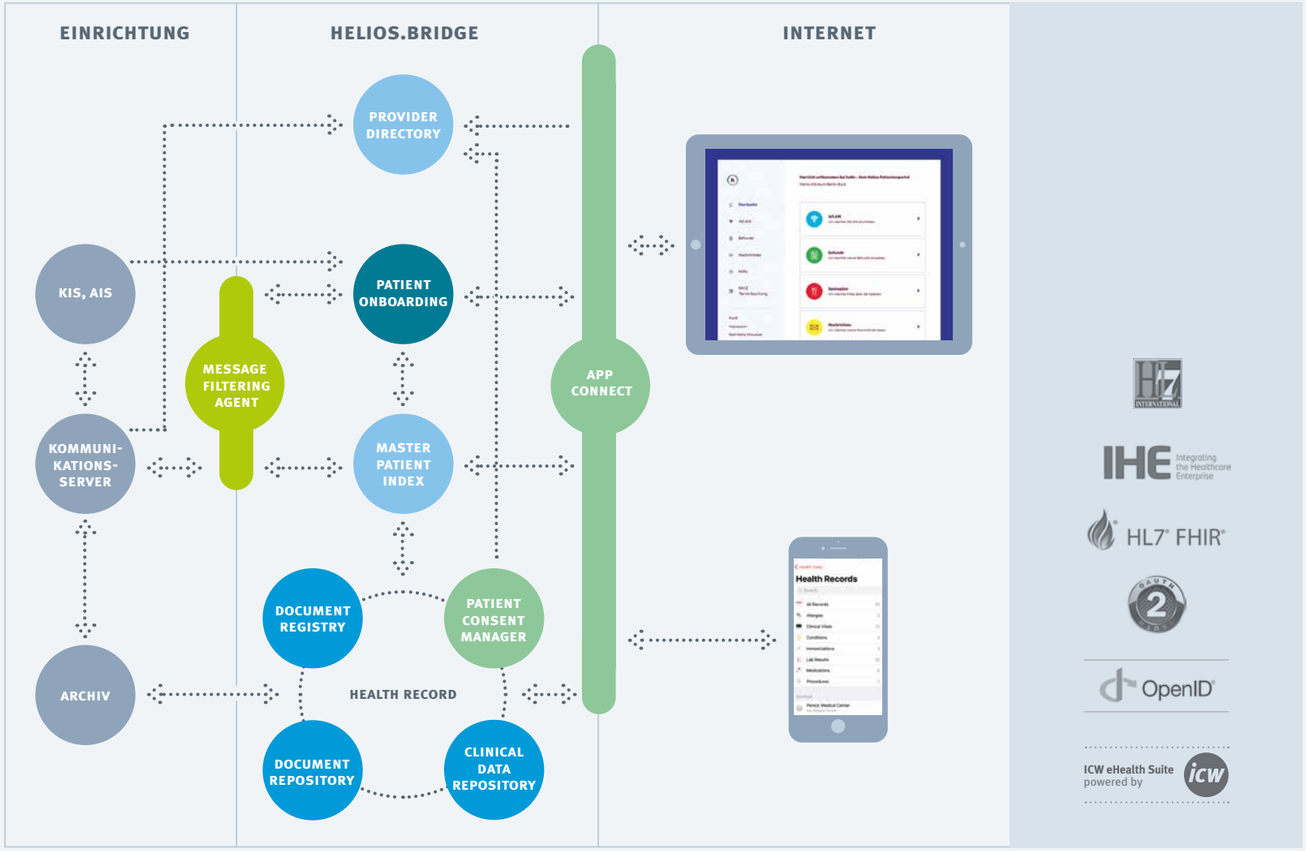
AUTOR: Dirk Herzberger

FUNKTION: Leiter Helios IT

EINRICHTUNG: HELIOS Kliniken GmbH

ARCHITEKTUR-ÜBERSICHT

Die zentrale Helios.bridge verbindet die Einrichtungen mit den digitalen Patienten-services und greift dafür auf verschiedene Standards zurück.



