Extended EHR@EU Data Space for Primary Use - Xt-EHR

Proposal number: 101128085

D8.2 – EHR Conformity Assessment Scheme - Assertion document

(Co-)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 HaDEA. Neither the European Union nor the granting authority can be held responsible for them.

Author(s)

Name	Surname	Country	Organisation	Role of the Organisation
Haralampos	Karanikas	Greece	IDIKA SA	AE
Angeliki	Katsapi	Greece	IDIKA SA	AE
Ioannis	Asproloupos	Greece	IDIKA SA	AE
Alexander	Berler	Cyprus	NeHA	CO
Andreas	Neocleous	Cyprus	NeHA	CO
Vanja	Pajić	Czechia	VR	CA
Zoltan	Lantos	Hungary	ESZFK	CA
Charles	Parisot	France	ANS	

Contributor(s)

Name	Surname	Country	Organisation	Role of the Organisation
Elpida	Fotiadou	Greece	IDIKA SA	AE
Nikolaos	Iosif	Greece	IDIKA SA	AE
Sofia	Terzi	Greece	IDIKA SA	AE
Lysette	Meuleman	Netherlands	NEN	
Dick	Hortensius	Netherlands	NEN	

Reviewed by

Name	Surname	Country	Organisation	Role of the Organisation
Alexander	Berler	Cyprus	NeHA	CO
Jordi	Carrere	Spain	IDIAPJGol	AE
Andreas	Neocleous	Cyprus	NeHA	CO
Zdenek	Gütter	Czech Republic	MoH	AE

ABBREVIATIONS

CAS	Conformity Assessment Scheme
CASCC	Conformity Assessment Scheme Coordination Committee
CASforEU	Conformity Assessment Scheme for Europe
CASO	Conformity Assessment Scheme Owner
CDA	Clinical Document Architecture
DGA	Data Governance Act
EEHRxF	European electronic health record exchange format
EHDS	European Health Data Space
EHR	Electronic health record
GDPR	General Data Protection Regulation
HL7	Health Level 7
IHE	Integrating the Healthcare Enterprise
IHE-CAS	Integrating the Healthcare Enterprise Conformity Assessment Scheme
QMS	Quality Management System
WP	Work Package
Xt-EHR	Extended EHR@EU Data Space for Primary Use

GLOSSARY

- **Adoption domain:** instantiation of a use case, with a specific business/real-world use application, that has meaning for a health system or clinical perspective, with implementable requirements defined, that has all the conditions and users to be ready for implementation, always considering the European Electronic Health Record Exchange Format health information domains.
- **Common data element:** data element that plays a role in multiple business use cases and/or priority categories of personal electronic health data.
- **Common specifications:** compliance with essential requirements on interoperability and security should be demonstrated by the manufacturers of Electronic health record systems through the implementation of common specifications.
- **Conformity**: a product, service, or process has met the requirements and criteria set by a given standard or a specification, which is often voluntary base.
- **Conformity Assessment Scheme**: set of rules and procedures that describes the objects of conformity assessment, identifies the specified requirements and provides the methodology for performing conformity assessment (ISO/IEC 17000); or a framework that allows eHealth solutions to be tested for their conformity with a selected set of eHealth standards and profiles (definition from EURO-CAS).
- **Compliance**: adherence of a product, service or process to legal and regulatory requirements, fulfilling legislative and contractual requirements.
- **EHR systems:** 'electronic health record system' or 'EHR system' means any system whereby the software, or a combination of the hardware and the software of that system, allows personal electronic health data that belong to the priority categories of personal electronic health data established under this Regulation to be stored, intermediated, exported, imported, converted, edited or viewed, and intended by the manufacturer to be used by healthcare providers when providing patient care or by patients when accessing their electronic health data.

- **Electronic health data:** personal or non-personal electronic health data.
- **Electronic health record:**
  - information relevant to the wellness, health and healthcare of an individual, in computer-processable form and represented according to a standardized information model (ISO 18308:2011)
  - comprehensive medical record or similar documentation of the past and present physical and mental state of health of an individual in electronic form, and providing for ready availability of these data for medical treatment and other closely related purposes
  - (*eHDSI,Glossary* *https://webgate.ec.europa.eu/fpfis/wikis/pages/viewpage.action?spaceKey=EHDSI&title=MyHealth@EU+Glossary#MyHealth@EUGlossary-E*)
- **Electronic health record exchange format:**
  - a commonly used, machine-readable format that allows transmission of personal electronic health data between different software applications, devices and healthcare providers. The format should support transmission of structured and unstructured health data, *EHDS*
  - a set of requirements and technical specifications, as well as endorsed support materials, targeted at ensuring the interoperability of electronic health record systems following the Regulation on the European Health Data Space and other applicable law. It is designed to enable the exchange of personal electronic health data between two or more Electronic health record systems or other digital health applications or medical devices in a meaningful way (XpanDH)
- **Electronic identification and trust services:**
  - European regulation on electronic identification and trust services for electronic transactions in the internal market (European Commission https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32014R0910&from=EN)
- **EURO-CAS:** EU eHealth Interoperability Conformity Assessment Scheme.

- **Fast healthcare interoperability resources:** an interoperability standard intended to facilitate the exchange of healthcare information between healthcare providers, patients, caregivers, payers, researchers, and any one else involved in the healthcare ecosystem. It consists of two main parts – a content model in the form of 'resources', and a specification for the exchange of these resources in the form of real-time RESTful interfaces as well as messaging and documents. (*HL7 http://www.hl7.org/implement/standards/product_brief.cfm?product_id=491*, *FHIR https://hl7.org/FHIR/*)
- **Health or wellness app**: app intended to be used specifically for managing, maintaining or improving health of individual persons, or the delivery of care (definition from ISO/TS 82304-2).
- **Refined eHealth European interoperability framework:** common refined framework for managing interoperability and standardisation challenges in the eHealth domain in Europe (eHealth Network)

EXECUTIVE SUMMARY

The current deliverable D8.2 establishes the basis for a Conformity Assessment Framework (EHDS-CAS) for Electronic Health Record (EHR) systems with respect to specifications and requirements that ensure compliance with the European Health Data Space (EHDS) Regulation, particularly with regards to aspects of interoperability, security and logging of healthcare professionals, as defined in Extended EHR@EU Data Space for Primary Use (XT-HER) work packages (WPs) 5-7.

The main aspects are the following:

- The governance framework of the EHDS-CAS;
- The rules and procedures and methodology for performing conformity assessment;
- A set of testable assertions that can be added to test tools necessary to support the interoperability;
- Means of verification (checklists) for other types of requirements.

This set of evaluation and testing criteria will enable the assessment of the conformity of EHR systems across Europe, based on the primary use of data by the European Electronic Health Record Exchange Format (EEHRxF) and MyHealth@EU, using a pragmatic, readiness-based approach according to the intended use of the EHR system.

The proposed Conformity Assessment Scheme (CAS) builds upon recognized international standards, methodologies, and best practices. By leveraging these foundations, the EHDS CAS ensures the integrity, interoperability, and ongoing improvement of EHR systems and Health applications. It supports manufacturers in meeting EHDS Regulation obligations through structured self-assessment, while fostering trust, innovation, and a harmonized approach to compliance and conformity assessment across Europe.
The scheme guarantees that any EHR system claiming conformity with the EHDS Regulation can

seamlessly interoperate with any other such system—regardless of the assessing body or location—ensuring a cohesive, interoperable digital health ecosystem.

D8.2 focuses on updating the governance (initial version in collaboration with WP4) and defining the content of a future CAS. The CAS comprises two distinct parts (see references EUROCAS project), one focusing on the governance of the CAS (how to apply conformity assessment in the context of the EHDS regulation), and the other focusing on the CAS content (testable assertions, test tools and means of verifications).

The CAS governance model ensures a) progressive adoption to allow EHR vendors to be able to adopt, test and incorporate EEHRxF in their products, b) comply with EHDS regulation articles about self-assessment procedures and c) ensure equitability of member states to incorporate the governance model.

The CAS content as testable assertions and means of verifications is driven by several sources such as previous established CAS models (EURO-CAS, Integrating the Healthcare Enterprise (IHE) CAS (IHE-CAS), Label2Enable CAS, etc), WP5, WP6 and WP7 set of specifications, Health Level 7 (HL7) EHR-FM model requirements. All those assertions are described in a way that they can be tested and verified to allow an impartial self-assessment CAS. Testable assertions cover both interoperability, security and logging specifications.

The CAS governance enables a versioning of the CAS content so that testing procedures and process can evolve based on the maturity models (i.e. XT-EHR maturity model, etc) allowing the release of versions of the testable assertions having required and optional assertions that can evolve over time to allow gradual adoption by member states and the Vendor's community across the European Union. The governance model includes change management processes and waves in a similar approach with the established processes for the myHealth@EU services. Means of verifications and test plans are based on proposing an evolution of the myHealth@EU testing platform.

Table of Contents

1. INTRODUCTION

The Xt-EHR joint action is working on implementation guides, technical specifications and a conformity assessment framework to facilitate the adoption of the EEHRxF and the implementation of security and logging mechanisms.

Manufacturers of EHR systems will only be allowed to place systems on the market for the prioritized categories if those systems comply with the common specifications for the harmonised components. Over time, this requirement will extend to systems processing the remaining categories.

EHR systems are defined as (see Article 2(2) point (k) EHDS Regulation) 'any system whereby the software, or a combination of the hardware and the software of that system, allows personal electronic health data that belong to the priority categories of personal electronic health data established under this Regulation to be stored, intermediated, exported, imported, converted, edited or viewed, and intended by the manufacturer to be used by healthcare providers when providing patient care or by patients when accessing their electronic health data'.

This definition has the following elements:

- EHR systems can be a combination of hardware and software or just software: an EHR system can be integrated as part of a physical device or be software on its own.
- They allow the storage, intermediation, export, import, conversion, editing, or viewing of priority categories of electronic health data: a system that only processes other kinds of data (such as a system for patients to book appointments) is not an EHR system.
- Systems do not need to provide all of storage, intermediation, export, import, conversion, editing, or viewing functionalities to be considered as an EHR system.
- They are intended by their manufacturer to be used:
    - By healthcare providers when providing patient care: the classic example would be systems used by clinicians for recording notes, test results etc, up to a patient management system; or

- By patients when accessing their electronic health data: this means that for example an app that connects to the electronic health data access service for patient will count as an EHR system.

This definition is intentionally broad to ensure interoperability throughout the chain of connected systems. It applies not only to systems that aggregate information, such as hospital information systems, but also to the systems that feed them.

Article 25(2) and recital 38 clarify that when general purpose software is used for these purposes, it does not count as an EHR system: standard text processing software can be used to edit any kind of textual information, including for example patient summaries, but it is not specifically intended by the manufacturer for use in providing patient care[1] and so does not count as an EHR system.

Products may have parts that fall under different conformity assessment systems such as under the Medical Devices Regulation[2], the Artificial Intelligence Act[3] or the EHDS. In such case, each part of the product needs to comply with the applicable conformity assessment framework.

To be placed[4] on the market or put into service in the Union, EHR systems shall contain the two harmonised software[5] components that describe capabilities of EHR systems, namely:

- The interoperability component. The interoperability component provides the capability to import/export data that falls under the priority categories in the EEHRxF. There is no requirement that EHR systems use the format internally.

[1] This mirrors a similar exclusion in recital 19 of the Medical Device Regulation 2017/745: clinical decision support software is considered a medical device, but if a health professional uses general purpose software such as spreadsheet software to create a spreadsheet template calculating dosage recommendations, that does not make the (generic) spreadsheet software itself a clinical decision support software.

[2] Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC, OJ L 117, 5.5.2017, p. 1–175.

[3] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828, OJ L, 2024/1689, 12.7.2024.

[4] Sources: Articles 2(2) points (m) to (o), 25, 26, 29; Recitals 36, 39

[5] While EHR systems as a whole can have physical/hardware and software parts, these two components will logically always be software.

- and the logging component. The logging component provides the capability to generate logs that can be used in the health data access service to provide transparency on data access.

Manufacturers will be obliged to test these components in digital testing environments prior to placing EHR systems on the market. While these will be the requirements for placing EHR systems on the market, Member States may also maintain or define specific rules for the procurement or financing of, or reimbursement for EHR systems. The EHDS requirements only cover the two harmonised components.

The digital testing environments[6] will test the two harmonised components of a EHR system (mentioned above) against the requirements in the EHDS Regulation. Manufacturers will have to do these tests before placing their systems on the market in the Union and they will receive a test report that will become part of their system documentation. If the system does not pass, the report will provide feedback on which parts the system did not pass and they will be able to try again. The report that becomes part of the system documentation is the final, successful, one, showing that the system passed all tests. Only the successful test report has to be made available[7]. The Commission will develop the software for the digital automated testing environment, enabling Member States to deploy such an environment for testing these components.

The requirement[8] for healthcare providers will be to be able to export and import data in the EEHRxF. That is a requirement they shall comply with – how they achieve it is left to them. They could for example upgrade their existing EHR systems to support this feature or use a system that "translates" between their internal file format and the EEHRxF. Member States can also mandate digital health authorities to provide additional instructions or national services to facilitate this.

[6] Sources: Articles 37(2), 40; Recital 36

[7] If the system does not pass, they must not make place it on the market. The documentation obligations apply when they place a system on the market.

[8] Sources: Articles 15(4), 23(5) and (6)

The rules in Chapter III of the EHDS Regulation will ensure that all new EHR systems offered in the Union will can import and export data using the EEHRxF.

1.1 Purpose of this document

In the introductory section, the purpose that is served by the document is described. D8.2 will elaborate the elements of the proposed CAS in accordance with EHDS requirements and will essentially include rules and procedures, describe the object of conformity assessment, identify the specified requirements and provide the methodology for performing conformity assessment. This document reviews the key references, concepts, and standards that shall be aligned with the intended scope in order to establish the necessary checkpoints and assertions for EHR conformity assessment in accordance with the provisions of the EHDS Regulation.

1.2 Basic ISO standards

In this section the relevant standards and ISO guidance are presented for the development of a CAS and the related processes that should be defined and followed. Conformity assessment is the demonstration that specified requirements are fulfilled. This includes activities such as testing, inspection, evaluation, examination, auditing, assessment, declaration, certification, accreditation, peer assessment, verification and validation.

Related references that will be discussed in this part are the following:

1. **ISO/IEC 17000:2004**, Conformity assessment – Vocabulary and general principles, especially its Annex A: Specifies general terms and definitions relating to conformity assessment, including the accreditation of conformity assessment bodies, and to the use of conformity assessment to facilitate trade. A description of the functional approach to conformity assessment is included as a further aid to understanding among users of conformity assessment, conformity assessment bodies and their accreditation bodies, in both voluntary and regulatory environments. ISO/IEC 17000:2004 does not set out to provide a vocabulary for all the concepts that may need to be used in describing particular conformity assessment activities. Terms and definitions are given only where the concept defined would not be

understandable from the general language use of the term or where an existing standard definition is not applicable.

2. **ISO/IEC 17007:2009**, Conformity assessment – Guidance for drafting normative documents suitable for use for conformity assessment: ISO/IEC 17007:2009 provides principles and guidance for developing normative documents that contain:
    a. specified requirements for objects of conformity assessment to fulfill.
    b. specified requirements for conformity assessment systems that can be employed when demonstrating whether an object of conformity assessment fulfills specified requirements.

ISO/IEC 17007:2009 is intended for use by standards developers not applying the ISO/IEC Directives, industry associations and consortia, purchasers, regulators, consumers and non-government groups, accreditation bodies, conformity assessment bodies, CAS owners, and other interested parties, such as insurance organizations.

3. **ISO/IEC 17065:2012,** Conformity assessment — Requirements for bodies certifying products, processes and services: This International Standard contains requirements for the competence, consistent operation and impartiality of product, process and service certification bodies. Certification bodies operating to this International Standard need not offer all types of products, processes and services certification. Certification of products, processes and services is a third-party conformity assessment activity.

4. **ISO/IEC 17025:2017,** General requirements for the competence of testing and calibration laboratories: ISO/IEC 17025 is the international standard for testing and calibration laboratories. It sets out requirements for the competence, impartiality, and consistent operation of laboratories, ensuring the accuracy and reliability of their testing and calibration results.

5. **ISO/IEC 17020:2012**, Conformity assessment — Requirements for the operation of various types of bodies performing inspection. This International Standard covers the activities of inspection bodies whose work can include the examination of materials, products, installations, plants, processes, work procedures or services, and the determination of their conformity with requirements and the subsequent reporting of results of these activities to clients and, when required, to authorities.

6. **ISO/IEC 27020:2015** provides guidelines in addition to guidance given in the ISO/IEC 27000 family of standards for implementing information security management within information sharing communities. ISO/IEC 27020:2015 provides controls and guidance specifically relating to initiating, implementing, maintaining, and improving information security in inter-organizational and inter-sector communications. ISO/IEC 27020:2015 is applicable to all forms of exchange and sharing of sensitive information, both public and private, nationally and internationally, within the same industry or market sector or between sectors. In particular, it may be applicable to information exchanges and sharing relating to the provision, maintenance and protection of an organization's or nation state's critical infrastructure.

7. **ISO 9001** Quality management systems – Requirements. ISO 9001 is a globally recognized standard for quality management. It helps organizations of all sizes and sectors to improve their performance, meet customer expectations and demonstrate their commitment to quality. Its requirements define how to establish, implement, maintain, and continually improve a quality management system (QMS). Implementing ISO 9001 means that a organization has put in place effective processes and trained staff to deliver flawless products or services time after time.

8. **ISO 13485** Medical devices — Quality management systems — Requirements for regulatory purposes. ISO 13485 is the internationally recognized standard for QMSs in the design and

manufacture of medical devices. It outlines specific requirements that help organizations ensure their medical devices meet both customer and regulatory demands for safety and efficacy.

9. **ISO/IEC 17050-1:2004** Conformity assessment — Supplier's declaration of conformity — Part 1: General requirements and **ISO/IEC 17050-2:2004** Conformity assessment — Supplier's declaration of conformity — Part 2: Supporting documentation. ISO/IEC 17050-1 and 17050-2 together provide a framework for a supplier's declaration of conformity. Part 1 outlines the general requirements for such declarations, where a supplier — acting as the first party — attests that a product, service, process, management system, or person complies with specified requirements. These requirements may be based on standards, technical specifications, laws, or regulations. The standard emphasizes that the supplier bears full responsibility for issuing, maintaining, and withdrawing the declaration, and that it shall be based on appropriate conformity assessment activities. The declaration shall clearly identify the responsible issuer, the object of conformity, the applicable requirements, and the authorized signatory. Part 2 complements this by specifying the supporting documentation required to substantiate the declaration. This documentation shall be traceable, transparent, and available upon request to relevant regulatory authorities. It typically includes technical descriptions, test or audit results, assessment methods used, and information about any involved conformity assessment bodies. The standard also requires that any changes affecting the validity of the declaration be documented and that the documentation be retained in accordance with legal or business needs. The standard provides example formats how to design a declaration of conformity. Together, these two parts establish a credible and structured basis for possible first-party declarations of conformity.

