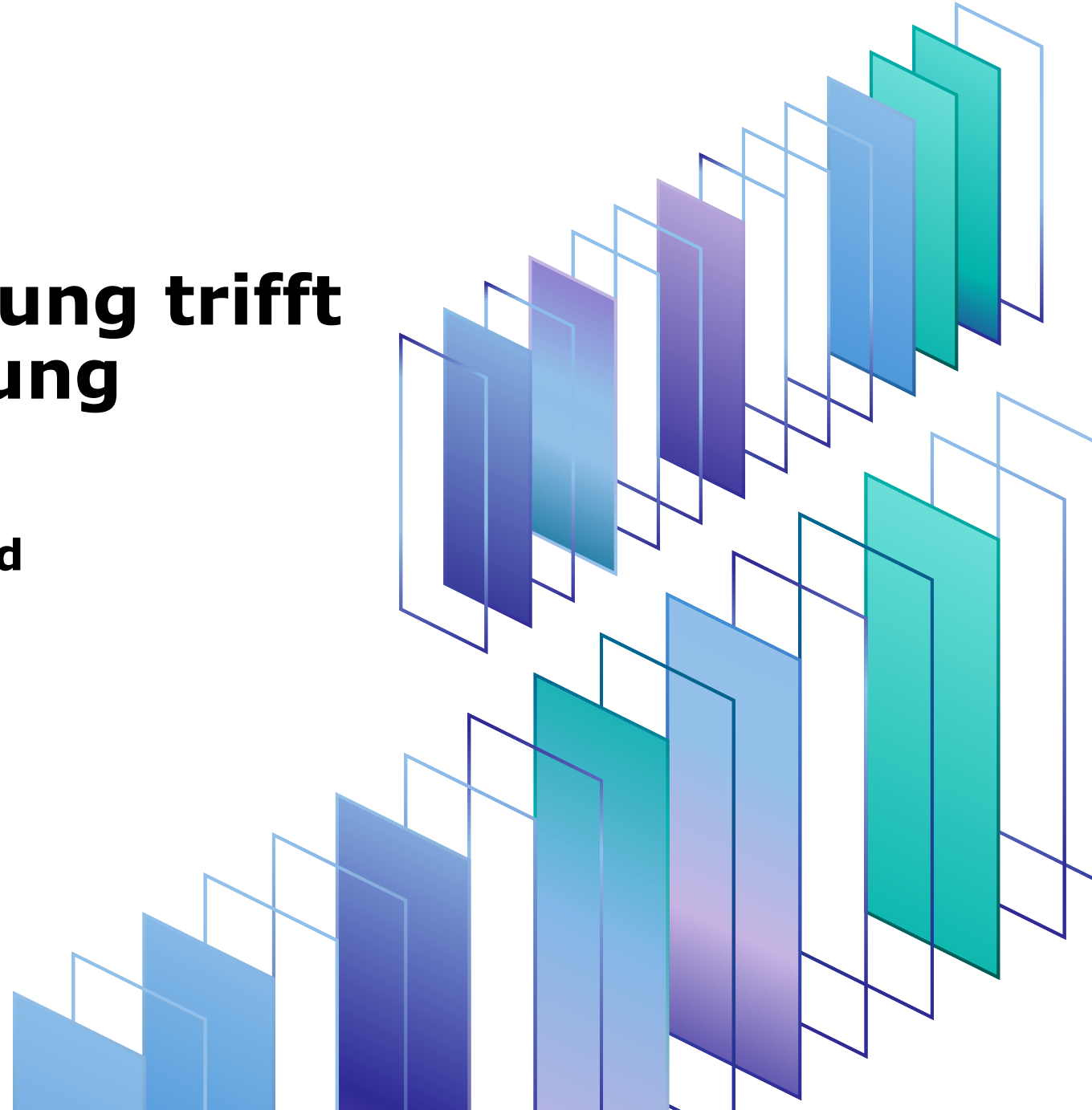


Transparente Einwilligung trifft sichere Zugriffssteuerung

**Ein Praxisansatz mit
HealthShare Unified Care Record und
Personal Community**

Nils Dittberner, Michael Brösdorf