und mit einer einrichtungsübergreifend eindeutigen Patientenidentität verknüpft. Im Modul **DOCUMENT & IMAGE EXCHANGE** sind Verweise auf registrierte Dokumente gespeichert. Die Dokumente selbst verbleiben in den lokalen Archivsystemen und werden erst beim Zugriff angefordert. Die Kommunikation mit den Archivsystemen erfolgt auf Basis von IHE PIX und IHE XDS.b. Strukturierte medizinische Daten wie Fallinformationen, Diagnosen, Prozeduren oder Laborwerte werden als HL7v2-Nachrichten übertragen und im Modul **CLINICAL DATA REPOSITORY** gespeichert. Das Modul **PROVIDER DIRECTORY** speichert Informationen zu Einrichtungen und Leistungserbringern in einem zentralen Verzeichnis, das für die eindeutige Identifizierung dieser Daten in Zuweiser-Szenarien genutzt wird. Über das Modul **PATIENT ONBOARDING** können sich Patienten als Benutzer registrieren und ihr Benutzerkonto mit der zugehörigen einrichtungsübergreifenden elektronischen Patientenakte verknüpfen. Darüber hinaus kann der Patient mithilfe dieses Moduls seine Einwilligungen zur Datenübertragung verwalten und seine Apps für den Datenzugriff berechtigen. Das Modul **APP CONNECT** bietet zahlreiche HL7 FHIR-Schnittstellen für den bidirektionalen, sicheren Datenaustausch zwischen der Helios.bridge und den verschiedenen Mehrwertdiensten.

Daten und Anwendungsfälle

Die Helios.bridge bietet den Patienten die Möglichkeit, auf vielfältige, und alle für sie relevanten medizinischen Daten zuzugreifen, sofern sie die Übermittlung aus den jeweiligen Einrichtungen explizit freigeschaltet haben. Diese Daten umfassen nach Abschluss der aktuellen Projektphase bis Ende des Jahres die folgenden Daten und medizinischen Dokumente:

- Administrative Daten
  - Patientendaten
  - Administrative Fälle
  - Termine
- Dokumente und Bilddaten
  - Unstrukturierte PDF-Dokumente (Arztbriefe, Epikrisen, Labor-, Pathologiebefunde, Medikationspläne ...)
  - Röntgen-, Ultraschall-, MRT-, CT-Bilder, Fotos (zumeist konvertiert)
- Strukturierte Daten
  - Laborwerte
  - Diagnosen
  - Prozeduren
  - Formulare

Auch der Benutzer selbst kann Daten in seine Akte der Helios.bridge einstellen, beispielsweise per mobiler App. Diese Daten stehen dann wiederum den Einrichtungen für weitere diagnostische und therapeutische Maßnahmen zur Verfügung. Drei beispielhafte Szenarien hierfür sind:

Szenario A: Vom Patienten auszufüllende Formulare (Self-Check-In) in verschiedensten Anwendungsfeldern. Zum Beispiel können die Betroffenen anamnestisch bereits im Vorfeld einer geplanten Rehabilitationsmaßnahme den mehr als zehn DIN-A4-Seiten umfassenden und komplexen MBOR-Fragebogen (Medizinisch-beruflich orientierte Rehabilitation) bequem zu Hause ausfüllen. Dieser enthält ausführliche Fragen zu Vorerkrankungen, Vortherapien, Medikation, Risikofaktoren, Status Quo, häuslicher und beruflicher Situation, sozialem Umfeld, Aktivitätseinschränkungen und Erwartungen an Reha. Die dort erhobenen Daten können als HL7 FHIR-Questionnaire Response in das KIS der aufnehmenden Reha-Klinik übernommen werden und stehen dann dem behandelnden medizinischen Personal beim Erstgespräch mit dem Patienten direkt zur Verfügung.

Szenario B: Erhebung von verschiedenen Parametern wie Körpergewicht, Blutdruck, Blutzucker, Sauerstoffsättigung durch Wearables und Übertragung dieser Gerätedaten mittels mobiler App in die Helios.bridge. Ein Anwendungsbeispiel ist die metabolische Chirurgie (Magenverkleinerung). Während der vorangehenden mehrmonatigen Vorbereitungsphase nimmt der Patient an verhaltenstherapeutischen Kursen teil und es werden regelmäßig Vitaldaten erhoben. Das ist besonders wichtig, gerade auch im Hinblick auf eine Kostenübernahme durch die gesetzlichen Kostenträger. Wearables/Smart Devices erfassen, übertragen und integrieren die Daten und unterstützen damit diesen komplexen Prozess in signifikanter Weise.

