Einwilligungsmanagement in IHE-basierten Systemarchitekturen für Versorgungs- und Forschungsszenarien

Oliver Heinze

TMF-Workshop
Berlin, 02.07.2014

Universitätsklinikum Heidelberg – Zentrum für Informations- und Medizintechnik

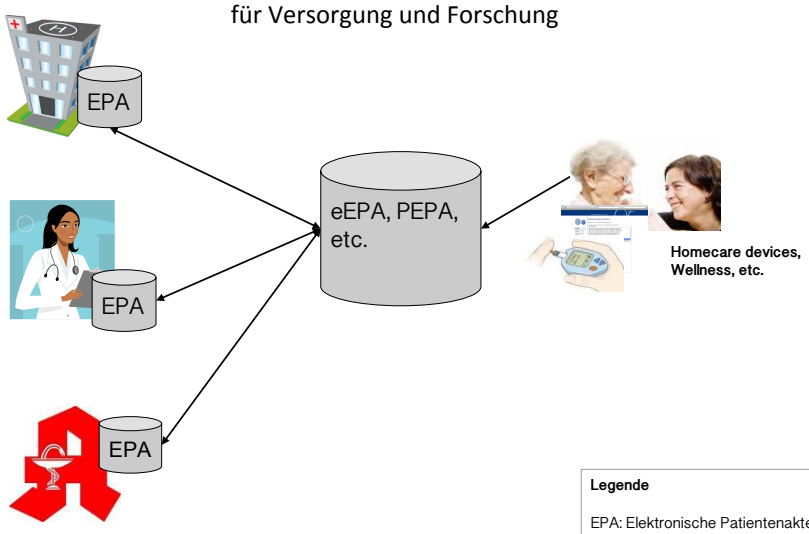
Agenda

- Hintergrund
- Einwilligungsmanagement
- Werkzeuge
- Umsetzungsaspekte
- Diskussion

HINTERGRUND

Einrichtungsübergreifender Austausch von Gesundheitsdaten

für Versorgung und Forschung

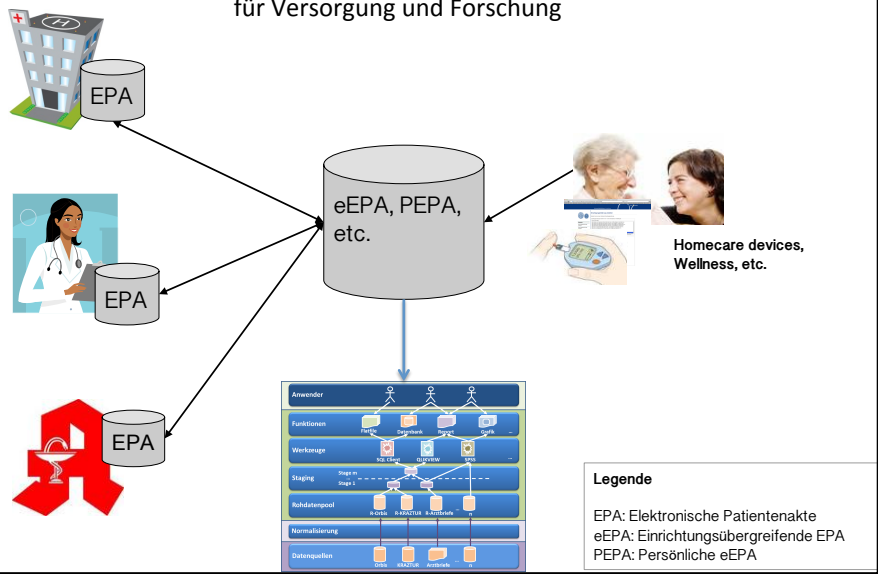


Legende

EPA: Elektronische Patientenakte
eEPA: Einrichtungsübergreifende EPA
PEPA: Persönliche eEPA

Einrichtungsübergreifender Austausch von Gesundheitsdaten

für Versorgung und Forschung



Zweck des Datenschutzes

- „Den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird“ (BDSG, 2009, §1)
- Wahrung des Rechts auf informationelle Selbstbestimmung als Ausprägung des allgemeinen Persönlichkeitsrechts (BVerfG, 1983)