1.3 Xt-EHR document interdependencies

In this section interdependencies of the CAS document with other relevant WPs and pre-existing documents will be explicitly described.

With respect to the regulation, this document proposes a the CAS for EHR systems as described in Chapter 3, Section 3, Articles 36, 37, 38, 40 and 41, and Annex II, Annex III (IV).

1.3.1 WP4 CAS Governance documentation

Task 4.3 initially described the process definition for assessing the specification for the CAS on the basis of which section 4.1 of this document further elaborates and proposes the final EHDS CAS. This EHDS CAS builds upon recognized international standards, methodologies, and best practices. These include the IHE Methodology, the IHE-CAS and relevant ISO/IEC frameworks. Established maturity models in use for evaluating healthcare providers, such as the Continuity of Care Maturity Model and the Electronic Medical Record Adoption Model, are also evaluated for their best practices in conformity assessment governance. Additionally, pre-existing frameworks — like CASforEU, Label2Enable, and Antilope's QMSs approach — inform the overall structure and processes within the CAS.

By leveraging these foundations, the EHDS CAS ensures the integrity, interoperability, and continuous refinement of EHR systems and mobile health applications. It also enables the manufacturers of EHR systems to comply with their obligations outlaid in the EHDS regulation by performing a self-assessment in a regulated manner. Ultimately, this scheme fosters trust among stakeholders, stimulates innovation, and provides a harmonized approach to conformity assessment within the European digital health ecosystem.

Creation of a Conformance Assessment Scheme that ensures that any EHR system placed on the European market claiming EHDS Regulation conformity as a given actor will be able to seamlessly interoperate with any other EHR system claiming EHDS Regulation conformity as the complementary actor for the given action, no matter which organization in what geographic locality performed the conformity assessment for the given EHR systems. Meeting this goal will ensure that the fabric of EHDS is formed of EHR systems seamlessly interwoven with each other.

The updated and final version of the governance developed in WP 4.3 is included in this WP 8.2 document.

1.3.2 WP5 General requirements and metadata

WP 5.1 provides a detailed requirements framework designed for EHR system manufacturers, healthcare providers, policy makers and regulators to achieve compliance with the EHDS Regulation, focusing on Annex II's essential requirements.

WP5.1 includes systems intended for placing on the market, EHR systems offered as a service as defined in Article 1(1), point (b), of Directive (EU) 2015/1535 (EHR systems offered through the SaaS licensing), and EHR systems that are developed and used in-house (e.g. by healthcare providers themselves).

This deliverable divides the requirements into three groups:

- **General Requirements:** Covers system performance, patient rights, safety, security and the integrity and instructions for supply, installation, and operational procedures.
- **Interoperability Requirements:** Specifies the design and technical capabilities needed for the secure exchange and receipt of personal electronic health data, including structured data entry and prevention of undue access or export restrictions.
- **Security and Logging Requirements:** Defines robust mechanisms for identification and authentication of health professionals, comprehensive logging of access events, and the tools necessary for log review and analysis.

The deliverable further distinguishes between mandatory requirement and recommended best practices, with some of the latter also applying to the broader EHR system architecture. It emphasizes compliance with the EEHRxF and provides a list of baseline requirements for manufacturers on implementing interoperable, secure, and user-focused systems. By addressing performance, interoperability, security, and patient safety, the deliverable offers comprehensive guidance to meet the EHDS Regulation objectives and ensures an unified healthcare ecosystem across Member States.

Two annexes are attached to D5.1. Annex I provides illustrative examples for implementation of the interoperability component of EHR systems. Annex II outlines the requirements for Scrutiny Testing, as is part of the CAS developed in this document.

It needs to be pointed out that the EHDS requirements only apply for harmonised components of EHR systems as laid down in the Article 25 of the EHDS Regulation and not for other components and functions of the EHR systems.

The relevance of the requirements laid down in D5.1 need to be considered regarding the intended purpose of the EHR system. Moreover, the position of the EHR system within the regional, national or cross-border infrastructure needs to be considered meaning that the details of implementation will differ depending on where the EHR system's API is connected. WP 8.1 describes the classification and functional profiles in this regard.

It should be noted that the requirements set by the EHDS Regulation are deferred by the Art. 105 of this Regulation for certain EHR systems.

1.3.3 WP6 PS and eP/eD specifications, implementation guides

While WP5 outlines the general requirements for EHR systems, WP6 and WP7 focus on use case–specific specifications. WP6 defines the detailed EEHRxF-based requirements for the patient summary and for electronic prescriptions and dispensations. Combined with the classifications and functional profiles developed in WP8.1, WP6 establishes the applicable requirements for EHR systems to be used in conformity assessments for these specific use cases.

1.3.4 WP7 Lab, medical imaging and discharge report specifications, implementation guides

WP7 then focuses on the use case specific requirements for the laboratory results and reports, for medical images and reports and for discharge reports. The implementation guides developed in this WP give substance to the EEHRxF format for those use cases. Combined with the

classifications and functional profiles developed in WP8.1, these define the requirements to be used in the conformity assessment.

1.3.5 WP8.1 Classification and functional profiles

WP8.1 defines guidelines for classification and functional profiles for EHR systems. This deliverable focuses on reviewing functional models for EHR systems and providing a series of functional profiles to be used to support the self-assessment, classification, and conformance to EHDS requirements for EHR systems. Classification and functional profiles for EHR systems aim to add clarity to the application of EHDS requirements for different types of EHR systems. Each EHR system has a specific intended purpose of use in terms of use context, users and functional scope. Manufacturers and users of EHR systems need to be able to position their systems in relation to EHDS requirements to be able to fulfil them.

2. BEST PRACTICES

In the frame of research and pilot programs in the EU there are significant outcomes and best practices revealed that should essentially feed the EHR conformity assessment including all scopes and relevant applications.

A short list of the reference projects include:

2.1 EURO-CAS

The EURO-CAS project successfully developed a comprehensive and harmonised framework for assessing the interoperability of eHealth solutions across Europe, promoting seamless and secure healthcare information exchange.

2.1.1 The Conformity Assessment Scheme

The EURO-CAS project (the eHealth Interoperability CAS for Europe) involves the implementation of a sustainable Conformity Assessment Scheme for Europe (CASforEU). This scheme allows eHealth solutions to be tested for conformity with the eHealth standards and profiles defined in the Refined eHealth European Interoperability Framework (ReEIF). CASforEU establishes the conditions for regional, national, and cross-border projects in Europe to procure assessed products, ensuring seamless interoperability.
Many countries, as well as international standard bodies, have successfully developed their own CASs. CASforEU builds on these existing schemes to avoid duplicate accreditations, which increase costs and the time it takes to reach the market.

Based on recommendations from the Antilope project and the current state of interoperability testing in eHealth, CASforEU defines an operational CAS scheme that is ISO/IEC 17065 and ISO/IEC 17067 compliant. It requires test laboratories to be ISO/IEC 17025 accredited to meet the conformance requirements of the standards and profiles used by European eHealth projects and national and regional eHealth programmes. CASforEU serves the needs of a broad ecosystem of healthcare ministries, providers and users by collaborating with the healthcare IT industry to

ensure EHR systems, mobile eHealth applications, medical sensors, gateways and health and fitness services readily interoperate with each other. Established conformity assessment criteria provide healthcare providers with assurance that procured devices will perform as expected. Uniform criteria and test methods help assure manufacturers of broad market access. Users benefit from open market competition and have more choice.

2.1.2 Scheme Scope

CASforEU conformity assessment includes conformance and interoperability testing. Conformance testing ensures that products conform to industry standards and specifications when connected in a healthcare system.

Interoperability testing demonstrates that products are able to interoperate with each other or with test artifacts when connected. Interoperability for purposes of conformity assessment is limited to procedures that run the product though the normal behaviours expected for the product type.

The following types of testing are specifically out of scope: non-functional, safety and efficacy, user interface, and white-box.

A product is declared conforming to a set of standards and specifications selected in the CASforEU scheme when:

- The Summary Test Report provided by the Execution Entity demonstrates that all required tests cases for the identified set of standards and specifications are passed;
- Payment of the assessment fee is received.

2.2 IHE Conformity Assessment Scheme

IHE International administers the IHE-CAS[9], which forms the basis for IHE Conformity Assessment Programs and any official certification of conformance to IHE Profiles associated with such testing programs.

[9] https://www.ihe.net/testing/conformity-assessment/

CASs are usually split into two parts. While the first part (CAS-1) draws the establishment of the scheme and its governance, including the process to evaluate the systems under test, and the information to be included in the test report; the second part (CAS-2, as referred to hereafter) identifies the features that are covered by the scheme and how to, practically, demonstrate that an EHR product complies with the applicable standards and specifications.

On the basis of the CAS, test laboratories are accredited in accordance with the ISO/IEC 17025 standard, General Requirements for Competence of Calibration and Testing Laboratories. Test reports produced in accordance with this standard are accepted worldwide. IHE International authorizes designated test laboratories accredited under this standard to assess the conformity of products with selected IHE profiles.

Profiles currently available for testing under the IHE International Conformity Assessment program are:

- Audit Trail and Node Authentication (ATNA)
- Consistent Time (CT)
- Cross-Community Access (XCA)
- Cross-Community Access for Imaging (XCA-I)
- Cross-Community Patient Discovery (XCPD)
- Cross-Enterprise Document Sharing (XDS.b)
- Cross-Enterprise Document Sharing for Imaging (XDS-I)
- Cross-Enterprise User Assertion (XUA)
- Device Enterprise Communication (DEC)
- Laboratory Analytical Workflow (LAW)
- Patient Administration Management (PAM),
- Patient Demographics Query (PDQ),
- Patient Demographics Query HL7 v3 (PDQV3),
- Patient Identifier Cross-Referencing (PIX)
- Patient Identifier Cross-Referencing HL7 v3 (PIXV3)

- Point-of-Care Infusion Verification (PIV)

2.2.1. Scope and Structure of CAS-2

The CAS-2:

- Reminds the reader about the versions of the specifications that are covered by the scheme (e.g. HL7 FHIR Implementation Guides, IHE Profiles),
- Defines the test plan to be executed.
- Lists the test tools (including their version) that shall be used to execute the test cases.

All the test cases are uniquely identified, and their versions are tracked down. The document is organised in a way that the test cases are grouped by feature (aka Profile/Actor/Option combination). If several versions of the scheme are issued, a change log section shall allow the reader to conduct a gap analysis and identify which test case shall be run again. The CAS-2 structure will align with the EHDS Regulation, particularly Annex II, which defines the harmonised EHR components. Each domain (e.g. Laboratory Results, Imaging, Vaccination Records, Discharge Letters) will be mapped to the corresponding specification and associated technical assertions.

2.2.2 Test Plan Development and Requirement Coverage

To establish the content of the CAS-2, the first step aims at identifying the version of the reference specifications that the systems under test (SUT) shall conform to. Those specifications shall be stable, meaning that it is admitted that backward compatibility will be preserved in future releases.

From these, the testable requirements shall be extracted and used for the test design and permit the test designers to know exactly what is to be tested.

The test designers write the test cases and identify the test tools that are needed to execute them. Each test case will cover one to many requirements. The full test plan (all the test cases) shall cover 100% of the identified requirements.

2.2.3 Tooling and Evidence Management

Once the coverage is complete and the test cases have been reviewed, the test cases are entered in a test management tool while the pointers to the test cases and to the relevant test tools are gathered in the CAS-2 document. The test management tool might be bound to a requirement management tool, to offer a mean to trace back the requirements from the test cases. In addition, the test management tool allows the applicant to generate the test plan based on the capabilities of his system under test. This tool is also the place where the applicant will execute the test cases and report evidence that demonstrate the correct implementation of the specifications in his product.

If test cases are automated, the applicant can conduct self-assessment, otherwise, it is recommended that the results of the test cases are reviewed by a neutral third party. The process is to be defined as part of CAS-1 document.

In addition to the test cases, requirements can be laid down to help the applicant with preparing his product for the conformity assessment.

2.2.4 Stakeholder Engagement

To ensure CAS-2 is practical and aligned with industry needs, stakeholder involvement is essential. The contractor will support the organisation of workshops and collaborative review sessions with solution providers, Member State authorities, and technical experts.

The objective is to validate test assertions, assess the feasibility of tooling, and ensure alignment with both the EUROCAS project outcomes and the MyHealth@EU ecosystem.

2.2.5 Example Structure of the CAS-2 Document

As per the content, the CAS-2 will first list the specifications with a precise reference, including the version that is covered by the document. For each part of the specification, the section that includes the tests is referenced. As shown below:

EEHRxF category	Link to specifications	Version assessed in this document	Test cases
Laboratory result report	[Link to IG]	[Version]	Section X.y.z

Each “test cases” section contains a table that refers all the test cases to be executed.

X.y.z

Test case permanent ID	Test case name	Test case summary	Test case and test data version
000001	A first test case	This test case aims at demonstrating requirement XXX	Version 1.0 Edited on 13/05/2025 10:48:55 CEST
000002	A second test case	This test case aims at demonstrating requirement YYY	Version 1.0 Edited on 13/05/2025 10:28:55 CEST
000003	A third test case	This test case aims at demonstrating requirement ZZZ	Version 1.0 Edited on 12/05/2025 11:28:55 CEST

Additionally, a document with all the details about the test cases (name, version, description, steps to execute, evaluation criteria) can be referenced in the section for the reader to download it without the need to log into the test management tool.

Finally, all the test tools needed to execute the test plan shall be clearly identified, and reference the sections that they cover.

Tool name	Classification	Version	Covered sections
Test management system	Test management tool	10.1.1	All
Content validator AB	Conformance checker	2.0.2	X.y.z

2.3 Label2Enable CAS

The quality requirements described in the ISO/TS 82304-2:2021 quality assessment framework form the basis for this Certification scheme. With subject matter experts in the very diverse quality requirements and legal counsel, related EU level legislation, standardisation, scientific research findings and common practice were explored to inform assessment methods, training requirements, what is considered sufficient evidence, referred to as the pass / fail, and reassessment policies.

To explore common practice, a comparison was made of the requirements of ISO/TS 82304-2 and EUnetHTA core model, and 5 European frameworks, being the Dutch Leidraad, German DiGA, Finnish Digi-HTA, French PECAN and English DAQ / DTAC. Interviews with the related organisations were and are used to gather the needed background and detail information.

To test and evolve the scheme 24 intentionally very diverse apps were assessed, each by two different Conformity Assessment Bodies from a group of five from five different countries. The consistency of their assessment results was analysed and used to evolve the scheme and thus achieve the consistency in results that promotes cross country recognition and ultimately in Europe and potentially beyond a digital single market with room for context-specific additional requirements. Efficiency, and if the documentation was self-explanatory, were measured and consistency between manufacturer responses and assessor results were analysed and discussed with manufacturers to realise a proportional, scalable, and self-explanatory Certification scheme.

As a final step, relevant EU authorities and key stakeholder bodies will be consulted to verify if the assessment provides the confidence that the certified health and wellness apps conform to the specified requirements and adequately and proportionally facilitates decision-making on (promoting) their use. Potential for more efficient assessment methods is explored to guide future development of this Certification scheme.

2.3.1 Operation of the Certification scheme

The Scheme Owner (SO) shall publish this Certification scheme and its reference and guidance documents.

The Stakeholders and Expert Organisation (SEO) through its scientific committee (subject matter experts) and steering board (key stakeholder representatives) shall maintain the scheme, the full version of the App assessors Handbook, and the reference and guidance documents. The SEO shall contract the Certification Bodies (CBs).

The CBs shall certify the products, issue the Certificate of conformity, and contract the Conformity Assessment Bodies.

The CABs shall execute the conformity assessments, supply the Statement of conformity and ensure the Certification agreement is signed by the Client.

The Client shall supply the CAB with the signed copy of the Certification agreement, responses to the ISO/TS 82304-2 requirements, access to the product and the evidence pack, notifying the CAB of changes affecting product conformity and applying the mark of conformity as specified.

Figure 1 Operation of this Certification scheme

2.3.2 Outline of the Certification scheme

The following functions, activities and elements are further described in this document:

a) Selection

The Client may apply for a Label2Enable Certification. The Conformity Assessment Body (CAB) shall supply the necessary information such as:

- the quality requirements as described in ISO/TS 82304-2:2021.
- this Certification scheme.
- the relevant guidance documents.
- the Certification agreement.
- the Certification procedures.
- the conformity assessment requirements and procedures.

Signing the Certification agreement is a prerequisite and confirms the Client shall comply to the Certification and conformity assessment requirements described in this Certification scheme.

The Client shall supply responses to the ISO/TS 82304-2 requirements, the evidence specified in ISO/TS 82304-2 and additional guidance and give the CAB access to the product for conformity assessment.

Determination

The CAB shall perform the conformity assessment as described in this Certification scheme. The assessment methods, the evidence and what is considered pass / fail are described in the App assessors Handbook.

After the conformity assessment the CAB shall supply the CB with a Statement of conformity.

Review of the conformity assessment results

The CB shall review the Statement of conformity provided by the CAB, conform the procedure provided by the SEO.

Decision on Certification and attestation of conformity

The CB shall decide on and issue the Label2Enable certificate as attestation of conformity for the requirements described in this Certification scheme which are fulfilled, conform the procedure provided by the SEO.

The procedure and actions to be taken by the parties involved in this Certification scheme if the decision is not to issue a Certification of conformity shall be defined by the SEO.

b) Licensing

After a positive decision of the CB to issue the certificate, the Client shall receive the Certificate of conformity and the related ISO/TS 82304-2 health app quality label (quality label) and health app quality report (quality report).

As of the date the CB issues the certificate the Client is allowed to publish the quality label and quality report. The publicity conditions and what is considered misuse of the certificate and reason to withdraw the certificate, quality label and quality report shall be described in the Certification agreement between the CAB and the Client.

c) Surveillance - suspending and the withdrawing of the certificate – managing changes affecting the Certification

The procedures for surveillance, suspending and withdrawing the certificate and managing changes affecting the Certification shall be provided by the SEO and shall be part of the Certification agreement.

