xShare

Expanding the European EHRxF to share and effectively use health data within the EHDS

xShare toolbox for data portability under GDPR

Coordinated by GNOMON

Date: 31.05.2025

Project title:	xShare - Expanding the European EHRxF to share and effectively use health data within the EHDS.
Grant Agreement:	101136734
Call identifier:	HORIZON-HLTH-2023-IND-06-02

This project has received funding from the European Health and Digital Executive Agency (HADEA) under grant agreement no. 101136734.

Working paper description

Number and name of working paper:	xShare toolbox for data portability under GDPR
Publishable summary:	This working paper presents the refined modular architecture and updated xShare toolbox enabling GDPR-aligned health data portability and interoperability under EHDS. It introduces open-source tools such as the CDA2FHIR converter, visualization utilities, and synthetic data support, validated through IHE Plugathon-style testing. This interim version lays the foundation for full interoperability and future certification, while identifying areas, such as consent management, that require further development.
Status:	Working Paper

Statement of originality

This working paper contains original unpublished work except where clearly indicated otherwise. Acknowledgement of previously published material and of the work of others has been made through appropriate citation, quotation or both.

Disclaimer

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

Table of Contents

List of abbreviations

Please refer to the i~HD Glossary: https://glossary.ramit.be/public/index.cfm

Abbreviation	Term
API	Application Programming Interface
AS	Adoption Sites - xShare Consortium members
ATNA	Audit Trail and Node Authentication (IHE profile)
CDA	Clinical Document Architecture (HL7 standard)
EEHRxF	European Electronic Health Record Exchange Format
EHDS	European Health Data Space
FHIR	Fast Healthcare Interoperability Resources
HL7	Health Level 7
IAM	Identity and Access Management
IHE	Integrating the Healthcare Enterprise
IG	Implementation Guide
IUA	Internet User Authorization (IHE profile)
JSON	JavaScript Object Notation
IPS	International Patient Summary
MHD	Mobile access to Health Documents (IHE profile)
NCPeH	National Contact Point for eHealth
PAP	Policy Administration Point
PDP	Policy Decision Point
PEP	Policy Enforcement Point
SHL(s)	Smart Health Links
SYNDERAI	Synthetic Data: Examples - Realistic - using AI
vi7eti	Visualize HL7 Example and Test Instances
XDS.b	Cross-Enterprise Document Sharing (IHE profile)
XSLT	Extensible Stylesheet Language Transformations
CTS	Central Terminology Server
MVC	Master Value Catalogue
CNIL	Commission Nationale de l'Informatique et des Libertés (French DPA)
PIA	Privacy Impact Assessment

Abbreviation	Term
DPIA	Data Protection Impact Assessment
JWT	JSON Web Token
OpenNCP	Open National Contact Point

List of Tables

List of figures

Executive summary

This Working paper presents the refined architecture and updated toolbox for the xShare Yellow Button, supporting secure and GDPR-compliant health data portability aligned with the European Health Data Space (EHDS)[1] and the European Electronic Health Record Exchange Format (EEHRxF). Building upon the foundations set in D3.3, this working paper introduces a modular, patient-centric architecture that integrates identity, consent, and data transformation services through standardized APIs and services. Moreover, it extends the existing toolbox with new open-source tools and outlines plans for upcoming developments. Crucially, also introduces the Yellow Button test bench designed for the IHE Connectathon 2025, enabling Adoption Sites and developers to validate their implementations against EEHRxF specifications and real-world scenarios. The xShare reference implementation presented here aims to accelerate trustworthy, interoperable, and citizen-empowering health data exchange across Europe.

[1] Data portability in xShare is grounded in Article 20 of the GDPR and Article 7 of the EHDS Regulation (EU) 2025/327, which establish the right of individuals to access and transmit their personal health data in structured, interoperable formats—immediately, free of charge, and without hindrance. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ%3AL_202500327

1. Introduction

This working paper focuses on the xSHARE toolbox for data transformation and data donation, by presenting the refined architecture, updated toolbox components, and reference implementations that support citizen access, data transformation, and sharing of personal health data in the European Electronic Health Record Exchange Format (EEHRxF). It builds directly on previous work and reflects further consolidation of toolbox functionalities into a modular, standards-aligned, and testable implementation.

The paper captures the progress toward that objective, enabling citizen access, data transformation, and sharing of personal health data in the EEHRxF, by describing the components that have been developed, tested, and made available as open tools, and highlighting the elements still in development. This version responds to the evolving technical landscape and stakeholder needs by:

- Introducing a modular architecture structured around key dimensions: security, privacy, consent, and interoperability layers.
- Updating and expanding the xShare Toolbox to include newly developed, existing, and forthcoming open-source tools.
- Presenting the Yellow Button reference implementation design and testing framework;
- Introducing the IHE-Europe Connectathon 2025 test bench to validate interoperability, trust, and compliance for Adoption Sites (AS).

The paper provides a blueprint for AS, industry stakeholders, and developers seeking to implement EEHRxF-compliant services, fostering convergence across Member States and contributing to the sustainability of a citizen-centred EHDS.

2. Refined Architecture

Since the publication of D3.3, the architecture of the xShare Yellow Button has undergone a significant refinement process, driven by feedback from AS and outcomes of technical workshops. Given the varying levels of infrastructure maturity across AS, the architecture was modularized to allow phased adoption and independent testing. Each component now supports alignment with EEHRxF, follows open standards (HL7 CDA, HL7 FHIR, and IHE profiles), and can be validated through IHE methodology, making the system flexible, interoperable, and reference ready.

The architecture follows core principles of privacy- and security-by-design, ensuring that all data access is governed by patient consent and strong authentication. It is modular and reusable, supporting AS with different levels of readiness. All interactions are standards-based, relying on HL7 FHIR, CDA, and IHE profiles like MHD, IUA, and ATNA. Finally, it is reference-implementation focused, designed for validation through IHE Connectathon and reusable by other EU projects.