Agenda

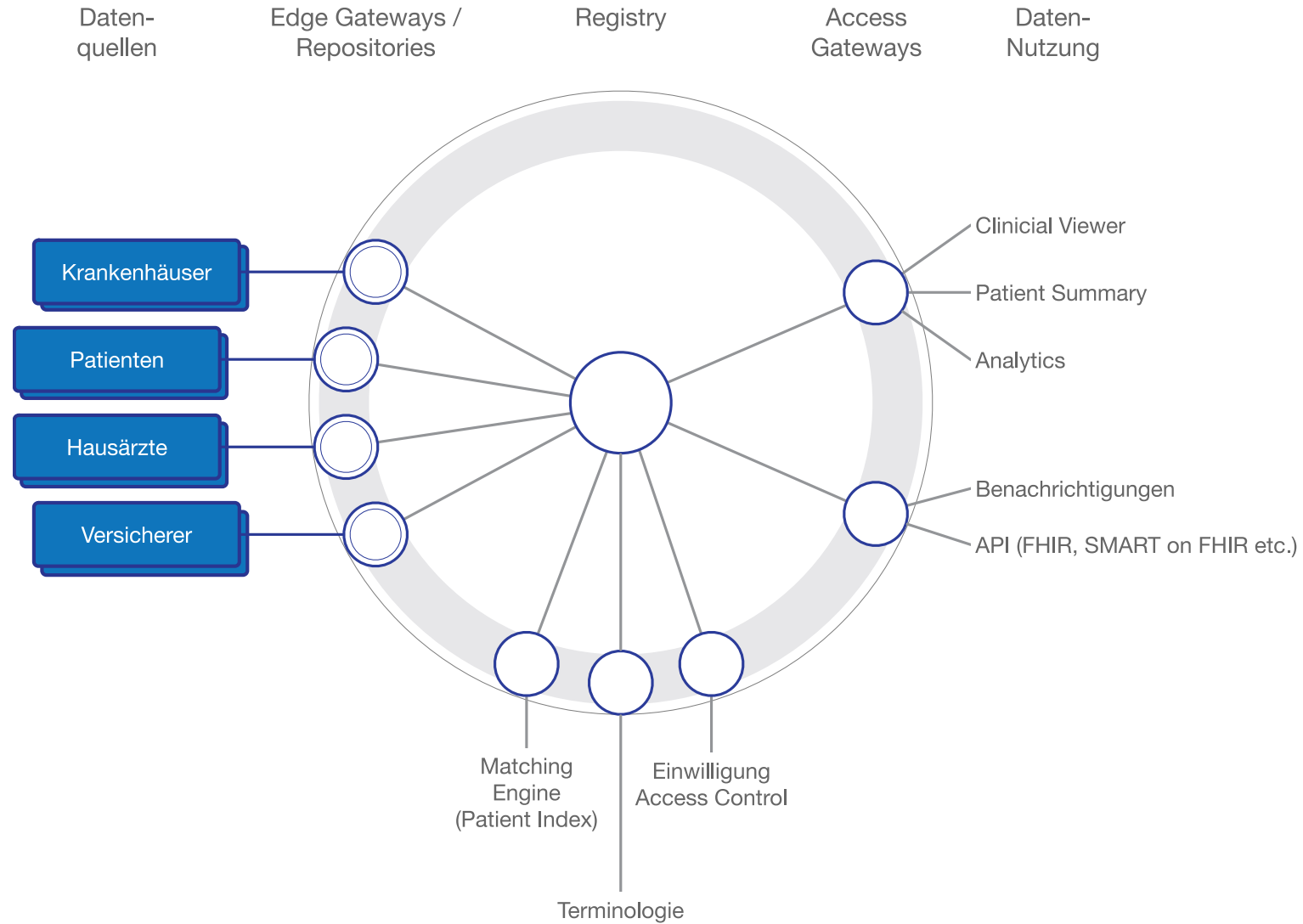


-
- 01 Digital Backbone – aber sicher
 - 02 Konzept: Dynamische Autorisierung
 - 03 Demo
 - 04 Vom Konzept zum Mehrwert
 - 05 Diskussion
-