2.4 myhealth@EU – eHealth Digital Service Infrastructure

The current testing tools used for the myHealth@EU services will be taken into consideration. The eHealth Digital Service Infrastructure enables the cross-border exchange of health data

within the EU, primarily for **healthcare providers** and patients. It facilitates the interoperability of EHRs, ensuring health data can be accessed securely across borders10. This gives EU countries the possibility to exchange health data in a secure, efficient and interoperable way. Citizens can easily recognize the availability of the services under the brand "MyHealth@EU". The following 2 electronic cross-border health services are currently being introduced in all EU countries:

- **ePrescription and eDispensation** (eHealth Network guidelines on ePrescription, Release notes) allows EU citizens to obtain their medication in a pharmacy located in another EU country, thanks to the online transfer of their electronic prescription from their country of residence where they are affiliated, to their country of travel.
- **Patient Summaries** (eHealth Network guidelines on Patient Summary, Release notes) provide information on important health related aspects such as allergies, current medication, previous illness, surgeries, etc. It is part of a larger collection of health data called an EHR. The digital Patient Summary is meant to provide doctors with essential information in their own language concerning the patient, when the patient comes from another EU country and there may be a linguistic barrier.

In the long term, **medical images, lab results and hospital discharge reports** will also be available across the EU, with the full health record to follow at a later stage. The exchange of ePrescriptions and Patient Summaries is open to all the EU countries. While primarily focused on healthcare providers, wellness applications could benefit from e HDSI's standards for data exchange. The myHealth@EU testing tools are provided as open-source based on the use of the open-source Gazelle software. Gazelle has been recognised as a GITB compliant test tool aligned with ITB test tools. Gazelle is also used for performing projectathon for the OOTS specifications maintained by DG DIGIT.

[10] https://health.ec.europa.eu/ehealth-digital-health-and-care/electronic-cross-border-health-services_en

656

3. EHDS CONFORMITY ASSESSMENT SCHEME GOVERNANCE

The EHDS CAS ensures the integrity, interoperability, and continuous refinement of EHR systems. It also enables the manufacturers of EHR systems to comply with their obligations outlined in the EHDS regulation by performing a self-assessment in a regulated manner. Ultimately, this scheme fosters trust among stakeholders, stimulates innovation, and provides a harmonized approach to conformity assessment within the European digital health ecosystem.

This chapter describes the governance of the EHDS-CAS and the rules and procedures applicable to the actors responsible for its implementation. Chapter 4 subsequently elaborates on the technical content of the scheme: the object of conformity assessment and the testing methodology for the actual performance of the conformity assessment.

3.1 Actors engaged in the EHDS CAS Governance for EHR Systems supporting primary care

An overview of these actors and their primary relationships is summarized by the figure 2 below.

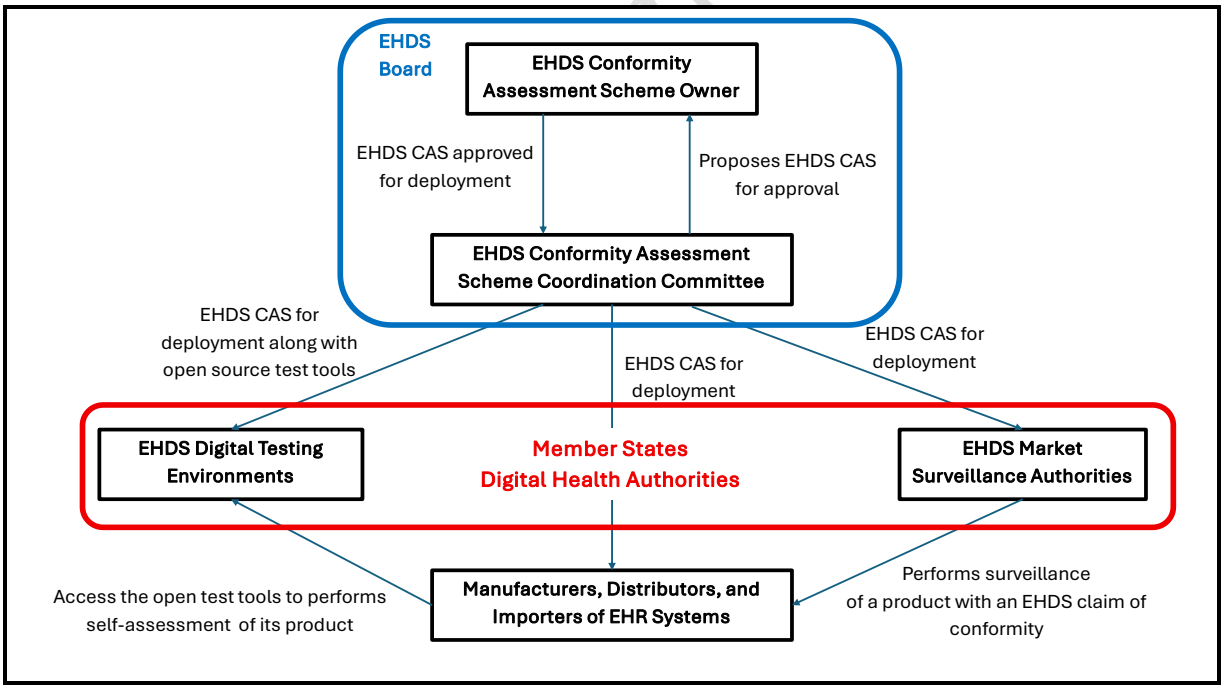


Figure 2: Overview of the main actors participating in the EHDS CAS

The legislative basis for this EHDS conformity assessment conformance is provided in Articles 30, 39, 40 European digital testing environment in Section 2 and 3 of the EHDS regulation. These actors are identified implicitly or explicitly in the EHDS regulation (See Appendix II).

The governance framework employs a layered and participatory approach, engaging multiple entities to ensure clarity of roles, responsibilities, and accountabilities.

3.1.1 The EHDS Conformity Assessment Scheme Owner (EHDS Board.CASO)

The EHDS Conformity Assessment Scheme Owner (CASO) is the actor ultimately responsible for the definition, evolution, placing in operation and interpretation of the EHDS CAS. It approves modifications or new versions of the schemes as the common specifications evolve. The EHDS CASO relies on the EHDS Conformity Assessment Scheme Coordination Committee (CASCC) to coordinate the implementation of the policy decisions made by the EHDS CASO.

The CASO needs to be an operational entity and is advised to be the EHDS board.

3.1.2 The EHDS Conformity Assessment Scheme Coordination Committee (EHSD Board.CASCC)

The CASCC, operating under the EHDS CASO, serves as the central coordinating body for EHDS conformity assessment activities. It is composed of representatives from Member States, EU institutions, as decision makers. It may consult, as needed, industry trade associations, professional associations and standards organisations.

The CASCC ensures that the strategic direction and policy alignment set by the Scheme Owner is implemented and harmonises testing and conformity assessment activities, in particular the development of the European digital testing environment for the assessment of harmonised software components of EHR systems.

The CASCC ensures consistency of the testing environments and conformity assessment processes identified by the EHDS regulation. The CASCC is also responsible for reviewing the information provided by Member States to the Commission about their digital testing environments for conformity with the common specifications.

Finally, it shall allow for a feedback loop and pace the continuous improvement of the EHDS CAS, as the common specifications evolve.

Following a revision of the EHDS CAS, the CASCC shall propose to the EHDS CASO a timeframe within which manufacturers shall update their EHR system and conduct a self-assessment and possible additional tests in the digital testing environment.

The CASCC may orchestrate a dynamic, iterative improvement cycle to guide the ongoing governance and supports sustainable interoperability growth.

Note: Such an improvement cycle may rely on a Plan-Do-Check-Act model:

1. Plan: Stakeholder engagement—through industry workshops, focus groups, and technical forums—enables the identification of best practices and the resolution of emerging challenges and identifying areas for enhancement.
2. Do: The CAS adapts to evolving technologies, updating IHE profiles, testing tools, and accreditation criteria to keep pace with the latest developments in digital health.
3. Check: Stakeholders, including Member States, standards bodies, and industry representatives, periodically review the CAS's performance, identifying what we learned.
4. Act: Annual revision cycles, combined with public consultations, ensure that lessons learned are integrated into updated governance policies, enhancing reliability, scalability, and resilience over time.

3.1.3 The EHDS Digital Testing Environments (DTE)

European digital testing environments should be set up to provide automated means to test whether the functioning of the harmonised software components of an EHR system is compliant with the requirements laid down in the EHDS Common Specifications. Member States shall operate these digital testing environments for the assessment of harmonised software components of EHR systems. Such digital testing environments shall comply with the common

specifications for the European digital testing environment. These testing environments shall operate under ISO/IEC 17025 or ISO/IEC 17020 accreditation, ensuring competence, impartiality, and consistency in their evaluations. CASCC should oversee the accreditation of Testing Environments for EHDS, to ensure harmonisation of testing procedures across Europe. Such Digital Testing Environments for EHDS ensure harmonisation of testing procedures across Europe.

To support that process, the Commission should develop the necessary software for the testing environments and make it available as open source. Member States should be responsible for the operation of digital testing environments, as they are closer to manufacturers and better placed to support them. Manufacturers should use those digital testing environments to test their products before placing them on the market while continuing to bear full responsibility for the compliance of their products.

Before placing EHR systems on the market, manufacturers shall use the digital testing environments offered for the assessment of harmonised software components of EHR systems.

The results of that assessment shall be included in the technical documentation of the EHR systems (See section 3.1.5). The software components of the EHR for which the results of the assessment are positive shall be presumed to be in conformity with the EHDS Regulation.

The EHDS CAS imposes a mandatory self-assessment of conformity as the basis for an EU declaration of conformity by the manufacturer. This should ensure that those requirements are fulfilled in a proportionate way, while avoiding an undue burden on Member States and manufacturers.

Member States will remain competent to define requirements relating to any other software components of EHR systems besides harmonised software components, and the terms and conditions for connection of systems operated by healthcare providers to their respective national infrastructures. Member States should not impose any specific obligations for testing environments in regard to compliance with the EHDS specifications on harmonised software

components of EHR systems to ensure the effective operation of a European single market for such devices.

The EHDS-CAS introduces an EHDS Seal of Compliance upon successful self-assessment. The Testing Environment produces a Test Report Summary (TRS). The seal is a mark of trust and interoperability readiness, signifying compliance with EHDS standards. The seal shall indicate the actor(s) where the transactions necessary for EHDS compliance are met by the given system. The seal is issued by the testing environment, and the manufacturer can include a reference to the seal in its own declaration of conformity.

EHDS Article 49 states that the commission shall establish and maintain a publicly available EU database with data on EHR systems for which an EU declaration of conformity has been issued, and for wellness applications for which a label has been issued. The manufacturer is responsible for entering the required data into the database before placing its system on the market or putting it into service. This publicly accessible registry promotes transparency, stakeholder confidence, and market visibility.

3.1.4 The EHDS Market Surveillance Authorities (MSA)

Member States shall designate the market surveillance authority or authorities responsible to enforce the obligations set forth in this section. The responsibilities of the market surveillance authority are specified in EHDS article 45.

Market surveillance authorities are empowered to request cooperation of manufacturer or another economic operator. In case a manufacturer fails to cooperate or if the information and documentation they have provided is incomplete or incorrect, the market surveillance authority may take all appropriate measures to prohibit or restrict the relevant EHR system from being made available on the market until the manufacturer or the economic operator concerned cooperates or provides complete and correct information, or to recall or withdraw such EHR system from the market.

For medical devices, in vitro diagnostic medical devices or high-risk AI systems referred to (See Article 27 of the EHDS regulation), the responsible authorities for market surveillance shall be those referred to in Article 93 of Regulation (EU) 2017/745, Article 88 of Regulation (EU) 2017/746 or Article 70 of Regulation (EU) 2024/1689, as applicable.

Where a market surveillance authority of one Member State has reason to believe that an EHR system poses a risk to the health, safety or rights of natural persons or to the protection of personal data, that market surveillance authority shall carry out an evaluation in relation to the EHR system concerned covering all relevant requirements laid down in the EHDS Common Specifications.

Where a market surveillance authority makes a finding of non-compliance, it shall require the manufacturer of the EHR system concerned, its authorised representative and all other relevant economic operators to take, by a specific deadline, adequate corrective action to bring the EHR system into conformity. Such findings of non-compliance include, but are not limited to, the following:

a) the EHR system is not in conformity with essential requirements laid down in the common specifications referred to in Article 36 of the regulation;
b) the technical documentation is not available, not complete or not in accordance with Article 37;
c) the EU declaration of conformity has not been drawn up or has not been drawn up correctly in accordance with Article 39;
d) the CE marking of conformity has been affixed in breach of Article 41 or has not been affixed;
e) the registration obligations of Article 49 have not been fulfilled.

Where, within a specific duration, of receipt of the above information, no objection has been raised by either a market surveillance authority from another Member State or the Commission in respect of a provisional measure taken by a market surveillance authority, that measure shall be deemed justified.

Where a manufacturer or another economic operator fails to cooperate with a market surveillance authority or where the information and documentation they have provided is incomplete or incorrect, the market surveillance authority may take all appropriate measures to prohibit or restrict the relevant EHR system from being made available on the market until the manufacturer or the economic operator concerned cooperates or provides complete and correct information, or to recall or withdraw such EHR system from the market.

Where the manufacturer of the EHR system concerned, its authorised representative or any other relevant economic operator does not take adequate corrective action within a reasonable period, the market surveillance authorities shall take all appropriate provisional measures to prohibit or restrict the EHR system from being made available on the market of their Member States, or to recall or withdraw the EHR system from that market.

The market surveillance authorities shall inform the Commission and the other Member States' market surveillance authorities, without delay, of those provisional measures. That information shall include all available details, in particular the data necessary for the identification of the non-compliant EHR system, the origin of that EHR system, the nature of the non-compliance alleged and the risk involved, the nature and duration of the measures taken by the market surveillance authorities and the arguments put forward by the relevant economic operator. In particular, the market surveillance authorities shall indicate whether the non-compliance is due to any of the following:

a) failure of the EHR system to meet the essential requirements set out in Annex II of the EHDS Regulation;
b) shortcomings regarding the common specifications referred to in Article 36.

Where the market surveillance authorities of a Member State consider that the non-compliance of the EHR system is not limited to their national territory, they shall inform the Commission and the other Member States' market surveillance authorities of the results of the evaluation.

Where, under Article 44(2) and Article 45(3) of the EHDS Regulation, objections are raised against a national measure taken by a market surveillance authority, or where the Commission considers a national measure to be contrary to Union law, the Commission shall without delay enter into consultations with that market surveillance authority and the relevant economic operators and shall evaluate the national measure concerned. On the basis of the results of that evaluation, the Commission shall adopt an implementing decision determining whether the national measure is justified. That implementing decision shall be adopted in accordance with the examination procedure referred to in Article 98(2) of the regulation. The Commission shall address its implementing decision to all Member States and shall immediately communicate it to them and to the relevant economic operators.

1. If the national measure is considered justified by the Commission, all Member States concerned shall take the necessary measures to ensure that the non-compliant EHR system is withdrawn from their market, and shall inform the Commission accordingly.
2. If the national measure referred to in paragraph 1 is considered unjustified by the Commission, the Member State concerned shall revoke that measure.

3.1.5 The Manufacturers, Distributors, and Importers of EHR Systems (MDI-EHRS)

Article 30 of the EHDS regulations places an obligation on manufacturers of EHR systems to ensure conformity with relevant specifications and paragraph 3 of article 40 specifies that they should do this by using the digital testing environments.

Recitals 36 and 39 make it clear that the intention of EHDS is to provide an opportunity (and also an obligation) for self-assessment, with ultimately the manufacturer being responsible for the accuracy of its declaration for conformity.

The CAS governance should contain the necessary elements to ensure that manufacturers conduct their self-assessment in compliance with the EHDS regulation.

Manufacturers of EHR systems shall include the results of the assessment in their technical documentation. The EHDS-CAS should require that these results include detailed Test Report Summaries (TRS) to confirm the reliability and accuracy of assessments.

The manufacturer is responsible for entering its EU declaration of conformity into the publicly available EU database with data on EHR systems, before placing its system on the market or putting it into service. This publicly accessible registry promotes transparency, stakeholder confidence, and market visibility.

Manufacturers of EHR systems placed on the market or put into service shall report any serious incident involving an EHR system to the market surveillance authorities of the Member States where such serious incident occurred and of the Member States where such EHR systems are placed on the market or put into service. That reporting shall also include a description of the corrective action taken or envisaged by the manufacturer. Member States may provide for users of EHR systems placed on the market or put into service to be able to report such incidents.

3.1.6. EHDS-CAS process and methodology

This part describes the process and methodology and elements that should be included in EHDS-CAS. It describes how a manufacturer should conduct a self-assessment, elaborates on guarantees for continued compliance and recommends a reporting template.

3.1.6.1 Object of Conformity

The object of conformity is an EHR system as defined in the EHDS, which is to be put on the market. The manufacturer of an EHR system shall demonstrate that the essential requirements referred to in Art. 36 and Annex II of the Regulation are met. In the sense of section 3 of the Regulation, the conformity assessment is only relevant for the harmonized components, namely the interoperability component and logging component. The EHR system will be classified according to the classification and functional profiles as elaborated in WP8.1, leading to specific requirements for that EHR system. The essential requirements set out in Annex II of the Regulation are divided into three categories: general, requirements for interoperability and

requirements for security and logging. Detailed requirements and thier applicability are the subject of deliverables of other WPs or tasks in Xt-EHR, particularly WP 5, WP 6, WP 7 and WP 8.

3.1.6.2 Process of conducting self-assessment

The following steps should guide the manufacturer in applying this CAS:

1. Determine the classifications and functional profiles of the EHR-system(s) (WP8/D8.1).
2. Define which requirements apply to the EHR system(s) (WP 5, WP 6, WP 7).
3. Define which level of conformity applies (WP8/D8.1).
4. Prepare a test plan identifying which requirements (verifiable assertions) should be tested in the digital testing environment.
5. Test the EHR system(s) using a digital test environment and include automatically and manually generated results when successful in technical documentation.
6. Provide evidence of conformity for non-testable requirements.
7. Prepare Technical Documentation (EHDS article 37).
8. Prepare Information Sheet (EHDS article 38).
9. Prepare EU Declaration of Conformity (EHDS article 39).
10. Register EHR system + declaration in Register (EHDS article 49).
11. Affix the CE-mark (EHDS article 41).
12. Keep EU Declaration of Conformity up-to-date.
13. When necessary, particularly is case of a substantial change, re-assess conformity of the EHR system.