The refined architecture is composed of several logical layers:

- At the security and privacy entry point, access is controlled by an Identity and Access Management (IAM) system that integrates with national or institutional Identity Providers (IdPs). Access to personal health data is additionally regulated by a Consent Management service, implementing Policy Administration and Decision Points (PAP/PDP) and enforced at the API layer by a Policy Enforcement Point (PEP).
- The data management layer is the heart of the Yellow Button experience. Applications can use dedicated APIs to allow citizens to:
    - View their documents,
    - Download them in human-readable (HTML, PDF) or machine-readable format in EEHRxF,
    - Share selected documents using Smart Health Links (SHL),
    - Transform documents between formats (e.g., CDA to HL7 FHIR),
    - Anonymize selected elements for data donation or secondary use.

These services are coordinated by a central data access controller, which logs events and handles document orchestration based on IHE MHD profiles.

A storage layer maintains cached EEHRxFs in a local repository (to prevent excessive querying of live clinical systems), stores user consent artifacts, and records audit logs that are available both to patients and institutional officers, in accordance with GDPR transparency principles.

Lastly, the connector layer ensures interoperability with external ecosystems. Planned integrations include MyHealth@EU via NCPeH, HL7 IPA-based app access, and SHL consumption endpoints.

The refined architecture is composed of several logical layers, as illustrated in Figure 1 below, depicting how the different services, APIs, and security components interact across layers. While all components can be integrated as part of a complete Yellow Button infrastructure, each can also be deployed independently, enabling incremental implementation at the national or institutional level.

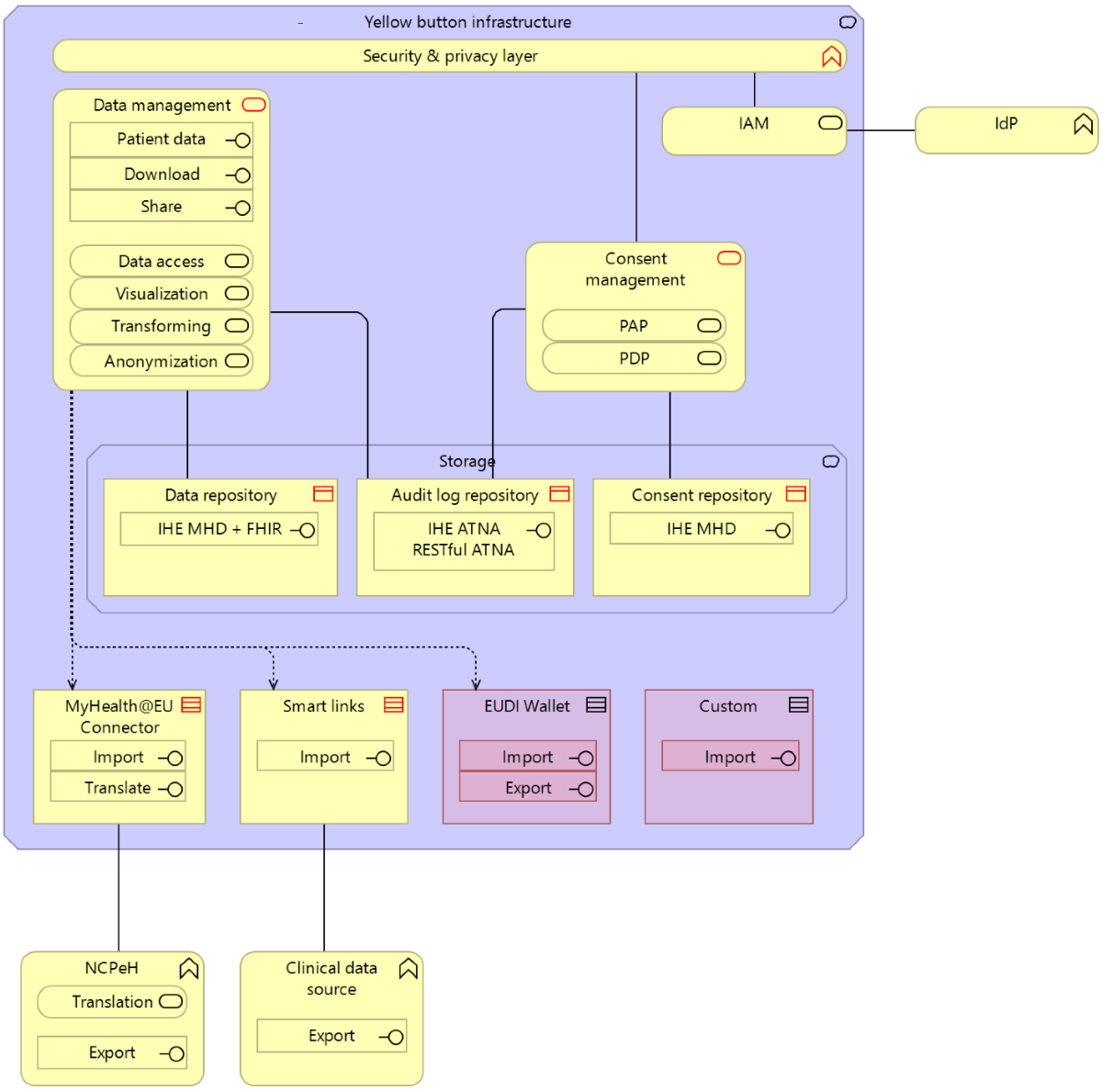


Figure 1: xShare Yellow Button refined infrastructure

Selected components developed under the xShare toolbox are available in the xShare GitHub[2] repository. The repository will continue to evolve until the end of the project and aims to provide modular, standards-aligned, and open implementations for reference and reuse.

[2] https://github.com/xSHARE-project-eu

3. xShare Toolbox

the working paper presents the updated state of the xShare Toolbox, which includes a modular set of components enabling secure, standards-aligned, and GDPR-compliant data portability. These tools are designed to support the implementation of the xShare Yellow Button across different institutional and national settings. The toolbox combines API-level services, transformation engines, visualization utilities, and testing support through synthetic data. Several components are already available and openly licensed, with others planned for the final release of the project. Table 1 from D3.3 described the core Yellow Button requirements, which guided the selection and prioritization of toolbox components.