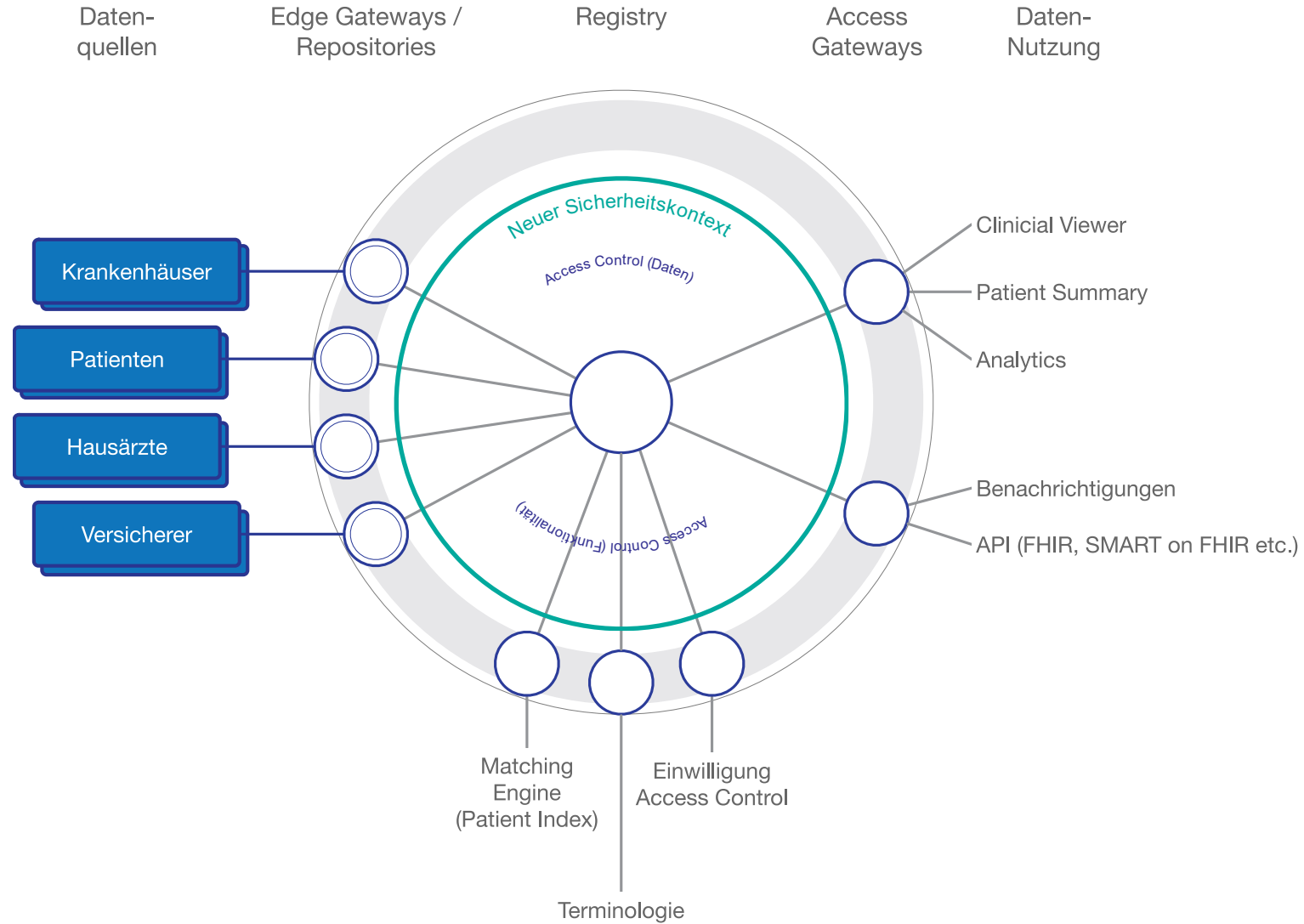


Das digitale Gesundheitswesen gestalten – mit einem Digital Backbone von InterSystems

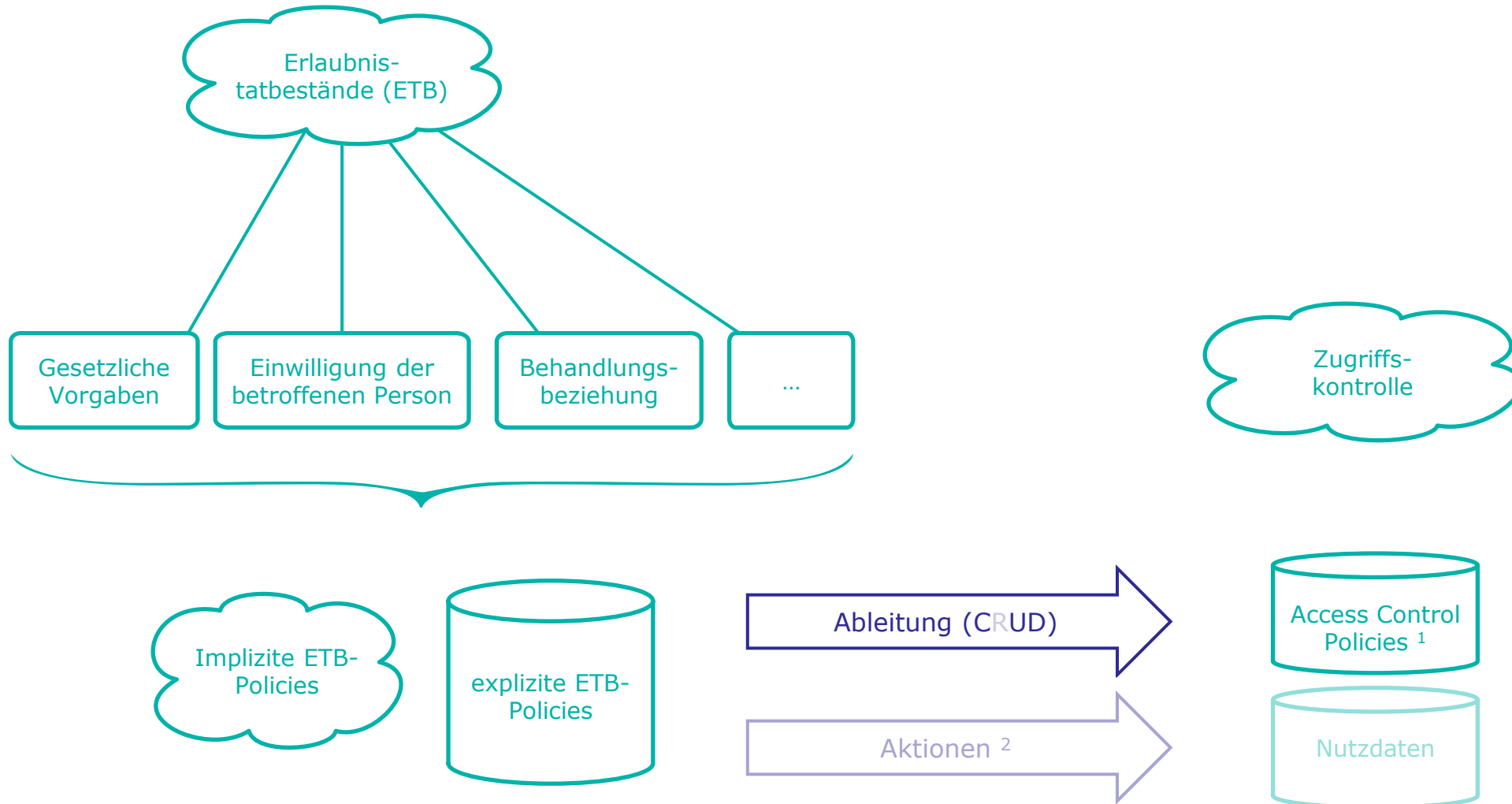
Digital Backbone – aber sicher!



