GUIDANCE DOCUMENT FOR

Using EEHRxF in Procurements in the Digital Health Ecosystem



WITH READY-TO-USE TENDER CLAUSES & CHECKLISTS

iscte UNIVERSITY INSTITUTE OF LISBON

xShare EHR Xchange Format

ESHIA EUROPEAN STANDARDS FOR HEALTH INTEROPERABILITY ALLIANCE

Co-funded by the European Union

101136734 - xShare - HORIZON-HLTH-2023-IND-06

FOR	Public procurers, hospital and healthcare-provider procurement and IT teams, and health-technology vendors involved in digital health system procurement across the EU.
ABOUT	Practical, procurement-ready guidance for translating European Health Data Space (EHDS) and European Electronic Health Record Exchange Format (EEHRxF) requirements into tender clauses, evaluation checklists, and vendor self-assessment tools.
DATE	October 2026
FROM WHOM	Developed by the ISCTE Business Research Unit – Digital Health International (BRU-DHI)[20], in collaboration with the xShare Procurement Task Force — procurement officers, SME and start-up vendors, national health authorities, and technical experts — coordinated under the xShare project (Grant Agreement No. 101136734).
CONTACT	For any concerns or questions, please contact Syed Abrar Ahmed at syed.ahmed@iscte-iul.pt or bru-dhi@iscte-iul.pt
ACKNOWLEDGEMENTS	Henrique Martins, Syed Abrar Ahmed, Simon Lewerenz, Sergio Ricardo Denis, Evangelos Markatos, Jens Declerck, Anderson Carno, Giorgio Cangioli, Catherine Chronaki **Procurement Task Force Members[21]** Paweł Złamańczuk, Dimitrios Georgoulis, Adam Skali, Mariam Shokralla, Andrés G Castillo Sanz, Eva Sabajova, Kimberly Harding, Michael Johansen, Mikael Rinnetmäki, Liesbeth Siderius, Hernani Duarte

[20] https://brudhi.iscte-iul.pt/ ; https://www.linkedin.com/company/bru-dhi/

[21] A collaborative work of over 40 Procurement Task Force members. Only members who explicitly permitted their names to be used are mentioned.

Table of Contents

Deliverable description....2
List of abbreviations....5
List of figures....10
Executive summary....11
1. Introduction....13
2. The Problem: Why Digital Health Procurement Needs Guidance....15
3. Methodology....17
4. Implication for the xShare Yellow Button Procurement....24
5. Key Recommendations....26
6. Conclusions and Next Steps....28
7. Annex....30
Table of Contents....33
Executive summary....35
Key Recommendations....35
Quick-Start Navigator....38
1. Introduction....39
2. General Considerations....42
3. Minimum Procurement-Ready Criteria for Interoperability....53
4. Minimum Procurement-Ready Criteria for Cybersecurity....81
5. Minimum Procurement-Ready Criteria for Data Quality by Design....93
6. Minimum Procurement-Ready Criteria for Embedding Usability and User-Centred Design....103
7. Innovative Procurement Approaches....109
8. Considerations for AI-Enabled Solutions....115
Annex....117
1. Procurement Checklists for Interoperability....118
2. Procurement Checklists for Cybersecurity....123

3. Procurement Checklists for Data Quality by Design 126

4. Procurement Checklists for User-Centered Approach.....129

5. Procurers Readiness Checklist 132

6. Vendors Readiness Checklist.....136

7. Reference Standards, Regulations and Tools 141

Disclaimer: This document is guidance. It is not legal advice, it is not a formal EU guideline, and it does not replace the EHDS Regulation or any act adopted under it. The implementing acts under the EHDS Regulation, including the technical specifications of the EEHRxF, are still under development, so references to them in this document are indicative and may change. Procurers and vendors are advised to confirm the current status of the implementing acts and, once they are published, to prefer them over this guidance. This document is intended to be read alongside the xShare Deliverable D7.4.

Executive summary

Most healthcare providers do not build their own digital health systems; they buy them. This guidance exists because that purchasing decision is where the European Health Data Space (EHDS) Regulation and the European Electronic Health Record Exchange Format (EEHRxF) "starts" to be implemented. While regulation and technical specifications alone do not tell a procurement officer what to write in a tender, or a vendor what evidence could be required as proof of compliance, this guidance tries to help. It sets out, pillar by pillar, what a procurer should ask for and a vendor should be ready to demonstrate across Interoperability (organised around the six EEHRxF priority data categories: Patient Summaries, Electronic Prescription, Electronic Dispensation, Medical Test Results, including laboratory and other diagnostic results, Medical Imaging Studies and related Imaging Report, and Discharge Report), Cybersecurity, Data Quality, and Usability, together with guidance on selecting an appropriate procurement procedure for complex digital health solutions. A short, deliberately light-touch chapter on AI-enabled solutions is added; it does not aim to be comprehensive but identifies how AI components relate to the four pillars. It closes with an Annex that holds the evaluation checklists, a Procurers Readiness Checklist for procurers defining requirements and managing contracts, and a Vendors Readiness Checklist for vendors preparing to demonstrate EEHRxF compliance and articulate value. Ready-to-use tender clauses, evaluation checklists, and self-assessment tools are provided throughout, designed to be used directly, alongside an active tender or vendor response, rather than read start to finish. This guidance is about the primary-use requirements of the EHDS, that is, the requirements for systems that handle health data in the context of healthcare delivery. Secondary use of health data is referred to only for context and is not covered by the procurement criteria. In future revisions several aspects can be more targeted and aligned with the implementing acts and technical specifications as they come out in the final adopted version, this was not possible at the time of preparation of this guidance which is limited by project xShare timetables.

Key Recommendations

Each Key Recommendation is labelled Strong or Moderate. The labels are the authors' qualitative judgement of the weight of the available evidence, which consists of the regulatory text and of workshops, surveys and reviews gathering experts' input. A Strong recommendation is well evidenced and reflects high consensus among the experts consulted; a Moderate recommendation is directionally useful but less tested or depends on specifications that are not yet final (see "**How to read this document**"). The label describes the weight of the evidence behind the advice; it is not the same as the SHALL/SHOULD language of the tender clauses.

Interoperability

1. Require vendors to demonstrate structured, data export through standard HL7 FHIR interfaces for each EEHRxF priority data category relevant to your procurement — a PDF or printed report is not sufficient evidence of structured capability. Such outputs can be produced without a genuinely structured data file behind them and cannot be reliably validated. **[Strong]**

2. Ask for a demonstrated mapping between the vendor's data model and the relevant Xt-EHR logical model or other to be published as part of Art 15 Implementing Act details[22]and HL7 Europe FHIR Implementation Guide, not a general claim of "HL7 FHIR support." **[Strong]**

Cybersecurity

3. Treat cybersecurity as a lifecycle obligation: require continuous, Key-Risk-Indicator-based oversight with a Corrective Action Plan, not a one-off audit, in line with the cybersecurity risk-management measures, including policies to assess their effectiveness and security in the supply chain, that the NIS2 Directive requires of essential and important entities[23]. [Moderate]

4. Require a published Vulnerability Disclosure Policy (VDP) and Software Bill of Materials (SBOM), with tiered patch-deployment service level agreements (SLAs) **[Moderate]**

Data Quality

5. Evaluate data quality through both process measures (for example a documented validation process with a named responsible person) and outcome measures (for example completeness, accuracy, timeliness and conformance rates against thresholds set in the tender), with data provenance and version history as a baseline, non-negotiable capability of the system, which supports the procurer's own data governance. **[Strong]**

6. Ensure the system supports your own obligations as a Health Data Holder under Article 60 EHDS, not only the vendor's data-capture features. **[Moderate]**

Usability

7. In addition to vendor self-declaration as evidence of usability, always require other means of proof, such as a live demonstration, prior user-test results and/or videos of functioning software interfaces. **[Strong]**

8. Involve end-users from the needs-assessment stage of procurement, not only during pre-award demonstrations. **[Strong]**

Procurement Strategy

9. Guard explicitly against vendor lock-in: require complete, machine-readable, bulk-exportable data portability at no additional cost. **[Strong]**

10. Match your procurement procedure to your organisation's technical capacity: use Competitive Dialogue or Innovation Partnership where in-house expertise is limited but external expert support is secured and the legal conditions for the procedure are met, and the Open Procedure where in-house expertise is sufficient **[Strong]**

[22] At the time of this guidance's publication, the Xt-EHR logical information models are the most mature available reference and are used throughout this guidance on that basis. They are a Joint Action recommendation, not yet a binding legal instrument: the EHDS Article 15/36 implementing acts, once adopted, will set the binding common specifications for the EEHRxF. Procurers and vendors should confirm the current status of those implementing acts and prefer them once published.

[23] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 (NIS2 Directive), Article 21(2), http://data.europa.eu/eli/dir/2022/2555/oj.

11. Include a future-proofing clause committing the vendor to track evolving EHDS Implementing Acts and successor specifications without requiring replacement of the core platform. **[Moderate]**

12. Run the procedure itself on an established e-procurement tool, in line with the European Commission's work on e-procurement. Tools that only map the supplier market are acknowledged, not recommended, because the market for them is still immature.[24] **[Strong]**

Artificial Intelligence

13. Where a solution incorporates AI, require the vendor to disclose which AI components are present, how they are used and which regulatory category the vendor assigns to each. **[Moderate]**

[24] European Commission, "Overview of digital procurement", https://commission.europa.eu/funding-and-tenders/tools-public-buyers/digital-procurement_en (accessed October 2026): the Commission supports digitising the major steps of the public procurement life cycle (for example eSubmission, eAccess and eInvoicing) and promotes eProcurement tools such as the European Single Procurement Document and eCertis. Standard notices (eForms) are published on Tenders Electronic Daily: https://single-market-economy.ec.europa.eu/single-market/public-procurement/digital-procurement_en.

Quick-Start Navigator

This guidance is long because it needs to be thorough, not because every reader needs every page. Use the two tables below to jump straight to what may more strongly apply to you, however, you are welcome and may find it useful to read other parts.

What Are You Procuring or Updating?

Table 1: Where to start, by type of system being procured or updated

If you're procuring/updating...	Priority categories that apply	Start here	Clauses / checklist
Electronic Health Record (EHR)[25]	Patient Summaries, Electronic Prescriptions, Electronic Dispensations, Medical Imaging Studies And Related Imaging Reports, Medical Test Results, Discharge Reports	**§3.3.1, §3.3.4**	**§3.4**
LIS (Laboratory Information System)	Medical Test Results	**§3.3.3**	**§3.4**
Radiology information system / picture archiving and communication system (RIS / PACS)	Medical Imaging Studies and Related Imaging Reports	**§3.3.5**	**§3.4**
Pharmacy / e-prescribing system	Electronic Prescriptions, Electronic Dispensations	**§3.3.2**	**§3.4**
Not sure, or more than one system	Read the five-category overview first	**§3.1**	—

Table 1 covers Interoperability only, since that is the one pillar organised by system type. Cybersecurity, Data Quality, and Usability are not organised this way: their requirements apply to every system you procure. Use Table 2 below to jump directly to those chapters.

What Do You Need to Do?

Table 2: Quick-reference guide to the parts of this guidance, by task

I need to...	Go to
Understand the underlying EU regulations	**§2**
Follow the guidance manual as a procurer, including the step-by-step Procurement Process Map with a visual flowchart	**Annex §5**
Follow the guidance manual as a vendor	**Annex §6**
Draft interoperability tender clauses	**§3.4**
Draft cybersecurity tender clauses	**§4.2**
Build a cybersecurity evaluation checklist	**Annex §2**
Draft data quality tender clauses	**§5.4**
Build a data quality evaluation checklist	**Annex §3**
Draft usability / user-centred design clauses	**§6.4**
Build a usability evaluation checklist	**Annex §4**
Plan end-user involvement and piloting (new system, replacement or update)	**§6.3**
Choose a procurement procedure and e-procurement tools	**§7**
Check what to look for when a solution incorporates AI	**§8**

[25] "EHR" is used here in its common commercial sense (an electronic health record product, as hospitals and vendors generally use the term), not as restatement of EHDS Regulation's own legal definition of "EHR system."

1. Introduction

The European Health Data Space (EHDS)[26] Regulation establishes a transformative framework for health data exchange across the European Union. At its core are three strategic objectives: i) empowering patients through health data rights (primary use), ii) enabling research and innovation through structured access to electronic health data (secondary use), and iii) establishing new governance for software processing health data. The EHDS Regulation complements the General Data Protection Regulation (GDPR) and does not replace it: the rights of data subjects and the obligations of controllers and processors continue to apply, and the EHDS adds specific rights for natural persons in the health context[27].

The European Electronic Health Record Exchange Format (EEHRxF) is the technical cornerstone of this vision. For procurers, whether hospital administrators, public health authorities, or regional procurement offices, understanding how to strategically purchase systems and services that support effective implementation of EEHRxF is critical to realising the EHDS's potential.

This guidance document addresses a fundamental gap: *most healthcare providers across Europe do not have internal development teams maintaining all software systems*. The majority rely on external vendors for electronic health records (EHRs), laboratory information systems (LIS), radiology systems, and other specialised applications. When regulatory requirements shift, as they do with the EHDS, these systems must be updated through procurement mechanisms. The effort required of vendors to implement interoperability components, logging components, and compliance with new EHDS standards is not optional; it is a cost that must be factored into procurement strategies.

This guidance, was created as part of project *xShare: Expanding the European EHRxF to share and effectively use health data within the EHDS* (Project: 101136734 - xShare - HORIZON-HLTH-2023-IND-06), in WP 7, as part of Task 7.3 (Building capacity in the digital health ecosystem for Open innovation and EHRxF procurement)[28] and through participated approach with several experts. It recognises two parallel but equally important audiences: **procurers**, those tasked with defining requirements, evaluating vendors, and managing contracts, and **vendors**, those who must articulate their capabilities and commit to delivering compliant solutions.

The methodology used for the creation of this guidance document has been detailed in xShare D7.4 “Guidance for using EHRxF in procurements in the digital health ecosystem”.

1.1 How to read this document

This document serves as a practical, hands-on guide for navigating the EEHRxF within the procurement landscape and should be viewed as a supportive starting point rather than a formal EU guideline. While Sections 3 through 6 provide shared technical and operational recommendations on

[26] Regulation (EU) 2025/327 of the European Parliament and of the Council of 11 February 2025 on the European Health Data Space and amending Directive 2011/24/EU and Regulation (EU) 2024/2847 (OJ L, 2025/327, 5.3.2025), ELI: http://data.europa.eu/eli/reg/2025/327/oj

[27] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), http://data.europa.eu/eli/reg/2016/679/oj; the relationship with the EHDS is explained in Article 1 and recital 9 of Regulation (EU) 2025/327, http://data.europa.eu/eli/reg/2025/327/oj.