Szenario C: Anbindung externer Quellen in verschiedenen Szenarien über IHE-Schnittstellen (Cross Enterprise Document Sharing XDS und Cross Community Access XCA).

Datenschutz und Datensicherheit

Die Helios.bridge wurde in enger Abstimmung mit den zuständigen Behörden realisiert. Somit sind Datenschutz und Informationssicherheit jederzeit gewährleistet. Der Zugang zur Helios.bridge ist dreistufig abgesichert. Je nach Sicherheitsstufe stehen den Benutzern verschiedene Funktionalitäten zur Verfügung:

DIE DREI SICHERHEITSSTUFEN SIND:

1 Registrierung und Login
- Allgemeine Informationen (z.B. Kliniken, Fachbereiche, Ansprechpartner)
- Buchungs- und Servicefunktionalitäten (z.B. Kontaktformular, Terminanfrage)
- Kostenfreie WLAN-Nutzung

2 Zwei-Faktor Authentifizierung
- Abruf von personenbezogenen Daten (Consent-, Accountmanagement)
- Zugriff auf das Nachrichtensystem „Messaging Center“
- Terminbearbeitung/-löschung

3 Freischaltung der Einrichtung
- Abruf von gesundheitsbezogenen Daten
- Zugriff auf medizinische Informationen, Daten und Dokumente

Damit Patienten die allgemeinen Informations- und Servicefunktionalitäten gemäß Sicherheitsstufe 1 nutzen können, ist lediglich eine formlose Registrierung zur Erstellung eines Benutzerkontos (Benutzername, Passwort und E-Mail-Adresse) erforderlich.

Die Sicherheitsstufe 2 schützt den Zugriff auf personenbezogene Daten. →

Datenschutz und Informationssicherheit werden durch drei Sicherheitsstufen gewährleistet.

Dazu ist ein zusätzliches Benutzer-Authentifizierungsverfahren, die Zwei-Faktor-Authentifizierung (2FA), erforderlich. Dieses Verfahren verlangt eine zweite, unabhängige Bestätigung der Identität des Benutzers. Realisiert wird die Zwei-Faktor-Authentifizierung über die mobile Helios Safe-App, die auf dem Gerät (Smartphone) des Nutzers installiert ist.

Bei der 2FA wird die Identität des Benutzers sichergestellt, indem zwei voneinander unabhängige, nur ihm verfügbare Faktoren überprüft werden (Challenge Response Methode), nämlich Besitz (das Smartphone) und Wissen (PIN). Möchte der Benutzer nun auf einen Service der Sicherheitsstufe 2 (oder 3) zugreifen, wird der zusätzliche Autorisierungsprozess mit der Helios Safe-App gestartet und der Access-Pass (ein Smart Icon) im Browser angezeigt. Gleichzeitig wird eine Anfrage auf das Smartphone des Benutzers gesendet. Nach Eingabe der persönlichen PIN (oder Touch ID) werden in der App mehrere Smart Icons angezeigt. Der Benutzer muss nun das im Browser angezeigte Bild auswählen. Nach erfolgreicher Freischaltung über die Helios Safe-App wird der Benutzer automatisch zum gewünschten Service weitergeleitet. Der Zugriff auf medizinische Patientendaten (Sicherheitsstufe 3) setzt neben dem Login und der Zwei-Faktor-Authentifizierung zusätzlich die explizite Freischaltung der Datenkommunikation voraus.