Ärztliche Pflichten

- Ärztliche Schweigepflicht (StGB §203, MBO-Ä §9)
  - Jegliche Informationen über den Tod hinaus
  - Ausnahme: Entbindung von der Schweigepflicht
    - Durch gesetzliche Regelungen
    - Durch Einwilligung des Patienten
- Dokumentationspflicht der ärztlichen Tätigkeit (BGB §§630a ff., MBO-Ä §10)

Rechte und Pflichten des Bürgers/ Patienten

- Freie Entscheidung über Einwilligung: Verweigerungsrecht (BDSG, 2009 §4a)

- Entbindung der Ärzte von ihrer Schweigepflicht mittels Einwilligung
- Entscheidung über den Grad der Entbindung
  - Welche Ärzte?
  - Wie lange?
  - Welche Inhalte?
- Auskunftsrecht (BDSG, 2009, §§ 19, 34)
- Widerspruchsrecht (BDSG, 2009, §§ 20, 35)
- Recht auf Berichtigung
- Recht auf Sperren/Löschen
- Recht auf Schadenersatz

Organisatorische und technische Pflichten für Betreiber von Informationssystemen

- Aufklärung über Umfang, Erhebungszweck und Verwendung der Daten
- **Einholung des Auftrags und der Einwilligung** (informed consent)
- Bereitstellung von Maßnahmen für den Nutzer ..
  - zum **Einwilligungsmanagement**
  - zum **Widerrufsmanagement** (zur Nutzungsbeendigung)
  - zur Auskunft über gespeicherte Daten
- Umsetzung der technischen und organisatorischen Maßnahmen nach §9 BDSG

ELEKTRONISCHES EINWILLIGUNGSMANAGEMENT

Anforderungen

- Einhaltung deutscher Datenschutzregelungen (Opt-in-Prinzip)
- Standard-basiert
- Feingranulare Abstufung der Einwilligung
- Dynamische Steuerung der Einwilligung
- Strukturierte Repräsentation der Einwilligung
- Berechtigungskonzept eines Aktensystems basiert auf der Einwilligung

Neues Paradigma

Attributbasierte Zugriffsverwaltung (dynamisch)

vs.

Rollenbasierte Zugriffsverwaltung (statisch)

Akteure und Anwendungsfälle

- Akteure
  - Bürger/Patienten, ihre Vertreter
  - Gesundheitsdiensteanbieter (Ärzte, Pflegekräfte, Aufnahmepersonal)
- Anwendungsfälle
  - Einwilligung erfassen / ändern (inkl. widerrufen)
  - Zugriffsberechtigungen entsprechend der Einwilligung prüfen und durchsetzen

Abhängigkeiten / Voraussetzungen

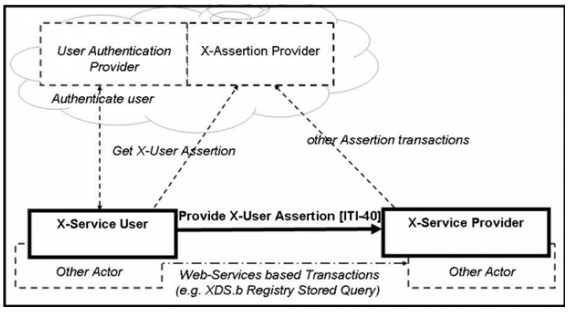
- Authentifizierte Systembenutzer
- Identifikation (inkl. Metadaten) der
  - Patienten (MPI)
  - Gesundheitsdiensteanbieter und Organisationen (Provider Directory)
  - Inhaltsobjekte (Dokumente) der Akte
- Verknüpfung bzw. Auflösung des Pseudonyms zu IDAT im Forschungskontext (broad vs. specific consent)

WERKZEUGE

Anwendungsfall	IHE-Profil
Authentifizierte Systembenutzer	XUA
Identifikation und Metadaten Patienten	PIX/PDQ
Identifikation und Metadaten Gesundheitsdiensteanbieter und Organisationen	HPD
Identifikation und Metadaten der Inhaltsobjekte der Akte	XDS.b
Einwilligung erfassen	**BPPC, Nationale Erweiterungen IHE-D**
Einwilligung prüfen und durchsetzen	**BPPC, Nationale Erweiterungen IHE-D**