A substantial change of an EHR system is when these three conditions are met:

(i) it modifies the original intended functions, type or performance of the product and this was not foreseen in the initial risk assessment;

(ii) the nature of the hazard has changed or the level of risk has increased because of the update; and

(iii) the product is made available / put into service.

3.1.6.3 Test Report

The results of testing in the digital testing environment shall be included in the technical documentation of the manufacturer (art. 37 EHDS and art. 40.3 EHDS). Upon successful testing, the Digital Testing Environment should therefore produce a Test Report Summary (TRS).

It is important that the information included in the technical documentation is comprehensible for other parties, including health care institutions. Other parties must be able to easily understand the results of the tests and if a product complies with relevant standards. In order to do so, a shared template for the TRS is advisable and the following elements should be included:

a) The version of the software product and/or service;
b) A title (e.g., "Test Report");
c) The modules/tests that have been performed;
d) A specification of the relevant level in the maturity model and specification of the type of system;
e) An assessment or declaration whether the test was successfully completed or not;
f) The date on which the test was conducted;
g) The name and address digital testing environment that is used for the testing;
h) A unique identifier ensuring all parts are included in the complete report, with a clear indication of the end;
i) An identification of the method used;
j) A description, clear identification, and, if necessary, the condition of the object;
k) The date of receipt of the object(s) to be tested and the date of the test, if this is critical for the validity and application of the results;
l) The date(s) of execution of the inspection activities;
m) The date of issuance of the report;
n) A statement indicating that the inspection results apply only to the tested objects;
o) The results, including measurement units where applicable;
p) Additions to, deviations from, or exclusions of the method;

q) An identification of the person(s) releasing the report;

r) A clear indication if the inspection results originate from external suppliers.

In addition to the above requirements, test reports shall include the following when necessary for the interpretation of test results:

a) A statement of conformity regarding compliance with requirements or specifications;

b) If applicable, measurement uncertainty, expressed in the same unit as the measured quantity or with a term related to the measured quantity (e.g., percentage). Measurement uncertainty may be relevant for performance requirements.

3.1.6.4 Declaration of Conformity

EHDS Regulation Annex IV provides requirements on the information included in the declaration of conformity:

a) The name of the EHR system, version and any additional unambiguous reference allowing identification of the EHR system.

b) Name and address of the manufacturer or, where applicable, its authorised representative.

c) A statement that the EU declaration of conformity is issued under the sole responsibility of the manufacturer.

d) A statement that the EHR system in question is in conformity with the provisions laid down in Chapter III and, if applicable, with any other relevant Union law that provides for the issuing of an EU declaration of conformity, complemented by the result from the testing environment mentioned in Article 40.

e) References to any relevant harmonised standards used and in relation to which conformity is declared.

f) References to any common specifications used and in relation to which conformity is declared.

g) Place and date of issue of the declaration, signature plus name and function of the person who signed and, if applicable, an indication of the person on whose behalf it was signed.

h) Where applicable, additional information.

The manufacturer is responsible for an up-to-date and correct declaration of conformity and for continued compliance with the EHDS Conformity Assessment. This also includes an updated self-assessment.

3.1.6.5 Continued compliance

Quality management

According to article 30, section 2, manufacturers of EHR systems shall ensure that procedures are in place to ensure that the design, development and deployment of the harmonised software components of an EHR system continue to comply with the essential requirements. A good practice to achieve this is to develop and validate a product under a QMS. A well-functioning QMS enables the manufacturer to be in control of the quality of its products, and, in case of software development, to be in control of all the changes in product and in the context. Besides, a QMS may help manufacturers to respond more easily to an evaluation by a Market Surveillance Authority. A QMS is not mandated by the EHDS Regulation.

A QMS certified under accreditation in accordance with ISO 9001, ISO 13485, or an equivalent standard is considered to be a best practice. The scope of the QMS should include the development, production, and modification of the software system.

Changes in context

After an initial self-assessment, including testing in the digital test environment, changes may occur to the EHR system or to the normative documents such as the Common Specifications or underlying standards. These changes might lead to the need for retesting. This paragraph describes when retesting is necessary.

1. Changes in the EHR system;

If a change occurs in the (technical) design, the manufacturer shall assess whether this change could affect the harmonised components for interoperability or logging.

If the change does not impact the harmonized component for interoperability or logging, no activities are required to reassess interoperability or logging. It might be relevant to update the technical documentation.

The manufacturer shallt maintain a record of such changes, including the justification that the change does not impact interoperability. This is a good practice and part of the 'management of change' process, see also the requirements for the QMS.

If a change does impact interoperability, i.e. in case of substantial change, the manufacturer shall reassess conformity of the EHR system including performing (or commission) a test in the digital testing environment to verify continued compliance with all interoperability requirements. These tests shall be performed before the product is made available to a customer. The test results shall be included in the technical documentation, as part of the self-assessment.

2. Changes in the Common Specifications or in the underlying standards (HL7 FHIR Implementation Guides, IHE Profiles, etc.);

When a normative document (Common Specification or underlying IG or Profile) is revised and the EHDS CAS is updated, the manufacturer shall assess whether the EHR system complies with the updated CAS/standard. This means that the product shall be retested in the digital testing environment. The test results shall be included in the technical documentation, as part of the self-assessment. This is required to demonstrate continued interoperability of the EHR system.

The manufacturer is responsible for monitoring the release of updates to the IHE-CAS and their applicability deadlines released by the EHDS CASCC.

Following a revision of the CS or standards, the European Commission or standards owner establishes the timeframe within which manufacturers shall update the EHR system and conduct a self-assessment and additional tests in the digital testing environment.

3. Changes in ownership or structure of management manufacturer;

The manufacturer shall have procedures in place to re-evaluate the validity of the declaration of conformity in case there are changes to the ownership or structure of the management of the manufacturer. The manufacturer is in all events responsible for an up to date EU Declaration of Conformity.

3.2 Conclusion

The EHDS CAS governance provides a cohesive, transparent, and trusted approach to governing interoperability and compliance across Europe's digital health landscape. Grounded in internationally recognized standards and informed by proven maturity models, this governance model ensures that EHR systems, and related digital health tools meet the highest quality benchmarks. Through a structured self-assessment, rigorous conformity testing, and continuous improvement cycles, the EHDS CAS elevates digital health innovation, strengthens stakeholder confidence, and supports the European Union's ongoing pursuit of integrated, patient-centered care for all citizens.

By fostering harmonisation, cooperation, and adherence to shared guidelines, the EHDS CAS serves as a vital instrument in achieving the EHDS vision: enabling secure, seamless, and meaningful health data exchange that ultimately improves health outcomes and quality of care across Europe.

4. CONFORMITY ASSESSMENT NECESSARY COMPONENTS (CONTENT)

Manufacturers of EHR systems will have to take some steps before they can place EHR systems on the market. They shall make sure that their EHR system complies with the requirements of the EHDS Regulation:

- The two harmonised components shall be supported by the system.
- The digital testing environment should be used to prove that it does so by passing the relevant tests.
- Draw up the technical documentation required under Article 37 and provide the information sheet required under Article 38.
- Draw up the EU declaration of conformity in accordance with Article 39.
- Affix the CE marking in accordance with Article 41.
- Register your system in the Article 49 database.

This section of the conformity assessment document describes:

- The set of specifications selected for Conformity assessment testing.
- The high-level testable assertions that shall be fulfilled by the EHR systems within the scope of the EHDS regulation
- The test cases including test cases, test tools and test data.

This section is built upon the governance and processes of conformity assessment specified within the previous chapters of this document. It provides requirements for assessing product conformance to the selected EHDS specifications.

4.1 Resources

4.1.1 Data-Level Obligations

This chapter lays the groundwork for ensuring that every data element in a heterogeneous, multivendor health information ecosystem behaves predictably and correctly, underpinning patient safety, seamless interoperability, and adherence to legal mandates. At its core is the Data

Level Obligations Model—a set of element level rules, drawn from the Xt-EHR logical models, that specify exactly how systems must capture, store, export, display, process, or transmit each piece of information. By treating each obligation (able-to-populate, populate-if-known, display, process, no-alter, alter) as discrete, testable requirements, implementers gain a clear path to automated instance validation and functional testing, while auditors obtain an objective basis for verifying technical conformance and regulatory compliance.

To apply these rules sensibly across the spectrum of EHR deployments, systems are first classified by their role(s)—Producer, Consumer, and Exchanger—and by scope (departmental modules, local/provider level platforms, shared registries, or crossborder gateways). For example, a laboratory analyzer acting as a Producer must guarantee mechanisms to set every relevant element (able-to-populate) and include any known values in outgoing messages (populate-if-known) but need not enforce display or processing rules. In contrast, a regional immunization registry functioning as both Consumer and Exchanger must faithfully render incoming data (display/process) and forward elements marked no-alter without modification, yet has no populate duties of its own.

Underpinning these obligations is a precise use of RFC 2119[11] terminology—SHALL for mandatory requirements, SHOULD for strong recommendations (permitting documented exceptions), and MAY for optional behaviors—ensuring clarity of intent and conformance assessment criteria. Complementing the obligation model, the chapter distinguishes “conformance” (following the technical specification through instance validation, audit trail- checks, and targeted test scenarios) from “compliance” (fulfilling all applicable legal, regulatory, and contractual mandates such as General Data Protection Regulation (GDPR) or EHDS audit trail- obligations).

To guide implementers in selecting appropriate levels of structure, three conformance tiers are defined: Level 1 (free text narrative), Level 2 (sectioned narrative), and Level 3 (fully structured coded data), each reflecting progressively stringent requirements for discrete element capture

[11] https://datatracker.ietf.org/doc/html/rfc2119

and machine actionable interoperability. Finally, the model makes a clear distinction between business level actors (e.g., prescribers, nurses, patients) and the system level roles their software components play, ensuring that conformance is assessed end-to-end—from user data entry through serialization, exchange, and downstream processing—so that every obligation is met wherever and whenever data flows.

For authoritative definitions and the full list of obligation codes (e.g., SHALL: populate-if-known, SHOULD: able-to-populate, SHALL: no-alter), see the HL7 FHIR Obligation Codes ValueSet[12].

4.1.1.1 Classification of EHR Systems by Role and Scope

In this section we distinguish four broad categories of EHR systems—departmental modules, local/provider-level platforms, shared/regional registries, and cross-border gateways—and map each to the Producer, Consumer, and Exchanger roles in the Conformance Framework. Understanding these types and their primary functions ensures we apply only the relevant data-level obligations to each system.

The Data-Level Obligations Model itself is standardized across all EHR types, but which obligations actually apply will vary depending on the role(s) each system plays:

- **Intra-organisational ("departmental") modules** (e.g. a lab analyzer or imaging PACS) act primarily as **Producers** (and sometimes Exchangers). They must support **able-to-populate** and **populate-if-known** for any data they originate, and **no-alter** if they forward results on to another system.

- **Local EHRs** run by a single provider typically play all three roles—**Producer**, **Consumer**, and **Exchanger**. They implement **able-to-populate**/**populate-if-known** for data entry, **display/process** for data they consume, and **no-alter** when they pass data to another system.

[12] https://build.fhir.org/ig/HL7/fhir-extensions/ValueSet-obligation.html

- **Shared/regional registries** (e.g. national prescription services, implant registries, immunization registries) function as **Consumers** of provider data and **Exchangers** to downstream systems. They therefore implement **display**, **process**, plus **no-alter** on forwarded resources, but have no populate obligations themselves.

- **Cross-border gateways** (EHDS services) also act as **Consumers** and **Exchangers**, enforcing access policies but never generating new clinical data—so they share the same consumer and exchanger obligations as regional HIEs, without producer duties.

Rather than imposing every obligation on all systems, the framework specifies that only the obligations tied to a system's actual role(s)—**Producer, Consumer, or Exchanger**—are applied during its conformance assessment, based on the classifications defined in D8.1.

4.1.1.2 Key Definitions: Conformance vs. Compliance

- **Conformance (Conformity)**
  - **Definition:** The fulfillment of a product, process, or service against all specified technical requirements in a given standard.
  - **Practical Meaning:** "You met the specification's mandatory requirements." Conformance is assessed by verifying that the EHR system can generate resource instances containing all required elements (including relevant terminology bindings) and appropriately handle optional elements—using documentation reviews, instance validation, targeted test scenarios, or formal audits. Instance validation confirms that individual resources include every mandatory data point, while system-level conformance testing demonstrates the software's ability to produce conformant instances under defined test conditions. In this framework, the labels required, recommended, and optional are set from the health-professional perspective, guiding implementers on which obligations must be satisfied versus those that enhance overall quality.

- **Compliance**

- **Definition:** Meeting all legal, regulatory, and contractual requirements that apply to a product, process, or service (ISO 37301).
- **Practical Meaning:** "You met all legal and contractual mandates." For instance, an EHR product must encrypt patient data at rest and in transit to satisfy GDPR security requirements; a patient-admission workflow must comply with national e-prescribing legislation; and a FHIR API service must record and log each data-access event in accordance with the EHDS audit-trail obligations (Article 29) or equivalent national audit regulations.

In short, **conformance** is about "following the tech spec," while **compliance** is about "following the law and contracts."

4.1.1.3 Conformance Levels

Conformance levels describe the extent to which an EHR system meets the defined data-level requirements—they indicate how fully a system implements the specification's structural and semantic rules. These levels focus on system behavior and data structure, quantifying a system's ability to capture and exchange information according to the Xt-EHR logical models.

In relation to EHDS, we define three conformance levels based on the degree of structure:

- **Level 1 – Narrative:** Clinical information is recorded as free-text narrative without enforced structure.
- **Level 2 – Sectioned Narrative:** Information is organized into defined sections or templates, still primarily narrative.
- **Level 3 – Fully Structured Coded:** All data elements are captured in discrete, coded fields, enabling advanced interoperability and automated processing.

4.1.1.4 Actors and Roles

Within the Data-Level Obligations Model we distinguish business-level actors—the real-world roles such as prescribers, nurses, pharmacists or patients—from system-level roles—the software components that intake, consume or forward data on their behalf. This separation is technology-agnostic: whether you use FHIR, C-CDA or another standard, the same obligations apply. In functional terms, each business actor maps to one or more system roles (e.g. a prescriber corresponds to a "prescription producer" component, a pharmacy system to a "medication consumer," and a health information exchange to an "exchanger"), and our model measures conformance by how well those software roles fulfill their data-element duties end to end.

Although it's the software that "produces," "consumes," or "exchanges" data, its purpose is to enable the health professional or patient to provide and receive exactly the information they need. Conformance is assessed by the outcome of the full process—from data entry through serialization and exchange—verifying that all obligations (able-to-populate, populate-if-known, display, process, no-alter) are satisfied end-to-end. Under the EHDS Regulation, an EHR system is defined as any software or device that stores, imports, exports, converts, edits, or presents personal electronic health data and that acts in one or more of these system-level roles to fulfill the data-level obligations.

5.1. Producer

- **Definition:** The system or component that creates data available to other systems or users.
- **Example:** A laboratory Information System that generates an EHDSLaboratoryObservation resource after a blood test has been performed.
- **Data-Level Obligations:** Producers must fulfill obligations such as **able-to-populate and populate-if-known.**

5.2. Consumer

- **Definition:** The system or component that receives, displays or otherwise ingests data.
- **Example:** A hospital's EHR clinical viewer that reads the incoming EHDSLaboratoryObservation and shows it to a clinician.
- **Data-Level Obligations:** Consumers must fulfill obligations such as **display** or **process**.

5.3. Exchanger

- **Definition:** An intermediary (e.g., interface engine, Health Information Exchange node, or message broker) that routes or translates resource instances between systems while preserving their core semantics and required data content, even if representations (such as code systems) are transcoded.
- **Example:** An HIE Node that passes a Discharge Report (DR) from a hospital's EHR to a specialist clinic's EHR; it must handle the DR exactly as received (no-alter).
- **Data-Level Obligations:** The exchanger's data obligations are **alter** or **no-alter**.

When describing data-level obligations, specify which actor(s) must fulfill them:

- **Producer obligations** dictate how data fields must be populated when sharing.
- **Consumer obligations** dictate how data fields must be displayed or processed.
- **Exchanger obligations** ensure certain elements pass unchanged through intermediaries, or transformed in certain ways.

4.1.1.5 Strength of Obligation (RFC 211913)

All rules in this framework use RFC 2119 keywords—**SHALL**, **SHOULD**, **MAY**—to indicate obligation strength:

- **SHALL**: "This is mandatory." Omitting or violating a SHALL rule renders the implementation non-conformant.

[13] https://datatracker.ietf.org/doc/html/rfc2119

- • **SHOULD:** "Strongly recommended." These behaviors are not mandatory—an implementer may choose not to support a SHOULD-level obligation, provided they fully understand, document, and accept the clinical and legal implications. Omitting a SHOULD-level behavior does not render the implementation non-compliant; it remains compliant so long as omission does not shift responsibility to clinicians and EHDS requirements to share the data (for example via free-text) are still satisfied. For critical data elements, implementers should treat SHOULD obligations with care, ensuring that alternative capture or sharing mechanisms are in place.

- **MAY**: "This is optional."

Whenever a data element is annotated with an obligation, the keyword (SHALL, SHOULD or MAY) is tied to a specific action (e.g., "able-to-populate (SHALL)").

4.1.1.6 Data-Level Obligations

Below is the list of **primary obligations** that apply at the data (element) level—each specifying exactly what a Producer, a Consumer or an Exchanger must (SHALL) or should (SHOULD) do for that element.

4.1.1.6.1 Producer's Data-Level Obligations

This section defines the obligations for systems acting as Producers to ensure full support for every required data element. It defines two key responsibilities: **able-to-populate** to guarantee a mechanism exists for entering or updating each individual element and **populate-if-known** to include any value the system already holds whenever it creates or modifies a record.

4.1.1.6.1.1 able-to-populate (SHALL)

Definition: Conformant systems creating or updating electronic data records SHALL provide at least one mechanism—such as a user-interface control, a configuration parameter, a default-assignment rule, or data-mapping logic—that enables a valid value to be assigned to the element in at least one supported scenario.

Explanation: This obligation ensures that the system can produce a record containing the element. During conformance testing, a validation framework will exercise that mechanism—by

invoking the create or update operation with the element populated—and verify the system accepts, persists, and returns the value unchanged. If there is no entry path for the element, the system fails to meet its data-producer obligations.

4.1.1.6.1.2 able-to-populate (SHOULD)

Definition: Conformant systems creating or updating data records SHOULD provide a mechanism—such as a user-interface field, a service parameter, or a data-mapping rule—that enables a value to be set for the element under normal operating conditions.