[28] https://xshare-project.eu/

tender language, for interoperability, cybersecurity, data quality, and usability that are essential for all stakeholders to understand, the guidance ultimately diverges into operational readiness checklists: Annex, Section 5 (Procurers Readiness Checklist) is specifically dedicated to procurers tasked with defining requirements and managing contracts, whereas Annex, Section 6 (Vendors Readiness Checklist) is tailored for vendors seeking to demonstrate their capabilities and align their solutions with these emerging standards.

The following terms are used consistently throughout the document.

- **Procurer:** the organisation that runs the procurement and signs the contract. In public procurement law it acts as the Contracting Authority, and the clauses use that term.
- **Vendor:** any organisation that offers a system or service in response to a tender. Where the EHDS Regulation places duties on the organisation that places an EHR system on the market, it calls it the manufacturer; “supplier” is used in the same sense.
- **Contractor:** the vendor once it has been awarded the contract. The tender clauses address the Contractor.
- **System:** the product or service that is bought, for example an EHR system, a laboratory information system or a patient portal, with the components that fall within the Contractor’s responsibility under the contract.
- **Operator:** the organisation that uses the system in care delivery, normally the healthcare provider, which is usually also the procurer. Some legal duties, for example under NIS2 and the rights that the EHDS gives to natural persons, fall on the operator and not on the Contractor; the system has to enable the operator to meet them

1.2 How to read Ready-to-Use Tender Clauses

Throughout this guidance document, and particularly in the Ready-to-Use Tender Clauses, the terms **SHALL** and **SHOULD**[29] are used with specific, deliberate meaning. This terminology follows the obligation-strength hierarchy defined in RFC 2119 and adopted for the EEHRxF interoperability framework in Xt-EHR Deliverable D8.1, Chapter 4.5, "Strength of Obligation"[30]:

Although this guidance document is itself non-binding, the Ready-to-Use Tender Clauses are designed to be copied directly into binding procurement documents, where RFC 2119-style obligation language is standard drafting practice; this is why that convention is used here even though the guidance itself is informative rather than normative.

- **SHALL** denotes an absolute requirement — a mandatory obligation, follows directly from an EU Regulation, that a system or contractor is expected to fulfil, and against which conformance can be assessed.

[30] https://www.xt-ehr.eu/wp-content/uploads/2026/05/D8.1-2.pdf (Xt-EHR Joint Action, Deliverable D8.1 "Classification and Functional Profiles of EHR Systems Guidelines," Section 4.5 "Strength of Obligation")

- **SHOULD** denotes a strong recommendation. There may be valid reasons, in particular circumstances, not to implement a SHOULD-level requirement, but the implications of not doing so should be understood and weighed before deciding against it.

Each SHALL-level clause is annotated in line with the specific Regulation and Article that mandates it. This is intended to ensure the Ready-to-Use Tender Clauses accurately represent the regulatory obligations a contracting authority is actually required to impose, rather than overstating them.

This is a starting point. The obligation level assigned to each clause reflects what EU regulation currently requires; it does not reflect the full range of a procurer's own institutional, operational, or policy needs. A contracting authority remains entirely free to raise the strength of any individual clause to match its own requirements, provided it does so knowingly and is prepared to enforce it as a mandatory condition of contract award.

For example, this document's accessibility-related tender clauses are expressed as SHOULD, because compliance with standards such as, for example, the **Web Content Accessibility Guidelines (WCAG)** is not itself mandated by the EU regulations in scope of this guidance. A procuring authority that wants to make accessibility compliance a hard requirement, for instance, because of national accessibility legislation, an internal digital-inclusion policy, or simply a strategic priority, can and should change the relevant clause from "The Contractor should ensure conformance with EN 301 549..." to "The Contractor shall ensure conformance with EN 301 549...". The same logic applies to any other SHOULD-level clause in this document: procurers are encouraged to review each clause against their own legal, organisational, and policy context and adjust its strength accordingly, rather than treating the SHALL/SHOULD assignments here as fixed.

2. General Considerations

2.1 The EHDS regulatory landscape

2.1.1 Primary and Secondary Use Pathways

When it comes to health data, the EHDS Regulation distinguishes between **primary use** (direct healthcare provision) and **secondary use** (research, innovation, public health, and regulatory decision-making). This distinction shapes procurement requirements.

Primary Use of Health Data Timeline

- **March 2029**: Mandatory exchange of the first tier priority data categories (patient summaries, electronic prescriptions and electronic dispensations) in all EU Member States
- **March 2031**: Mandatory exchange of the second tier priority data categories (medical imaging studies and related imaging reports, medical test results, discharge reports)

Secondary Use of Health data Timeline

- **March 2029**: Rules on secondary use enter into application for most electronic health record data
- **March 2031**: Rules extend to remaining data categories including genomic data

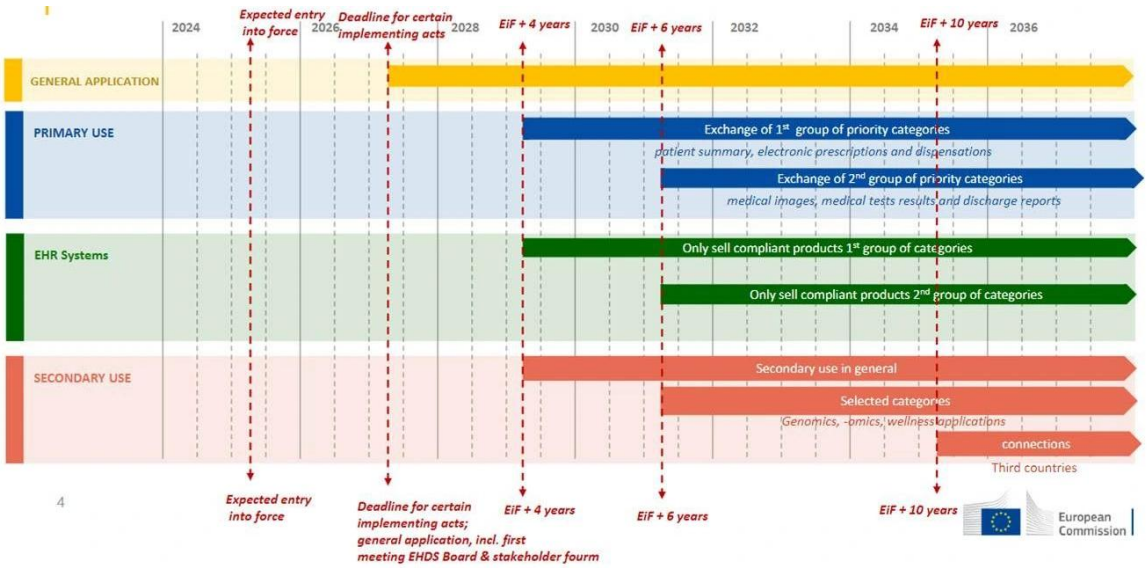


Figure 3: EHDS application timeline for primary use, EHR systems and secondary use

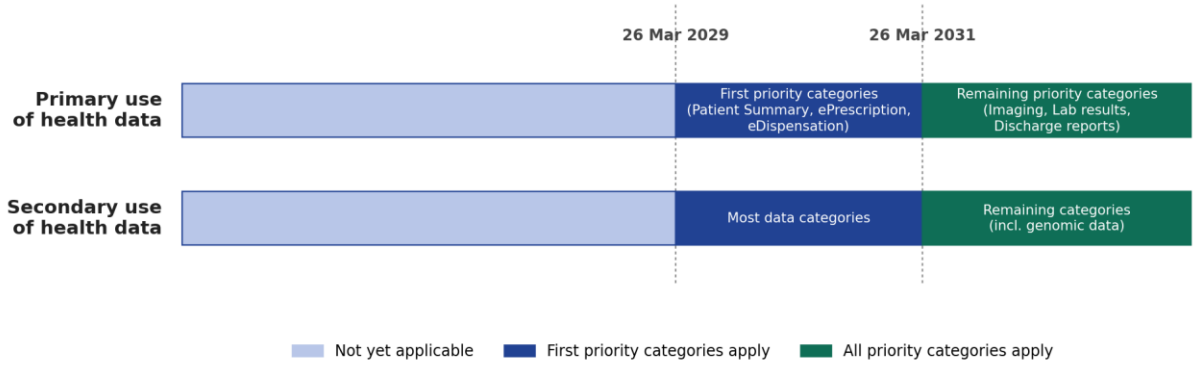


Figure 4: Application dates of the EHDS priority data categories for primary and secondary use (26 March 2029 and 26 March 2031). Adapted by authors from European Commission Sources.

Data Quality Requirements

Article 13 of the EHDS Regulation establishes that by 26 March 2027, the Commission shall, by means of implementing acts, determine data quality requirements, including in relation to semantics, uniformity, consistency, accuracy and completeness, for the registration of personal electronic health data in an EHR system as relevant. Those implementing acts shall be adopted in accordance with the examination procedure referred to in **Article 98(2)**.

However, the implementing acts remain under development as of this guidance's publication. Current regulatory language refers to semantics, uniformity, consistency, accuracy, and completeness, but does not yet define operational thresholds or measurement methodologies.

Implication for Procurers: While specific regulatory requirements continue to evolve, procurers should begin embedding data quality assurance mechanisms and contractual accountability into procurements now. This positions organisations to achieve compliance with future implementing acts and, importantly, to optimise the value of data for patient care and research.

Legacy Data and Consolidated Views

Article 3(1) gives natural persons the right to access at least the personal electronic health data relating to them that belong to the priority categories and are processed for the provision of healthcare, in an easily readable, consolidated and accessible format through the electronic health data access services, and **Article 3(2)** gives them the right to download an electronic copy in the EEHRxF. The Regulation does not oblige healthcare providers to harmonise legacy records retrospectively, and no regulatory pathway for doing so currently exists, so historical records of unmeasured and potentially unknown quality may remain outside the harmonised format. Procurers should nevertheless make the handling of legacy data a procurement requirement and clarify with vendors how legacy systems will be managed during transitions to EEHRxF-compliant systems, for example whether, how and at what price historical records can be converted or exported.

It is worth distinguishing two related but different problems here. **Legacy systems** are the EHR, laboratory, imaging, and other platforms already deployed in a healthcare provider, which may predate EEHRxF entirely. **Legacy data** is the historical patient information already held inside those systems, often of unmeasured or inconsistent quality. Procurement can address one without the

other — replacing the system does not automatically clean up the data it holds, and cleaning up the data does not by itself make an old system EEHRxF-capable.

On legacy systems specifically, the Commission's official EHDS guidance confirms that healthcare providers are not required to replace systems already deployed: they must be able to export and import data in the EEHRxF, but how they achieve this is left to them, either by upgrading the existing system directly, or by introducing a translation layer that converts between the system's internal format and the EEHRxF[31]. A system built specifically to perform this conversion is itself explicitly recognised as an EHR system under the Regulation, and procurers evaluating a translation-layer approach should hold it to the same EEHRxF conformance evidence as a native upgrade.

On legacy data, no implementing act currently defines a harmonisation pathway for historical records, and this guidance is not aware of one being imminent. Procurers should treat this as an open question to raise directly with vendors, not an oversight to work around silently:

- Ask whether historical records will be migrated into the new system's structured fields or only remain accessible as scanned or read-only legacy documents.
- Ask how the vendor handles a consolidated view spanning both migrated and non-migrated records, since **Article 3** requires that patients receive their data in a consolidated, easily readable format, without excluding historical records simply because they predate EEHRxF.
- Budget migration and data-quality remediation as a distinct line item, separate from the core system procurement, since its scope and cost depend entirely on the condition of the specific legacy data being carried forward.

2.2 Key Building Blocks of the EEHRxF

The building blocks below reflect the standards and specifications **most widely used in current EEHRxF-aligned implementations**. They are named deliberately and concretely, to give procurers and vendors a testable reference rather than a placeholder, but they are not yet formally mandated by the EHDS Regulation itself. The binding technical detail will ultimately be set by the implementing act under **Article 15** (the EEHRxF itself: technical representations, metadata, category-specific data models, coding systems and value sets) and by the common specifications under **Article 36** (the interoperability and logging requirements for EHR systems), which may adopt these same standards, adapt them, or specify others; procurers should treat the list below as the current best-available reference and confirm against the published implementing acts and specifications once adopted.

- **HL7 FHIR (Fast Healthcare Interoperability Resources):** the international standard for representing clinical data as structured, machine-readable resources and for exchanging them through APIs; it is the technical basis of most of the building blocks listed below. FHIR is applied through HL7 FHIR Implementation Guides (IGs).
- **HL7 FHIR Implementation Guides:** the guides that specify how the HL7 FHIR standard should be used to implement the EEHRxF/EHDS requirements. The normative EEHRxF implementation guide is expected to be developed by the Commission together with the

[31] https://health.ec.europa.eu/document/download/4dd47ec2-71dd-49fc-b036-ad7c14f6ed68_en?filename=ehealth_ehds_qa_en.pdf (European Commission, Frequently Asked Questions on the European Health Data Space, Qs 22 and 29)

Member States and approved by the EHDS Board; the guides named here are the main existing work on which it can build. They include the European guides that profile the priority categories for use in Europe, which build on the HL7 Europe Base and Core guide[32]. This suite comprises also a European specialized version of the International Patient Summary (IPS), a standardised, minimal dataset of essential clinical information (medications, allergies, problems, immunisations) supporting cross-border and cross-organisation continuity of care, compliant with the ISO IPS. For example, the MyHealth@EU Patient Summary is based on the HL7 Europe Patient Summary, and the other priority categories follow the same approach.

- **Transport:** for the exchange of EHDS data, the expected technical basis is the HL7 FHIR REST API, with authorisation tokens that carry a defined minimum content (issuer, validity period, the health professional and healthcare provider, the natural person concerned, the scope of access). The Commission may publish implementation guides for this in the form of an "EHDS API". The specifications to look for are the EU Health Data API FHIR Implementation Guide developed under the EURIDICE project (joint HL7 Europe and IHE Europe)[33] and, for imaging, the EU Imaging Manifest and Access Implementation Guide (the IHE MADO additions)[34]. At the time of writing, both are works in progress and have not been adopted by the Commission; they are candidates for, and not yet, the specification of the EHDS API.
- **Imaging and unstructured content:** DICOM is the standard for images, which are transported through DICOMweb REST Services. Where data are not yet available in structured form, a PDF/A document or an HL7 FHIR narrative is expected to remain a permitted way of exchanging them, but the aim is structured data, and procurers should ask for the structured representation wherever the system holds it.
- **IHE Profiles:** IHE profiles are standards-based integration specifications that define how to exchange clinical and administrative information for specific use cases. The transport specifications mentioned above reuse and specialise for the European purposes some of these profiles. For example IHE MADO and XC-WADO for imaging study exchange; IHE MHD for document search and retrieval; and so on.
- **Structured Data Formats and Standard Vocabularies:** standardised coding systems (for example SNOMED CT, in the EEHRxF in the form of the SNOMED Global Patient Set (GPS), for clinical concepts; LOINC for laboratory observations and document types; ICD-10, ICD-O and Orphacode for diagnoses; the WHO ATC classification, EMA SPOR substance terms and EDQM Standard Terms for medicinal products; and UCUM for units of measure) that allow data entered in one system to be understood, unambiguously, by another. Elsewhere in this guidance, named vocabularies are generally given as illustrative examples. For EEHRxF exchange, preferred code systems will be identified for each data field, and technical specifications will specify the value sets expected to be used. Where Member States adopt

[32] HL7 Europe, Base and Core FHIR Implementation Guide, STU 1.0 (R4 and R5), https://hl7.eu/fhir/base and https://hl7.eu/fhir/base-r5, and HL7 Europe Extensions Implementation Guide, https://hl7.eu/fhir/extensions (accessed 9 November 2026).