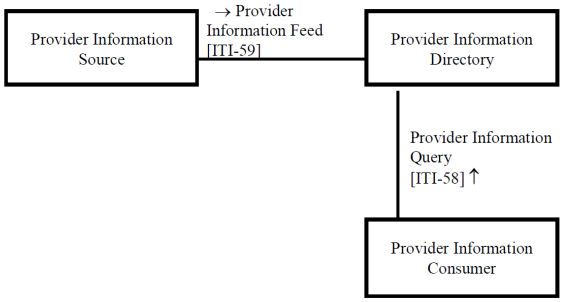
Cross Enterprise User Assertion (XUA)

- Bestätigung der Identität eines authentifizierten Benutzers zur systemübergreifenden Autentifizierung und Autorisierung (SSO)
- Übertragen der Benutzeridentität via SOAP (zusätzlich zur System Authentifizierung)
- Zusätzliche Übertragung von Benutzerattributen
- Basis: SAML 2.0 Identity Assertions



Healthcare Provider Directory (HPD)

- Speichern und Abfrage von Leistungserbringerdaten
- Datenstruktur basiert auf LDAP
- Schnittstellen nutzen kein LDAPv3 sondern DSML („LDAP via SOAP“) Protokoll
- Basis: LDAP



Basic Patient Privacy Consent (BPPC)

- Statische, durch die AD vorgegebene Zugriffsregeln
- Regeln haben eine ID, einen Text, einen Patientenbezug und eine Gültigkeit
- Regeln werden in einem HL7 CDA Dokument gespeichert
- Regeln werden von Document Consumer und der Source durchgesetzt
- Keine dynamischen Regeln
- Keine Berücksichtigung von nicht-XDS-Transaktionen

Organization for the Advancement of Structured Information Standards (OASIS)

XML-basierte, offene Standards

- XACML (eXtensible Access Control Markup Language)
- SAML (Security Assertion Markup Language)

SAML

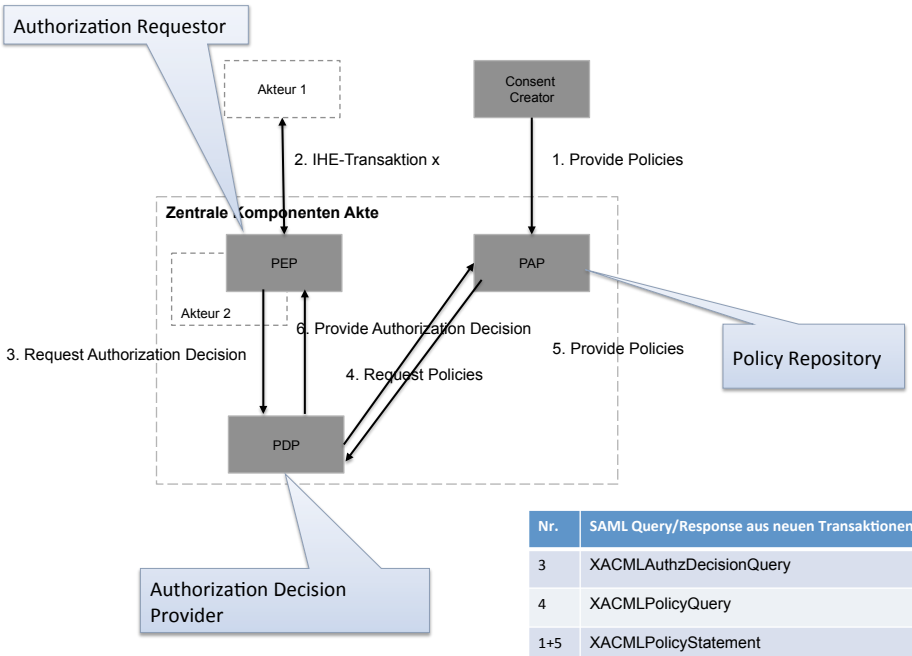
- Austausch von Sicherheitsinformationen
  - Web Single Sign-On
  - Identity Federation
- Assertions (Sicherheitsbehauptungen) in Form von Statements:
  - Authentication
  - Attribute
  - Authorization Decision
- Protokolle für Anfragen und Antworten
- Bindungs: HTTP oder SOAP
- Profile: z.B. XACML Attribute Profile