3.1 CDA2FHIR

The **CDA2FHIR[3] converter is a core component of the xShare toolbox** that bridges legacy document-based health records (in CDA format) with the structured, modern HL7 FHIR format required by the EEHRxF. It supports Member States and vendors in transforming existing data structures to meet EHDS compliance. The converter focuses on key document types, including the International Patient Summary (IPS), which is widely used in both cross-border and national exchanges.

Developed in Java, the converter uses the FreeMarker[4] template engine to perform precise, rule-based transformations between CDA and HL7 FHIR. FreeMarker allows for deterministic mapping through FreeMarker Template Language (.FTL) templates, which process XML inputs and generate equivalent HL7 FHIR outputs. The architecture cleanly separates transformation logic from code, enabling transparency and customization. Each mapping template is modular and corresponds to a specific section or resource (e.g., Medications, Problems, Allergies), allowing developers to adapt or extend them for national localization or additional data elements.

The tool can be used in multiple ways: as a RESTful service or integrated into the core infrastructure as a library. To demonstrate the functionality of the converter, the following example showcases the transformation of patient demographic data from CDA to HL7 FHIR through a structured template-based pipeline.

The CDA file, as depicted in Figure 2, includes the patient's demographic information within the <recordTarget> block, including identifiers, name, gender, birth date, and address. This XML structure is parsed by the "patient.ftl" template, as shown in Figure 3, which extracts the relevant values and formats them as an HL7 FHIR Patient resource illustrated in Figure 4. It also handles date formatting and code normalization (e.g., F → female).

[3] https://github.com/xSHARE-project-eu/cda2fhir
[4] https://freemarker.apache.org/

```
<recordTarget>
 <patientRole>
  <id extension="CAT-ROSS-01"/>
  <addr>
   <streetAddressLine>1234 Main St</streetAddressLine>
   <city>Amsterdam</city>
   <postalCode>1012</postalCode>
   <country>NL</country>
  </addr>
  <patient>
   <name>
    <given>Cat</given>
    <family>Ross</family>
   </name>
   <administrativeGenderCode code="F" />
   <birthTime value="19820101"/>
  </patient>
 </patientRole>
</recordTarget>
```

Figure 2: Example CDA patient demographic information

```
{
 "resourceType": "Patient",
 "id": "${cda.id.extension}",
 "name": [{
  "family": "${cda.patient.name.family}",
  "given": ["${cda.patient.name.given}"]
 }],
 "gender": "${cda.patient.administrativeGenderCode.code?lower_case}",
 "birthDate": "${cda.patient.birthTime.value?substring(0,4)}-
${cda.patient.birthTime.value?substring(4,6)}-
${cda.patient.birthTime.value?substring(6,8)}",
 "address": [{
  "line": ["${cda.addr.streetAddressLine}"],
  "city": "${cda.addr.city}",
  "postalCode": "${cda.addr.postalCode}",
  "country": "${cda.addr.country}"
 }]
}
```

Figure 3: Transformation Template: patient.ftl

```
{
 "resourceType": "Patient",
 "id": "CAT-ROSS-01",
 "name": [{
  "family": "Ross",
  "given": ["Cat"]
 }],
 "gender": "female",
 "birthDate": "1982-01-01",
 "address": [{
  "line": ["1234 Main St"],
  "city": "Amsterdam",
  "postalCode": "1012",
  "country": "NL"
 }]
}
```


Figure 4: Output to HL7 FHIR Patient Resource

This example demonstrates how the CDA2FHIR converter serves as a practical and adaptable solution for bringing existing CDA-based health records into compliance with modern HL7 FHIR-based specifications. It is a foundational enabler for cross-border and national interoperability workflows under the xShare's Yellow button architecture.

3.2 Smart Health Links

Smart Health Links (SHLs)[5] offer a lightweight, privacy-preserving mechanism to share structured health data between systems, individuals, and applications. They are designed to enable citizens to generate secure, time-limited, and controlled access to their health data, supporting the Yellow

[5] https://docs.smarthealthit.org/smart-health-links/spec

Button's goal of citizen-driven data sharing in compliance with GDPR and aligned with EEHRxF requirements.

In the xShare toolbox, SHL is introduced as a reference-compatible component to enable patient-mediated sharing of HL7 FHIR Bundles. An SHL is essentially a compact URL that contains or references a digital health payload, such as a Patient Summary or Lab Report, and allows the recipient to view or import the data. The payload may be inline, signed, or hosted externally with proper metadata and encryption support.

SHL is implemented as a simple JSON "manifest", as show in Figure 5, which describes:

- Which data is being shared (e.g., an HL7 FHIR Bundle),
- How the data should be retrieved (inline or remote),
- Whether encryption or signatures are included,
- Optional constraints like expiration time or access tokens. For adoption sites, it is strongly recommended to enforce these constraints as mandatory to ensure proper security, data governance, and controlled access.

```
{
 "iss": "https://shl.example.org",
 "nbf": 1700000000,
 "exp": 1700600000,
 "vc": {
  "type": ["VerifiableCredential", "HealthDocument"],
  "credentialSubject": {
   "fhirBundle": {
    "resourceType": "Bundle",
    "type": "document",
    "entry": [ ... ]
   }
  }
 }
}
```

Figure 5: Example SHL manifest structure

The manifest can be:

- Encoded into a compact JWT, then converted into a URL (e.g., https://shl.example.org/#shlink=...)
- Shared via QR code, secure messaging, or app-to-app flow
- Validated by the recipient using embedded metadata, public keys, or symmetric decryption

In a typical use case:

1. A citizen uses the Yellow Button to select a document (e.g., IPS),
2. The document is transformed and visualized (via CDA2FHIR and vi7eti),
3. The SHL service creates a secure shareable URL or QR code,
4. The recipient application retrieves and validates the shared document, only after successful authentication, if a passcode or other access constraint is present.