Explanation: This recommendation encourages implementations to support entry of the element but permits omission when justified. If an implementer elects not to include an input path, they must fully understand and document the clinical or legal ramifications and ensure that alternative methods satisfy EHDS data-capture requirements.

4.1.1.6.1.3 populate-if-known (SHALL)

Definition: Conformant systems creating or updating data records SHOULD provide a mechanism—such as a user-interface field, a service parameter, or a data-mapping rule—that enables a value to be set for the element under normal operating conditions.

Explanation: This obligation ensures that no known data are lost when records are exported. During conformance testing, a validation framework will preload a test value into the system's data store and then retrieve the record; the returned record must include that element with the same value. A follow-up test—where the test value is removed—confirms that the element may be omitted if no data are known. By enforcing this rule, implementers guarantee that all available clinical information is shared whenever it exists.

4.1.1.6.1.4 populate-if-known (SHOULD)

Definition: Conformant systems creating or updating data records SHOULD include this element in any exported record whenever they hold a valid, non-null value for it. If the system has no known value—or if the data is not applicable—omitting the element is permitted without causing a conformance failure.

Clarification: This obligation does not require inserting default or placeholder values when none exist; it simply encourages the export of actual, known data. For example, a Patient.pregnancyStatus element should only appear if the system has confirmed the patient's pregnancy; it must not be populated for patients whose pregnancy status is unknown or inapplicable (e.g., male patients).

Explanation: By adopting this recommendation, implementers improve data completeness wherever possible, yet retain flexibility under valid constraints (such as limited data quality or privacy/consent restrictions). Any decision to defer or omit a SHOULD-level field should be documented, and alternative methods must ensure EHDS data-sharing requirements remain met.

4.1.1.6.2 Exchanger's Data-Level Obligations

This section defines the obligations for systems acting as data exchangers—components whose primary role is to route or translate data records between systems. Such exchangers SHALL preserve any element designated **no-alter** without modification, while they MAY perform authorized transformations on elements designated **alter**.

4.1.1.6.2.1 no-alter (SHALL)

Definition: Conformant intermediary components—such as health-information exchange nodes or message brokers—SHALL route or translate data records without modifying the value of any element designated **no-alter**.

Explanation: This requirement preserves data fidelity across system hops. Even if a gateway needs to transcode code systems or adjust message wrappers, it must leave the actual clinical values—identifiers, status codes, measurements—unchanged. Any change to a no-alter element would effectively turn the exchanger into a producer/consumer and thus fall outside the scope of a pure exchange role.

Example: An HIE receives a Patient with identifier = "12345" and forwards it to another system; a no-alter obligation on Patient.identifier guarantees the outgoing message also contains identifier = "12345", even if other envelope metadata are rewritten.

4.1.1.6.2.2 alter (MAY)

Definition: Conformant intermediary components **MAY** change the value of this element when forwarding or translating data records.

Explanation: Use this obligation when a gateway or broker legitimately needs to transform data—such as remapping local codes to standardized ones—while still honoring the exchange role. It makes clear that modification is permitted under the profile, in contrast to no-alter elements which must remain untouched.

4.1.1.6.3 Consumer's Data-Level Obligations

This section defines the obligations for systems acting as **Consumers**—those that receive data records —and specifies how they must surface and act on incoming data. By mandating **display** and **process** behaviors, we ensure that received information is consistently visible to users and drives the correct automated workflows or decision-support actions.

4.1.1.6.3.1 display (SHALL)

Definition: Conformant applications **consuming** data records **SHALL** present the value of this element in any human-readable context—such as a UI screen, report, or printed document—whenever it is present in the resource.

Explanation: This requirement guarantees that no critical data remain hidden from users. Whether in an on-screen summary, a generated PDF, or a clinician's printout, every element marked with **display (SHALL)** must be surfaced clearly and consistently, even though the precise placement or styling may vary across products.

Example: If an incoming AllergyIntolerance.code element is populated, the consumer's allergy section must visibly list the allergy (e.g., "Penicillin") under the "Allergies" heading in both the electronic chart and any printed patient summary.

4.1.1.6.3.2 display (SHOULD)

Definition: Conformant applications **consuming** data records **SHOULD** present the value of this element in any human-readable context (UI, report, printout) whenever it is present in the resource, unless there is a documented justification for omission.

Explanation: This recommendation promotes consistent visibility of data across certified systems, while allowing implementers flexibility—such as hiding low-priority fields in compact views or specialized workflows—provided they fully understand and record the clinical and usability implications of not displaying the element.

4.1.1.6.3.3 process (SHALL)

Definition: Conformant applications consuming data records SHALL consider the value of this element when executing any automated logic or workflows specified by the implementation guide.

Explanation: This obligation ensures that critical data elements drive downstream behavior—such as decision-support alerts, routing rules, or validation checks—rather than being ignored. A consumer that receives a resource must incorporate the element's value into its processing pipelines exactly as prescribed by the profile.

Example: If an incoming Observation of systolic blood pressure (Observation.code = LOINC 8480-6) carries a valueQuantity above a hypertension threshold (e.g. > 140 mmHg), a consumer with process (SHALL) must fire the corresponding clinical alert or flag in its decision-support module.

4.1.1.6.3.4 process (SHOULD)

Definition: Conformant applications **consuming** data records **SHOULD** consider the value of this element when executing any automated logic or workflows specified by the implementation guide, unless they document an alternative handling strategy.

Explanation: This recommendation encourages consistent use of key data elements in decision-support, routing, or validation processes, while allowing implementers to defer or omit processing in non-critical contexts (e.g., performance-sensitive scenarios or specialized workflows). Any deviation from processing a SHOULD-level element must be justified and recorded to ensure transparency and maintain EHDS data-use requirements.

4.1.2 Technical requirements

The requirements are the technical constraints to be fulfilled by a system claiming conformance to the technical specifications. The authors of the technical specifications shall ensure that any requirement incorporated in the CAS complies with the following requirements and guidelines. The requirements:

a) Shall be uniquely identified.
b) Shall be a comprehensive, contextual, non-ambiguous narrative that defines a clear expected result based on given inputs.
c) Shall refer to the related technical requirement (reference of the source document), including where to find it in the technical specifications:
    a. Section number and name
    b. Page number for PDF documents
    c. Anchor URL for specifications published as HTML page
d) Shall be linked to the category to which it applies (e.g. Logging component, Laboratory Result Report, ePrescription).
e) Shall list the actors (Producer, Consumer) it applies to
f) Shall be assigned a level of prescription among the following:
    a. Mandatory (SHALL): Failing at demonstrating the conformance to a testable assertion renders the implementation non-conformant.
    b. Recommended (SHOULD): Implementers can choose not to meet this testable assertion, it will not render the implementation non-conformant, but they acknowledge the risks of not fulfilling it.
    c. Optional (MAY): Implementer can choose not to conform to the testable assertion without incidence on the conformance of the implementation.
    d. Should be linked to the related test case(s)

This document distinguishes two types of requirements based on the mean of verification that can be used:

- Testable assertions: they are the requirements that can be tested using a test tool, ideally the test execution can be automated.
- Checklist items: they are requirements that cannot be assessed by the use of a test tool. In that case, the implement shall verify manually whether the requirement is implemented in the EHR and report the result of the check, including evidence such as screenshots.

4.1.3 Test case requirements

According to the definitions from the International Software Testing Quality Board (ISTQB):

- A **test case** is a set of preconditions, inputs, actions (where applicable), expected results and postconditions, developed based on test conditions.
- A **test plan** is documentation describing the test objectives to be achieved and the means and the schedule for achieving them, organized to coordinate testing activities.

Authors of test cases in Section 4.3 shall ensure that the test cases comply with the following requirements and guidelines. The test cases:

a) Shall specifically address the testable assertions (4.2.1) that formed the basis of the technical specifications. Each test case can cover one to many requirements.
b) Shall include the list of testable assertions they cover
c) Shall be uniquely identified
d) Shall be under version control
e) Shall define success criteria
f) Shall contain detailed and readable instructions for execution
g) Should be automated and easy to use for the tester
h) Should define input criteria and test data
i) Should not mix automated steps (to check testable assertions) and manual step (as a verification mean for checklist items) to ease the execution of the automated tests

For sake of simplification for the implementer, the checklists should be turned into manual test cases, where each test case relate to a checklist item. It would allow the implementer to use a single tool to demonstrate the conformance of his EHR.

The final test plan (the set of test cases for a given component) shall be:

- Comprehensive (it covers at least all the mandatory requirements)
- Prioritized
- Efficient and pragmatic:
    - It should avoid unnecessary repetition of the same actions in different test cases.
    - It should simplify the execution by grouping requirements in a way that the implementer can cover sequentially several requirements to reach the goal of the test case.

4.1.4 Test data requirements

Authors of Test Cases in Section 4.3 shall ensure that any test data incorporated as input of the test case complies with the following requirements and guidelines. The test data:

a) Should be dynamically generated or drawn from a large pool to prevent gaming of the system

b) Should be clinically accurate (as vetted by clinicians)

c) Shall contain data that is consistent within a test case and across test cases when relevant

4.2 Overview of the Profile/Actor pairs for which Conformity Assessment is available

The table below stands for a summary of the scope of the conformity assessment. The implementer can identify which actors are part of his EHR systems and find the reference to the technical specifications that shall be fulfilled as well as the reference to the section of this document where test cases are listed.

An implementer seeking conformity assessment of its product may select the one or the two harmonized components listed below.

For each harmonized component, an implementer seeking conformity assessment may select one or more Categories among those listed in the table below.

For each Category, an implementer seeking conformity assessment may select for testing the one or the two actors listed in the table below.

Disclaimer to be removed in final version: This table is not yet final; it is an example to show how it shall be filled for all the categories that form the EHDS regulation. It might be populated based on the outcome of T8.1.

Table 1 List of tested component and link to their specifications

Harmonized component	Category	Actor	Link to specifications	Test cases
European Logging software component	Security and logging	Logging component	D5.1 – section 5	4.3.1
European interoperability software component	Laboratory Result	Content Producer	D7.1	4.3.2
		Content Consumer	D7.1	4.3.3
	Discharge Report	Content Producer		4.3.4
		Content Consumer		4.3.5

4.2.1 Requirements

Disclaimer to be removed in final version: As of 11 July 2025, this section of the document is a proposal, providing a few examples based on the D5.1 deliverable and the laboratory result report obligations. The purpose of this section is to provide a template for the high-level testable assertions, which will be defined in the final deliverable. To improve readability and usability, it is

recommended that these testable assertions are managed using a requirements management tool with search capabilities, rather than being listed as plain text in a Word document. This section does not constitute a final or comprehensive list of testable assertions. (APPENDIX IIII: Detailed requirements)

The requirements in this section are derived from the technical specifications defined in the deliverables that form the technical specifications for the EHDS. They aim to provide a clear and comprehensive list of high-level checks:

- The test designers shall cover these when writing the test cases. Test cases should be prioritised so that all requirements with a level of 'Required' are covered first.
- The implementers shall fulfil these requirements to claim conformance to the EHDS technical specifications.

To claim conformance to an actor and a category, an implementer shall demonstrate that their product complies with every “Mandatory” level requirement within the relevant scope. In other words, it shall successfully execute all the related test cases.

Logging Component

Requirement id	Level	Summary	Type	Category and Actor
LOGGING-001	Mandatory	eIDAS recognized authentication	Checklist item	Security and logging / Logging component
LOGGING-002	Recommended	Two-factor authentication	Checklist item	Security and logging / Logging component
LOGGING-003	Mandatory	Record HP identity upon authentication	Checklist item	Security and logging / Logging component
LOGGING-004	Recommended	Record detailed data upon HP authentication	Checklist item	Security and logging / Logging component
LOGGING-005	Mandatory	Record identity of the reader upon data access	Checklist item	Security and logging / Logging component
LOGGING-006	Mandatory	Record identity of the natural person whose data was accessed	Checklist item	Security and logging / Logging component

LOGGING-007	Mandatory	Record category of data accessed	Checklist item	Security and logging / Logging component
LOGGING-008	Mandatory	Record date and time of data access	Checklist item	Security and logging / Logging component
LOGGING-009	Mandatory	Record the source of the data accessed	Checklist item	Security and logging / Logging component
LOGGING-010	Mandatory	Log records are exchanged as FHIR AuditEvent	Testable assertion	Security and logging / Logging component
LOGGING-011	Mandatory	Use of logical references within FHIR AuditEvent	Testable assertion	Security and logging / Logging component
LOGGING-012	Mandatory	Flag log record with "breaking the glass" when appropriate	Checklist item	Security and logging / Logging component

Laboratory

Requirement id	Level	Summary	Category	Category and Actor
LAB-001	Mandatory	Produce conformant FHIR Laboratory Result Report	Testable assertion	Laboratory report / Content Producer
LAB-002	Mandatory	Fill SHALL able-to-populate fields	Testable assertion	Laboratory report / Content Producer
LAB-003	Recommended	Fill SHOULD able-to-populate fields	Testable assertion	Laboratory report / Content Producer
LAB-004	Recommended	Fill SHALL populate-if-known	Testable assertion	Laboratory report / Content Producer
LAB-005	Mandatory	Handle conformant FHIR Laboratory Result Report	Checklist item	Laboratory report / Content Consumer
LAB-006	Mandatory	Display SHALL display elements	Checklist item	Laboratory report / Content Consumer

4.3 Test cases

For each of the actors described in Section 4.2, a subsection provides an exhaustive list of test cases that the implementer shall execute to demonstrate their system or component's conformance with the technical specifications. The associated test data and tools are also reported so that all implementers can all test in the same way.

To claim conformance to a given actor, the implementer shall:

- successfully execute all the applicable test cases for this actor that cover a mandatory testable assertion.
- execute all the other test cases.

Failure of a test case covering a recommended testable assertion will not result in failure for the entire actor but will result in the inclusion of a warning clause in the test report.

Failure of a test case covering an optional testable assertion will not result in failure of the entire actor but will trigger the inclusion of an informative clause in the test report.

Disclaimer to be removed in final version: The test cases detailed in this section stand for examples and do not preclude on the final list of test cases. The final version of this document should only reference the test cases; the latter should be managed in a test management tool under version control.

4.3.1 Test cases for the Logging component

Name	Version	Description	Test data	Covered assertions
Logging of HP authentication events	0.1-draft	Demonstrate the ability of your system to authenticate HP and to create associated log records	**Last modified on**: 16/07/2025 **Authored by**: xtEHR consortium **Last modified by:** xtEHR consortium	LOGGING-001 (Mandatory) LOGGING-002 (Recommended) LOGGING-003 (Required) LOGGING-004 (Required)
Conformance of FHIR AuditEvent for HP authentication	0.1-draft	Demonstrate the conformance of the FHIR AuditEvent produced when HP authenticate himself	**Last modified on**: 16/07/2025 **Authored by**: xtEHR consortium **Last modified by:** xtEHR consortium	LOGGING-010 (Required) LOGGING-011 (Required)

1456 4.3.2 Test cases for the Content Producer of Laboratory results

Name	Version	Description	Test data	Covered assertions
Produce compliant laboratory result report	0.1-draft	Demonstrate the ability of your system to produce a conformant FHIR Laboratory Report Result Document	**Last modified on**: 16/07/2025 **Authored by**: xtEHR consortium **Last modified by:** xtEHR consortium	LAB-001 (Required) LAB-002 (Required)

1457

1458 **4.4 Test tools**

1459 The Testing tools for the validation of the EHR harmonised components will be provided by the
1460 Commission under Article 40 (1) as open-source tools. Under Article 40 it is mentioned that
1461 Member States shall operate digital testing environments for the assessment of harmonised
1462 software components of EHR systems. Such digital testing environments shall comply with the
1463 common specifications for the European digital testing environment. Under Article 42 Member
1464 States have the right to extend the EU EHDS conformance scheme without altering it and should
1465 be informing the EU Commission. Also, Article 37 mentions that Market Surveillance Authorities
1466 may require to have a test performed by an independent body at its own expense within a
1467 specified period in order to verify the conformity.

1468 The Commission has already started drafting the digital testing tools environment based on the
1469 Interoperability Testing Benchmark of the Commission. The Commission also maintains and
1470 expands since 2016 the myHealth@EU testing tools for the operation of the myHealth@EU
1471 services that will also have to enforce the use of the EEHRxF as a mandatory implementation for
1472 all Member States for cross border operation (Article 23). MyHealth@EU test tools are open-
1473 source and ITB compliant. MyHealth@EU test tools are being used by Member States since EU

LP epSOS, they as sustainable, well maintained and operate under a well-established testing strategy and governance.

Based on those facts, and recognising the need to establish a set of test tools that can cover the requirements of Articles 23, 37, 40 and 42 on one hand but also be incorporated into existing of future testing platforms operated by the Member States, it would be beneficial to have one set of testing tools by expanding the myHealth@EU testing tools, covering the needs of the regulation but also facilitating the adoption of the EEHRxF at the Member States' level. In addition, the testing tools can also be adopted or connected to industry laboratories during the deployment of EHDS compliant software facilitating the product lifecycle development.

Consequently, the authors of Test cases in Section 4.3 shall ensure that Digital Test Environment (DTE/test tools) comply with the following candidate/potential requirements and guidelines:

- Shall have technical documentation, including the supporting operating system and development environment.
- Shall have an identified organization committed to maintaining the tool Shall have its source code available as open source.
- Shall issue proof for its validation (e.g. test reports) Shall have demonstrated integration with a test management tool.
- Shall have a documented track record of use in similar context. Shall generate reports and documentation (observer notes, check points, documentation templates) and enable efficient observer documentation generation.
- Should be easy to install for MS and use for the implementers.
- Shall be "extensible" to incorporate testing additional details for national extensions or other interoperability project specifications (in accordance with art. 42 of the EHDS regulation).
- Shall offer an API to integrate with member states' existing test beds.
- Validators must exhibit reproducible behavior.

- Shall include test plans that incorporate sequence diagrams, interaction diagrams or other means of documenting test cases.
- Shall be usable for Ad Hoc testing, without requiring a dedicated test session or a specific user account, or without storing the test report to ensure privacy as these can be managed by the overarching Member State system with which it is integrated.
- Shall provide traceability between requirements and corresponding tests to ensure clear and verifiable coverage and ease the maintenance as the specifications evolve.
- Shall support testing needs by providing features such as automated test case execution, completion of checklist items (including manual tests with the ability to upload evidence), and terminology verification.
- Should have undergone a testing process to demonstrate its suitability for interoperability testing objectives, such as evaluation with a panel of implementers or during an interoperability testing event.
- Should have the capability to manage testable assertions
- Should have the capability to run online or integrated into test events.