Digital Backbone – Aber sicher!



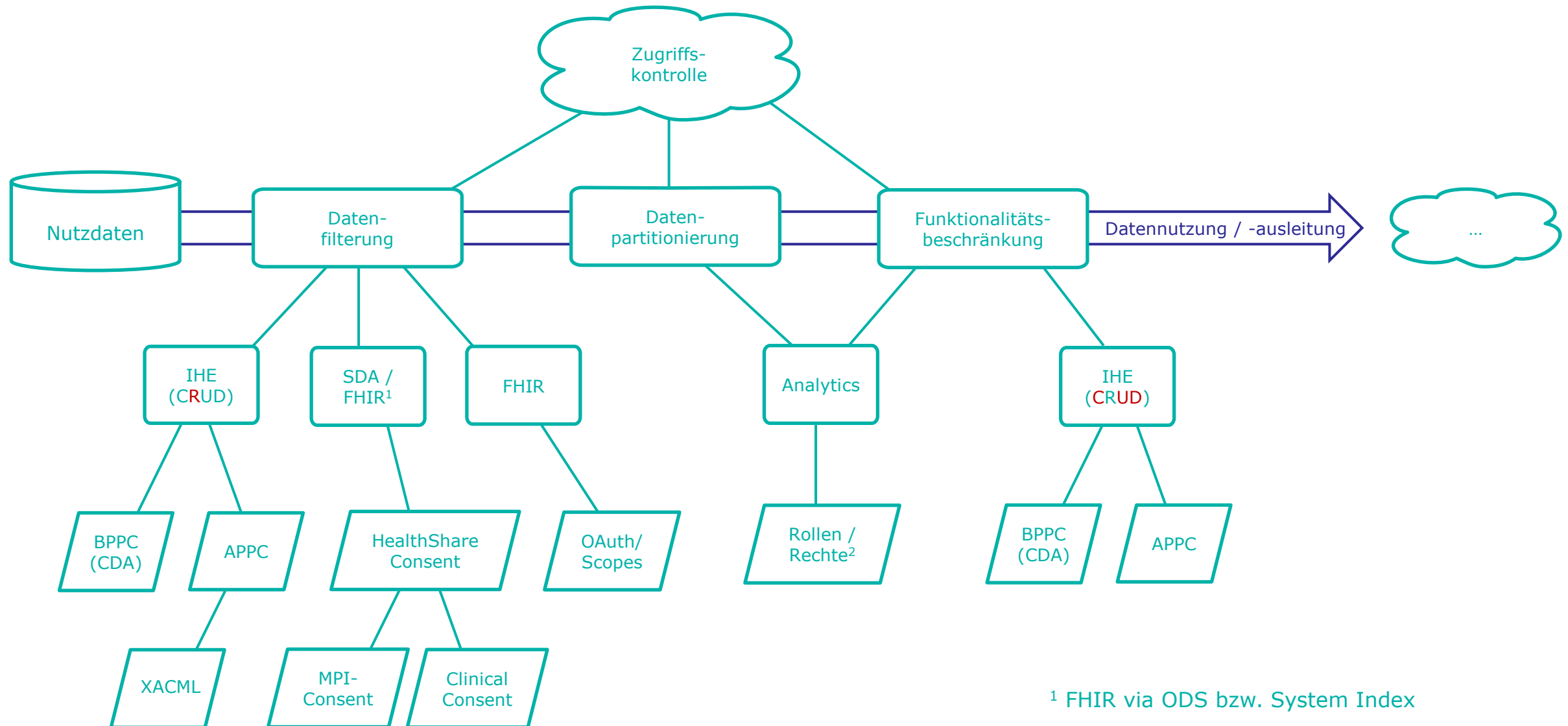
Erlaubnistatbestände und Zugriffskontrolle für Nutzdaten



¹ RBAC, ABAC etc.