SHL is a key enabler of "low-friction" health data exchange in xShare. It complements the existing infrastructure by offering a secure, flexible mechanism for patient-mediated sharing. As development progresses, SHL will be tested in Yellow Button reference workflows and made available via the xShare toolbox for broader reuse by AS and future EHDS-aligned projects.

3.3 vi7eti - Reference Visualization Tool

Within the xShare architecture, visualization of the technical health data instances plays a critical role in ensuring that health data, even when represented in highly structured and machine-readable formats such as HL7 FHIR, remains accessible, understandable, and meaningful to end-users. This is especially important under the GDPR's principles of transparency and intelligibility, which apply when citizens access or share their health data through the Yellow Button.

To meet this need, xShare has adopted and integrated vi7eti[6] (Visualize HL7 Example and Test Instances), an open-source tool developed by HL7 Europe and now publicly available as a fork under the xShare GitHub repository[7] and maintained as part of the visualization component of the toolbox. It serves as the reference implementation for rendering HL7 FHIR resources into HTML in a way that respects both content structure and user-facing presentation.

The tool follows a real-time transformation pipeline as depicted in Figure 6:

1. Accepts HL7 FHIR-compliant instance in JSON or XML format
2. If JSON format was provided it converts instance to HL7 FHIR XML
3. Applies XSLT stylesheets to HL7 FHIR XML that renders the structure
4. Visualizes the resulting HTML with CSS and Vanilla JavaScript support
5. Outputs a clean, user-friendly visual representation of the health data content.

[6] https://vi7eti.net/
[7] https://github.com/xSHARE-project-eu/visualization

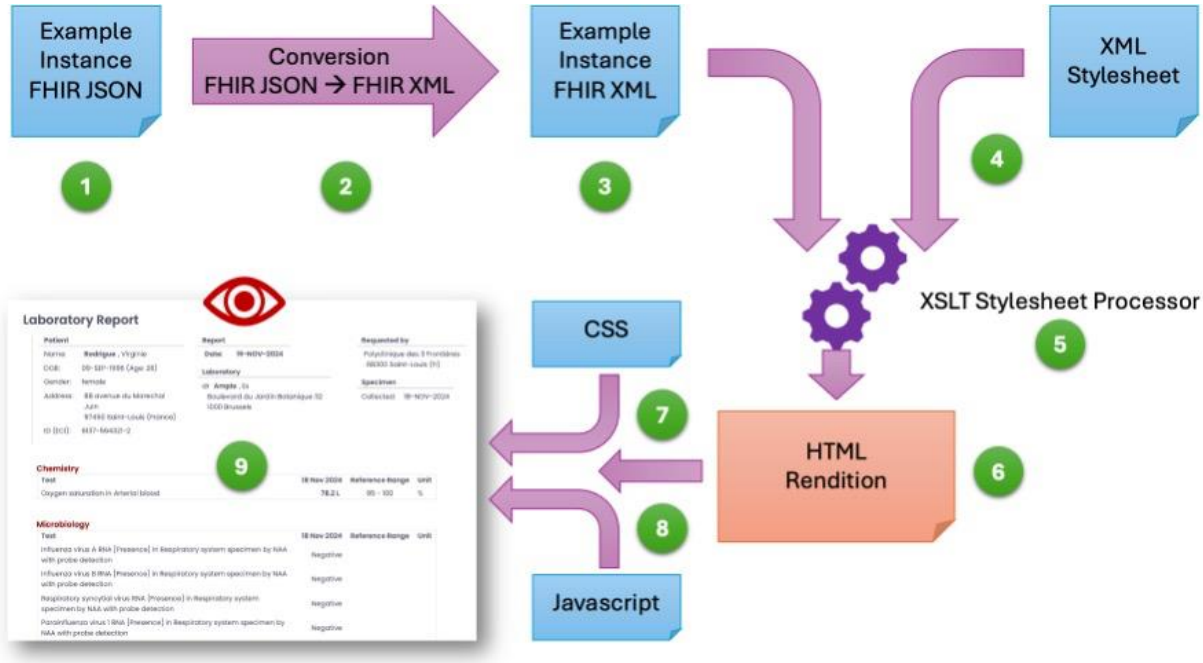
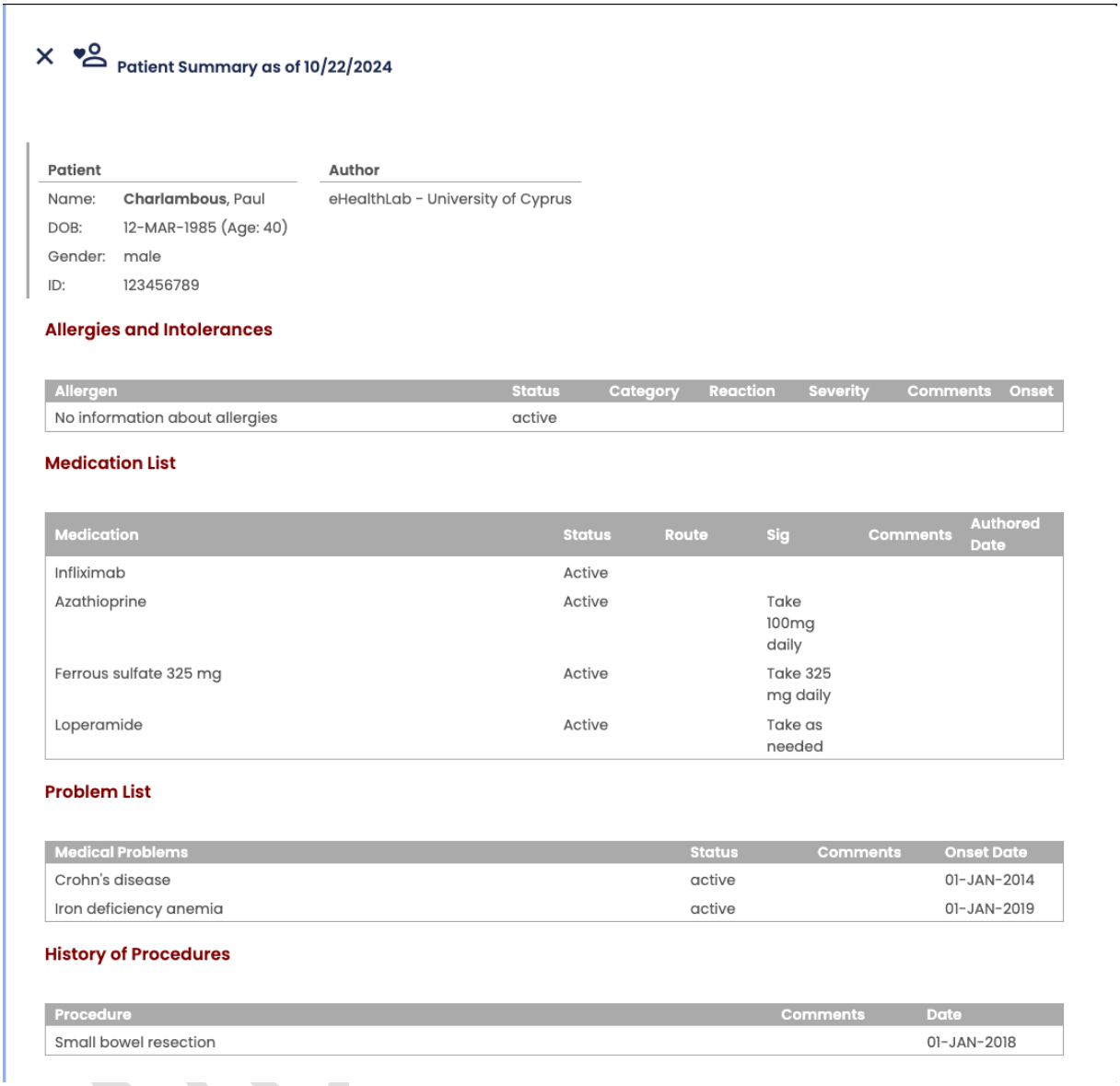