[33] EURIDICE (HL7 Europe and IHE Europe), EU Health Data API FHIR Implementation Guide, version 1.0.0-ballot (STU 1 ballot), https://hl7.eu/fhir/health-data-api/1.0.0-ballot (accessed 9 November 2026).

[34] HL7 Europe and IHE Europe, EU Imaging Manifest and Access Implementation Guide (IHE Manifest-based Access to DICOM Objects, MADO, additions), https://build.fhir.org/ig/hl7-eu/imaging-manifest/ (development build, accessed 9 November 2026); see also https://euridice.org/mado/.

different code systems or value sets, mapping rules will need to be defined for cross-border exchange purposes.

Procurers need not become experts in these specifications; however, they should require vendors to demonstrate explicit support for them and to provide test evidence of compliance.

2.3 Compulsory Elements (by regulatory obligation)

The regulatory landscape creates both compulsory requirements (derived from binding EU directives and regulations) and optional enhancements that drive toward the regulation's aspirational goals.

Responsibility under these rules is shared between the vendor and the organisation that operates the system. Some obligations fall on the supplier of the product, for example under the Cyber Resilience Act (CRA), the Medical Device Regulation (MDR) and the EHDS requirements for EHR systems. Others fall on the healthcare provider that operates it, for example under NIS2 and under the rights that the EHDS gives to natural persons (for example, the xShare Yellow Button, which lets a natural person download or share their data in the EEHRxF, is one way of implementing the access and portability rights in Articles 3 and 7). A procured system does not discharge the provider's duties; it has to enable the provider to meet them. For example, it is not the vendor's task to make sure that patients actually read their discharge summaries, but the system must be capable of offering the possibility to access in a structured format. The tender requirements in this guidance should be read in this light: they ask what the product must be able to do, and they leave to the Contracting Authority what only the operator can do.

The table below is a scanning aid, not a substitute for the detailed treatment of each regulation that follows. It gives the article(s) this guidance cites and, in one line, why.

Table 3: Compulsory regulatory elements: key articles and why they matter for procurement

Regulation	Key article(s) cited here	Why it matters for procurement
GDPR	Arts. 9, 20, 25, 28, 32	Health data as a special category; data portability; security and processor obligations.
NIS2 Directive	Cited generically (see below)	Cybersecurity risk management, incident reporting, and supply-chain oversight — transposed differently per Member State.
MDR	Art. 21; Annex I §17.2, 17.4; Rule 11, Annex VIII	Governs devices and, via Rule 11, AI-enabled clinical software embedded in or interoperating with the EHR.
EHDS Regulation	Arts. 3, 15–17, 25, 36	Establishes primary-use rights, EEHRxF technical requirements, and common specifications for EHR systems.
Data Act	Regulation (EU) 2023/2854	Vendor lock-in and switching protections for all data processing services (IaaS, PaaS, SaaS), protection against unfair data-related terms, access to connected-product data and safeguards against third-country governmental access.

AI Act	Art. 27 (FRIA, scoped)	Fundamental Rights Impact Assessments (FRIA) for specific high-risk AI deployers using clinical decision support.

2.3.1 General Data Protection Regulation (GDPR)

- **Article 9:** Specific requirements for processing "special categories of personal data" (health data).
- **Article 20:** The "Right to Data Portability," specifically the technical capability for data export.
- **Article 25:** Compliance for Data Protection by Design/Default
- **Article 28:** Clear definition of responsibilities for the vendor acting as a "Processor".
- **Article 32:** Compliance for Security of Processing.

2.3.2 NIS2 Directive

- The guidance references the NIS2 Directive **generically** ("the solution shall comply with the NIS2 Directive") rather than citing specific articles.
- This is a deliberate departure from the article-specific approach used elsewhere in this section. NIS2, as a **directive** rather than a regulation, is transposed differently into national law in each Member State, so a single EU-wide article reference risks being locally inaccurate. Procurers should confirm the specific national transposition applicable to their jurisdiction.
- At minimum, tenders should require evidence of: risk-management measures, incident-reporting procedures aligned with national timelines, asset management (including supply-chain components), and third-party/supply-chain security oversight — see Section 4.2 for ready-to-use clause language regarding Cybersecurity.

2.3.3 Medical Device Regulation (MDR)

- **Article 21:** Devices for special purposes[35] (investigational and custom-made devices).
- For AI-enabled and other software components specifically, the more directly relevant MDR provision is the software classification framework in **Rule 11 of Annex VIII**[36], which determines the risk class, and therefore the conformity assessment route, that clinical decision-support and other medical-purpose software must follow.
- **Annex I §17.2**: State-of-the-art, secure software development and risk management, plus manufacturer-set minimum IT-security requirements under §17.4.
- **MDR-AI Act Interplay:** Procurement specifications for AI-enabled EHR components must account for the dual compliance requirements of both the MDR and the upcoming EU AI Act.

2.3.4 European Health Data Space (EHDS)

- **Articles 15–17:** Focus on the primary use of health data and the technical requirements for EHR systems.
- **EEHRxF:** Support for EEHRxF-compliant data exchange in priority categories aligned with EHDS timelines

[35] https://eur-lex.europa.eu/eli/reg/2017/745/oj/eng (MDR)

[36] https://health.ec.europa.eu/system/files/2020-09/md_mdcg_2019_11_guidance_en_0.pdf (MDCG 2019-11, Guidance on Qualification and Classification of Software)

- **Article 36:** Requires the Commission to adopt implementing acts setting the common specifications for the interoperability and logging components that Article 25 requires every EHR system must contain before it can be placed on the EU market; from the date these apply, an EHR system may only be sold if it meets them for the priority categories then in scope.
- **Use-Case Alignment:** Procurement clauses for EHDS should be "modular." For example, requirements for secondary use (research/innovation) should only be mandatory if the specific use case of the hospital or health authority requires it, to avoid unnecessary vendor costs.

2.3.5 Data Act

- Added as a compulsory element **covering every data processing service, not only SaaS**. The Data Act defines a data processing service as a digital service that gives on-demand network access to a shared pool of configurable, scalable and elastic computing resources (**Article 2(8)**). It therefore applies whether the service is delivered as infrastructure, platform or software as a service (IaaS, PaaS, SaaS) or as a storage or database variant of these (StaaS, DBaaS)[37]. A hosted EHR, the cloud platform beneath a vendor's product and a managed database service are all covered, and cloud hosting is the deployment model in which most EHR systems are now procured. Its absence from the compulsory baseline was raised independently on multiple instances and was treated as a priority gap under this guidance's own rule that recurring, independently-raised concerns take priority for revision.
- **Regulation (EU) 2023/2854 (Data Act):** requires providers of data-processing services (cloud services in any delivery model: IaaS, PaaS, SaaS, StaaS or DBaaS) to remove technical and contractual barriers to switching provider ("vendor lock-in") and to progressively eliminate data-egress charges, with charges for switching prohibited from **12 January 2027**.
- The Contractor shall provide a documented **Switching and Exit Plan**, specifying the formats, methods, and timeframe required to export all Exportable Data and Digital Assets to a new environment. The maximum transitional period shall not exceed **30 calendar days** following the applicable notice period, which itself shall not exceed two months. Where 30 calendar days is technically unfeasible, the Contractor shall notify the Contracting Authority within 14 working days of the switching request, justify the unfeasibility and indicate an alternative transitional period of no more than seven months, with full-service continuity throughout (Data Act Article 25(2) and (4))
- The Contractor shall not impose switching charges, including data-egress charges, on the Contracting Authority for actions mandated by the switching process *(mandated by Data Act Article 29),* and shall make open interfaces available to support switching *(Data Act Article 30(2); for services consisting only of infrastructure elements (IaaS), Article 30(1) requires reasonable measures to enable functional equivalence in the destination service instead),* consistent with common specifications and harmonised standards published in the central Union standards repository for data-processing service interoperability *(Data Act Article 30(3); repository established under Article 35(8))*.

[37] https://eur-lex.europa.eu/eli/reg/2023/2854/oj/eng (Data Act, Regulation (EU) 2023/2854, Article 2, point (8), definition of data processing service; recital 81, which sorts data processing services into the delivery models infrastructure as a service, platform as a service and software as a service and treats storage as a service and database as a service as variations of them; Article 31(1), under which Articles 23, point (d), 29 and 30(1) and (3) do not apply to services that are custom-built for an individual customer and not offered at broad commercial scale)

- Where the Contractor's standard terms on access to and use of data, or on liability and remedies for breach or termination of data-related obligations, have been unilaterally imposed on the Contracting Authority, they are not binding if they are unfair (Data Act Article 13(1)). Terms presumed unfair include those that inappropriately limit remedies or liability, prevent termination within a reasonable period or prevent the customer from obtaining a copy of its data (Article 13(5)). The protection applies between enterprises, so a Contracting Authority should confirm with its legal advisers whether and how it can rely on it and should in any case negotiate these terms and not accept vendor standard conditions as offered.
- Where the solution includes connected products, for example connected medical or monitoring equipment (IoT), and related services, the Contracting Authority as user is entitled to access the product data and related service data they generate, easily, securely and free of charge, in a structured, commonly used and machine-readable format, and to have them shared with third parties of its choice (Data Act Articles 3 to 5). Article 3(1) applies to connected products placed on the market after 12 September 2026. Where these data are personal data, the GDPR applies in addition.
- Providers of data processing services must take adequate technical, organisational and legal measures, including contracts, to prevent international and third-country governmental access to, and transfer of, non-personal data held in the Union where this would conflict with Union or national law, and must inform the customer of a third-country authority's access request before complying with it, unless the request serves law enforcement purposes (Data Act Article 32(1) and (5)). Personal health data remain subject to the GDPR rules on transfers to third countries (Chapter V). The corresponding tender clause is in Section 4.2.6 (Data Exchange Security).

Ready-to-use Standard Contractual Clauses implementing these obligations are provided in Section 3.4, alongside the EEHRxF-specific interoperability clauses, since vendor lock-in was raised by workshop participants as fundamentally an interoperability and data-portability concern rather than a separate compliance domain.

2.3.6 Additional Compulsory Regulations

- **AI Act:** Inclusion of FRIA and Assessment List for Trustworthy AI (ALTAI)[38]services, prior to deploying the high-risk AI systems named in **Article 6(2)** of the AI Act, a public hospital deploying an AI-driven diagnostic support tool would typically be in scope; a private clinic procuring the same tool for internal use only may not be. Separately, where a system includes AI that generates clinical content itself (for example, an AI scribe drafting a discharge note or consultation summary), the AI Act's transparency rule for synthetic content (**Article 50(2)**)[39] is directly relevant: AI-generated content must be marked in a machine-readable, detectable format, which procurers should ask vendors to confirm and demonstrate.

[38] https://eur-lex.europa.eu/eli/reg/2024/1689/2026-07-27/eng (AI Act, Article 27)

[39] Regulation (EU) 2024/1689 (AI Act), Article 50(2): providers of AI systems, including general-purpose AI systems, generating synthetic audio, image, video or text content shall ensure the output is marked in a machine-readable format and detectable as artificially generated or manipulated. https://eur-lex.europa.eu/eli/reg/2024/1689/oj

- **Cyber Resilience Act (CRA):** Essential for the baseline cybersecurity of EHR hardware and software products.
- **Data Governance Act & Digital Services Act:** General compliance for digital health ecosystem participants.
- **EIDAS:** Access controls and authentication aligned with eIDAS standards

- **Alignment with National Requirements:** While focusing on EU-wide standards (EEHRxF), vendors should demonstrate readiness to adapt to specific national health data nuances. This is listed here as a vendor-readiness signal rather than a formal compliance category, but the distinction matters: national health data rules are binding requirements in their own right, not optional extras, and procurers should treat this bullet as a prompt to identify their own applicable national rules directly, rather than as evidence that national compliance is itself negotiable.

2.4 Additional Elements

To encourage innovation and market competitiveness, procurers should consider the following "Nice-to-Have" elements during the vendor evaluation phase:

- **Open APIs (Free of Charge):** Vendors should provide open, well-documented APIs without additional licensing fees to prevent vendor lock-in and support ecosystem growth. A standards-based, documented API is the usual technical route for an EHR system to support the EEHRxF (the EHDS Regulation requires a system that stores or intermediates personal electronic health data to provide an interface to that data in the EEHRxF, Annex II, points 2.1 to 2.3), and it is the practical basis for supporting the rights of natural persons to access and share their data, for example through the Yellow Button. Downloading and uploading an electronic copy in the EEHRxF is a complementary route for those rights.
- **SMART App Launch Support:** Support for the SMART on FHIR standard to allow third-party clinical applications to run seamlessly within the EHR or a patient portal. Listed here, alongside Open APIs, because it is a concrete, testable way to deliver on the same underlying goal stated at the top of this section: letting a hospital add best-of-breed clinical applications without being locked into a single vendor's app ecosystem.
- **Implementation Capacity:** Evidence of the vendor's ability to ground technical interoperability standards in the practical operational reality of a hospital environment.

2.5 Balancing Generic vs. Specific Regulatory References

While general compliance with EU regulations is a baseline requirement, this guidance recommends that procurers cite specific articles as "Minimum Procurement-Ready Criteria". This approach serves as an expectation matching exercise, ensuring that both the procurer and vendor share a technical understanding of high-level legal requirements (e.g., defining what "security by design" specifically entails under GDPR Article 25). This reduces the risk of contractual disputes and ensures that local interpretations of EU directives do not lead to fragmented implementations.

Generic references are faster to draft but create an "expectation-matching" gap, because directives such as NIS2 are transposed differently across Member States, and regulatory articles are often broadly worded; a generic clause leaves procurer and vendor to much freedom, a gap that surfaces only after the contract is signed. Participants also warned against the opposite extreme: listing every conceivably relevant article regardless of use case, likened by one participant to specifying four-wheel drive and snow tyres for a buyer who will never drive on ice; it inflates vendor cost without

adding value and can unnecessarily exclude well-suited vendors. This guidance therefore binds specific articles to specific use cases wherever possible (for example, tying secondary-use provisions to whether the procuring organisation is research-active) rather than applying both extremes uniformly. The recommendations wherein are the result of a co-creation exercise between experts, they serve to highlight and, whenever possible, to give concrete examples on what regulations are key and can be called upon in procurement. Naturally, if a solution needs to be compliant with a certain regulatory aspect that compliance is not eliminated by an absence to its reference in this guidance or in the procurement documents themselves.