XACML

- Model für Attribut- und Regel-basierte Zugriffssteuerung
- Sprache für die Definition von Zugriffsregeln (Policy-Sets, Policies, Rules)
- Algorithmen für das Herbeiführen von Entscheidungen bei Zugriffsversuchen
- Trennung von Zugriffsentscheidung und „Point of Use“
- Rollen:
  - PEP: Policy Enforcement Point
  - PDP: Policy Decision Point
  - PAP: Policy Administration Point

Neue Akteure und Transaktionen als nationale Erweiterung im IHE-D Cookbook

- Akteure
  - PEP: Authorization Requestor
  - PDP: Authorization Decision Provider
  - PAP: Policy Repository
  - Advanced Consent Creator: Erstellt Einwilligungsdokumente auf Basis von XACML
- Transaktionen
  - Request Authorization Query
  - Provide Authorization Decision
  - Request Policies
  - Provide Policies



Nr.	SAML Query/Response aus neuen Transaktionen
3	XACMLAuthzDecisionQuery
4	XACMLPolicyQuery
1+5	XACMLPolicyStatement
6	XACMLAuthzDecisionStatement

Zentrale Frage für die Erstellung von Regeln

- WER ist berechtigt,
- welche OPERATION auf
- welche IINFORMATIONSOBJEKTE auszuführen
- in welcher ZEIT und
- für welchen ZWECK?

Quelle: Heinze, O. ; Bergh, B.: A model for consent-based privilege management in personal electronic health records. In: MIE 2014 Proceedings (Zur Publikation angenommen), 2014

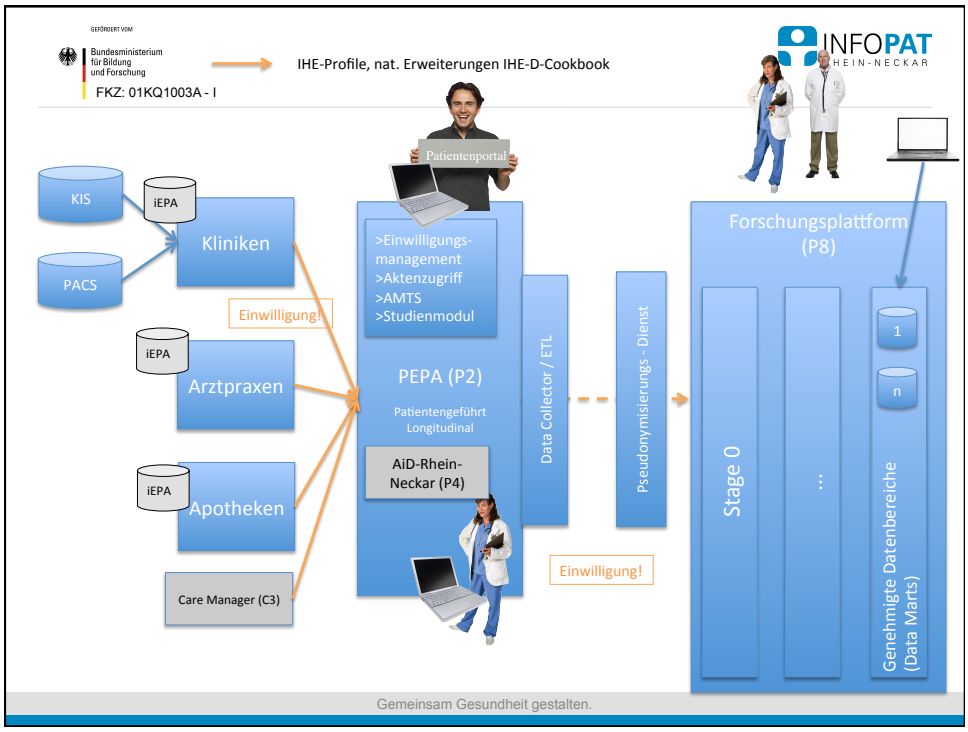
Datenmodell für ein einwilligungsbasiertes Berechtigungskonzept