Figure 6: Visualization flow

This pipeline allows both:

- Live previewing of HL7 FHIR instances as a development and validation aid, and
- Pre-rendered, stable output that can be embedded in web portals or apps for patient consumption.

vi7eti is also used to validate conformance with the style and structural constraints of specific IGs (e.g., IPS), making it not just a visualization tool but a compliance validation aid as depicted in Figure 7.



Patient Summary as of 10/22/2024

Patient		Author
Name:	**Charlambous**, Paul	eHealthLab - University of Cyprus
DOB:	12-MAR-1985 (Age: 40)	
Gender:	male	
ID:	123456789	

Allergies and Intolerances

Allergen	Status	Category	Reaction	Severity	Comments	Onset
No information about allergies	active					

Medication List

Medication	Status	Route	Sig	Comments	Authored Date
Infliximab	Active				
Azathioprine	Active		Take 100mg daily		
Ferrous sulfate 325 mg	Active		Take 325 mg daily		
Loperamide	Active		Take as needed		

Problem List

Medical Problems	Status	Comments	Onset Date
Crohn's disease	active		01-JAN-2014
Iron deficiency anemia	active		01-JAN-2019

History of Procedures

Procedure	Comments	Date
Small bowel resection		01-JAN-2018

Figure 7: Example vi7eti output for HL7 FHIR IPS document

3.4 SYNDERAI - Synthetic Data for Testing

One of the recurring challenges in developing, testing, and validating HL7 FHIR-based systems is the availability of realistic, safe, and standards-compliant datasets. To address this, xShare integrates synthetic data generated under the SYNDERAI[8] initiative (Synthetic Data: Examples - Realistic - using AI), coordinated by HL7 Europe.

SYNDERAI provides synthetic, high-quality HL7 FHIR instances that replicate real-world clinical records without exposing personal health information. These instances are used across the xShare toolbox,

[8] https://github.com/hl7-eu/SYNDERAI

from transformation to visualization to sharing, enabling fully privacy-compliant test workflows, aligned with the EEHRxF and GDPR principles.

SYNDERAI datasets are designed to:

- Represent realistic clinical scenarios, including medications, problems, encounters, and vital signs.
- Conform to HL7 FHIR Implementation Guides, including IPS, EU Laboratory Report, and Hospital Discharge Summary.
- Avoid the use of real patient data, ensuring safety in both development and demonstration environments.

The project provides HL7 FHIR JSON files with associated resource metadata and is designed to support multilingual rendering and structured narratives. Within xShare, SYNDERAI synthetic data are:

- Used in architecture testbeds for download, share, and visualize flows
- Prepared to support IHE Connectathon test cases
- Embedded in documentation and walkthroughs as examples of valid HL7 FHIR structures

This data enables AS and developers to:

- Test the Yellow Button tools without privacy concerns
- Simulate end-to-end workflows with repeatable, traceable data
- Demonstrate compliance with technical and legal requirements

SYNDERAI plays a critical role in enabling safe, reusable, and standards-aligned testing of the Yellow Button components. It supports transparency, traceability, and validation across the xShare toolbox and provides a solid foundation for future testbeds, certification frameworks, and developer onboarding efforts in support of the EHDS.

Compared to the earlier D3.3 working paper, the SYNDERAI component has evolved significantly. What was previously described as a conceptual asset is now implemented and actively integrated into xShare workflows. The dataset is openly available, continuously expanded, and aligned with HL7 FHIR Implementation Guides such as IPS, EU Laboratory Report, and Hospital Discharge Summary. It is now validated through real-world use in visualization rendering (via vi7eti), Smart Health Link generation, and IHE Connectathon test case development. These advancements make SYNDERAI a critical enabler for privacy-preserving, standards-compliant, and repeatable validation processes across the toolbox.

3.5 OpenXDS

To support efficient, standards-based document storage and retrieval, the xShare toolbox includes integration with OpenXDS, a widely adopted, open-source implementation of the IHE Cross-Enterprise Document Sharing (XDS.b) profile. OpenXDS serves as the document repository layer in the Yellow Button architecture, enabling caching and controlled access to HL7 CDA or HL7 FHIR documents that form part of the citizen's EEHRxF record.