Every regulation below is legally binding on the parties it applies to, nothing in this guidance treats compliance itself as optional. What varies is how this guidance recommends citing each one in a tender, which is a different question. The table provides a snapshot of different regulations and their application/citation for the type of product being procured. For the EHDS/EEHRxF, the citation remains subject to the implementing acts under Articles 15 and 36, which are not yet adopted.

Table 4: Legally binding regulations: how this guidance cites each regulation

Regulation	Applies to	How this guidance cites it	Citation approach
GDPR	Every procurement in scope	Specific articles (9, 20, 25, 28, 32)	Specific article(s)
EHDS / EEHRxF	Every procurement in scope	Specific articles (3, 15–17, 36)	Specific article(s)
NIS2 Directive	Every procurement in scope	Generic reference — national transposition varies by Member State	Generic reference
MDR (incl. Rule 11 for software)	Only where the system is, or embeds, a medical device or AI-driven clinical decision support	Specific article (21) plus Rule 11 for software classification	Conditional — device/software-dependent
IVDR	Only where the system interfaces with in-vitro diagnostic devices (e.g., a LIS)	Applied by analogy with MDR, little details are covered but it should be verified for applicability case-by-case	Conditional — device-dependent
Data Act	Only where the solution is, or relies on, a data processing service (IaaS, PaaS, SaaS) or includes connected products	Standard Contractual Clauses, Section 3.4.9	Conditional — deployment-dependent
AI Act (FRIA)	Only high-risk AI, deployed by public bodies or private entities providing public services	Specific article (27), scoped	Conditional — deployer-dependent
eIDAS	Every procurement in scope, for authentication	Referenced generically for access-control alignment	Generic reference

Additionally, convergence on “must-have” status is itself uneven across regulations: GDPR compliance was the only item to receive unanimous support, followed by ISO/IEC 27001 and the NIS2 Directive; further down the technology stack, with IVDR and ISO 27799. This is consistent with the guidance's approach of treating lower-convergence items as conditional on the specific solution being procured, rather than compulsory in every tender.

2.6 From Technology-Centred to User-Centred Procurement

Traditional procurement emphasizes technology-centred requirements: what a system does, on paper, in a specification document. User-centred procurement asks a complementary question: whether the people who will use the system, clinicians, nurses, patients, administrative staff, can, and will use it safely and as intended.

Table 5: Technology-centred versus user-centred procurement

Traditional, technology-centred	**User-centred**
Specifies technical features and compliance checkboxes.	Starts from the real needs, goals, and working context of end-users.
Treats all users as interchangeable.	Recognises diverse user profiles and designs inclusivity into adoption strategies.
Assumes deployment ends at go-live.	Provides structured support and guidance to embed the system into daily practice, beyond go-live.

Why This Matters for EHDS?

- The success of EEHRxF implementation depends not only on technical correctness but on clinicians' willingness to use new interoperability features in their workflows.
- Patient engagement with their own data is a key EHDS objective and requires usable, trustworthy interfaces (see Section 6 for detailed procurement language and evaluation frameworks for usability and user-centred design).

3. Minimum Procurement-Ready Criteria for Interoperability

3.1 Operationalising Interoperability Concepts

Interoperability in EHDS context means the ability of systems to exchange, interpret, and use health data across organisational and geographic boundaries in standardised formats. In procurement terms, this translates to specific technical requirements and contractual obligations.

A procurer does not buy the EEHRxF itself; EEHRxF is a specification, not a product. A procurer buys a **product**, an EHR, a LIS, a RIS/PACS, a pharmacy system, and what this chapter defines is the set of **features and evidence** that product must have for it to genuinely support EEHRxF, rather than merely claim to. Every requirement below should be read this way: not “comply with EEHRxF” as an abstract obligation, but a specific, checkable feature the vendor either has or does not have.

Two different questions should be kept apart throughout this chapter. The first is a **readiness** question: is this vendor able, and likely, to bring its product into conformity with the EHDS requirements? Most of the questions below are of this kind and can be asked today. The second is a **conformity** question: is this product actually conformant? The manufacturer states this in the EU declaration of conformity (Articles 30(1)(e) and 39 of the EHDS Regulation)[40]. What exactly has to be demonstrated for that can only be specified precisely once the implementing acts and EHDS Board guidance documents have been adopted.

3.1.1 The EEHRxF Priority Data Categories

Article 14 of the EHDS Regulation designates six categories of personal electronic health data as **priority categories**, which in practice group into five exchange domains around which essentially all current European technical specification work, including the xShare project's own scope, is organised:

- **Patient Summary** — a standardised overview of essential clinical information (allergies, active problems, medications, immunisations, implants, procedures). Mandatory exchange from **26 March 2029**.
- **Electronic Prescription and Electronic Dispensation**[41] — electronic medicine prescriptions and records of their dispensing. Mandatory exchange from **26 March 2029**
- **Medical Test Result, including laboratory and other diagnostic result and related report —** the outcomes of laboratory and other diagnostic examinations and the reports that interpret them. Mandatory exchange from **26 March 2031**.
- **Medical Imaging Studies and Related Imaging Reports** — imaging studies and their associated radiologist/reporting findings. Mandatory exchange from **26 March 2031**.
- **Discharge Report** — the clinical summary of an inpatient episode, including diagnoses, procedures, and follow-up recommendations. Mandatory exchange from **26 March 2031**.

[40] https://eur-lex.europa.eu/eli/reg/2025/327/oj/eng (EHDS Regulation, Article 30(1)(e), manufacturer obligation to draw up the EU declaration of conformity, and Article 39, EU declaration of conformity)

[41] Note: in EHDS regulation text they are separated categories, but both in projects, services and documentation created so far, they always are considered together.

This chapter is organised around these five domains directly, following section 3.3 below, because this is how a procurer actually experiences the problem: not by asking "is this system EEHRxF-compliant" in the abstract, but by evaluating "will the discharge reports this system produces be usable outside this hospital in 2031, and what should I be asking the vendor right now."

3.1.2 How the Specifications Fit Together

For each of the categories, a set of specifications already exists, in varying states of maturity, and a procurer does not need to track all of it independently. The technical-specification in this list (everything below the Regulation itself) are not yet normative and have not yet been adopted by the European Commission or the Member States at the time of publication of this guidance; the list below is therefore indicative and non-exhaustive. It is not a fixed hierarchy: the implementing acts may adopt, adapt or supersede some of these artefacts (for example the Xt-EHR logical models). The list runs from the legal basis down to the testable specifications that are currently available:

- **The EHDS Regulation**[42] ((EU) 2025/327) sets the legal obligation and the timeline (Article 14), and will be further specified by **Implementing Acts**, most of which are not yet adopted at the time of writing. Where this guidance cannot yet point to a final Implementing Act, it says so explicitly rather than presenting a draft specification as settled law.
- **eHealth Network (eHN) Guidelines**[43] provide the clinical, implementation-independent definition of what each report should contain (for example, the eHN Hospital Discharge Report (HDR) Guideline). These predate EHDS and were produced under the eHealth Network established by Directive 2011/24/EU; they are the clinical requirements source that everything downstream is built from.
- **Xt-EHR EHDS Logical Information Models**[44], produced by the EU4Health-funded Xt-EHR Joint Action, translate the eHN guidelines into structured, technology-neutral data models, covering all priority categories. These are the models the future EEHRxF technical specifications and Implementing Acts are expected to be built on. The regulatory (and procurement-relevant) definition of the logical model will be made in the implementing act under Article 15 of the EHDS Regulation.
- **HL7 Europe FHIR Implementation Guides**[45] turn the Xt-EHR models into concrete, testable HL7 FHIR specifications, one per category, Xt-EHR, MyHealth@EU, and, specifically, with direct XpanDH[46] and xShare[47] project involvement.
- **MyHealth@EU FHIR Implementation Guides**[48] adapt the HL7 Europe Implementation Guides (IGs) for actual cross-border exchange between Member States, adding the specific profiles and value sets used in production cross-border services.

[42] Regulation (EU) 2025/327: https://eur-lex.europa.eu/eli/reg/2025/327/oj
[43] https://health.ec.europa.eu/ehealth-digital-health-and-care/digital-health-and-care/eu-cooperation/ehealth-network_en
[44] https://build.fhir.org/ig/Xt-EHR/xt-ehr-common/
[45] https://hl7.eu/fhir/
[46] https://xpandh-project.iscte-iul.pt/ ; CORDIS: https://cordis.europa.eu/project/id/101095594
[47] https://xshare-project.eu/
[48] https://fhir.ehdsi.eu/

- **IHE Profiles**[49] define the actors and transactions that can be used for the exchange of the priority category data, for example IHE Mobile access to Health Documents (MHD) for document exchange, Manifest-based Access to DICOM Objects (MADO) for access to imaging studies.
- **EURIDICE**[50] **specifications** EURIDICE is a joint HL7 Europe / IHE Europe initiative that brings together the methodologies and expertise of both organizations, with the explicit aim of providing the European Commission with implementable and testable specifications to support the EHDS Implementing Acts.
  The term EURIDICE specifications is not used only for the jointly developed FHIR Implementation Guides; but it refers more broadly to specifications published and maintained by HL7 Europe, IHE Europe, or jointly by both organizations, which are considered suitable for use in the context of the EHDS. These include HL7 Europe FHIR Implementation Guides, IHE profiles such as MADO, and jointly developed specifications as for example the **EU Health Data API specification**, currently undergoing its STU1 ballot, which defines how EHR systems provide and consume EEHRxF data (see Section 3.2.1).

A vendor that can point to a concrete artefact at the EURIDICE (HL7 Europe / IHE-Europe) or MyHealth@EU for a given category is demonstrably closer to EEHRxF readiness than one that only cites the EHDS Regulation or the eHN guideline. Regarding EURIDICE artefacts these are not yet endorsed or adopted by the European Commission, so they indicate direction of travel rather than formal compliance. The domain-by-domain guidance in Section 3.3 asks, for each category, exactly which artefact to ask for.

3.2 Cross-Cutting Technical Foundations

The following six requirements apply across all six priority data categories, and should be established as baseline procurement criteria before turning to the category-specific guidance in Section 3.3. They are the questions that, across all the sources surveyed for this guidance, most reliably separate vendors that are close to EEHRxF readiness from those that are not.

3.2.1 HL7 FHIR-Based Interoperability (Interface Level)

The EEHRxF-related specification proposals currently available, are built on HL7 FHIR, although binding technical specifications have not yet been adopted (Articles 15 and 36 of the EHDS Regulation). Many deployed systems are legacy applications built on other architectures (for example HL7 v2 or proprietary APIs); this is not in itself disqualifying. What matters is that the vendor can show how the product will provide and receive EEHRxF data through the European interoperability software component, for example through a HL7 FHIR-based interface layer; a dedicated HL7 FHIR server is not itself required. In plain terms: can the product exchange data through standard, publicly documented interfaces rather than closed ones? Ask the vendor for:

- Confirmation of which HL7 FHIR versions is supported today (R4/R5 or other) and the vendor's migration roadmap. The HL7 FHIR version(s) required for the EHDS are expected to be defined

[49] https://profiles.ihe.net/ITI/MHD/ (IHE ITI, Mobile access to Health Documents, MHD); https://profiles.ihe.net/RAD/MADO/ (IHE Radiology, Manifest-based Access to DICOM Objects, MADO, v1.0.0 trial-use)
[50] https://euridice.org/

in EHDS Board guidance once available. Procurers are advised to check with their national digital health authorities which version(s) are endorsed nationally and at the EU level at each moment.

- Articles 30 and 39 of the EHDS Regulation require the manufacturer to draw up an EU declaration of conformity[51]; the details of this declaration are, at the time of publication of this guidance, still to be laid out in the corresponding implementing acts and EHDS Board guidance documents. If not already demanded for the declaration of conformity, vendors should in addition provide a published, system-specific **CapabilityStatement**, the HL7 FHIR resource that formally declares which resources, operations, and search parameters a server actually supports, rather than a general claim of "HL7 FHIR support."
- Evidence of a working **HL7 FHIR REST API** (ideally conforming to the EURIDICE EU Health Data API specification), not only batch file export.
- Support for **Bulk FHIR export** ("$export" operation)[52], recommended for any scenario involving migration, population-level extraction, or large-scale data portability.
- Support for SMART-based or IHE IUA authorization as described in the EURIDICE EU Health Data API specification.

3.2.2 Terminology and Vocabulary Requirements

Most interoperability failures in practice are failures of **coding**, not of message format: two systems can both be technically HL7 FHIR-conformant and still fail to exchange usable data if they use different, unmapped local code lists. Ask which of the following the vendor supports:

- **SNOMED CT** for clinical concepts (problems, procedures, findings).
- **LOINC, NPU** for laboratory and other observations.
- **ICD-10,** with a documented ICD-11 migration path, for diagnoses.
- **ATC** for the classification of medicinal products and for the type of an immunisation
- **SNOMED GPS, EMA PMS, EMA SPOR SMS, EDQM** for the identification of a medicinal products, substances and other medication attributes
- **UCUM** for units of measure.

At the time of publication of this guidance, it is still under discussion in which way specific terminologies will be mandated for the EHDS. The terminologies listed above are given, throughout this guidance, as **illustrative examples of established terminology systems, not an exhaustive or exclusive list**; a system using another valid, equivalent terminology should not be excluded on that basis alone. Ask the vendor directly: which terminologies are supported, how are terminology updates maintained and versioned, and how are local or legacy codes mapped to the standard terminology. Manufacturers are not required to operate a terminology server within their product: Member States, and potentially care providers, may instead operate terminology servers from which vendor products can create their mapping tables. This places responsibility for correct mapping and

[51] https://eur-lex.europa.eu/eli/reg/2025/327/oj/eng (EHDS Regulation, Article 30(1)(e), manufacturer obligation to draw up the EU declaration of conformity, and Article 39, EU declaration of conformity)

[52] The FHIR **$export** operation is a standardized bulk data API defined by HL7 that lets you export large volumes of healthcare resources from a server asynchronously. Requests are sent using GET or POST with headers Accept: application/fhir+json and Prefer: respond-async, returning newline-delimited JSON (.ndjson) files.

its maintenance where it belongs and encourages harmonised use of terminologies across Europe; the contract should state clearly who maintains the mapping.

3.2.3 Structured Data, Not Only Documents

Many EHR, LIS, RIS/PACS and similar systems can already generate a human-readable PDF or narrative report. That is necessary but not sufficient. The direction of the proposed EHDS specifications is toward **structured, computable data**: individual elements (a diagnosis, a medication, a lab result value) that can be extracted, queried, and reused independently of the document they originated in, alongside the narrative document itself. The eHN guidelines and the EURIDICE / HL7 Europe specifications consistently expect both a narrative and a structured representation to coexist, not one or the other. The single most useful procurement question here is a direct one:

Can every data element in this report be exported as structured data, independently of the document? The answer the vendor gives, and how confidently they can demonstrate it, rather than merely assert it, is a strong, fast indicator of how far along the EEHRxF path a product is. Be cautious of systems where key clinical content (diagnoses, medications) exists only as free text inside a PDF or narrative block. This question applies until the implementing acts, and EHDS Board guidance documents are available; it can then be made more specific. For example, the EURIDICE EU Health Data API specification defines the actors “EEHRxF Resource Access Provider” and “EEHRxF Resource Consumer”, and support for the relevant actor(s) should be requested from vendors for each relevant priority data category.