Die Freischaltung der Kommunikation in die Helios.bridge erfolgt einrichtungsbezogen und durch den Patienten selbst:

- Patienten erhalten anlässlich eines Aufenthaltes in einer Helios Einrichtung einen PIN-Brief mit einem zufällig erzeugten und zeitlich limitierten PIN-Code. Durch die Eingabe des Codes sowie ausgewählter weiterer, nur dem Patienten bekannten Angaben (Secrets) in ein Online-Formular, erfolgt die Freischaltung der Datenübertragung (Whitelist-Eintrag im Modul Message Filtering Agent) aus der jeweiligen Einrichtung in die Helios.bridge.
- Patienten können ihre an die jeweilige Einrichtung gebundene Zustimmung zur Datenübermittlung jederzeit zurückziehen. Das über die Zwei-Faktor-Authentifizierung zugängliche Benutzerprofil enthält eine Übersicht der vom Benutzer freigeschalteten Einrichtungen (Standortliste). Hier kann der Benutzer die Löschung von bereits in der Helios.bridge vorliegenden Daten des gewünschten Standortes vornehmen und/oder die Nachrichtenweiterleitung aus diesem Standort (auch befristet) deaktivieren.

Nach der Freischaltung der Datenübertragung durch den Patienten werden die verschiedenen Daten und Dokumente, die im Rahmen der Behandlung entstehen, in einer einrichtungsübergreifenden IHE Document Registry registriert und bei Bedarf aus den lokalen Archivsystemen geladen.

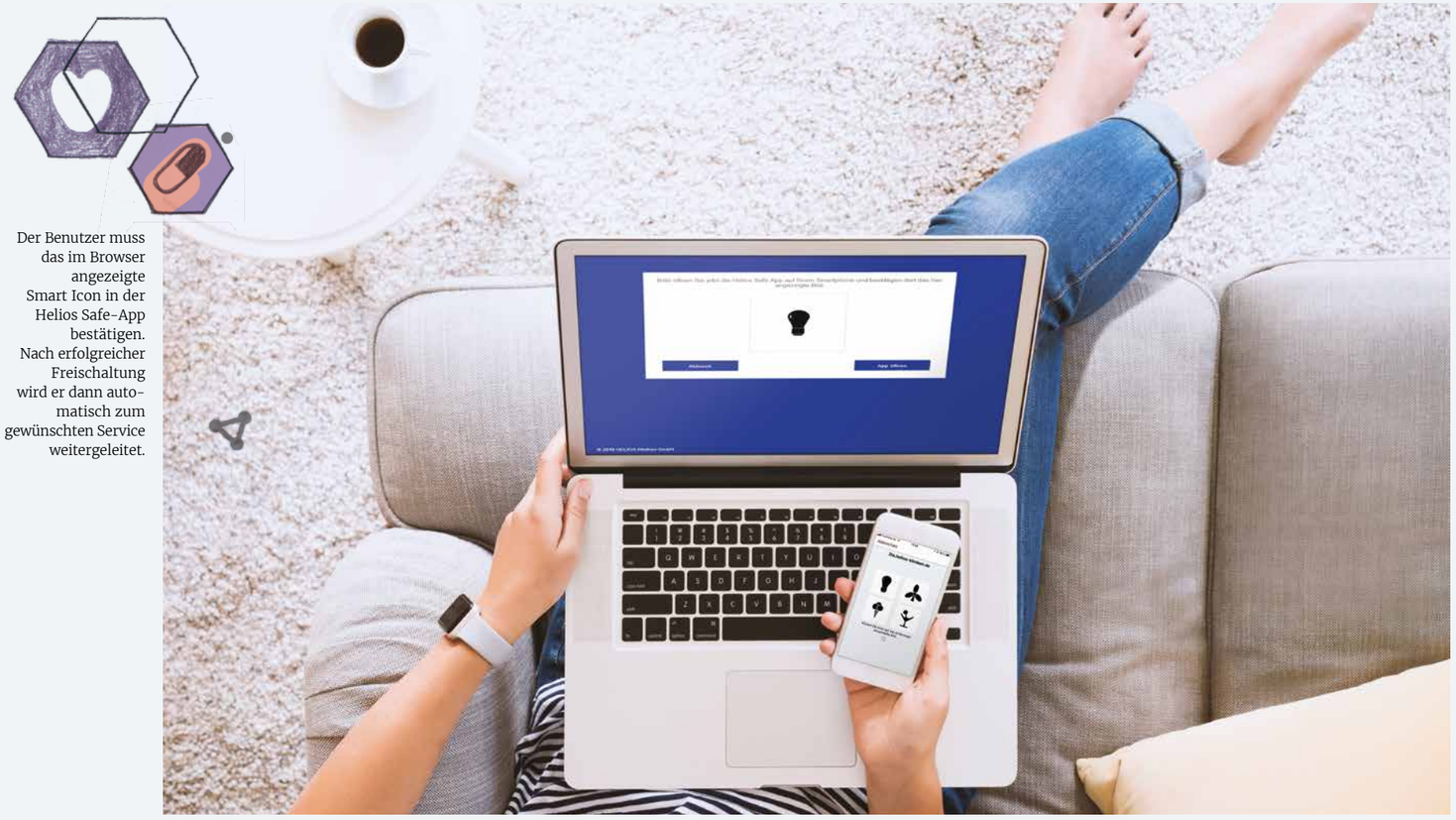
Sämtliche Identity-Management- und Authentifizierungsverfahren (inclusive PIN-Service) der Helios.bridge nutzen das Modul Patient Onboarding, das eine webbasierte grafische Benutzeroberfläche zur Verfügung stellt. Die Authentifizierung erfolgt hier über das OAuth2-Verfahren via OpenID Connect. Die Nutzung dieses Verfahrens ist ebenfalls verbindlich für sämtliche Authentifizierungsvorgänge des Patientenportals hello und die Berechtigungssteuerung von weiteren mobilen Apps.