In the context of xShare, OpenXDS plays a critical role in ensuring that documents retrieved from clinical systems or generated through toolbox components (e.g., CDA2FHIR or vi7eti outputs) are:

- Stored reliably, with proper indexing and metadata,
- Made available for download or sharing, as part of the citizen interface,
- Accessible via standard IHE profiles, particularly MHD and XDS.b.

OpenXDS can be deployed as a standalone microservice or integrated into the Yellow Button reference stack. It acts as both a Document Consumer and a Document Responder, depending on the transaction being handled. It supports both:

- Push scenarios: where documents are published to the repository (e.g., via a processing pipeline or upload),
- Pull scenarios: where documents are retrieved via APIs or through an SHL resolution mechanism.

In line with the project's emphasis on modularity and reusability, OpenXDS[9,10] in xShare is used as a plug-and-play component that connects to the Data Management Layer and supports IHE-based transactions. The use of OpenXDS in Yellow Button workflows is summarized in Table 1.

Use Case	**Description**
Document caching	EEHRxF records retrieved from clinical data sources are cached in OpenXDS to avoid repeated external queries
Sharing enablement	Documents can be referenced in SHLs or downloaded in HL7 CDA or HL7 FHIR form
Auditability & standards compliance	Each transaction follows IHE protocols, with audit logging support when paired with ATNA
Testing support	OpenXDS is used as part of the IHE Connectathon test bench, supporting MHD/XDS.b test scripts

Table 1: OpenXDS usage in Yellow Button Workflows

[9] https://hub.docker.com/r/uwitech/openxds
[10] https://github.com/jembi/openxds

4. Legal Framing Table — GDPR & EHDS Alignment

The following Table 2 maps key components of the xShare toolbox to the applicable articles of the GDPR 2016/67911 and EHDS12 Regulation (EU) 2025/327, highlighting how each tool contributes to legal compliance in terms of data portability, access, consent, transparency, and security.

xShare Toolbox Feature	GDPR Article(s)	EHDS Article(s)	Compliance Role
CDA2FHIR Converter	Art. 20 (Portability), Art. 25 (Data protection by design)	Art. 3(2) (Download), Art. 7(4) (Transmission in EEHRxF format)	Enables export and conversion to interoperable formats for download and cross-border transmission.
Smart Health Links (SHL)	Art. 7 (Consent), Art. 20, Art. 32 (Security)	Art. 4(2) (Proxy services), Art. 7(1–3) (Portability), Art. 8	Facilitates secure, patient-mediated sharing and delegation of access to health data.
vi7eti Visualization Tool	Art. 12 (Transparency), Art. 15 (Access)	Art. 3(1) (Access), Art. 4(5) (Accessibility), Art. 9(2) (Audit)	Ensures transparency and human-readable access to health data; supports auditing visibility.
SYNDERAI Synthetic Data	Recital 26 (Anonymisation), Art. 89 (Research safeguards)	Art. 78 (Data quality and utility labels)	Provides privacy-safe, high-quality test data; supports alignment with reuse obligations under EHDS.
Consent Management Module[13]	Art. 6–7 (Lawfulness and consent), Art. 25 (by design)	Art. 4(2) (Authorisation), Art. 10 (Opt-out rights)	Supports lawful processing, informed consent, and flexible access control aligned with national laws.
OpenXDS Repository	Art. 30 (Records of processing), Art. 32 (Security)	Art. 3(2) (Download), Art. 7(1) (Data access), Art. 9 (Audit logs)	Provides traceable, standards-compliant storage with auditable access logs.
IHE-Based Testing & Test Bench	Art. 25 (By design), Art. 32 (Security), Art. 35 (DPIA)	Art. 40 (Certification & testing environment)	Aligns toolbox testing with the EHDS digital testing infrastructure for conformity

[11] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679
[12] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ%3AL_202500327
[13] The Consent Management component described in this working paper reflects preliminary design considerations based on interactions with AS and alignment with relevant GDPR and EHDS requirements. However, this component has not yet been implemented or validated within WP3. Further development, stakeholder consultation, and technical exploration are required to deliver a deployable solution.

xShare Toolbox Feature	GDPR Article(s)	EHDS Article(s)	Compliance Role
			assessments.infrastructure for conformity assessments.

Table 2: Legal Framing Table

5. IHE-Based Testing & xShare Test Bench

The xShare project supports implementation-focused validation by aligning its toolbox and workflows with IHE testing methodologies, using structured testing sessions to evaluate real-world interoperability, conformance, and usability. A central part of this approach is the use of IHE Plugathon-style events, where testing is open not only to AS but also to other consortium members and external participants, including SMEs and system integrators interested in aligning their implementations with the EHDS.

These Plugathon-style events serve as piloting environments where new applications are developed, and early-stage solutions can be explored. As shown in the Figure 8 the goal is to test innovative implementations and assess their maturity. Unlike Connectathons, which are primarily intended for product managers, developers, and national eHealth programme experts to validate products against stable IHE profiles using mature testing tools, Plugathons allow for more experimental testing in a guided setting. In contrast, Projectathons are tailored to deployment and procurement phases, featuring project-specific testing tools and specifications. They result in documented conformity with those requirements and help inform procurement decisions.

From a management perspective, Plugathons are supported by *facilitators*, domain experts familiar with the project who guide participants toward higher implementation maturity. Connectathons, on the other hand, are supervised by *monitors*, who are neutral, qualified experts responsible for validating tests in a structured and impartial manner.

In this context, testing activities are being conducted through IHE Plugathon-style workflows, focused on the IPS. These workflows are structured to simulate real-world health data exchanges involving HL7 FHIR documents and are used to validate modular components of the toolbox, such as CDA2FHIR, SHL, and download APIs. Crucially, this approach establishes a practical pathway toward future compliance with the EHDS certification framework foreseen under Article 40[14]. Each workflow is accompanied by facilitator checklists, technical validation steps, and manual review processes to ensure not only conformance to the relevant Implementation Guides, but also clarity and usability.