APPENDIX I: SURVEY RESULTS

A survey was conducted in May 2024 to a selected professional group from each of the 27 Member States, represented by the below organisations/institutions.

The purpose of this survey was to identify the status of the following topics per MS:

- EHR systems guidelines and harmonised requirements, including harmonised component of EHDS systems.
- EHR CAS
- Wellness application labelling guidelines.

The listed topics above are the key elements in related EHDS articles and Xt-EHR WP8. Some questions of this questionnaire complement and deepen the content on legal and regulatory requirements in Xt-EHR WP4 and D4.1.

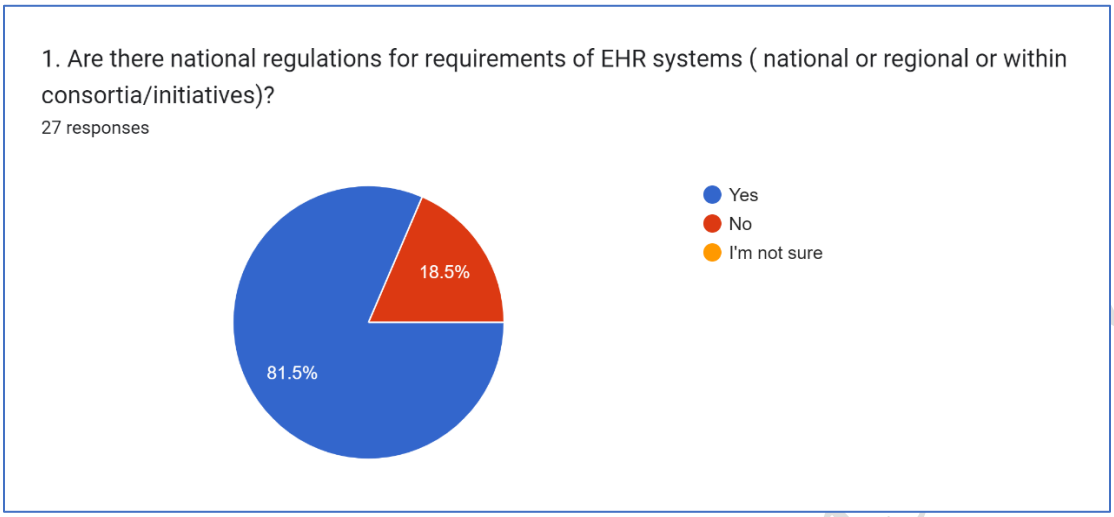
The results will be used to prepare guidelines supporting conformity and compliance assessment in EHDS and for the adoption of the EEHRxF, at a European Level.

We received responses from 25 MS. (situation 13.9.2024). Some of the MS responded as a team while others responded individually. Double answers were allowed, and received from Croatia, Hungary, Ireland, and Spain. We didn't receive replies from Poland and Belgium.

Regulations and other widely used documents in MS

24 respondents have national regulations for EHR systems and 5 do not. Many of the national requirements in different MS apply to:

- data protection and security (many respondents refer to GDPR)
- data sets that health care providers must produce for clinical reports.
- patient's rights e.g., to view their medical records
- requirements for a national centralized e-health point where the national EHR must join and produce health data.



Picture 1. National regulations of EHR systems in MS

National laws in MS are regulating:

- **Austria**: authentication, access control, IHE integration profiles, terminologies
- **Slovenia**: healthcare databases
- **Sweden**: requirements on what and how to document and reporting to registries.
- **Spain**:
  - patients' rights to access to their medical records and the confidentiality of health information
  - minimum data set for clinical reports
  - medical prescriptions and dispensing orders ensuring cross-border healthcare.
  - regulations related to the individual health card.
  - on the National Security Framework
  - Personal Data Protection and Guarantee of Digital Rights, aligning with GDPR for data protection.
  - criteria for the processing of patient data: regulation on data protection.
  - Rights related to scientific research and experimentation.
  - Rights regarding party autonomy includes the consist of e.g. regulations for the conservation of samples for research purposes.

- the rights regarding clinical documentation
- data protection and information security policy

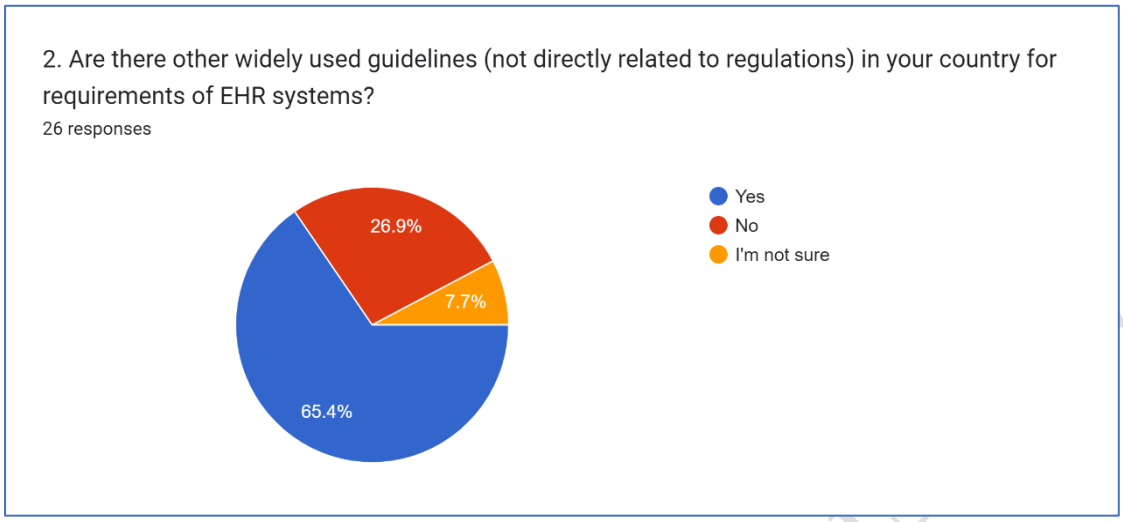
- **Hungary**:
  - law which determines the range of data that healthcare providers must reported to the National eHealth Infrastructure (EESZT). The obligation to transmit data to the EESZT is implemented in three categories, three "modules" (logged doctor-patient encounter; Health documents; patient summary).
  - laws for management and protection of personal data
  - the Central eHealth Cloud's services, containing also the EHR service. A regulation prescribes all hospital, clinics, GPs must connect to the Central eHealth Cloud EHR service using healthcare information systems.
- **Estonia**: national interoperability requirements
- **Ireland**: Health Information Bill
- **Cyprus**: National eHealth law covers several aspects regarding data protection (and GDPR) and security, consent management, right for secondary use of health data.
- **Lithuania**: technical and legal regulations for national centralized e-health system and hospitals information's systems
- **Croatia**: Subordinate Act on the Scope and Content of Data and the EHR Governance
- **Norway**:
  - The Health Records act governs all processing of health information. It provides a legal framework applying to the Summary Care Record, and the Norwegian e-prescription system.
  - Regulation of Standards and National e-Health Solutions describes requirements for software functionality in ICT systems and messaging functionality and mandates the use of national e-health solutions and interoperability standards.

- Personal Data Act ensures data protection and privacy adherence in the healthcare sector.

- **France**:
  - law regarding the organization and transformation of the healthcare system.
  - Public Health Code regarding data privacy. Requirements applicable to hosting personal health data (HDS). Requirements regarding information security in health systems (PGSSI-S)
- **Germany**: Certification of Health IT Software by Federal Association of Statutory Health Insurance Physicians For various communication and prescription systems and laboratory communication (Germany)
- **Latvia**: Regulations Regarding the Unified Electronic Information System of the Health Sector
- **Romania**: health care reform has determined European Card and National Health Insurance Card

17 respondents have also other commonly used guidelines than national ones. 7 don't have while 2 weren't sure (one respond was blank). Two contradictory answers from Hungary and Spain: yes and no (Hungary) and yes and I'm not sure (Spain).

These other widely used guidelines replace and complement the missing legislation to allow the exchange of patient data within a country. Examples of these kind of guides are user guides, functional requirements, and implementation guides for EHR systems.



Picture 2. Share of other widely used guidelines of EHR systems.

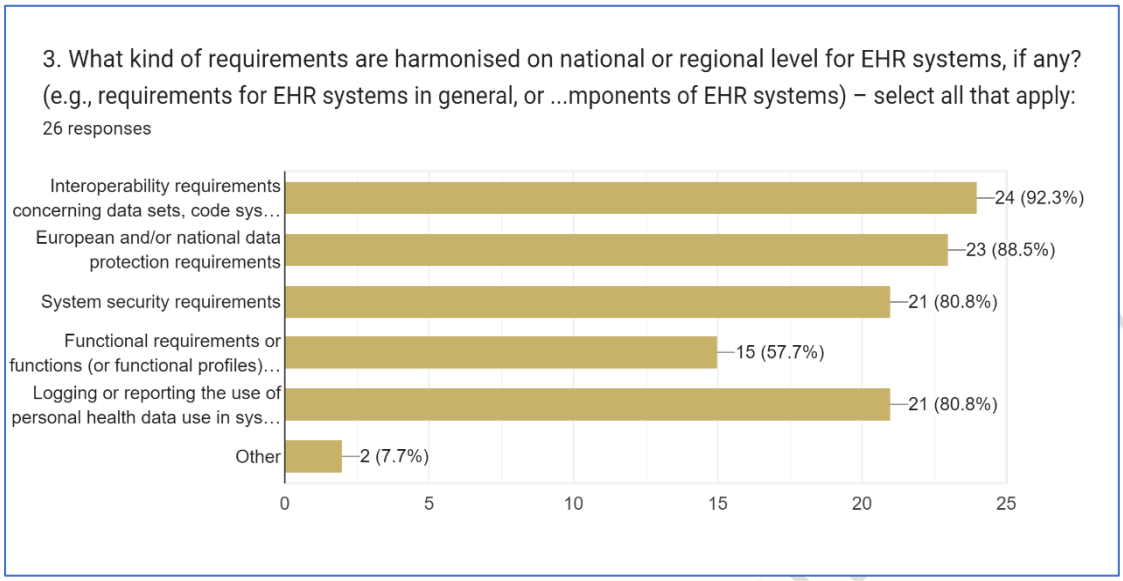
Summary of other widely used of guidelines:

- **Austria**: Recommendation a set of standards to be used for healthcare data.
- **Slovenia**: Technical specifications for national EHR Exchange system.
- **Czech Republic**: national interoperability requirements
- **Sweden**: recommendations, fx usage of standards
- **Spain**: guidance for the implementation and use of EHRs
- **Hungary**: functional requirements (e.g., system API description, cybersecurity requirements) related to the use of the EESZT (national contact point).
- **Ireland**:
  - HSE standard terms for information communications, for services & supplies, for service provider data processing, for network access, for information security, for passwords standards policy, for cloud guiding and for accessibility in addition to GDPR.
  - Policies for: I.T. Acceptable Use, Electronic Communications, Mobile Phone Device, Password Standard, Encryption, Access Control, Remote Access, Information Classification, Data Protection Breach Management, Internet Content Filter Standard

- **Cyprus**: guidance for reimbursement purposes
- **Norway**: a catalogue of mandatory and recommended eHealth standards e.g.: information security, code systems/terminologies, interoperability standards for reporting to national health registries and other standards for referrals, discharge letters and test results
- **Italy**: HL7 digital guidelines
- **Latvia**: guidelines how to use eHealth systems functionality.
- **Greece**:
  - Patient Summary Guidelines (eHealth Network),
  - DRG related guidelines,
  - HL7 EHR-System Functional Model,
- **Romania**: Guidelines to implement HL7 CDA

Harmonised requirements on national level

Majority of the respondents (92,3 %) have harmonised requirements on national level for interoperability, data protection (88,5 %), system security (80,8 %) as well as logging or reporting of use of personal health data (80,8 %). Functional requirements are not so common covered (57,7 %).



Picture 3. Harmonised requirements on national or regional level

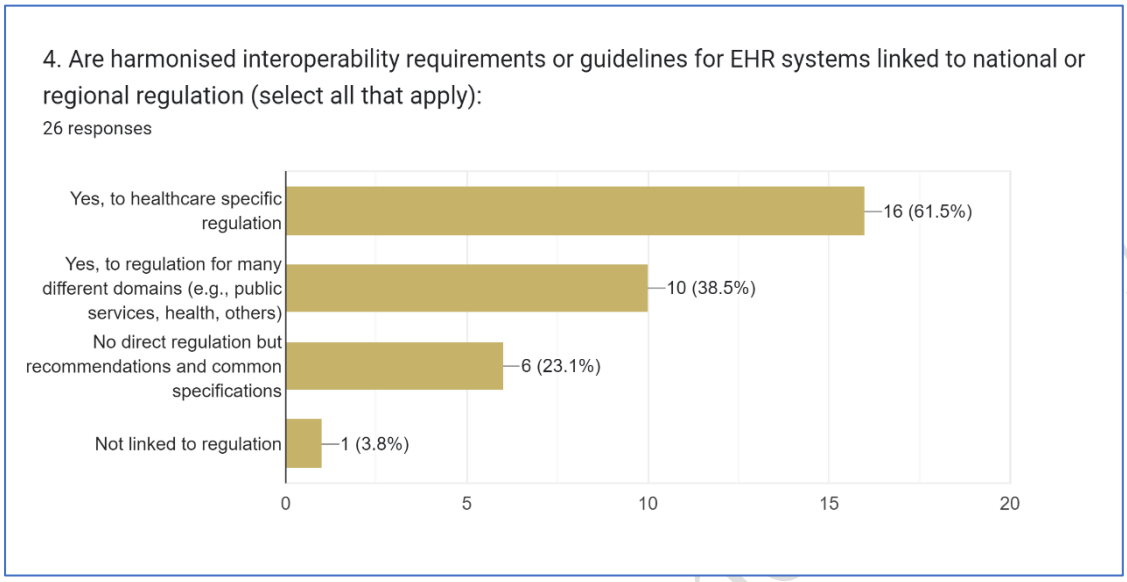
Summary of harmonised documents on national level:

- Interoperability is achieved through central national eHealth applications. EHR systems need to integrate in conformance with this application. (Slovenia)
- national data protection requirements (Slovenia)
- Most of the above is regulated by law and/or managed by requiring usage of national/regional solutions (to be part of data sharing you must comply with certain requirements, and you don't want to be on the outside hence you are complying). (Swe)
- For interoperability purposes: standardized Data sets and Code systems/Terminologies e.g.,
  - SNOMED-CT for allergy,
  - ATC for drugs,
  - ICD-10-CM for MBDS,
  - LOINC for laboratory,
  - HL7 v2.x and HL7 CDA R2 for clinical process integration and report standardization,
  - FHIR,

1662 - National program, UNICAS, is going to work with FHIR (Spain),
1663 - OpenEHR is being increasingly considered for its data archetype approach in EHR
1664 systems. (Spain)
1665 - Implementation guides and specifications for APIs (Spain)
1666 - GDPR and national data protection laws (Spain)
1667 - security measures such like data encryption, secure access controls, regular security
1668 audits, incident response protocols (Spain)
1669 - functional requirements (Spain):
1670 - clinical documentation (including patient histories, treatment plans, and
1671 diagnostic information),
1672 - medication
1673 - Integration with laboratory and imaging systems
1674 - logs of access and use of personal health data (Spain)
1675 - patient portals to enable patients to access their health information, communicate with
1676 healthcare providers, and manage appointments and prescriptions. (Spain)
1677 - advanced analytics and reporting functionalities to support clinical decision-making and
1678 healthcare management. (Spain)
1679 - medical softwares functional requirements (Hungary)
1680 - Maintainer of EESZT describes the standard, data sets and code systems, which must be
1681 used by the medical systems to connect to EESZT. Connecting to EESZT requiers security
1682 standards also, eg.: TLS 1.2, SAML. Medical systems must use an API to connect EESZT
1683 which specifies the necessary functions and riportings. (Hungary)
1684 - Estonia is interested to set additional security standards and to define mutual
1685 interoperability standards in EU-level for cross-border exchange for every priority
1686 category (Estonia)
1687 - National Release Centre for SNOMED CT, Healthlink Online Message Specification,
1688 National Data Protection Act 2018. Adhere to EHDS and GDPR. (Ireland)

- The national EHR is currently subject to revision. A national legislation will be adapted also according to the new EHDS requirements. (Luxemburg)
- Croatia has:
    - Interoperability requirements concerning data sets, code systems / terminologies, interoperability standards, interface / API specifications or implementation guides.
    - European and/or national data protection requirements
    - System security requirements
    - Functional requirements or functions (or functional profiles) of EHR systems
    - Logging or reporting the use of personal health data use in systems.
    - and other:
- The Norwegian Directorate of Health publish a catalogue of standards listing mandatory and recommended eHealth standards. This includes several topics such as information security, code systems/terminologies, interoperability standards for reporting to national health registries and other standards for referrals, discharge letters and test results. In addition to the standards there are several recommended guidelines on relevant topics. (Norway)
- The Code of Conduct for information security and data protection in the healthcare and care services (The Code). EU directives applicable under the EEA Agreement, such as GDPR implemented via the Personal Data Act 2018. A guideline for logging when sharing data and documents in the healthcare sector. All EHR systems are required to perform extensive logging of use. (Norway)
- Interoperability: CI-SIS, Functional requirements: DMP implementation guide, Security: PGSSI-S, HDS. Data protection: RGPD, HDS (France)
- DRG requirements in order to operate with grouper software (Greece)

1715 Interoperability requirements

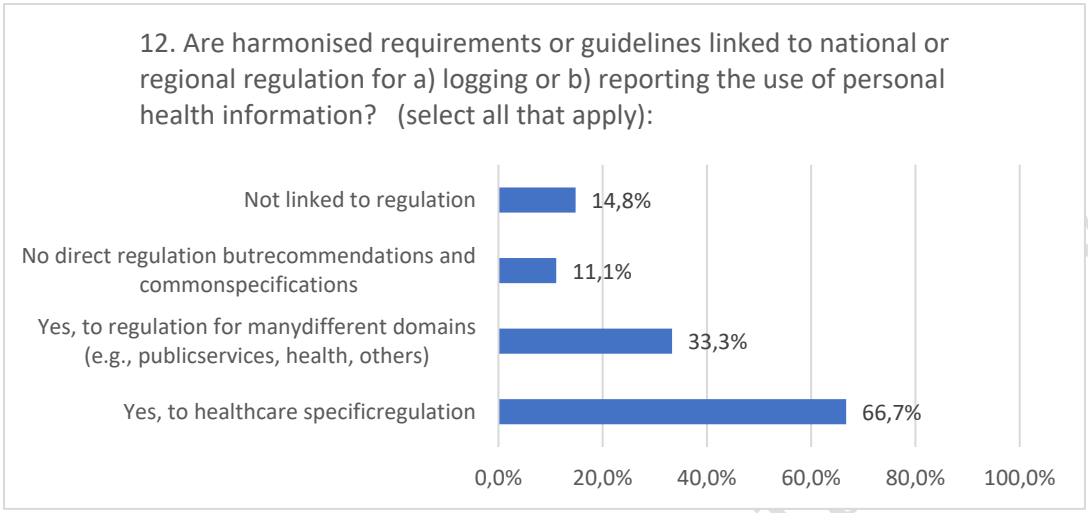


1716

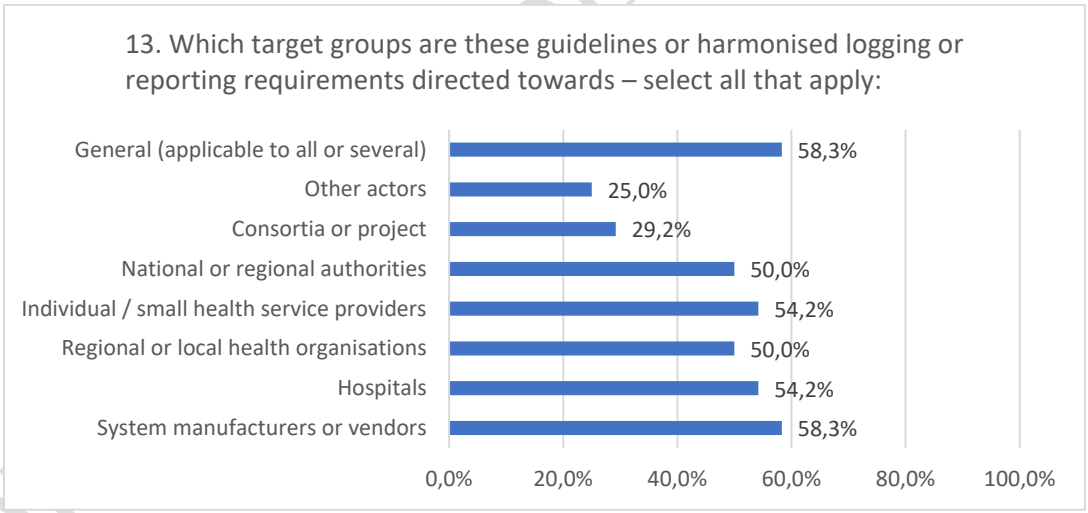
1717 Picture 4. Harmonised requirements linked to national or regional regulation.