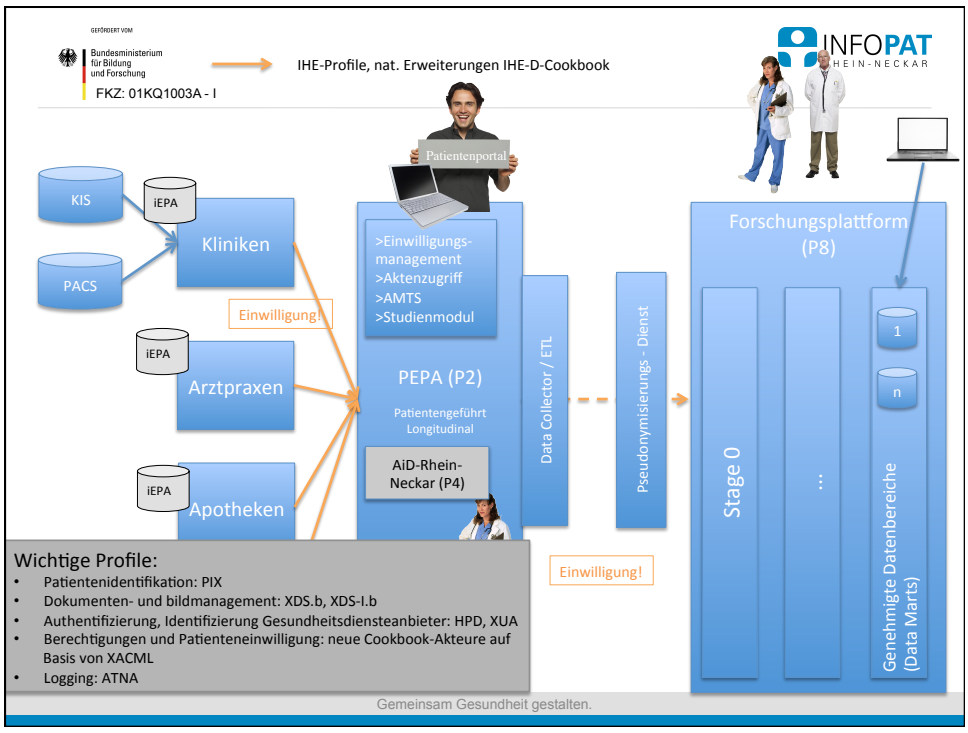
- Ab Veröffentlichung im September 2014 auf Anfrage
- Heinze, O. ; Bergh, B.: A model for consent-based privilege management in personal electronic health records. In: MIE 2014 Proceedings (Zur Publikation angenommen),2014

authorInstitution	languageCode
authorPerson	legalAuthenticator
authorRole	limitedMetadata
authorSpecialty	mimeType
authorTelecommunication	**patientId**
availabilityStatus	practiceSettingCode
classCode	repositoryUniqueId
comments	serviceStartTime
confidentialityCode	serviceStopTime
creationTime	size
entryUUID	sourcePatientId
eventCodeList	sourcePatientInfo
formatCode	title
hash	**typeCode**
healthcareFacilityTypeCode	uniqueId
homeCommunityId	URI