Accountmanagement, Berechtigungssteuerung & Consent

Größten Wert legt Helios auf das Primat der informationellen Selbstbestimmung der Benutzer/Patienten. Selbstverständlich ist daher die Nutzung der Helios.bridge grundsätzlich freiwillig und hat keinerlei Auswirkungen auf den eigentlichen Behandlungsprozess.

Die Steuerung des Umfangs der an die Helios.cloud kommunizierten und von dieser Cloud konsumierten Daten liegt einzig beim Benutzer, dem über das Accountmanagement Werkzeuge zur feingranularen Steuerung von Einwilligungen (Consent) und Berechtigungen zur Verfügung stehen. So steht es ihm frei, für jede einzelne Institution eine Freischaltung durchzuführen, oder dies eben nicht zu tun. Besteht eine Freischaltung, so kann die Datenübertragung jederzeit beendet oder unterbrochen und wieder aufgenommen werden. Weiterhin können durch den Benutzer einzelne Daten und Dokumente, alle Daten einer Institution oder alle in der Helios.cloud gespeicherten Informationen gelöscht werden. Im Hinblick auf Zugriff und Zulieferung von Daten durch externe Dritte steht dem Benutzer eine Berechtigungssteuerung zur Verfügung, die es ihm erlaubt, fein granular festzulegen, wer welche Daten des Benutzers lesen und liefern darf.

Dritte in diesem Sinne sind zum einen (mobile) Apps, die mit der Helios.bridge Daten bidirektional austauschen wollen; zum anderen sind dies weitere Personen (vornehmlich Ärzte als Zuweiser, Hausärzte, Vor-, Mit- und Nachbehandler), welche im Provider Directory vorgehalten werden. In beiden Fällen muss eine explizite Berechtigung durch den Benutzer erfolgen. Schließlich kann die Gesamtlöschung des Benutzeraccounts (einschließlich aller Daten) direkt vom Benutzer vorgenommen werden.



Der Benutzer muss das im Browser angezeigte Smart Icon in der Helios Safe-App bestätigen. Nach erfolgreicher Freischaltung wird er dann automatisch zum gewünschten Service weitergeleitet.

AUTOR: Nils Alwardt

FUNKTION: Leiter klinische Anwendungen

EINRICHTUNG: HELIOS Kliniken GmbH

AUTOR: Andreas Hempel

FUNKTION: Leiter Entwicklung & eHealth

EINRICHTUNG: HELIOS Kliniken GmbH

AUF EINEN BLICK

Unternehmen:	**HELIOS KLINIKEN GMBH**
Art des Unternehmens:	**Europas führender privater Krankenhausbetreiber.**
Jährliche Patientenzahl:	**rund 15 Mio.**
Sitz des Unternehmens:	**Berlin**
Mitarbeiter:	**› 100.000**
Website:	***→ www.helios-gesundheit.de***