1718 Almost half of the respondents (16/27) have healthcare specific regulation linked to national of
1719 regional regulation. Minor of the respondents (8/27) also have linked regulation for many
1720 different domains like public or health services. 7/27 respondents have recommendations and
1721 common specifications but not direct regulation. One doesn't have linked their interoperability
1722 requirements to regulation.

1723



Picture 5. Harmonised Requirements or guidelines linked to national or regional regulation for logging or reporting the use of personal health information.

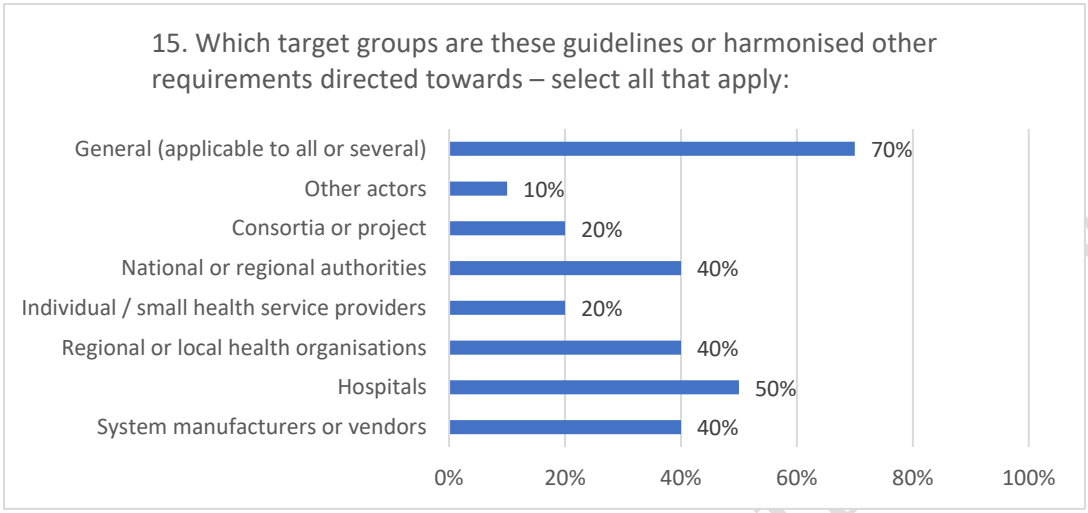


Picture 6. Target groups that guidelines/ harmonized logging/ reporting requirements are directed towards to.

None apart from the aforementioned regultaions on healtcare databases, national eHealth and personal data protection act
Health Information Exchange Standards: Mandated for secure sharing of patient data.
Clinical Decision Support (CDS) Requirements: Tools for evidence-based decision-making.
Medication Management Protocols: Guidelines for safe medication use.
Quality Reporting and Performance Measures: Mandates for assessing healthcare outcomes.
Clinical Coding Standards: Standardized representation of clinical data.
Patient Engagement and Health Literacy Requirements: Support for patient interaction.
Disaster Recovery and Business Continuity Planning: Ensuring EHR system availability during emergencies
We are working in the Spanish Health space data (for secondary use) and in one Health electronic record inside the Spanish National Health Service.
Except the DRG related requirements, there are recommendations on specific document templates to be produced by the HIS/EHR system of hospitals
Government Decision 34/2015 for the approval of the Methodological Norms regarding the way to use and complete the patient's EHR.
Order no. 1,123 of October 12, 2016 for the approval of the data, information and operational procedures necessary for the use and operation of the patient's EHR (DES), issued by MINISTRY OF HEALTH No. 1,123 of October 12, 2016
NATIONAL HEALTH INSURANCE HOUSE No. 849 of October 11, 2016
Published in the OFFICIAL MONITOR no. 806 of October 13, 2016"
If you are a HCP you have to be able to link to the national infrastructure, deliver data to a number of national registries and adhere to standards in the national standards catalogue. These requirements apply to all who want to provide healthcare services.
A binding agreement between State, five Regions and 98 Municipalities, ensure that all EHR only can be connected to the national infrastructure, when Certified by MedCom to conform to interoperability standards.

1732

1733 Table 2. Other harmonised requirements or guidelines for EHR systems linked to national or
1734 regional regulation.



Picture 7. Target groups that guidelines/ harmonized other reporting requirements are directed towards to.

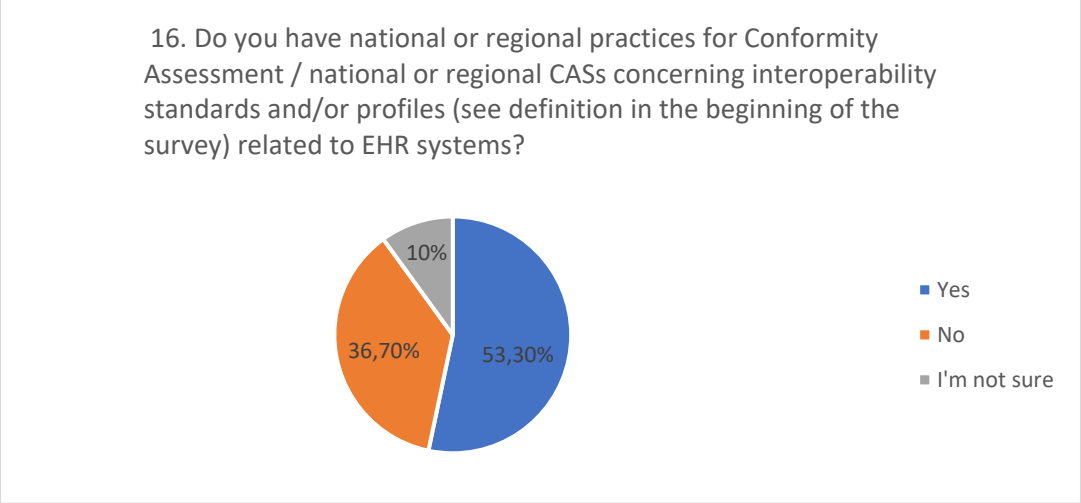
70% of the participants replied that available and currently applied guidelines are general.

50% of them replied that there are hospital- related guidelines.

40% refer to national/ regional authorities, 40% to regional or local healthcare organizations and another 40% to system vendors.

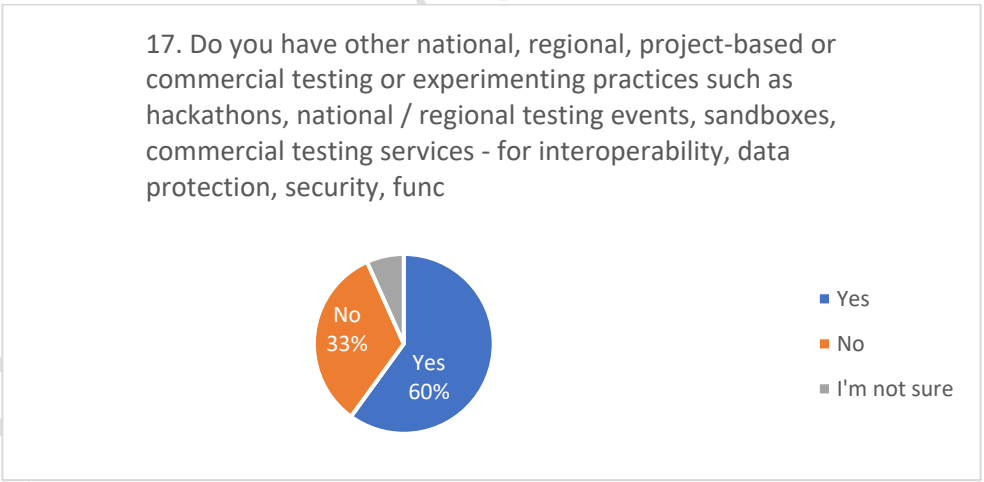
20% refer to consortia or project related guidelines and another 20% is about individual or small health service providers

10% is about other actors.



Picture 8. National or regional practices for Conformity Assessment / national or regional CASs concerning interoperability standards and/or profiles related to EHR systems.

53% of the participants replied positively and provided details about the existing framework for conformity assessment to interoperability requirements (ranging from ''Connectathon'' and testing practices to local certification schemes)



Picture 9. Other national, regional, project-based or commercial testing or experimenting practices such as hackathons, national / regional testing events, sandboxes, commercial testing services - for interoperability, data protection, security, function.

60% of the participants replied that there is national- regional or project-based commercial testing or other experimental practice for interoperability or other technical attributes of their EHR.

In Spain, as in most countries, there is a national accreditation body (ENAC, www.enac.es) responsible for accrediting any public or private entity that wishes to provide services for the evaluation and/or certification of requirements established in European directives or regulations. For example, ENAC has approved and aligned with ENISA the certification scheme for entities that wish to certify products based on the EUCC (Regulation (EU) 2024/482)

APPENDIX II: CAS GOVERNANCE - EHDS REGULATION

Mapping the content of the "T4.3 EHDS Conformity Assessment Scheme Governance" document (hereafter "CAS GovernanAce") to relevant sections of the EHDS Regulation (as per the Corrigendum version and its Annexes).

It highlights how specific points of CAS Governance correspond to EHDS Regulation provisions and annexes, and where additional detail could be incorporated into the CAS Governance to fully align with the Regulation's requirements.

1. General Purpose and Scope

- **CAS Governance, Introduction**

  The introductory sections explain that the proposed CAS aims to ensure interoperability among EHR systems across Europe, referencing established standards (ISO/IEC 17025, IHE profiles, etc.) and the aim to foster trust in digital health. This overarching objective reflects the Regulation's core goal of "improving natural persons' access to and control over their personal electronic health data ... in the context of healthcare" and ensuring that data can move freely and securely across Member States (Article 1 and Recital 1, 2, 7 of the EHDS Regulation).

  (CAS Governance) aligns generally with Recitals 2, 3, 5, 7, and 9 of the EHDS Regulation , which stress the need for secure and interoperable exchange of personal electronic health data.

- **Further Detail That Could Be Added**

  While the CAS Governance statement of purpose aligns with the high-level goals of the EHDS Regulation, the Regulation also includes references to additional specific data categories (Annex I) and essential requirements on interoperability and security (Annex II). CAS Governance could add a short statement cross-referencing these Annexes to show that its scope (interoperability testing) covers or references the priority data categories (patient summaries, e-prescriptions, medical imaging, etc.) and the essential interoperability requirements.

2. Correspondence with Article 30 (Obligations of Manufacturers)

- **CAS Governance, Sections on Manufacturers**

CAS Governance explicitly refers to Article 30 of the EHDS Regulation when describing how EHR system manufacturers must ensure compliance through self-assessment and/or testing in accredited environments.

describes that “The task will Support Article 30 – (Obligations of manufacturers of EHR systems) ... by performing a self-assessment in a regulated manner.” This directly addresses Article 30(1) and (3) EHDS Regulation, which set out that manufacturers of EHR systems must ensure their products conform to the EHDS essential requirements and be prepared to demonstrate conformity.

Additionally, CAS Governance highlights that the final responsibility for the correctness of a declaration of conformity rests with the manufacturer, reflecting Article 30(4) on manufacturer liability for accurate compliance claims.

- **Further Detail That Could Be Added**

Article 30 of the Regulation also specifies requirements on incident reporting, instructions for use, and the obligation to keep technical documentation. CAS Governance focuses on interoperability and does not deeply elaborate on how manufacturers could be guided to maintain these other documentation and risk-management aspects. A supplementary section that guides manufacturers on aligning with the product documentation obligations under Article 30(5) and the technical documentation elements detailed in Annex III of the Regulation would help completeness.

3. Article 40 (European Digital Testing Environment) and National Implementations

- **CAS Governance, Section 3 (Governance Structure) & 4 (Certification Process)**

CAS Governance repeatedly references Article 40, which outlines the establishment of European and national digital testing environments to assess EHR systems’ harmonised software components (Article 40(1), (2), (3), (5)).

Specifically, CAS Governance calls for:

- A central Conformity Assessment Coordination Committee (CACC) at EU level, mirroring the Commission's coordination role under Article 40 EHDS Regulation.
- Member State national supervisory bodies to oversee their local digital testing environments, consistent with Article 40(2) and (3).
- A link between these testing environments and manufacturers' self-assessment obligations.

- **Further Detail That Could Be Added**

CAS Governance could clarify how the "European digital testing environment" under the Commission's responsibility (Article 40(3)) integrates with existing IHE Connectathons or other test platforms. The CAS Governance does mention reusing IHE's Gazelle, but it could explicitly articulate how local or "national" environments feed into and are recognized by the overarching European environment in line with Article 40(4) EHDS Regulation (on compliance checks by the Commission).

4. Recitals 36 and 39 (Self-Assessment, Avoiding Market Fragmentation)

- **CAS Governance, Section 4.1 (Self-Assessment)**

The document references Recitals 36 and 39, emphasizing that manufacturers can self-assess EHR systems for compliance, aligning with the Regulation's recognition that self-assessment reduces fragmentation, fosters uniformity, and speeds up cross-border availability of compliant solutions.

This part of CAS Governance describes a "structured self-assessment" procedure and a Test Report Summary (TRS) to promote transparency.

- **Further Detail That Could Be Added**

While Recital 39 EHDS Regulation notes that self-assessment is intended to lighten the burden, it also indicates that appropriate safeguards (e.g., oversight, publication of summary results) are needed. CAS Governance covers TRS publication but might add detail about the minimum content of the report or methods for ensuring the veracity of reported

test results, tying these specifically to the Regulation's emphasis on patient safety and data protection.

5. References to Annex II (Essential Requirements for EHR Systems)

- **CAS Governance Focus vs. Annex II**

CAS Governance lays out test and accreditation processes referencing ISO 17025 and IHE's technical profiles (HL7-FHIR, DICOM, etc.). Annex II of the EHDS Regulation, however, itemizes "Essential Requirements" (e.g., interoperability, security controls, data portability features, logging mechanisms).

Although CAS Governance discusses the high-level need for "IHE-based testing" and "interoperability," it does not explicitly enumerate how each essential requirement of Annex II is verified. For instance, Annex II 3.4 or 3.5 revolve around specific logging obligations, including emergency access logging.

- **Further Detail That Could Be Added**

A beneficial addition would be an item-by-item explanation linking the testing steps or IHE profile checks in CAS Governance to the requirements in Annex II. This would confirm that the proposed test plan addresses everything from "secure access, identification, authentication" to "structured data exchange."

6. References to Annex III (Technical Documentation) and Annex IV (EU Declaration of Conformity)

- **CAS Governance Mentions vs. Annex III & IV**

CAS Governance briefly alludes to manufacturers "publishing test report summaries" and maintaining proof of compliance (Section 4.3). However, Annex III sets out a structured list of technical documentation contents (e.g., system architecture, versions, performance claims, references to common specifications used) that EHR systems must have ready. Similarly, Annex IV outlines the mandatory elements of the EU Declaration of Conformity (e.g., references to relevant standards used, signature, references to common specs). CAS

Governance references a “Conformity Mark” or “EHDS Seal,” but the Regulation’s Annex IV requires more formal statements than simply a seal.

- **Further Detail That Could Be Added**

The CAS Governance text could devote a short section mapping the test documentation (TRS, lab reports, self-assessment checklists) to the more formal documents that Article 24 and Annex IV require, such as the “EU declaration of conformity.” This would ensure that after testing, manufacturers can compile everything needed (e.g., references to any common specifications under Article 23) into the official EU declaration.

7. Interaction with MyHealth@EU (Articles 11–15) and Cross-Border Data Exchange

- **CAS Governance, Overarching Objective**

A key theme in the EHDS Regulation is data exchange across borders via MyHealth@EU. While CAS Governance focuses on verifying that EHR systems can interoperate, it does not explicitly cross-reference MyHealth@EU or the national contact points for digital health that the Regulation (Articles 11–15, 33–35) mandates. However, CAS Governance’s reference to cross-border interoperability testing in IHE Connectathons (Section 4.2) aligns in spirit with MyHealth@EU’s requirement for consistent data formats and structured datasets.