Testing is structured in three levels:

1. Technical validation: HL7 FHIR IPS documents are validated against the xShare Implementation Guide[15] (IG) using the Gazelle Validator[16], ensuring structural compliance.
2. Visual and semantic inspection: Facilitators manually inspect documents against defined Personas, checking for clinical coherence, proper use of terminologies (e.g., SNOMED CT), and alignment with visual tools like vi7eti.
3. Functional verification of toolbox components: Through real application workflows, AS demonstrate:
    - Document download using the Yellow Button (“Download” test case),

[14] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ%3AL_202500327#d1e3558-1-1
[15] https://build.fhir.org/ig/hl7-eu/xShare/
[16] https://gazelle.racsel.org/GazelleFhirValidator/validators/displayResourceValidator.seam?id=1.3.6.1.4.1.12559.11.1.2.1.12.155

- Secure, controlled sharing using Smart Health Links (“One-Time Share” test case),
- Optional interoperability testing with peer sites when available.

Each of these test flows ensures that the tools developed in WP3 can function independently and in combination, and that they conform to IHE profiles such as MHD, XDS.b, and IUA, as appropriate. Testing also prepares the project for participation in the IHE Plugathon in Vienna 2025[17], where the same flows will be formally validated across multiple implementations.

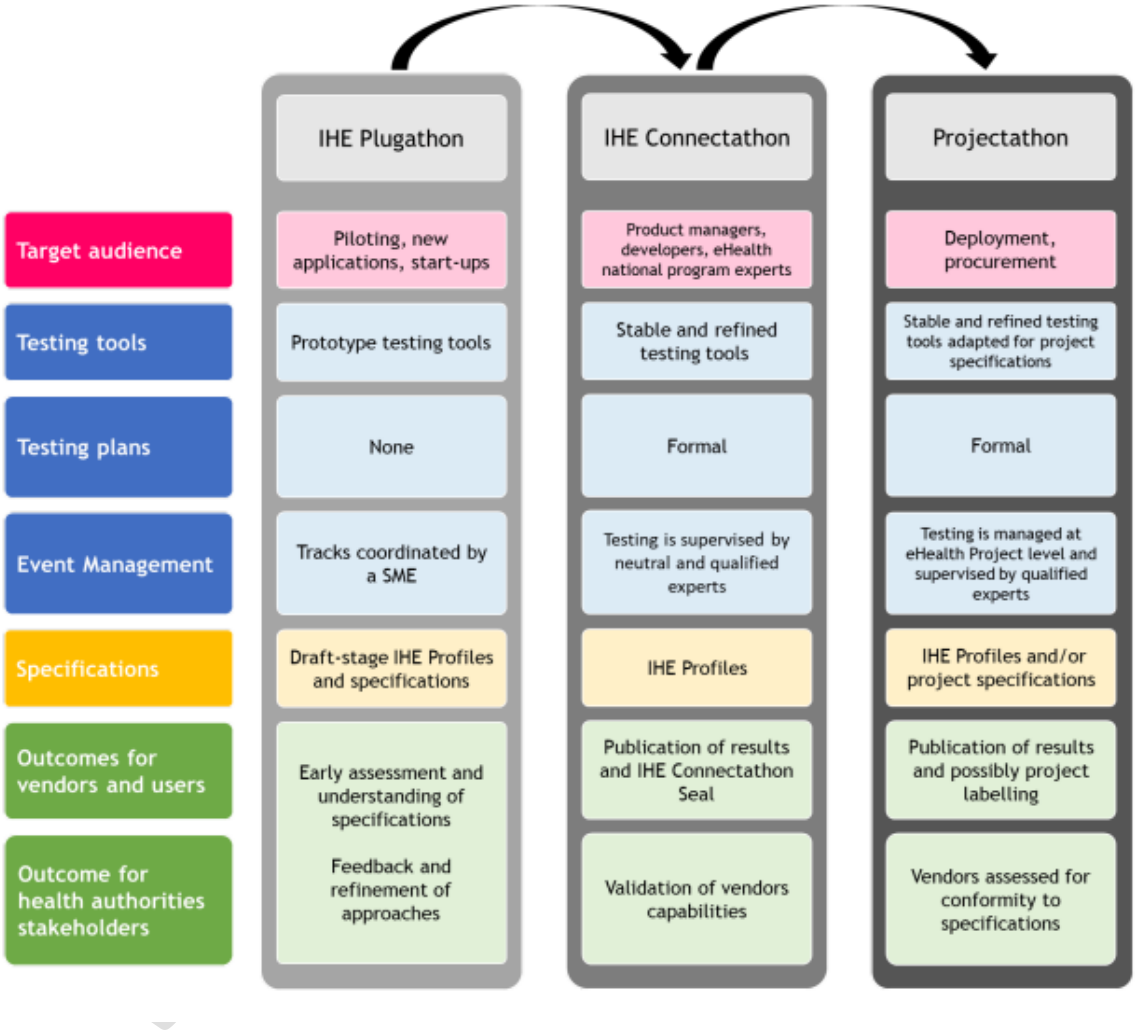


Figure 8: IHE Connectathon eco-system

[17] https://connectathon.ihe-europe.net/ihe-plugathon-2025

6. Next Steps and Toolbox Roadmap

Working paper presents a refined and testable version of the xShare architecture and toolbox. Since D3.3, the project has progressed from a conceptual model to a modular, standards-aligned, and partially implemented reference toolkit. The architecture now supports layered adoption, testability via IHE methodology, and integration across multiple document workflows under the EEHRxF.

The following components have been implemented and validated in workflows or early testing:

- CDA2FHIR Converter: HL7 CDA to HL7 FHIR transformer, used in IPS document preparation.
- Smart Health Links (SHL): Enables one-time, patient-mediated sharing via compact URLs.
- vi7eti: Visualization engine for rendering HL7 FHIR documents (IPS, EU-Lab, HDR) in human-readable format.
- SYNDERAI Synthetic Data: Realistic, standards-conformant HL7 FHIR test data used for validation, visualization, and Connectathon scenarios.
- OpenXDS Repository: IHE-compliant document storage and retrieval system supporting MHD and XDS.b profiles.