3.2.4 Data Portability and Avoiding Vendor Lock-In

This overlaps directly with the Data Act obligations already established as compulsory for data processing services (cloud services in any delivery model: IaaS, PaaS, SaaS) elsewhere in this guidance (Section 2.3.5) but is worth restating here in interoperability-specific terms, since it is where lock-in is actually experienced. Annex II, point 2.6 of the EHDS Regulation provides that the harmonised software components of an EHR system shall not include features that prohibit, restrict or place an undue burden on authorised exporting of personal electronic health data for the purpose of replacing the EHR system by another product[53]. Require:

- Complete, machine-readable patient data export, not a partial or summary-only export.
- API-based access to the underlying data, not only a manual export function. This is recommended good practice; so far it is not mandated by the EHDS Regulation.
- Bulk extraction capability for full-population migration scenarios.
- No contractual or technical penalty for exporting data to a competing system.

A direct, useful procurement question to put to any vendor: **if we replace this system in five years, how exactly do we export all of this category's data in EEHRxF,** and at what effort and cost? A vendor who cannot answer this concretely during procurement is unlikely to answer it any more easily once the contract is signed.

[53] https://eur-lex.europa.eu/eli/reg/2025/327/oj/eng (EHDS Regulation, Annex II, points 2.1, 2.2 and 2.6)

One further signal worth asking about, though it sits outside EEHRxF itself: whether the system is openEHR-compliant. OpenEHR[54] is a distinct, broader clinical modelling standard (not an HL7 FHIR alternative, and not an EHDS requirement) that captures substantially more clinical detail than the EEHRxF priority categories cover. It is not something to require, but a system built on an openEHR-style archetype foundation underneath its HL7 FHIR export layer is, in practice, less likely to lose clinical detail when data, beyond the EHDS priority data categories are extracted, are extracted for migration or research than one where HL7 FHIR is the only structured representation the system has.

3.2.5 xShare Label and Other Readiness Signals

The xShare project has developed an experimental, voluntary, pre-regulatory **industry label** specifically to help EHR and wellness-application manufacturers demonstrate technical readiness for EEHRxF ahead of mandatory conformity processes. The label has three levels, Bronze, Silver and Gold, which are different evidence models rather than successive steps of one certification scheme: Bronze is a structured self-declaration based on a self-assessment survey; Silver is bidirectional interoperability (consuming and producing data) validated through external technical testing for example on the Gazelle testing platform operated by IHE-Europe; Gold is real-world integration in a national or regional ecosystem, confirmed with a recognised authority. Participation is not mandatory and does not substitute for future formal EHDS conformity assessment, but it is a concrete, checkable signal of a vendor's engagement with the emerging requirements landscape. Ask vendors directly whether they are participating in xShare , at what label level, and whether they have assessed their product against the published requirements. A different kind of signal is the **Label2Scale** quality label for health and wellness apps. Label2Scale is a European Commission-funded project that builds on Label2Enable, which developed a quality label for health and wellness apps in app stores[55]; the label covers aspects such as the veracity of health claims, safety, ease of use, data security and software quality. It does not assess readiness for the EEHRxF and is not a substitute for the xShare Label, so a procurer may ask about it separately, for example when a patient-facing app is procured.

Participation in IHE Connectathons and EHDS Projectathons. A further checkable signal is whether the vendor has taken part with its product in IHE Connectathons and/or EHDS-related Projectathons, or equivalent National or Regional level testing events. In such events vendors test products against those of other vendors, and if testing is documented as successful this could indicate whether a vendor can implement the interoperability requirements in a way that enables real, working interoperability with other vendors' products. Connectathon results are recorded in the IHE Connectathon results database, and Projectathon participation can be confirmed by the owner of the

[54] https://openehr.org/

[55] Label2Enable, "Label2Enable (Horizon Europe) enables an EU quality label for health and wellness apps", https://label2enable.eu/news/label2enable-horizon-europe-enables-eu-quality-label-for-health-and-wellness-apps; European Patients' Forum, Label2Enable project page, https://www.eu-patient.eu/projects/completed-projects/label2enable/. Label2Scale is the follow-up project funded by the European Commission (https://euraxess.ec.europa.eu/jobs/468722) (accessed 9 November 2026).

Projectathon. IHE-Europe offers also online testing of the proposed EHDS technical specifications, besides in person at the EU IHE Connectathons[56].

3.2.6 Contracting for a Moving Target

Because the EHDS Implementing Acts and EHDS Board guidance documents that will formally define the EEHRxF technical specifications are, at the time of writing, still being finalised, a system that is fully aligned with today's specifications could still require rework once the final Implementing Acts are adopted. This guidance recommends including a forward-looking maintenance clause of the following kind drafted as a review clause within the meaning of Article 72(1)(a) of Directive 2014/24/EU[57]. Such a clause has to be clear, precise and unequivocal, has to state the scope and nature of the possible modifications and the conditions under which they may be used, and may not alter the overall nature of the contract. The clause below is drafted to that standard:

"*During the term of the Contract, the Contractor shall ensure that the EHR system and the components falling within its contractual responsibility remain compliant with the requirements of EHDS Regulation that are applicable to the contracted EHR system, including the common specifications adopted by the European Commission pursuant to Article 36 and the technical specifications of the European electronic health record exchange format laid down in implementing acts under Article 15(1), in the versions published in the Official Journal of the European Union (the "Applicable Specifications", identified in [Schedule X] at the date of the Contract and including later versions only where they are adopted by a Union act under those Articles), within the implementation periods established by the relevant Union acts (mandated by EHDS Articles 30(1)(a) and 36). The Contractor shall implement such requirements through the maintenance, updating or evolution of the contracted solution, in accordance with the terms of this Contract, and should likewise track the EHDS Board guidance documents and the technical specifications relevant for the EHDS; the Contractor is not obliged to implement a document that is not an Applicable Specification, for example non-binding guidance or a version of a specification that no Union act has adopted, unless the Parties add it to [Schedule X] under the change-control provisions of this Contract. Any material modification or substitution of the contracted solution shall be subject to the Contract's change-control provisions and to the applicable public-procurement rules governing modifications of contracts during their term (Article 72 of Directive 2014/24/EU and its national transposition). The Tenderer shall describe in its tender its concept for delivering such updates, including the scope of the updates, the delivery dates, the change-control procedure, the commercial terms on which they are provided (pricing and allocation of costs) and the evidence on which the Contracting Authority will accept them [pricing methodology stated in the tender documents and fixed in the Contract before signature, for example:*

[56] https://connectathon.ihe-europe.net/xt-ehr-projectathon-2026 (IHE-Europe, Xt-EHR Projectathon 2026, held 24–26 March 2026 during Connectathon Week in Brussels, 23–27 March 2026)

[57] https://eur-lex.europa.eu/eli/dir/2014/24/oj/eng (Directive 2014/24/EU, Article 72(1)(a): modifications provided for in the initial procurement documents in clear, precise and unequivocal review clauses, which may include price revision clauses or options; such clauses state the scope and nature of possible modifications or options and the conditions under which they may be used, and may not provide for modifications that would alter the overall nature of the contract. Recital 111: review or option clauses may ensure that, for example, communications equipment continues to be suitable in the case of changing communications protocols or other technological changes, and contracts may include both ordinary maintenance and extraordinary maintenance interventions)

updates needed to keep the system compliant with the Applicable Specifications included in the maintenance fee (ordinary maintenance), and a rate card or price formula for extraordinary modifications; select or adapt]; that concept shall form part of the Contract."

This clause does not ask a vendor to predict the future; it asks them to commit, now, to the maintenance model rather than the replacement model when the specifications firm up. The clause is also drafted to meet the conditions for a review clause. Its scope and nature are fixed by reference to the Applicable Specifications, that is, the requirements that Union acts set for the contracted system, and not to every document that an institution or standards body may publish; non-binding guidance, and versions of specifications that no Union act has adopted, fall outside the obligation unless the Parties add them to the list by change control. Its conditions are the application dates and implementation periods set by those acts, and it separates ordinary maintenance that keeps the system compliant with the Applicable Specifications from extraordinary modifications, for example a change that makes the system a new product (see below) or a change of architecture, which are priced under the methodology stated in the tender. Recital 111 of the Directive recognises review clauses of this kind, which keep equipment or technology suitable when communications protocols or other technological requirements change. A clause that only refers to "future versions" of "relevant" specifications from a wide range of sources, for example HL7 Europe, Xt-EHR or MyHealth@EU, would not be clear, precise and unequivocal enough, and could be read as an open-ended obligation that alters the overall nature of the contract.

What counts as a new product? An EHR system that undergoes a substantial modification is considered a new product, which triggers testing in the digital testing environment under Article 40 of the EHDS Regulation, an update of the technical documentation and registration in the EU database. Substantial modifications are: adding a new priority category, adding a new main characteristic of a patient summary, introducing a new data operation, and a significant change in the technical architecture or in the technology used to perform data operations (for example replacing the underlying platform or the database engine, major changes in user-interface technology, or new integrations with a significant impact on data processing). Bug fixes and security updates that restore functionality are not substantial.

For procurement this has two consequences. A "maintenance, not replacement" clause covers updates that keep the system within its existing classes and categories; extending the system to a further priority category (for example adding Discharge Report after Patient Summary) or to a new data operation is likely to make it a new product with its own conformity cycle, and the contract should say who carries that effort and cost. The tender should also ask the vendor which of its planned changes it would consider substantial.

A genuine tension sits underneath this clause: an unconditional "no additional cost" obligation for future updates risks pricing smaller or more cautious vendors out of the tender entirely, or simply getting bid up front into a higher base price that the Contracting Authority pays regardless of whether new specifications ever materialise. There is no single right answer, and no final guidance on a "no additional cost" sentence can be given, as there are pros and cons depending on market conditions. Saying nothing may expose the Contracting Authority to being charged for every small update, while a "no additional cost" clause may either scare offers away or lead vendors to build a much higher cost into their price a priori, because of their uncertainty about future changes. A "reasonable and pre-identified (or pre-negotiated) cost" formulation can be a sensible middle path.

The clause above therefore keeps the obligation that matters most to the buyer, a working upgrade path with no forced platform replacement, and asks each tenderer to describe its own concept for delivering future updates and the commercial terms on which they are provided. Vendors can come up with different approaches, and a capped-fee or fixed-price model should not be assumed, since the extent of future changes cannot be known in advance. One view put forward is that, where a product was built on documents that were not yet final, bringing it to the final specification is the vendor's own responsibility, whereas major upgrades that break backward compatibility or trigger a new conformity assessment (for example under the MDR) can fairly attract a fee.

3.3 Procurement Guidance by Priority Data Category

This section works through each of the priority data categories in turn as full worked examples, Patient Summary, Electronic Prescription, Electronic Dispensation, Medical Test Results, and Discharge Report each set out the level of detail a procurer actually needs when drafting a tender for a specific system (an EHR, a pharmacy system or a LIS). Medical Imaging Study and Imaging Report are covered at reference depth rather than as a full worked example, reflecting that its EHDS technical specification is, at the time of writing, still at an earlier, ballot stage of maturity, with fewer settled procurement questions to work through.

3.3.1 Patient Summary — Worked Example for Procuring an EHR or GP System

Regulatory basis: EHDS Regulation Article 14(1)(a); mandatory exchange from 26 March 2029.
Specification maturity: the most mature of the five categories, and, together with ePrescription/eDispensation below, already live in cross-border production use: 15 EU Member States were already exchanging Patient Summaries and ePrescriptions via MyHealth@EU by early 2025[58], years ahead of the other three categories. Implementation of patient summaries nevertheless remains quite diverse across Member States, and how national implementations will align with an EU Patient Summary definition in practice remains to be seen; in addition, this exchange is mostly handled by Member State eHealth infrastructure rather than by individual vendor EHR system products.

I. Make EHDS interoperability a contractual requirement, specifically

Ask vendors to demonstrate alignment with, specifically for the Patient Summary:

- The EHDS Regulation's Patient Summary priority category (Article 14(1)(a)).
- The eHealth Network Patient Summary Guideline[59], In the cases where cross-border use of the PS maybe anticipated, services following such guidelines are already live for cross-border data exchange and in use under MyHealth@EU.
- The Xt-EHR Patient Summary logical information model.
- The HL7 FHIR IPS Implementation Guide[60], the international specification this category is built on.

[58] https://health.ec.europa.eu/ehealth-digital-health-and-care/electronic-cross-border-health-services_en
[59] https://health.ec.europa.eu/ehealth-digital-health-and-care/electronic-cross-border-health-services_en
[60] https://hl7.org/fhir/uv/ips/

- The newer **HL7 Europe Patient Summary (EPS)** FHIR Implementation Guide[61], which specialises IPS specifically for the European and EHDS context and aims for conformance with both IPS v2.0.0 and the HL7 FHIR EU Core profiles. This is a genuinely newer specification than the IPS reference already used in this guidance, it opened its first STU1 ballot in June 2026, and procurers should ask vendors specifically whether they track EPS..
- MyHealth@EU's own Patient Summary specifications[62] for cross-border exchange, already operating in production.

II. **Prioritise semantic interoperability over document generation**

Nearly every EHR and GP system can already print a patient summary. The eHN dataset, formalised in the Xt-EHR logical model, defines individual elements, active problems, medications, allergies and intolerances, immunisations, implanted devices, past procedures, and functional status, as independently extractable data, not only narrative text. The procurement question is direct: **can every patient summary element be exported as structured data, independently of the printed or PDF summary?** For this category, in particular, the answer should already be yes; a vendor unable to confirm this for Patient Summary specifically, given how mature this category is, is a stronger warning sign than the equivalent gap would be for a less mature category such as Imaging.

III. Require HL7 FHIR-based interfaces

As set out in Section 3.1, ask for the vendor provides HL7 FHIR-based interfaces (a dedicated HL7 FHIR server is not required), and ask for its published CapabilityStatement, supported HL7 FHIR version(s), and specifically their **IPS and EPS conformance testing evidence**. Given how mature this category is, a vendor should be able to point to a working, testable IPS export today, not a roadmap promise.

IV. Verify support for the Xt-EHR Patient Summary logical model

Ask the vendor to show how their data model maps to the Xt-EHR Patient Summary logical model, covering at minimum:

- Administrative: patient identification, author, custodian, encounter context.
- Clinical: allergies and intolerances, active problems, medications, immunisations, past procedures, implanted devices, and functional/pregnancy status where relevant.

V. Demand terminology compliance

Ask about support for (illustrative examples; see Section 3.2.2):

- **SNOMED CT** for problems, allergies, and procedures.
- **ATC** for medications.