- **Further Detail That Could Be Added**

CAS Governance might add explicit mention of how tested EHR systems can integrate into MyHealth@EU gateways, clarifying that they satisfy the “EEHRxF” building blocks (Recitals 25, 26) and thereby enabling cross-border care continuity.

8. Missing or Complementary Aspects

- **Data Categories from Annex I**

Although CAS Governance emphasizes interoperability in general, it does not single out or map its testing scope to each category from Annex I (patient summaries, e-prescription and dispensation, medical images, lab results, discharge reports). A short reference in CAS

Governance that enumerates these categories as priority data sets for testing would demonstrate direct alignment with the Regulation.

- **Security and Data Protection**

Annex II includes numerous security-related provisions. CAS Governance references ISO/IEC 17025-based testing laboratories and alludes to "robust data exchange mechanisms," but it could expand on the security testing dimension—such as compliance with role-based access, authentication, logging, and (where relevant) emergency-access overrides.

- **Post-Market Surveillance**

CAS Governance focuses on the upfront certification process. The EHDS Regulation also implicitly contemplates ongoing compliance and incident handling (e.g., Article 30(5) and Recital 36). CAS Governance could add a short section addressing how EHR system updates, new versions, or discovered nonconformities feed back into recertification or re-testing.

9. Summary of Alignment and Recommendations

- **What CAS Governance Covers Well**
  - Aligns with EHDS Article 30 by providing a structured model for manufacturer obligations and self-assessment.
  - Coordinates with Article 40 on the digital testing environment by defining a central Conformity Assessment Coordination Committee (CACC) and national supervisory roles.
  - Reflects Recitals 36 and 39 in promoting self-assessment as a way to reduce fragmentation.
  - Invokes ISO/IEC 17025 labs and referencing IHE Connectathons, consistent with Annex II's emphasis on interoperability requirements and the spirit of Article 23 (common specifications).

- **What Could Be Expanded**

- Establishing an explicit mapping of each essential requirement in Annex II to the CAS testing procedures or IHE profile checks.
- Explaining how test documentation aligns with Annex III (technical documentation) and Annex IV (EU declaration of conformity).
- Incorporating references to Annex I's priority data categories, clarifying that the CAS covers these specifically.
- Adding a statement on alignment with MyHealth@EU (Articles 11–15) to clarify how certified EHR systems fit into cross-border data exchange.
- Detailing any ongoing monitoring or post-market checks.

In conclusion, CAS Governance already reflects many crucial points in the EHDS Regulation by embedding the concept of testing environments, referencing the obligations of manufacturers (Article 30), and providing for self-assessment and accredited-testing environments routes. It would benefit from an explicit cross-reference to the Annexes (in particular Annexes I–IV) and a clearer description of how test results align with the formal technical documentation and EU declaration process. With these additional elements, the CAS Governance can comprehensively meet the EHDS Regulation's requirements and ensure a fully harmonized approach to EHR system interoperability, security, and market transparency.

APPENDIX III: LEGISLATIVE TEXTS

Legislative framework and regulative documents that provide a mandatory basis to be followed is hereby presented covering the entire scope and functional areas as appropriate.

- **GDPR:** GDPR is the primary regulation governing data protection and privacy in the European Union. It applies to all organizations that process personal data of EU citizens, including wellness application providers.
- **Data Governance Act (DGA):** There are two EU acts regarding data: Data Act and DGA. The DGA regulates processes and structures that facilitate voluntary data sharing. The Data Act clarifies who can create value from data and under which conditions. These are relevant as one of the key- aims of this effort is to create Common European Data Spaces - such as the EHDS - in a number of strategic fields. The DGA establishes rules for data sharing within the EU, including **personal data** and **non-personal data**. It aims to promote a **trusted environment** for data exchange across sectors, including healthcare[14]. The DGA entered into force on 23 June 2022 and, following a 15-month grace period, is applicable since September 2023. It aims to make more data available and facilitate data sharing across sectors and EU countries to leverage the potential of data for the benefit of European citizens and businesses. For wellness applications that share health data, the DGA helps create an environment that ensures secure and transparent data sharing. The provisions of EHDS specifying elements of the DGA, support the creation of integrated frameworks, which could allow wellness applications to participate in shared data pools for health research, innovation, or public health purposes. The obligation to share data under the Data Act should in no way contradict or compromise the obligations for medical technologies required under other EU legislation (Medical Device Regulation and other provisions). The Data Act needs to be interpreted in a way that recognizes the safety, performance, and efficacy requirements of medical technologies, given their direct impact on the health and safety of patients.[15]

[14] https://digital-strategy.ec.europa.eu/en/policies/data-governance-act
[15] https://www.mhc.ie/latest/insights/the-eu-data-act-spotlight-on-digital-health

- **Clinical Trials Regulation (EU) No. 536/2014**[16]**:** This regulation governs the conduct of clinical trials within the EU, including the collection and sharing of health data for clinical research purposes. There are provisions in the EHDS (Article 51) for the secondary use of health data that originate from wellness applications. Health data holders that utilize this data for clinical trials or research will need to comply with the Clinical Trials Regulation when handling sensitive health information, ensuring that user consent is obtained, and data is handled securely during research studies. The Clinical Trials Regulation repealed the Clinical Trials Directive on 31 January 2022. Although the Regulation entered into force on 16 June 2014 the timing of its application depended on the development of a fully functional EU clinical trials portal and database. EMA Management Board confirmed to the European Commission on 21 April 2021 that the EU Portal and Database were fully functional.
- **Regulation (EU) 2024/2847 of the European parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements** and amending Regulations (EU) No 168/2013 and (EU) No 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act): EHDS complements the essential cybersecurity requirements laid down in Regulation (EU) 2024/2847. Synergies of EHDS with the Cyber Resilience Act:
    - EHR systems which are products with digital elements within the meaning of Regulation (EU) 2024/2847 (Cyber Resilience Act) should also comply with the essential cybersecurity requirements set out in that Act.
    - The manufacturers of those EHR systems should demonstrate conformity as required by this Regulation.
    - To facilitate that conformity, manufacturers should be allowed to draw up a single set of technical documents containing the elements required by both legal acts. It should be possible to demonstrate conformity of EHR systems with essential cybersecurity

[16] https://health.ec.europa.eu/medicinal-products/clinical-trials/clinical-trials-regulation-eu-no-5362014_en#:~:text=The%20Clinical%20Trials%20Regulation%20repealed,clinical%20trials%20portal%20and%20database.

requirements laid down in the Cyber Resilience Act through the assessment framework under this Regulation.

- However, the parts of the conformity assessment procedure under this Regulation which relate to the use of testing environments should not be applied, since those testing environments do not allow for an assessment of conformity with the essential cybersecurity requirements. As Regulation (EU) 2024/2847 does not cover Software as a Service (SaaS) directly as such, EHR systems offered through the SaaS licensing and delivery model do not fall within the scope of that Regulation. Similarly, EHR systems that are developed and used in-house do not fall within the scope of that Regulation, as they are not placed on the market.

- **Artificial Intelligence Act:** In April 2021, the European Commission proposed the first EU artificial intelligence law, establishing a risk-based AI classification system. AI systems that can be used in different applications are analyzed and classified according to the risk they pose to users. The different risk levels mean more or less AI compliance requirements.

APPENDIX IIII: CAS-CONTENT EXAMPLES OF DETAILED REQUIREMENTS

Logging component

Requirement Id: LOGGING-001 (Checklist item)

Predicate: A system claiming conformance to the EHDS regulation as a logging component SHALL use authentication means which are recognized under eIDAS (EU 910/2014, updated in 2024) for authenticating the healthcare professional (see EHDS art. 12) accessing patient data.

Level: Mandatory

Category: Security and logging

Actor: Logging component

Reference: D5.1 – Section 5.1.2.1 / 2 ii page 45

Coverage: Authentication of healthcare professional

Requirement id: LOGGING-002 (Checklist item)

Predicate: A system claiming conformance to the EHDS regulation as a logging component SHOULD offer a minimum of two forms of identity verification to the healthcare professional when he authenticates himself into the system.

Level: Recommended

Category: Security and logging

Actor: Logging component

Reference: D5.1 – Section 5.1.2.1 / 3 i page 45

Coverage: Two-factor authentication of healthcare professionals

---

Requirement id: LOGGING-003 (Checklist item)

Predicate: A system claiming conformance to the EHDS regulation as a logging component SHALL create a record containing at least the identity of the healthcare professional each time the healthcare professional authenticates himself into the system.

Level: Mandatory

Category: Security and logging

Actor: Logging component

Reference: D5.1 – Section 5.1.2.4 / 2 i page 46

Coverage: placeholder for the unique identifier of the test case

---

Requirement id: LOGGING-004 (Checklist item)

Predicate: A system claiming conformance to the EHDS regulation as a logging component SHOULD create a record for each authentication attempt (successful or failed) and containing the timestamp when the healthcare professional authenticates himself into the system, the IP address and the identifier of the device that issued the authentication request.

Level: Recommended

Category: Security and logging

Actor: Logging component

Reference: D5.1 – Section 5.1.2.4 / 2 i page 46

Coverage: placeholder for the unique identifier of the test case

---

Requirement id: LOGGING-005 (Checklist item)

Predicate: A system claiming conformance to the EHDS regulation as a logging component SHALL for, each access event or group of events, create a record that contains the identifier of the healthcare professional, or individual having accessed the data.

Level: Mandatory

Category: Security and logging

Actor: Logging component

Reference: D5.1 – Section 5.2.2.1 / 2 i page 48

Coverage: placeholder for the unique identifier of the test case

---

Requirement id: LOGGING-006 (Checklist item)

Predicate: A system claiming conformance to the EHDS regulation as a logging component SHALL for, each access event or group of events, create a log record that contains the identifier of the natural person(s) whose data was accessed.

Level: Mandatory

Category: Security and logging

Actor: Logging component

Reference: D5.1 – Section 5.2.2.1 / 2 i page 48

Coverage: placeholder for the unique identifier of the test case

---

Requirement id: LOGGING-007 (Checklist item)

Predicate: A system claiming conformance to the EHDS regulation as a logging component SHALL for, each access event or group of events, create a log record that contains the categories of data accessed.

Level: Mandatory

Category: Security and logging

Actor: Logging component

Reference: D5.1 – Section 5.2.2.1 / 2 i page 48

Coverage: placeholder for the unique identifier of the test case

---

Requirement id: LOGGING-008 (Checklist item)

Predicate: A system claiming conformance to the EHDS regulation as a logging component SHALL for, each access event or group of events, create a log record that contains the date and time when the data have been accessed.

Level: Mandatory

Category: Security and logging

Actor: Logging component

Reference: D5.1 – Section 5.2.2.1 / 2 i page 48

Coverage: placeholder for the unique identifier of the test case

---

Requirement id: LOGGING-009 (Checklist item)

Predicate: A system claiming conformance to the EHDS regulation as a logging component SHALL for, each access event or group of events, create a log record that contains the identification of the source of the data accessed.

Level: Mandatory

Category: Security and logging

Actor: Logging component

Reference: D5.1 – Section 5.2.2.1 / 2 i page 48

Coverage: placeholder for the unique identifier of the test case

---

Requirement id: LOGGING-010 (Testable assertion)

Predicate: A system claiming conformance to the EHDS regulation as a logging component SHALL be able to produce an FHIR AuditEvent resource that conforms to the structure definition defined

at https://www.hl7.org/fhir/R4/auditevent.html to exchange any of the log records locally stored.

Level: Mandatory

Category: Security and logging

Actor: Logging component

Reference: 5.2.3 page 51

Coverage: placeholder for the unique identifier of the test case

---

Requirement id: LOGGING-011 (Testable assertion)

Predicate: A system claiming conformance to the EHDS regulation as a logging component SHALL use logical references within the FHIR AuditEvent Resources it produces.

Level: Required

Category: Security and logging

Actor: Logging component

Reference: 5.2.3 page 51

Coverage: placeholder for the unique identifier of the test case

---

Requirement id: LOGGING-012 (Checklist item)

Predicate: A system claiming conformance to the EHDS regulation as a logging component SHALL for, each access event or group of events, if the “breaking the glass” scenario has occurred, the record SHALL flag the event as such.

Level: Mandatory

Category: Security and logging

Actor: Logging component

Reference: D5.1 – Section 5.2.2.1 / 2 ii page 48

Coverage: placeholder for the unique identifier of the test case

---

Requirement id: LAB-001 (Testable assertion)

Predicate: A product claiming conformance to the Laboratory Result Report as a Content Producer shall produce a FHIR Bundle resource of type "document" that complies to the EU Laboratory Result Report StructureDefinition (http://hl7.eu/fhir/laboratory/StructureDefinition/Bundle-eu-lab).

Level: Mandatory

Category: Laboratory Result Report

Actor: Content Producer

Reference: D7.1

Coverage:

Requirement id: LAB-002 (Testable assertion)

Predicate: A product claiming conformance to the Laboratory Result Report as a Content Producer shall produce a FHIR Bundle resource in which all the elements with obligation set to "SHALL able-to-populate" are filled with relevant values.

Level: Mandatory

Category: Laboratory Result Report

Actor: Content Producer

Reference: D7.1

Coverage:

Requirement id: LAB-003 (Testable assertion)

Predicate: A product claiming conformance to the Laboratory Result Report as a Content Producer shall produce a FHIR Bundle resource in which all the elements with obligation set to "SHOULD able-to-populate" should be filled with relevant values.

Level: Recommended

Category: Laboratory Result Report

Actor: Content Producer

Reference: D7.1

Coverage:

Requirement id: LAB-004 (Testable assertion)

Predicate: A product claiming conformance to the Laboratory Result Report as a Content Producer shall produce a FHIR Bundle resource in which all the elements with obligation set to "SHALL populate-if-known" should be filled with relevant value when known to the Content Producer.

Level: Recommended

Category: Laboratory Result Report

Actor: Content Producer

Reference: D7.1

Coverage:

Laboratory result as Content Consumer

Requirement id: LAB-005 (Checklist item)

Predicate: A product claiming conformance to the Laboratory Result Report as a Content Consumer shall be able to handle any FHIR Bundle resource complying with the Laboratory

Results Report StructureDefinition (http://hl7.eu/fhir/laboratory/StructureDefinition/Bundle-eu-lab).

Level: Mandatory

Category: Laboratory Result Report

Actor: Content Consumer

Reference: D7.1

Coverage:

Requirement id: LAB-006 (Checklist item)

Predicate: A product claiming conformance to the Laboratory Result Report as a Content Consumer shall be able to display all the elements of the Laboratory Results Report StructureDefinition that are set with an obligation level equal to “SHALL display”.

Level: Mandatory

Category: Laboratory Result Report

Actor: Content Consumer

Reference: D7.1

Coverage:

Detailed test cases

Logging component

Name: Logging of HP authentication events

Version: 0.1-draft

Last modified on: 21/07/2025

Authored by: xtEHR consortium

Last modified by: xtEHR consortium

Covered requirements: LOGGING-001, LOGGING-002, LOGGING-003, LOGGING-004

Description:

This test case aims at demonstrating that your system

- Supports at least one authentication mean which is recognized under the eIDAS regulation (LOGGING-001)
- Creates a log record upon authentication of the healthcare professional and populates the log record with at least all the mandatory information (LOGGING-003)

The following features might be implemented as well by your system:

- Offering a minimum of two forms of identity verification to the healthcare professional when he authenticates himself into the system. (LOGING-002)
- Populating the log record with additional information such as the IP address and identifier of the device used by the HP (LOGGING-004)

You are a healthcare professional that needs to access patient data. You first need to authenticate to the EHR using an authentication mean recognize under eIDAS regulation.

Test steps

Step 1: Authenticate to your EHR as a healthcare professional with the goal to access patient data. Make sure the HP is successfully authenticated.

- ☐ Checklist item (required): The authentication mean is recognized under eIDAS regulation (True / False)
- ☐ Checklist item (optional): The healthcare professional is offered to use a two-factor identification (True/False)

- ☐ Checklist item (required): A log record is created that contains the identity of the healthcare professional (True / False)
- ☐ Checklist item (optional): The log record contains the IP address of the device used by the HP to authenticate.
- ☐ Checklist item (optional): The log record contains the identifier of the device used by the HP to authenticate.

Requested evidence (to be attached to the test run)

- Provide the name of the authentication method and any proof of its implementation in your system (might be a screenshot)
- Provide the list of available factors (could be a screenshot of the screen offered to the HP)
- Provide a copy of the log record as available in your system

---

Name: Conformance of FHIR AuditEvent for HP authentication

Version: 0.1-draft

Last modified on: 21/07/2025

Authored by: xtEHR consortium

Last modified by: xtEHR consortium

Covered requirements: LOGGING-010, LOGGING-011

Description:

This test case aims at demonstrating that your system produces a FHIR Audit Event resource conformant to the technical specification when it needs to exchange a log record with an external system.

Your system is expected to create log records for different types of events. The purpose of this test is to gather a sample FHIR resource for each type of event to verify their conformance to the related FHIR Implementation Guide. The following events shall be implemented by your system:

- Authentication attempt of a healthcare professional
- Access to patient data

[...]

For each test step, upload the JSON file representing the requested FHIR Audit Event, it will be automatically sent to the conformance checker tool, and you will receive a validation report back.

Prerequisite

Before executing this test, make sure your system contains such log records and make your system generating (and or sharing if necessary for the proper functioning of your system) the related FHIR Audit Event resources.

Test steps

Step 1: Upload a FHIR Audit Event related to the authentication of a HP.

Expected result: The validation report shows a Passed.

Step 2: Upload a FHIR Audit Event related to the access of patient data.

Expected result: The validation report shows a Passed.

Laboratory result as CP (Content Producer)

Name: Produce compliant laboratory result report

Version: 0.1-draft

Last modified on: 16/07/2025

Authored by: xtEHR consortium

Last modified by: xtEHR consortium

Covered testable assertions: LAB-001, LAB-002

Description: This test case aims at demonstrating that your EHR can export the data of a laboratory result of a given patient as a conformant FHIR Bundle that complies with the Laboratory Result Report profile at http://hl7.eu/fhir/laboratory/StructureDefinition/Bundle-eu-lab.

Test steps

1. Import the attached test data into your system. You might need to first create the identity of the patient
    a. Expected result: data are available in your system.
2. Export the laboratory result as a FHIR Bundle document and upload it to the test step
    a. Expected result: the report received from the conformance checker tool does not report any failure.

Laboratory result as CC (Content Consumer)