6.1 Pseudonymization Component

To support lawful secondary use of health data and enable privacy-preserving sharing, the xShare project has undertaken substantial foundational work on pseudonymization and data protection. This effort, which will be detailed in D7.1, reviews the state of the art in anonymization and pseudonymization[18] and synthesizes multiple authoritative sources including the European Data Protection Board (EDPB), the ISO 25237 standard, and relevant regulatory frameworks under the GDPR and EHDS.

The process of pseudonymization begins with defining the purpose and legal basis for data release, such as secondary use under the European Health Data Space, followed by identifying the minimum dataset necessary for that purpose. The methodology emphasizes a deep understanding of the dataset, identifying all fields that could contain Personally Identifiable Information (PII), quasi-identifiers, or outlier variables. These may include structured identifiers like name, ID, address, and unstructured content such as free-text fields or embedded notes.

Key steps outlined in the process include:

- **Identification of Person Identifying Variables**: Name, patient identifiers, biometrics, and contact details must be detected and flagged.
- **Classification of Quasi-Identifiers**: Combinations of seemingly non-unique attributes (e.g., birth date + zip code) that can enable re-identification are analysed.
- **Assessment of Aggregation Risks**: Variables such as religion, language, or rare diseases are reviewed to ensure they do not create unique patient profiles.
- **Differentiation between Pseudonymization and Anonymization**: The former maintains the ability to re-link with the subject via securely stored keys, while the latter removes this

[18] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ%3AL_202500327#d1e5116-1-1

possibility entirely at least with means reasonably likely to be used - thereby rendering the data outside the scope of GDPR.[19]

- **Risk Assessment and Data Utility Trade-offs**: Each data transformation is weighed against disclosure risks and data utility loss, following principles defined in both ISO 25237 and EDPB guidance.

The ISO 25237 standard provides precise definitions and operational boundaries between anonymized and pseudonymized data. It emphasizes that no single de-identification technique suffices across all health datasets. Instead, each release must undergo risk analysis to define the disclosure context, minimal information necessary, risk of re-identification, and acceptable release strategy.

Additionally, the EDPB guidelines describe a detailed operational process for pseudonymization, covering everything from attribute selection, cryptographic methods, key management, domain separation, and risk evaluation. These methods include omission, generalization, randomization, and secure lookup of pseudonyms. The guidelines stress that all pseudonymization strategies should be executed under clearly defined roles (e.g., controller, processor) and that transformation secrets must be managed with strict technical and organizational controls.

Moreover, special attention is given to non-structured data such as free-text entries, audio files, and scanned documents, where identifying information may be unintentionally embedded. The documentation outlines scenarios in which such fields must be excluded or passed through advanced scrubbing techniques.

Risk assessment is central to the pseudonymization process. As highlighted by both EDPB and ISO standards, every release of data must be preceded by a privacy risk analysis that evaluates re-identification likelihood, data context, user profiles, and residual risks. The use of tools such as the CNIL Privacy Impact Assessment (PIA) toolkit is recommended.

In the upcoming work within this task, the project will investigate and evaluate existing technical solutions that operationalize these principles. This includes reviewing and testing open-source and commercial tools such as:

- Microsoft Tools for Health Data Anonymization (FHIR-aware)[20]
- ARX (TU Munich) for structured data and k-anonymity[21]
- Amnesia (OpenAIRE) for structured data de-identification[22]
- Privitar and IBM's data privacy toolkit[23]
- OpenDP (Harvard) for differential privacy[24]

[19] However, total anonymisation with zero risk of re-identification cannot be guaranteed – as the EHDS Regulation acknowledges in its Recital 92.
[20] https://github.com/microsoft/Tools-for-Health-Data-Anonymization
[21] https://arx.deidentifier.org/
[22] https://amnesia.openaire.eu/
[23] https://github.com/IBM/data-privacy-toolkit
[24] https://opendp.org/

These tools will be assessed for alignment with the guidelines above, potential integration into the xShare toolbox, and suitability for Adoption Site requirements.

6.2 Consent Management

A dedicated consent management component is under design. It will implement:

- Policy-based access control (PAP, PDP)
- Reusable consent logging and evaluation across download, share, and pseudonymization workflows
- Integration with IHE profiles such as BPPC/APPC
- A user-facing UI component for consent capture

This component is essential for ensuring full compliance with GDPR and national-level patient rights.

6.3 Translation and MyHealth@EU Interoperability

The integration of translation services and the connection with the MyHealth@EU infrastructure builds upon work initiated in the PATHeD[25] project. In PATHeD, translation capabilities were implemented within regulated cross-border workflows using OpenNCP, the Master Value Catalogue (MVC), and Central Terminology Server (CTS).

In xShare, the scope of integration with OpenNCP and MyHealth@EU extends beyond translation. In several AS, specifically Greece, Cyprus, and Ireland, OpenNCP already serves as a data source for retrieving cross-border patient documents via MyHealth@EU workflows. While xShare has not yet standardized a connector for this purpose, these national deployments demonstrate the feasibility of aligning Yellow Button workflows with existing infrastructure.

Future work in this task will explore the potential to reuse or adapt elements from PATHeD or other OpenNCP components. The goal is to define a standardized integration approach that enables Yellow Button services to interoperate with MyHealth@EU-compliant infrastructures wherever available.

The paper sets the foundation for a fully operational, standards-based Yellow Button implementation. With its modular components, aligned testing methodology, and strategic roadmap, the toolbox now offers a concrete path for Adoption Sites and developers to contribute to the emerging EHDS ecosystem. The final working paper, D3.12, will complete integration, validate all tools, and deliver a reference-ready, reusable asset base for European digital health.

[25] https://heiresearch.com/PATHed/index.php?lang=en