[61] https://hl7.eu/fhir/eps/
[62] https://fhir.ehdsi.eu/

- **LOINC**, **NPU** where laboratory-derived data is referenced within the summary.

Ask which terminologies are supported and how local diagnosis or allergy codes are mapped to the reference terminologies defined for data transfer outside the care provider (SNOMED CT is the usual reference for problems and allergies; some Member States may prefer to keep their established terminologies and have the mapping done at the national contact point, which the implementing acts will settle).

The codes themselves carry no licence fee here: the SNOMED CT [63] International provides the Global Patient Set - GPS (https://www.snomed.org/gps). The GPS offers global access to all SNOMED CT unique identifiers, fully specified names (FSNs), preferred terms in international English, and active/inactive indicators — made available at no cost to users. The IPS Free Set is part of this. The IPS free set[64] (8,000+ terms) has been free to use worldwide since a 2019 HL7/SNOMED International agreement. GPS does not include SNOMED CT's relationships, hierarchies and remaining descriptions. The same was/is true for the IPS free set. This is regardless of whether the implementing country holds a national SNOMED CT licence. The costs of using SNOMED CT as any other structured terminology go beyond the licence costs and include for example the governance of the mapping: someone has to maintain the crosswalk between the vendor's local codes and SNOMED CT as both change over time, and that maintenance effort regarding local products installed is what procurers should ask vendors to resource.

VI. Ensure narrative and structured content coexist

The IPS and EPS specifications expect both a human-readable narrative and structured sections. Avoid a system where allergies or current medications are recorded only as free text in a clinical note rather than as discrete, coded entries.

VII. Evaluate MyHealth@EU readiness

Because Patient Summary is already live in cross-border production, this question is less hypothetical than for the other categories. Under Article 23 of the EHDS Regulation it is the Member States, not EHR manufacturers, that designate national contact points for digital health and ensure that healthcare providers are connected to them[65]; in some jurisdictions the connection is mediated by national gateways or national patient portals. The questions below therefore concern the product's experience with data flowing through that national infrastructure, not an obligation on the manufacturer to connect directly to a national contact point.

[63] https://www.snomed.org/news/hl7-and-snomed-international-announce-agreement-for-free-set-of-terms-for-use-in-the-international-patient-summary
[64] https://www.snomed.org/other-snomed-products
[65] https://eur-lex.europa.eu/eli/reg/2025/327/oj/eng (EHDS Regulation, Article 23(2) and (5): each Member State designates a national contact point for digital health and ensures that all healthcare providers are connected to it and able to perform two-way exchanges)

Ask the vendor directly:

- Is the system already processing data which originates from MyHealth@EU Patient Summary exchange, or is data generated by the system used in such exchange, in any Member State?
- If not yet used in such exchange in your country, has this product been used in such exchange in any other Member State?

Experience with MyHealth@EU-based exchange is a useful readiness signal for systems that process Patient Summaries, but it is not a pass/fail criterion: how providers connect to MyHealth@EU differs between Member States, and under Article 23 the connection is a Member State responsibility.

VIII. Look carefully at data portability

Require complete, machine-readable export of the full patient summary history, API access, and bulk extraction[66], consistent with Section 3: " **if we replace this system in five years, how do we export every patient's IPS-conformant summary in EEHRxF, and at what effort and cost?"**

IX. Investigate readiness signals, for example the xShare Label

Ask whether the vendor is participating in xShare and at what label level. Given the maturity of this category, Patient Summary is often one of the first categories a vendor demonstrates for Gold-level, Gazelle-validated xShare certification. This is an optional example of a readiness signal: because most vendors have not taken part in xShare, its absence must not be treated as disqualifying. Participation in IHE Connectathons or EHDS Projectathons (see Section 3.2.5) can serve the same purpose.

X. Include a future Implementing Act clause

Use the standard future-proofing clause in Section 3.2.6 (Contracting for a Moving Target), naming Patient Summary specifically, with particular attention to the transition from the international IPS baseline to the newer, EU-specific EPS specification as it matures out of ballot.

A consolidated, fillable checklist version for this data category, alongside the other four priority categories, is provided in Annex, Section 1 (Procurement Checklists for Interoperability) at the end of this document.

Because this category is the most mature, the bar for an acceptable vendor answer is correspondingly higher: for systems that process Patient Summaries, experience of MyHealth@EU-based exchange through the Member State's national contact point and a demonstrated IPS export are reasonable expectations today, not aspirational goals.

[66] According to the European Commission's official Interoperable Europe Portal, vendor lock-in is defined as: "A situation whereby a customer becomes dependent on a product or service provided by a commercial supplier and cannot move to another vendor without substantial costs and/or inconvenience."

3.3.2 Electronic Prescription and Electronic Dispensation — Worked Example for Procuring a Pharmacy or e-Prescribing System

Regulatory basis: EHDS Regulation Article 14(1)(b)–(c); mandatory exchange from 26 March 2029. **Specification maturity:** high and already live in cross-border production via MyHealth@EU in multiple Member States, though the underlying FHIR specification itself is newer than the international IPS. This subsection applies to e-prescribing modules within an EHR, standalone e-prescribing systems, and pharmacy dispensing systems alike.

I. Make Readiness for EHDS interoperability a contractual requirement, specifically

Ask vendors to demonstrate alignment with:

- The EHDS Regulation's Electronic Prescription and Electronic Dispensation priority categories (Article 14(1)(b)–(c)).
- The eHealth Network ePrescription Guideline[67], the clinical requirements source for this category, already used operationally for cross-border dispensing today.
- The Xt-EHR ePrescription and eDispensation logical information model.
- The **HL7 Europe Medication Prescription and Dispense (MPD)** FHIR Implementation Guide[68], published at version 1.0.0 (STU1) in May 2026 for both FHIR R4 and R5, developed jointly by IHE, HL7 Europe, Xt-EHR, and the xShare project itself.
- MyHealth@EU's ePrescription and eDispensation cross-border service[69], already allowing citizens in multiple Member States to have a prescription issued in one country dispensed in another.

II. Prioritise semantic interoperability over document generation

A prescription that exists only as a printed or PDF document cannot be dispensed cross-border, checked automatically for interactions, or reconciled against a patient's medication list. The Xt-EHR model defines the prescription and dispense as structured, linked records: the prescribed medicinal product, dosage instructions, prescriber, validity period, and, critically, since a prescription and its dispense(s) are separate, linked events, the dispense record itself, which may cover a whole prescription or only part of it. Ask directly: **can the full prescription-to-dispense chain be exported as structured, linked data, not only as a printed prescription and a separate, disconnected pharmacy log?**

III. Require FHIR-based interfaces

As set out in Section 3.2.1, ask which HL7 FHIR version(s) the vendor's MPD implementation supports. The MPD IG is unusual among the priority categories in publishing for both R4 and R5 simultaneously, but the version(s) required for the EHDS are expected to be defined in EHDS Board guidance once available (and further HL7 FHIR versions, such as R6, may follow and are

[67] https://health.ec.europa.eu/document/download/b744f30b-a05e-4b9c-9630-ad96ebd0b2f0_en
[68] https://hl7.eu/fhir/mpd/
[69] https://health.ec.europa.eu/ehealth-digital-health-and-care/electronic-cross-border-health-services_en

expected to cover add data categories), so a newer version should not be assumed to be better. Also request a working implementation example, not only a claim of conformance.

IV. Verify support for the Xt-EHR ePrescription/eDispensation logical model

Ask the vendor to walk through the mapping for:

- The prescription: medicinal product, dosage, quantity, validity period, prescriber, and any substitution permissions.
- The dispense: linked prescription reference, dispensed product and quantity, dispensing pharmacist/pharmacy, and handling of partial or declined dispenses.

Partial dispensing in particular is a common real-world scenario, a patient collecting only part of a multi-item prescription, and the Xt-EHR model handles this explicitly; a vendor unable to describe how their system represents a partial or declined dispense has likely not implemented this model in any depth.

V. Demand terminology compliance

Ask about support for (illustrative examples; see Section 3.2.2):

- **ATC, SNOMED GPS, EMA PMS, EMA SPOR SMS** for medicinal products
- **UCUM, EDQM** for dosage units.
- A documented approach for mapping national medicinal product registries and local formulary codes to the product identification coding designated in the EEHRxF (and to ATC where the classification is exchanged), since most national prescribing systems are still built around domestic product catalogues.
- SNOMED GPS (preferred), ICD-10 or Orphacode for the indication of a prescription

VI. Ensure narrative and structured content coexist

Dosage instructions still are too often written as free text (“take one tablet twice daily with food”) alongside a structured, computable dosage representation. Require both: free-text instructions for the patient and pharmacist to read, and structured dosage timing, route, and quantity for computable use (e.g., interaction checking, adherence monitoring).

VII. Evaluate MyHealth@EU readiness

As with Patient Summary, this is already a live production question rather than a hypothetical one for many Member States. Ask the vendor:

- Is the system already processing data which originates from MyHealth@EU ePrescription/eDispensation exchange, or is data generated by the system used in such exchange, in any Member State?
- Has the vendor's MPD implementation been tested against the MyHealth@EU cross-border profiles specifically, not only the base HL7 Europe MPD IG?

VIII. Look carefully at data portability

Require complete, machine-readable export of the full prescription and dispense history, with no vendor lock-in, consistent with section 3.2. A useful procurement question: **if we replace this system in five years, how do we export the complete prescription and dispense history, in in EEHRxF format, for every patient, and at what effort and cost?**

IX. Investigate readiness signals, for example the xShare Label and capacity to deploy eProduct Information contents (ePI)

Ask whether the vendor is participating or aware of xShare and at what label level, and specifically whether Electronic Prescription and/or Electronic Dispensation was among the categories tested, since xShare's own working group explicitly names Electronic Prescription implementation as one of its adoption-site activities. This involves connecting a medication to the relevant patient information leaflect, as is or personalized through G-lens. This is an example of a readiness signal: its absence must not be treated as disqualifying. Participation in IHE Connectathons or EHDS Projectathons (see Section 3.2.5) can serve the same purpose.

Explore with your vendor the knowledge of and value of eProduct Information, especially if this is already supported by your national drug agency. You want to explore its capacity to deploy eProduct Information contents (ePI).

X. Include a future Implementing Act clause

Use the standard future-proofing clause in Section 3.2.6 (Contracting for a Moving Target), naming Electronic Prescription and Electronic Dispensation specifically, including tracking of the MPD IG's progression from its current STU1 release through subsequent versions.

A consolidated, fillable checklist version **for this data category, alongside the other priority categories, is provided in Annex, Section 1 (Procurement Checklists for Interoperability) at the end of this document.**

As with Patient Summary, the maturity of this category means the practical bar for an acceptable vendor answer is higher than for Medical Test Results, Medical Imaging and Related Imaging Reports, or Discharge Report: a working, demonstrable MPD implementation and , where applicable to the product, experience of MyHealth@EU-based exchange through the Member State's national contact point are reasonable expectations, not future aspirations.

3.3.3 Medical Test Results (including Laboratory Reports and Other Diagnostic Results and Related Reports) — Worked Example for Procuring a LIS

Regulatory basis: EHDS Regulation Article 14(1)(e); mandatory exchange from 26 March 2031.
Specification maturity: developing — the HL7 Europe Laboratory Report Implementation Guide[70] has a published STU1 release (FHIR R4). This subsection works through what a procurer buying a new **LIS** today should ask for, treating it as an EHDS readiness procurement exercise rather than a narrow

[70] https://hl7.eu/fhir/laboratory/

functionality purchase, since the LIS is where most of a healthcare provider's Laboratory Report data actually originates.

I. Make EHDS interoperability a contractual requirement, specifically

Ask the vendor to demonstrate alignment with, specifically for laboratory data:

- The EHDS Regulation's Medical Test Results (including laboratory and other diagnostic results and related reports) priority category (Article 14(1)(e)).
- The eHealth Network Laboratory Report Guideline.
- The Xt-EHR Laboratory Report logical information model.
- The HL7 Europe Laboratory Report FHIR Implementation Guide.
- MyHealth@EU's adoption of the HL7 Europe Laboratory Report IG for cross-border laboratory report exchange.

As with the other categories, cite the current reference specification and require the Contractor to track the eventual EHDS Implementing Act for this category, per the future-proofing clause in Section 3.2.6.

II. Prioritise structured results over a PDF report

Most LIS platforms can already generate a laboratory report PDF. That is not the bar. The HL7 Europe Laboratory Report IG defines individual, independently extractable data elements: specimen information, test/observation identifiers, result values and units, reference ranges, abnormal-result flags, and the performing laboratory's identity, rather than only a narrative report. The procurement question is direct: **can every result element be exported as structured data, independently of the PDF?** The answer should be yes for the core in-vitro diagnostic domains this IG covers — clinical biochemistry, haematology, immunohematology, microbiology, and immunology — while specialised domains such as histopathology or medical genetics may still require a separate conversation with the vendor about roadmap and timeline, since the current IG explicitly does not yet cover them.

III. Require HL7 FHIR-based interfaces

As set out in Section 3.2.1, ask specifically for the LIS's:

- How FHIR-based interfaces are provided (a dedicated FHIR server is not required) and published CapabilityStatement.
- Supported FHIR version (R4 today; migration path to R5).
- FHIR REST API and Bulk FHIR export capability, relevant for both individual result retrieval and full-database migration scenarios.

IV. Verify mapping to the Xt-EHR Laboratory Report logical model

The single most useful procurement question for a LIS, mirroring the equivalent question for Discharge Report below, is:

Show how **your data model maps to the Xt-EHR Laboratory Report logical model.**

A vendor should be able to walk through this mapping for, at minimum:

- Administrative elements: patient identification, ordering clinician, performing laboratory, specimen collection and receipt timestamps.
- Clinical elements: the individual test/observation results, reference ranges, interpretation flags, and any narrative comments attached to a result.

A vendor unable to demonstrate this mapping concretely, rather than describe it in general terms, is likely behind the European interoperability roadmap for this category.

V. Demand terminology compliance

For laboratory data specifically, terminology failures are the most common source of non-interoperability in practice. Require:

- **LOINC** codes for test/observation identifiers, this is the single highest-impact terminology requirement for a LIS specifically. In parts of Northern Europe, **NPU**[71] natively, treat this as equivalent to LOINC rather than requiring a migration.
- **SNOMED CT** for qualitative findings and microbiology organism/specimen coding.
- **UCUM** for result units.

Ask the vendor which terminologies are supported, how LOINC updates are maintained and versioned, and, critically for laboratory systems, which very commonly carry years of local, in-house test codes, how existing local codes are mapped to LOINC, and whether that mapping work is included in the contract or charged separately.

VI. Ensure narrative and structured content coexist

The eHN and HL7 Europe specifications expect a laboratory report to comprise both a human-readable narrative (for direct clinical reading) and structured data sections (for computable reuse), with optional attachments. Avoid a system where interpretive commentary from the laboratory exists only as free text disconnected from the structured result it refers to.