² z.B. Löschung von Nutzdaten

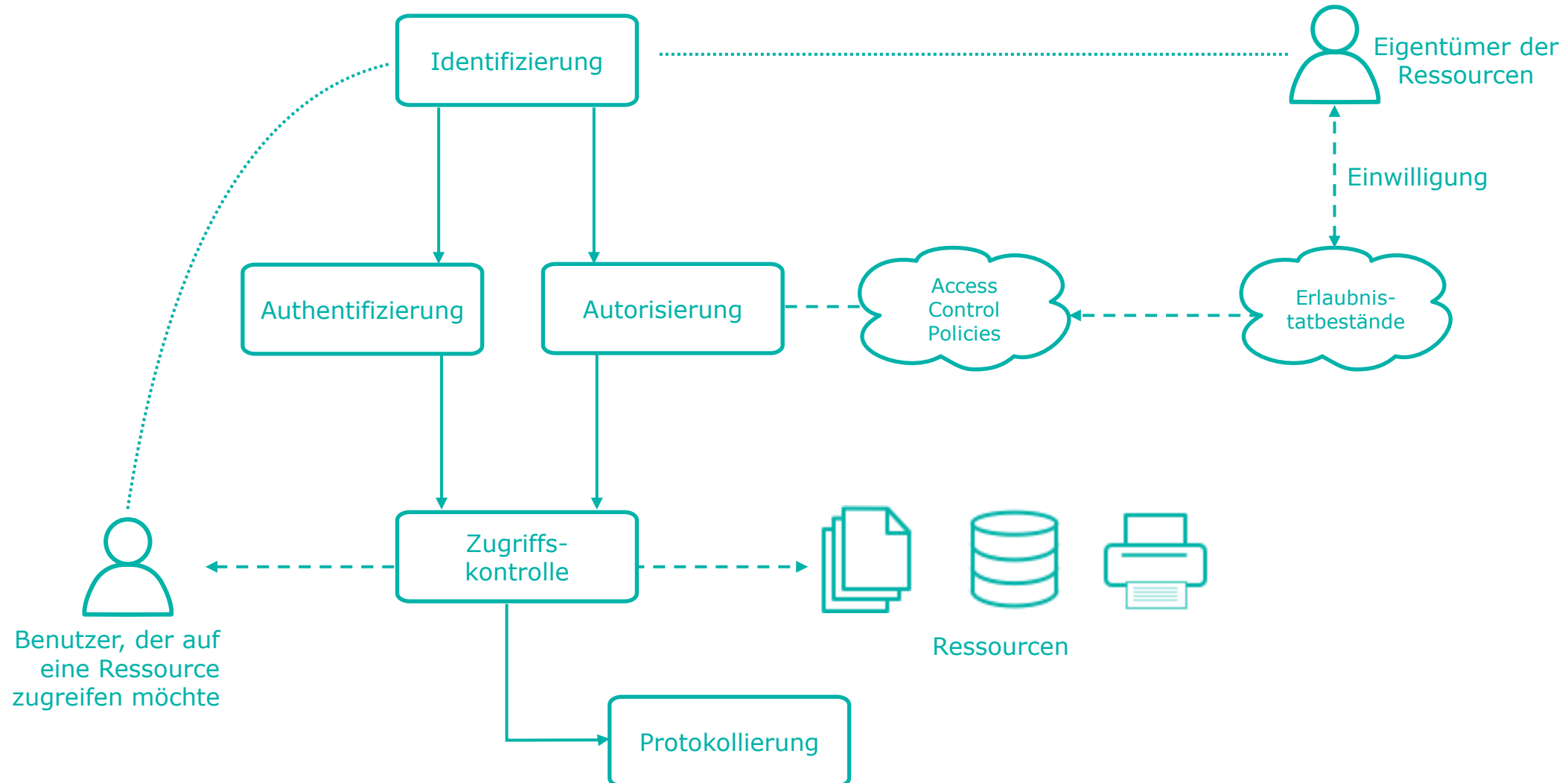
Erlaubnistatbestände und Zugriffskontrolle für Nutzdaten



¹ FHIR via ODS bzw. System Index

² z.B. auf Health Insight Subject Areas / Cubes

Einwilligung und Zugriffskontrolle



Einwilligungen in HealthShare



- Datengetriebene UI in Personal Community für Einwilligungen
- BPPC (**Dokumentation** und Durchsetzung von Zugriffsrechten)
- Anbindung von dedizierten Tools für Einwilligungen via API

Zugriffskontrolle (für Nutzdaten) in HealthShare



Unified Care Record:

- BPPC (Dokumentation und **Durchsetzung** von Zugriffsrechten)
- APPC (Import von MPI-Consent)
- HealthShare Consent Engine für granulare Zugriffssteuerung auf diskrete Daten
 - Patientenstammdaten
 - Klinische Daten
- XACML (Policy Repository, Policy Decision Point, Policy Enforcement Point)

Health Insight:

- Rollen und Rechte



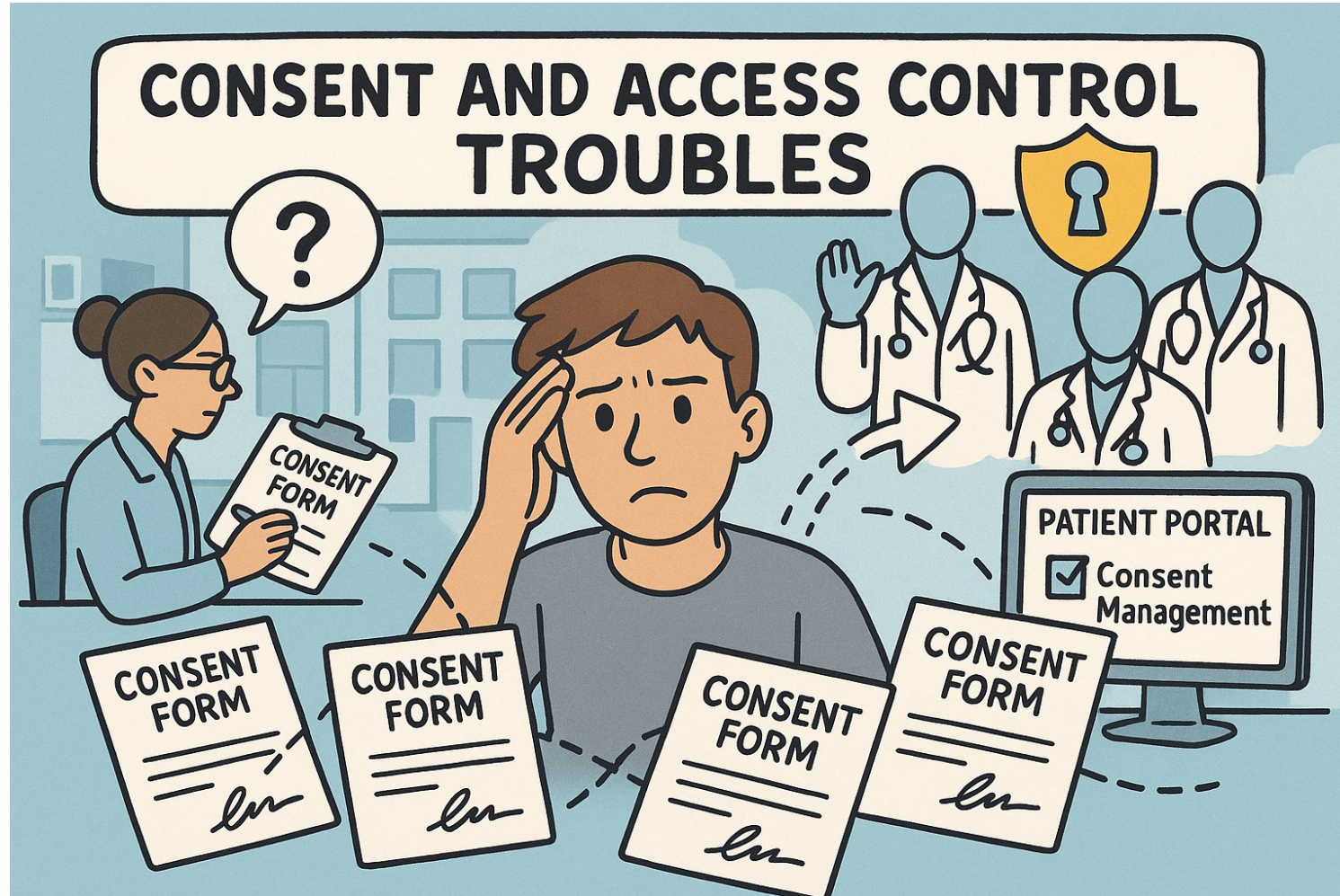
Konzept: Dynamische Autorisierung

Patienteneinwilligung

Praxisansatz Dynamische Autorisierung



Warum ist das wichtig?



Praxisansatz Dynamische Autorisierung



Warum ist das wichtig?