INFOPAT

INFORMATIONSTECHNOLOGIE FÜR EINE PATIENTENORIENTIERTE GESUNDHEITSVERSORGUNG

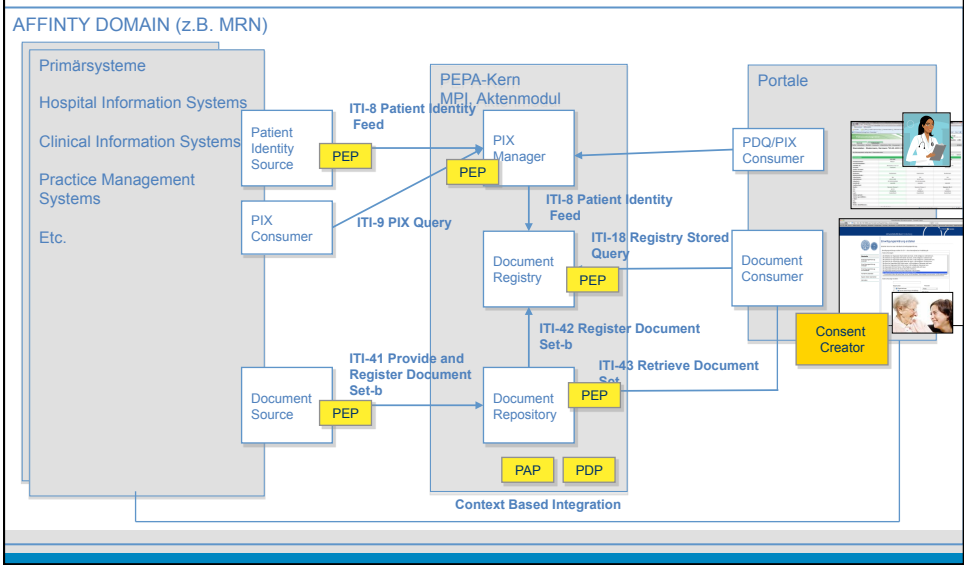

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung
FKZ: 01KQ1003A - I
IHE-Profile, nat. Erweiterungen IHE-D-Cookbook
INFOPAT
RHEIN-NECKAR
Patientenportal
KIS
PACS
iEPA
Kliniken
Einwilligung!
iEPA
Arztpraxen
iEPA
Apotheken
Care Manager (C3)
>Einwilligungs-management
>Aktenzugriff
>AMTS
>Studienmodul
PEPA (P2)
Patientengeführt
Longitudinal
AiD-Rhein-Neckar (P4)
Data Collector / ETL
Pseudonymisierungs - Dienst
Einwilligung!
Forschungsplattform (P8)
Stage 0
...
1
n
Genehmigte Datenbereiche (Data Marts)
Gemeinsam Gesundheit gestalten.


GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung
FKZ: 01KQ1003A - I
IHE-Profile, nat. Erweiterungen IHE-D-Cookbook
INFOPAT
RHEIN-NECKAR
Patientenportal
KIS
PACS
iEPA
Kliniken
Einwilligung!
iEPA
Arztpraxen
iEPA
Apotheken
>Einwilligungs-management
>Aktenzugriff
>AMTS
>Studienmodul
PEPA (P2)
Patientengeführt
Longitudinal
AiD-Rhein-Neckar (P4)
Data Collector / ETL
Pseudonymisierungs - Dienst
Einwilligung!
Forschungsplattform (P8)
Stage 0
...
1
n
Genehmigte Datenbereiche (Data Marts)
Wichtige Profile:
• Patientenidentifikation: PIX
• Dokumenten- und bildmanagement: XDS.b, XDS-I.b
• Authentifizierung, Identifizierung Gesundheitsdiensteanbieter: HPD, XUA
• Berechtigungen und Patienteneinwilligung: neue Cookbook-Akteure auf Basis von XACML
• Logging: ATNA
Gemeinsam Gesundheit gestalten.

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung
FKZ: 01KQ1003A - I

INFOPAT RHEIN-NECKAR

PEPA: IHE-Akteure und Transaktionen (Auswahl)



Umsetzungsaspekte

- Abzusichernde Transaktionen
  - Zentral: Anfragen
  - Dezentral und Zentral: Datenübermittlung
- Abstimmung in Affinity Domain
  - Codesysteme
  - Granularität des Modells
  - Ggf. Parsing-Algorithmus für die XACML-Regeln
- Container für Regeln
  - Reines XACML vs.
  - XACML im CDA

DISKUSSION

Diskussion

- Vorteile
  - Übertragbar auf weitere IHE-Profile durch Gruppierung der Akteure
  - Flexibel: Nicht alle Teile des Models müssen umgesetzt werden (Affinity-Domain-Entscheidung über Granularität)
  - Erweiterbar: Einbindung weiterer Regel-Domänen (z.B. Organisationen, ADs)
  - Anpassbar an beliebige regionale und überregionale Settings
- Nachteile
  - Komplexität
  - Bestehende Akteure (z.B. Document Sources müssen erweitert bzw. gruppiert werden mit neuen Consent-Akteuren
- Forschungsszenario
  - Erweiterung erforderlich
  - Befindet sich in Konzeption (Projekt INFOPAT)
- Praktikabilität wird sich in INFOPAT zeigen
  - Implementierung
  - Anwendung: Erfolgsfaktor Usability des Consent Creators

Vielen Dank! Fragen?

Kontakt:

Universitätsklinikum Heidelberg
Zentrum für Informations- und Medizintechnik

Oliver Heinze

oliver.heinze@med.uni-heidelberg.de

+49 6221 56 37572