VII. Evaluate MyHealth@EU readiness

Even where cross-border exchange is not an immediate need, ask the vendor:

- Has the system participated in any MyHealth@EU pilot for laboratory report exchange?
- Are laboratory reports exportable in a form aligned with the MyHealth@EU Laboratory Report specifications?

---

[71] https://pubmed.ncbi.nlm.nih.gov/39507572/ (“History, Implementation and Current Use of the IFCC-IUPAC’s Nomenclature for Properties and Units (NPU) Terminology in Denmark, Norway and Sweden”); see also https://ifcc.org/ifcc-scientific-division/sd-committees/c-npu/ (IFCC Committee on Nomenclature for Properties and Units)

- Has the system been tested in a National Contact Point for eHealth (NCPeH) environment?

VIII. Look carefully at data portability

Require complete, machine-readable patient laboratory history export, API access, and bulk extraction, with no vendor lock-in, consistent with Section 3.2. A useful, concrete procurement question: **if we replace this LIS in five years, how do we export the full laboratory result history, in EEHRxF format, for every patient, and at what effort and cost?**

IX. Investigate readiness signals, for example the xShare Label

Ask whether the vendor is participating in the xShare project, pursuing the xShare Label, and at what level (Bronze self-declaration through to Gold, validated interoperability). This is not mandatory, but it is a concrete, checkable indicator of EHDS preparedness specifically for laboratory and other priority-category data. This is an optional of a readiness signal: because most vendors have not taken part in xShare, its absence must not be treated as disqualifying. Participation in IHE Connectathons or EHDS Projectathons (see Section 3.2.5) can serve the same purpose.

X. 10. Include a future Implementing Act clause

Use the standard future-proofing clause set out in Section 3.2.6 (Contracting for a Moving Target), naming the Medical Test Results category specifically, so that the Contractor's obligation to track evolving specifications is unambiguous for this domain.

A consolidated, fillable checklist version for this data category, alongside the other priority categories, is provided in Annex, Section 1 (Procurement Checklists for Interoperability) at the end of this document.

In practice, the single best discriminator when comparing LIS vendors today is whether they can show a concrete mapping between their internal data model and the Xt-EHR Laboratory Report logical model, together with a working HL7 Europe Laboratory Report FHIR export. Vendors that can already do both are the closest to future EHDS compliance for this category.

3.3.4 Discharge Report — Worked Example for Procuring an EHR

Regulatory basis: EHDS Regulation Article 14(1)(f); mandatory exchange from 26 March 2031.
Specification maturity: advanced — the HL7 Europe HDR Implementation Guide[72] has reached a continuous-build v1.0.0-ci state, built directly on the eHN Hospital Discharge Report Guideline and the Xt-EHR discharge-report logical model, with direct involvement from the XpanDH and xShare projects themselves. If you are procuring a new EHR today and want to maximise future compliance with this category, treat it as an **EHDS readiness procurement exercise**, not merely an EHR functionality purchase.

I. Make EHDS interoperability a contractual requirement, specifically

Ask vendors to demonstrate alignment with, specifically for discharge reporting:

[72] https://build.fhir.org/ig/hl7-eu/hdr/

- The EHDS Regulation's Discharge Report priority category (Article 14(1)(f)).
- The eHealth Network HDR Guideline.
- The Xt-EHR discharge-report logical information model.
- The HL7 Europe HDR FHIR Implementation Guide.
- MyHealth@EU's HDR specifications for cross-border exchange.

The HL7 Europe HDR IG states its own purpose explicitly as supporting the EHDS discharge-report priority category and providing the foundation for EEHRxF and cross-border exchange, this is not a peripheral or speculative specification.

II. Prioritise semantic interoperability over document generation

Many EHRs can already generate a discharge letter as a PDF. That is not enough. The eHN guideline's dataset, formalised in the Xt-EHR logical model, defines individual, independently extractable information elements, including:

- encounter information
- diagnoses and problems
- procedures
- medications
- implants and devices
- laboratory findings relevant to the admission
- functional status
- care plan and follow-up recommendations

The procurement requirement should ask directly: **can every discharge-report data element be exported as structured data, independently of the document?** The answer should be yes.

III. Require HL7 FHIR-based interfaces

As set out in Section 3.2.1, a future-proof EHR discharge module should support the HL7 FHIR version(s) that EHDS Board guidance will define once available (with a migration path to later versions), a HL7 FHIR REST API, Bulk FHIR export, and HL7 FHIR-based document generation, since the European HDR implementation work is itself built on HL7 FHIR. Ask vendors how they provide HL7 FHIR-based interfaces (a dedicated FHIR server is not required), for their published CapabilityStatement, supported profiles, and implementation examples specifically for discharge reports, not only for other categories.

IV. Verify support for the Xt-EHR discharge-report data model

One of the most valuable procurement questions available for this category is direct:

Show how your data model maps to the Xt-EHR discharge-report logical model.

Important discharge areas to walk through with the vendor include:

- Administrative: patient, author, custodian, encounter, intended recipient.
- Clinical: conditions, observations, procedures, medications, devices, care plans.

A vendor unable **to** demonstrate this mapping is likely behind the European interoperability roadmap for this category.

V. Demand terminology compliance

The biggest **interoperability** failures typically come from coding, not from message technology. Ask about support for (illustrative examples; see Section 3.2.2):

- SNOMED CT
- ICD-10, Orphacode, with a documented ICD-11 migration path
- LOINC
- ATC, SNOMED GPS, EMA PMS
- UCUM

Ask vendors which terminologies are supported, how terminology updates are maintained, and how local codes are mapped to the standard terminology.

VI. Ensure narrative and structured content coexist

The eHN and HDR specifications envisage a discharge report comprising human-readable narrative, structured data sections, and optional attachments together. A compliant solution should produce all three. Avoid systems where important information exists only in PDFs, where key diagnoses are free text only, or where medications are stored only as narrative text.

VII. Evaluate MyHealth@EU readiness

Even if cross-border exchange is not an immediate need, EHDS points strongly toward future interoperability with MyHealth@EU. Ask the vendor:

- Has the system participated in MyHealth@EU pilots for discharge reports?
- Are discharge reports exportable according to the MyHealth@EU HDR specifications?
- Has the system been tested in a NCPeH environment?

VIII. Look carefully at data portability

Require complete, machine-readable patient export, API access, and bulk extraction, with no vendor lock-in, consistent with Section 3.2. A useful procurement question: **if we replace this EHR in five years, how do we export all discharge-report data in EEHRxF format, and at what effort and cost?**

IX. Investigate readiness signals

Ask whether the vendor is participating in xShare, is pursuing the xShare Label, and has assessed their product against the published requirements. Even where not mandatory, this is a strong indicator of **EHDS** preparedness. This is an example of a readiness signal: because most vendors have not taken part in xShare, its absence must not be treated as disqualifying. Participation in IHE Connectathons or EHDS Projectathons (see Section 3.2.5) can serve the same purpose.

X. Include a future Implementing Act clause

Use the standard future-proofing clause set out in Section 3.2.6 (Contracting for a Moving Target), naming the Discharge Report category specifically. This protects the Contracting Authority from buying a **system** that is compliant with today's draft specifications but becomes obsolete once the final EEHRxF specifications and Implementing Acts are adopted.

A consolidated, fillable checklist version for this data category, alongside the other priority categories, is provided in Annex, Section 1 (Procurement Checklists for Interoperability) at the end of this document.

The single best discriminator when evaluating EHR vendors today for this category is whether they can demonstrate a concrete mapping between their internal data model and the Xt-EHR discharge-report logical model, together with a working HL7 Europe HDR FHIR export. Vendors that can already do both are the closest to future EHDS compliance for this category.

3.3.5 Medical Imaging Study and Imaging Report

Regulatory basis: EHDS Regulation Article 14(1)(d); mandatory exchange from 26 March 2031.
Specification maturity: early — the HL7 Europe Imaging Study Report FHIR Implementation Guide[73], developed jointly with IHE-Europe under the EURIDICE collaboration, entered its first coordinated ballot in March 2026 and remains at ballot/STU1 stage at the time of writing. This is genuinely the least mature of the priority categories, and procurement language should reflect that directly rather than treat it as equally settled.

This category applies to RIS/PACS systems and to any EHR module that stores or references imaging studies and their reports. Two distinct things are in scope, and vendors should be asked about both separately: the **imaging study** itself (the pixel data, typically DICOM), and the **imaging report** (the radiologist's structured and narrative findings), since a system can handle one well without handling the other. Previously, DICOM Structured Reports normally transport evidence information beyond the images, which is then used when creating the HL7 FHIR imaging report; they are not, in themselves, the imaging report in the meaning of the EHDS. Not every system that processes imaging studies also processes (still less exports) imaging reports, so the points below are split into imaging studies and imaging reports, and each applies only to the extent that the system handles the object concerned.

- Imaging studies: where the system stores or exchanges imaging studies, it should support DICOM for the underlying study and manifest-based access to it (for example IHE Manifest-based Access to DICOM Objects (MADO) on which the proposed EHDS technical specifications build)[74].
- Imaging reports: where the system produces or stores imaging reports, it should support export of the imaging report as structured data conforming to the HL7 Europe Imaging Study Report FHIR Implementation Guide (current ballot version), not only as an attached PDF or a DICOM Structured Report wrapped as an opaque document.

[73] https://hl7.eu/fhir/imaging/
[74] https://profiles.ihe.net/RAD/MADO/ (IHE Radiology, Manifest-based Access to DICOM Objects, MADO) ; https://build.fhir.org/ig/hl7-eu/imaging-manifest/ (HL7 Europe Imaging Manifest IG based on IHE MADO)

- The system should code imaging findings using SNOMED CT and should support mapping of procedure/study codes to internationally recognised imaging procedure terminologies *(recommended, non-exclusive bindings).*
- Given the earlier maturity stage of this specification, the Contractor should commit to tracking the Imaging Study Report IG through to its stable release and updating the system's conformance accordingly, under the future-proofing clause in Section 3.2.6, on the commercial terms agreed under that clause.

Because this specification is still maturing, the single most useful procurement question here is forward-looking rather than a conformance check against a finished standard: **how is the vendor tracking the EURIDICE Imaging Study Report ballot, and what is their committed timeline for supporting the stable release once published?** A vendor with no clear answer to this is signalling that imaging interoperability is not yet a priority for them, which matters directly for a 2031 compliance deadline.

3.4 Ready-to-Use Tender Clauses for Interoperability

The clauses below are organised the same way as Section 3.2: a set of cross-cutting clauses that apply regardless of which system is being procured, followed by clauses specific to whichever priority data category (or categories) the procurement concerns. A procurer buying a LIS, for example, would use the cross-cutting clauses together with the Medical Test Result clauses only, not all five categories' clauses.

3.4.1 Cross-Cutting Clauses (All Categories)

- *The Contractor **warrants** that the proposed solution supports structured health data exchange in compliance with the European Electronic Health Record Exchange Format (EEHRxF), as specified in Commission implementing acts adopted under Article 15 of Regulation (EU) 2025/327 (European Health Data Space Regulation), for the priority data category or categories relevant to this procurement, namely: [list applicable categories].*
  Note: What this warranty actually commits a vendor to is worth spelling out: EEHRxF conformance means the system can transition between its own internal format and the structured EEHRxF format on **both** sides of an exchange, generating EEHRxF-conformant structured output when sending data, and correctly parsing and ingesting EEHRxF-conformant structured data received from another system, not only one direction. A vendor that can export but not import (or vice versa) does not meet this requirement, even if their one-directional capability is technically well-built. Accordingly, the system shall accept and correctly read EEHRxF-conformant data received from another system, not only generate it *(mandated by EHDS Article 15(4)).*
- *The system **should** provide a published HL7 FHIR CapabilityStatement, support the HL7 FHIR REST API, and support Bulk FHIR export (a recommended technical approach to satisfying the EEHRxF exchange requirement; the Commission has not yet mandated these specific mechanisms in the Article 36 common specifications, which remain pending). Current FHIR version supported: [R4; state version]. Migration path to subsequent FHIR versions: [describe].*
- *The Contractor **shall** provide complete, machine-readable, API-accessible export of all data within scope of this contract, with no significantly additional charge for export and no contractual or technical restriction that would impede migration to a replacement system*

(mandated by EHDS Annex II (2.6) and, where the solution is, or relies on, a data processing service other than IaaS, Data Act Article 30(2); for IaaS, Article 30(1)).

- *In line with the principles of Data Portability and the duties of all health data holders to provide dully anonymized health data for secondary use proposes, Contractors **should** work with Procurers ways for products to support autonomous export by the organization, these **should** contain features and in-built capabilities that make such export effortless and autonomous to internal teams.*
- *During the term of the Contract, the Contractor **shall** ensure that the EHR system and the components falling within its contractual responsibility remain compliant with the requirements of EHDS Regulation that are applicable to the contracted EHR system, including the common specifications adopted by the European Commission pursuant to Article 36 and the technical specifications of the European electronic health record exchange format laid down in implementing acts under Article 15(1), in the versions published in the Official Journal of the European Union (the "Applicable Specifications", identified in [Schedule X] at the date of the Contract and including later versions only where they are adopted by a Union act under those Articles), within the implementation periods established by the relevant Union acts (mandated by EHDS Articles 30(1)(a) and 36). The Contractor **shall** implement such requirements through the maintenance, updating or evolution of the contracted solution, in accordance with the terms of this Contract, and **should** likewise track the EHDS Board guidance documents and the technical specifications relevant for the EHDS; the Contractor is not obliged to implement a document that is not an Applicable Specification, for example non-binding guidance or a version of a specification that no Union act has adopted, unless the Parties add it to [Schedule X] under the change-control provisions of this Contract. Any material modification or substitution of the contracted solution **shall** be subject to the Contract's change-control provisions and to the applicable public-procurement rules governing modifications of contracts during their term (Article 72 of Directive 2014/24/EU and its national transposition). The Tenderer **shall** describe in its tender its concept for delivering such updates, including the commercial terms on which they are provided [pricing methodology stated in the tender documents and fixed in the Contract before signature, for example: updates needed to keep the system compliant with the Applicable Specifications included in the maintenance fee (ordinary maintenance), and a rate card or price formula for extraordinary modifications; select or adapt]; that concept shall form part of the Contract.*

3.4.2 Patient Summary Clauses related to xShare Yellow Button

- *The system **shall** be capable of exporting patient summary data conforming to the HL7 FHIR International Patient Summary (IPS) Implementation Guide (current version at the time of delivery), including to the extent held by the system: medications, allergies and intolerances, problems, and immunisations. Once a technical specification for the EU Patient Summary has been adopted under Article 15 of the EHDS Regulation, the system **shall** also conform to that specification (mandated by EHDS Annex II, point 2.1).*
- *The system **should** support standardised code systems, illustrated by, but not limited to, SNOMED CT for clinical concepts and LOINC for laboratory observations (a recommended, non-exclusive binding; the Commission has not yet mandated specific code systems under Article 36).*
- *The system **should** validate conformance to IPS profiles prior to transmission and **shall** preserve data provenance when receiving external IPS documents.*