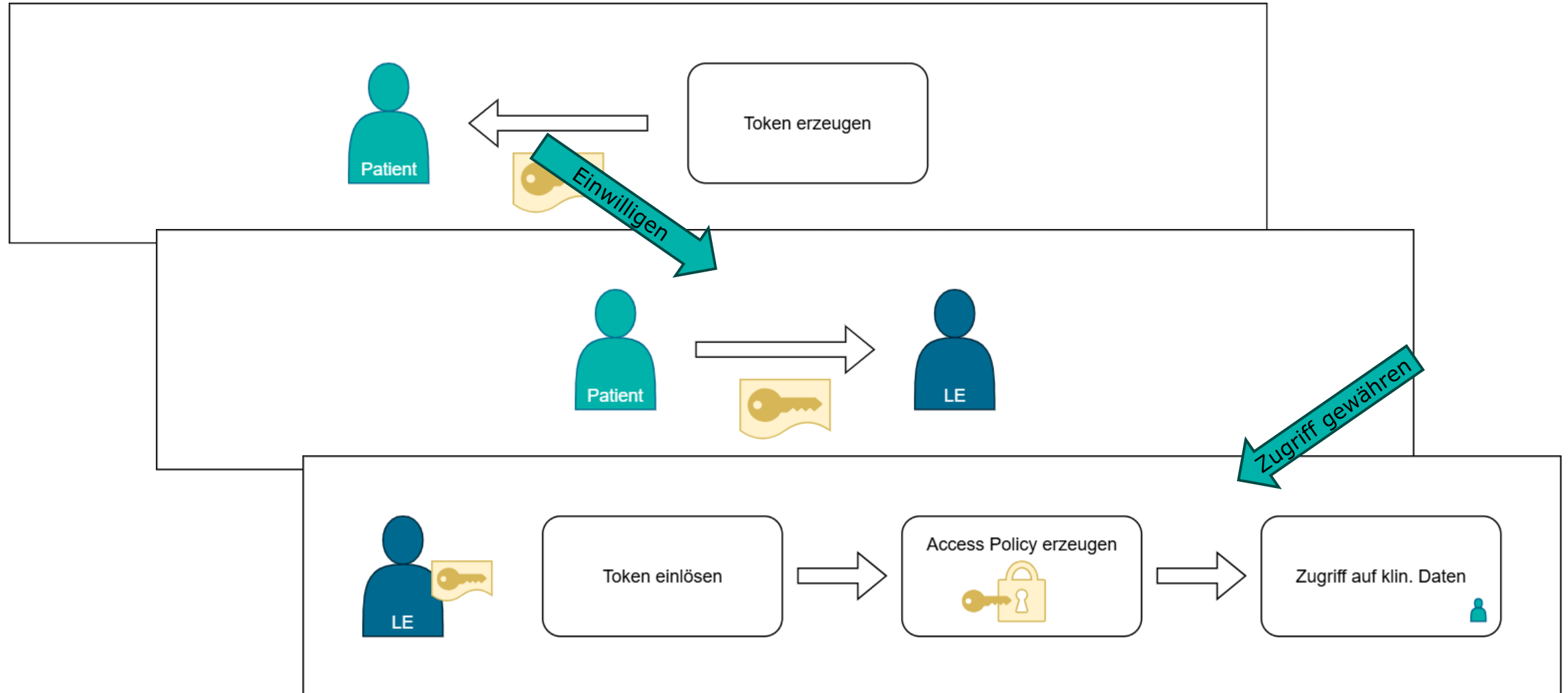


Patient

Praxisansatz Dynamische Autorisierung



Idee und Konzept



Praxisansatz Dynamische Autorisierung



Steuerung der Zugriffskontrolle über Token

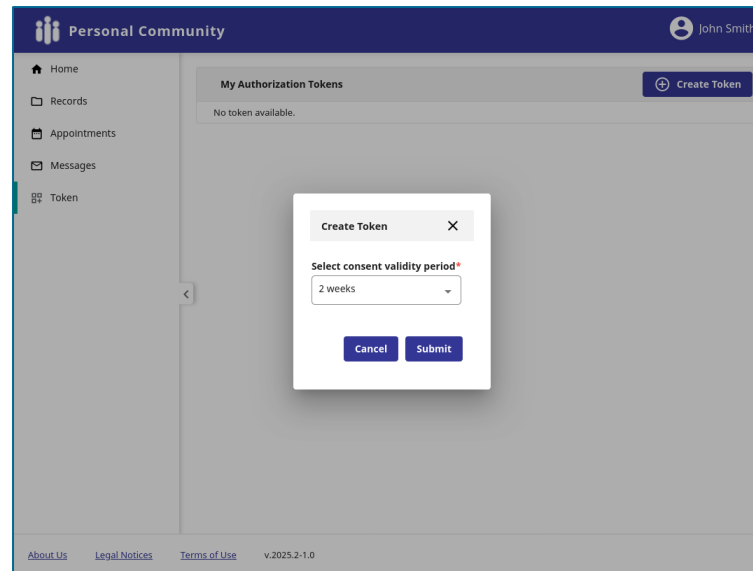
- Projektspezifisches Back-End für die Token-Verwaltung, REST-APIs zum Erzeugen, Einlösen und Löschen von Tokens
- Tokens beinhalten Metadaten wie Zugriffszeitraum, Identität des einlösenden Behandlers, Zeitstempel etc.
- beim Einlösen eines Tokens wird eine zeitlich begrenzte Beziehung zwischen dem einlösenden Behandler und dem Patienten angelegt
- Die angelegten Beziehungen werden von vordefinierten Zugriffsrichtlinien für die Durchsetzung entsprechender Zugriffsrechte genutzt

Praxisansatz Dynamische Autorisierung



Nutzung durch Patienten in Personal Community über eine Custom Application

- Angular MFE (Micro-FrontEnd)
- Patienten können Tokens über eine übersichtliche Benutzerschnittstelle erzeugen, nachverfolgen und widerrufen
- Die Tokenliste zeigt sowohl neue als auch bereits eingelöste Tokens an:



Praxisansatz Dynamische Autorisierung



Nutzung durch Patienten in Personal Community über eine Custom Application

- Datengetriebene Benutzerschnittstelle zeigt aktive Beziehungen
- Patient können Beziehungen über Auswahllisten behalten oder löschen
- Bei der Speicherung der Änderungen werden die Beziehungen in Unified Care Record direkt aktualisiert:

Personal Community John Smith

Account Settings **Consent Management**

On this page, you can view and update your consent preferences.

Current patient-clinician relationships

Your current patient-clinician relationships

Last Updated 06/03/2025
Updated By _Ensemble

ISCDACH.Consent001 - Proxine Jones	Keep
ISCDACH.Consent001 - Nursula Miller	Keep
ISCDACH.Consent001 - Sam Farrell	Keep

[Edit](#)

[About Us](#) [Legal Notices](#) [Terms of Use](#) v.2025.2-1.0

Personal Community John Smith

Account Settings **Consent Management**

On this page, you can view and update your consent preferences.

Current patient-clinician relationships

Your current patient-clinician relationships

ISCDACH.Consent001 - Proxine Jones
Keep

ISCDACH.Consent001 - Nursula Miller
Keep

ISCDACH.Consent001 - Sam Farrell
Revoke

[Cancel](#) [Update](#)

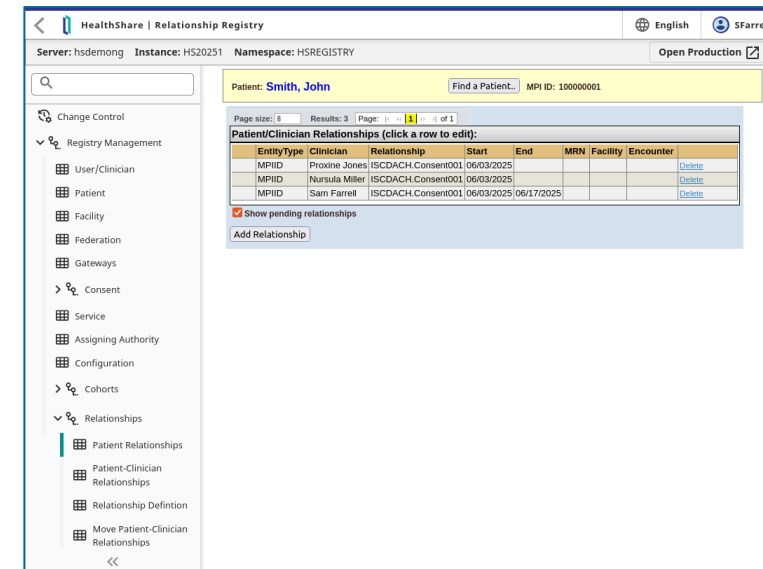
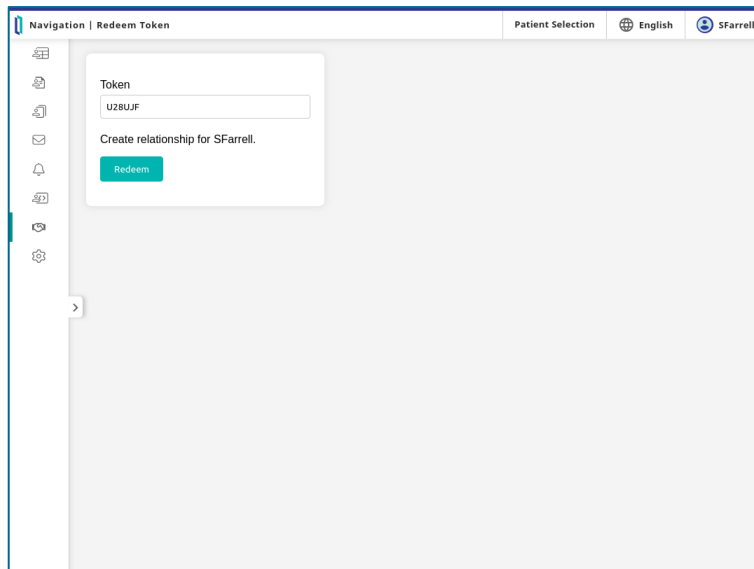
[About Us](#) [Legal Notices](#) [Terms of Use](#) v.2025.2-1.0

Praxisansatz Dynamische Autorisierung



Durchsetzung von Zugriffsrechten in Unified Care Record

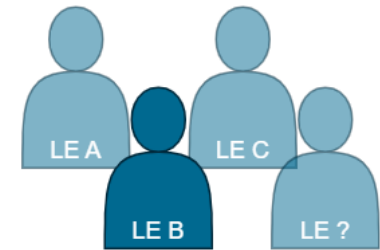
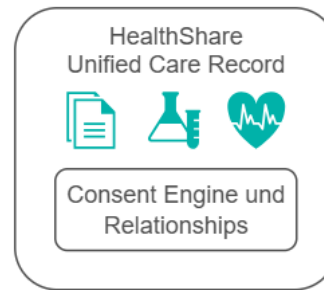
- auf Systemebene wird zunächst jeder Zugriff blockiert („Standardmäßig blockieren“ bzw. „Default block“)
- Richtlinien auf Basis von Beziehungen erlauben den Zugriff für den jeweiligen Behandler
- Der Patient kann damit direkt steuern, wer wann Zugriff auf seine Daten hat



Praxisansatz Dynamische Autorisierung



Lösung





Demo: Dynamische Autorisierung in Aktion



Vom Konzept zum Mehrwert

Vom Konzept zum Mehrwert



- Stärkung der Eigenverantwortung der Patienten
 - Self-Service mit Personal Community
 - Keine Anrufe, kein Papierkram, keine manuellen Prozesse
 - Sekundenschnelles Erteilen und Widerrufen von Einwilligungen und Zugriffsrechten
- Sicherheit
 - Zeitliche Beschränkung der Einlösbarkeit von Tokens, jedes Token kann nur einmal eingelöst werden
 - Opt-In mit expliziter Berechtigung von Behandlern über Beziehungen
 - Protokollierung für umfassende Nachvollziehbarkeit
 - Die Gültigkeit der angelegten Beziehungen kann zeitlich beschränkt werden

Vom Konzept zum Mehrwert



- Flexibilität
 - Der zu berechtigende Behandler muss nicht vorab bekannt sein
 - Berücksichtigt reale Bedingungen und Verfügbarkeiten von Behandlern
- Transparenz
 - Patienten können einsehen, welcher Behandler ein Token wann eingelöst hat und für welchen Zeitraum damit Zugriff erteilt wurde
 - Vertrauen und Einhaltung gesetzlicher Vorgaben
- Berechtigung über Beziehungen
 - Personal Community zeigt die aktiven Beziehungen aus Unified Care Record an
 - Patienten können einem Behandler jederzeit den Zugriff entziehen



Diskussion

Diskussion



- Beispiel für eine Umsetzung von patientengesteuerten Einwilligungen und Zugriffsrechten
- Nutzung vorhandener Funktionen soweit möglich (z.B., HealthShare Consent Engine, Relationship-API)
- Verbesserungspotential
 - Mehr Informationen in den Token
 - Zusätzliche Optionen beim Anlegen/ Entfernen von Einwilligungen/ Zugriffsrechten
 - Erweiterung der UI/UX (z.B. mit QR-Codes)



Vielen Dank