3.4.3 Electronic Prescription and Electronic Dispensation Clauses

- *The system **shall** support the generation, transmission, and receipt of medication prescription and dispense data conforming to the HL7 Europe Medication Prescription and Dispense (MPD) FHIR Implementation Guide.*
- *The system **should** represent medicinal products and related medication data with the product coding, designated in the EEHRxF (SNOMED GPS, the EMA PMS identifier or a national coding system for the product; EMA SPOR SMS for substances; EDQM Standard Terms for pharmaceutical dose forms and routes of administration; UCUM for units of measure; with ATC as a non-binding classification), with a documented approach for mapping local formulary codes to that coding (a recommended, non-exclusive binding).*

3.4.4 Medical Test Results (including Laboratory and Other Diagnostic Results and Related Reports) Clauses

- *The system shall support structured export of laboratory results conforming to the HL7 Europe Laboratory Report FHIR Implementation Guide (or the EHDS technical specifications that supersede it), independently of any PDF or narrative report.*
- *The system should code test/observation identifiers using LOINC (or NPU, where that is the established regional terminology) a recommended, non-exclusive binding; where mapping is required, the Contractor should disclose, in writing, both the price of mapping existing local test codes to the target terminology and the methodology used to perform and maintain that mapping over time.*
- *The system should support SNOMED CT for qualitative and microbiology findings, and UCUM for result units (recommended, non-exclusive bindings).*

3.4.5 Medical Imaging Study and Related Imaging Report Clauses

- *Where the system processes imaging studies, it **should** support DICOM for those studies and manifest-based access to them (for example IHE MADO), or the EHDS technical specifications that supersede these.*
- *Where the system processes imaging reports, it **should** support structured export of the imaging report conforming to the HL7 Europe Imaging Study Report FHIR Implementation Guide (current ballot version), or the EHDS technical specifications that supersede it, in addition to any narrative or DICOM Structured Report format.*
- *The Contractor **should** track the Imaging Study Report Implementation Guide through to its stable release and update the system's conformance within [X days or months[75]] of stable publication, on the commercial terms agreed under the future-proofing clause in Section 3.2.6.*

3.4.6 Discharge Report Clauses

- *The system **should** support structured export of every discharge-report data element (encounter, diagnoses, procedures, medications, implants/devices, relevant laboratory findings, functional status, care plan and follow-up recommendations) independently of the discharge document, conforming to the HL7 Europe Hospital Discharge Report FHIR Implementation Guide or the EHDS technical specifications that supersede it.*

[75] To be set by the Contracting Authority; products falling under the MDR can need substantially longer lead times for functional changes, often 6–12 months or more

- *The system **shall** produce a discharge report comprising human-readable narrative and structured data sections together and shall not store key diagnoses or medications as narrative text only.*
- *The Contractor **should** demonstrate mapping between the system's internal data model and the Xt-EHR discharge-report logical information model or the EHDS technical specifications that supersede it.*

3.4.7 Validation and Conformance Testing

- *The Contractor **should** conduct and document conformance testing of interoperability functionality The specific platform is not prescribed; Gazelle is one recognised option, but several Member States run their own national testing tools derived from the European Commission's Digital Testing Environment, and a Gazelle-specific requirement would exclude vendors validated through an equally valid national route. Acceptable evidence includes any of the following, or an equivalent recognised by the Contracting Authority's Member State:*
- *Patient Summary validation through Gazelle Conformity Assessment Framework, a national testing tool derived from the EC Digital Testing Environment, or equivalent*
    - *HL7 FHIR conformance testing using Inferno FHIR testing suite or equivalent*
- *XDS document exchange testing using IHE testing infrastructure where applicable*
- *The test report should state which kind of evidence it provides: (i) tests against current draft or published profiles and implementation guides; (ii) tests run with a project or national testing tool (Gazelle, or a national tool derived from the EU Digital Testing Environment); or (iii) formal EHDS conformity, that is the digital testing environment under **Article 40**, the EU declaration of conformity under **Article 39** and the CE marking under **Article 41**. Only the third establishes conformity with the Regulation; the first two are evidence of readiness.*
- *Prior to system deployment, the Contractor **should** provide the Contracting Authority with detailed test reports demonstrating successful conformance to interoperability standards. Test reports shall include:*
    - *Sample data exchanges showing successful generation and receipt of standards-compliant records*
    - *Screenshots or logs demonstrating data validation and error handling*
    - *Documentation of any deviations from standards and remediation plans*
- *The Contractor **should** maintain an ongoing testing and certification programme, with revalidation at a regular cadence [monthly, annually etc] agreed with the Contracting Authority and providing updated certification reports to the Contracting Authority.*
- *The Contractor **shall** re-assess the conformity of the EHR system's harmonised software components for each product release that, under the EHDS Regulation and its implementing acts, requires a renewed conformity assessment, and **shall** provide the Contracting Authority with the updated EU declaration of conformity and, where applicable, the updated CE marking (mandated by EHDS Articles 30(1)(a) and (e), 39 and 41). Any further revalidation requested by the Contracting Authority **should** follow the Contractor's release cycle for interoperability-relevant changes [for example: each release containing such changes] and should be limited to what is not already covered by this obligation.*

3.4.8 EHDS Conformity for EHRs

The EHDS Regulation imposes conformity obligations on EHR systems that are independent of, and additional to, the interoperability clauses above.

- *The Contractor **warrants** that, from the date on which **Article 25** applies, the offered EHR system incorporates the mandatory European interoperability software component and European logging software component required under the EHDS Regulation (mandated by EHDS Article 25(1)).*
- *The Contractor shall provide documented evidence that these harmonised components have been successfully tested in the European digital testing environment established under Article 40 of the EHDS Regulation, prior to the system being placed on the market.*
- *The Contractor **shall** provide an EU Declaration of Conformity (mandated by EHDS Article 39) and affix the CE marking (mandated by EHDS Article 41), confirming fulfilment of the requirements set out in Chapter III of the EHDS Regulation.*
- *Prior to production go-live, the Contractor **shall** demonstrate that the system is registered in the EU database for EHR systems and wellness applications (mandated by EHDS Article 49). For a go-live before that date, this is a readiness check, and the Contractor **should** state when it will register the system. Where the Contractor also offers wellness applications claiming interoperability with the core EHR system, those applications **shall** be held to the same labelling obligation (mandated by EHDS Article 47, which applies to wellness applications specifically, distinct from the EHR system's own declaration-of-conformity and CE-marking route) in addition to the shared Article 49 registration obligation.*
- *The Contractor **should** state how the contracted system will enable the Contracting Authority, as healthcare provider, to register, receive, read and issue priority-category data in the EEHRxF by the date that applies to it under Chapter II (Articles 13 and 15(4) of the EHDS Regulation), for example through a vendor software upgrade, a middleware or translation layer, or system modernisation, and by when each of these would be available.*

3.4.9 Data Act – Switching and Vendor Lock-In Protections

Applies where the solution is a data processing service, or relies on one, in any delivery model (IaaS, PaaS, SaaS, StaaS, DBaaS), and the connected-product clause applies where it includes connected products (see Section 2.3.5, “Data Act”, for the underlying compulsory-element rationale). Procurers are advised to incorporate the European Commission’s Standard Contractual Clauses for cloud computing contracts (Commission Recommendation C(2025) 7750, Annexes VI to XII)[76] into the tender documentation, to secure standardised, non-discriminatory terms for cloud switching, termination, security and liability. They are voluntary and non-binding, they do not replace the obligations below, and they contain no GDPR provisions, so controller-processor and transfer clauses have to be added where personal data are processed. The clauses below set the minimum a tender should state:

- *The Contractor **shall** provide a documented Switching and Exit Plan, specifying the formats, methods, sequence of operations, and estimated timeframe required to export all Exportable Data and Digital Assets to a new environment. The maximum transitional period **shall** not exceed 30*

[76] https://digital-strategy.ec.europa.eu/en/library/draft-recommendation-non-binding-model-contractual-terms-data-access-and-use-and-non-binding (European Commission, Recommendation on non-binding model contractual terms on data access and use and non-binding standard contractual clauses for cloud computing contracts, C(2025) 7750 final, 19 November 2025, prepared under Article 41 of the Data Act; the standard contractual clauses for cloud computing contracts are in Annexes VI to XII. The Commission’s publication page titles the document a draft Recommendation)

*calendar days following the applicable notice period, and the maximum notice period for initiating the switching process shall not exceed two months. Where 30 calendar days is technically unfeasible, the Contractor **shall** notify the Contracting Authority within 14 working days of the switching request, provide a technical justification and indicate an alternative transitional period of no more than seven months, ensuring full-service continuity throughout (mandated by Data Act Article 25)).*

- *In line with Article 29 of the Data Act, the Contractor **shall** not impose switching charges, including data-egress charges, on the Contracting Authority for actions mandated by the switching process, with charges prohibited from 12 January 2027.*
  - *For data processing services other than IaaS, the Contractor **shall** make open interfaces available to facilitate switching (mandated by Data Act Article 30(2)) and ensure compatibility with common specifications and harmonised standards published in the central Union standards repository for the interoperability of data-processing services (mandated by Data Act Article 30(3); the repository is established under Article 35(8)).*
  - *Where the service consists only of infrastructure elements (IaaS), the Contractor shall take all reasonable measures in its power to enable the Contracting Authority, after switching to a service of the same service type, to achieve functional equivalence in the use of the destination service, and **shall** provide capabilities, information, documentation, technical support and, where appropriate, tools for that purpose (mandated by Data Act Article 30(1)).*
  - *The Contractor **should** confirm that its standard terms on access to and use of data, and on liability and remedies for breach or termination of data-related obligations, apply only as set out in this Contract and have been negotiated and not unilaterally imposed on the Contracting Authority; terms that are unfair within the meaning of Data Act Article 13 are not binding on the Contracting Authority (Data Act Article 13(1); a recommended contractual safeguard).*
  - *Where the solution includes connected products, for example connected medical or monitoring equipment, and related services, the Contractor, or the manufacturer or data holder on which it relies, **shall** make the product data and related service data accessible to the Contracting Authority as user, by default, easily, securely, free of charge and in a structured, commonly used and machine-readable format, and shall make them available to third parties designated by the Contracting Authority on its request (mandated by Data Act Articles 3 to 5; Article 3(1) applies to connected products placed on the market after 12 September 2026).*

3.4.10 Interoperability Support and Maintenance

- *During the support and maintenance phase, the Contractor **shall**:*
  - *Monitor updates to HL7 FHIR, IPS, related standards and technical specifications relevant for the EHDS.*
  - *Assess impact of standards updates on the system's conformance*
  - *Provide the Contracting Authority with written notification of any standards changes affecting interoperability functionality within [X days, for example 90] of publication*
  - *Develop and implement necessary system updates to maintain standards compliance*
  - *The Contractor should provide at least [X, number of updates, for example 1] system updates during each [12-month] support period to address new standards versions, regulatory changes, or identified interoperability gaps.*
  - *The Contractor should disclose the basis (for example a reasonable, pre-identified or pre-negotiated cost) of any fees for updates required to maintain baseline*

interoperability standards compliance as defined in this contract; at the time of contract signature rather than at the point the update is delivered.

3.4.11 A Note on Secondary Use and Common Data Models

This guidance is primarily concerned with **primary use** of health data interoperability, the priority data categories as they support direct patient care and cross-border care continuity. Where a procurement genuinely requires secondary-use capability (research cohort extraction, population-level analytics), the system should support structured extraction to a recognised common data model, such as, but not limited to, OMOP, together with transparent documentation of the data transformations applied and metadata describing completeness, accuracy, timeliness, and consistency at the data-element level. Procurers whose use case is exclusively primary use of health data should treat this as an optional, use-case-bound addition rather than a baseline requirement, consistent with the modular approach to EHDS clauses.

4. Minimum Procurement-Ready Criteria for Cybersecurity

Cybersecurity requirements in digital health procurement should not be treated as isolated technical controls, but as lifecycle obligations spanning planning, sourcing, and operational management. ENISA[77] emphasises that procurement is a critical lever shaping the cybersecurity posture of healthcare organisations and that security considerations must be embedded holistically across all procurement phases. Consistent with this approach, xShare adopts a lifecycle-oriented model whereby cybersecurity requirements are defined during planning, contractually enforced during sourcing, and continuously monitored during system operation. ENISA identifies five broad categories of threats relevant to hospital environments: natural phenomena, supply chain failures, human errors, malicious actions (including ransomware and phishing), and system failures. These threat categories highlight that cybersecurity risks originate not only from external attackers, but also from organisational processes, legacy technologies, and vendor dependencies. Building on ENISA's guidance, xShare recommends that minimum cybersecurity requirements in tenders explicitly cover the following domains. Throughout this chapter, a requirement is grounded in the EU legal act it follows from (EHDS, GDPR, NIS2, CRA, MDR/IVDR or the AI Act) and cited accordingly; also reflects ENISA guidance, a standard or an xShare recommendation. ENISA updated its procurement guidelines for hospitals and healthcare providers in July 2026.[78]

The table below summarises these domains at a glance; the detailed prose that follows gives the full requirement, and the standards it draws on.

Table 6: Cybersecurity domains, requirements and key standards

Domain	What's required	Key standard(s)
Governance and compliance	Documented compliance with applicable EU cybersecurity law	GDPR, NIS2, CRA, MDR/IVDR, ISO/IEC 27001 & 27799, AI Act Art. 15 (if AI-enabled)
Risk assessment	Documented risk assessment covering CIA and patient-safety impacts, per threat category	ISO/IEC 27005 or equivalent
Secure design and development	Security by design and by default, secure Software Development Lifecycle (SDLC), minimised attack surface	GDPR Arts. 25 & 32; NIS2; CRA Annex I

[77] https://www.enisa.europa.eu/publications/good-practices-for-the-security-of-healthcare-services

[78] https://www.enisa.europa.eu/publications/procurement-guidelines-for-the-cybersecurity-of-hospitals-and-healthcare-providers (ENISA, Procurement guidelines for the cybersecurity of hospitals and healthcare providers, July 2026, ISBN 978-92-9204-804-4, DOI 10.2824/2503342; see requirements MANAGE-01 and PLAN-05 on vulnerability handling and defined timelines for critical fixes; accessed October 2026)

Access control, logging, monitoring	Role-based access control (RBAC); comprehensive audit logging; continuous monitoring	EHDS Annex II, IHE ATNA or equivalent; eIDAS ≥ substantial (where eIDAS applies)
Secure configuration	Hardened default configuration; no default credentials; least privilege	CRA Annex I Part I; GDPR Art. 25
Secure remote access	Time-bounded, authenticated, logged remote maintenance access only	NIS2 Art. 21(2) (access control)
Business continuity	BC/DR plan with agreed RTO/RPO, tested at least annually	NIS2 Art. 21(2)
Vulnerability management	Public VDP, SBOM per release, tiered patch SLAs (48h critical / 72h high)	NIS2 Art. 21; CRA Annex I Part II; ENISA guidance
Incident response	Incident response aligned with NIS2 reporting timelines (24h / 72h / 1 month)	NIS2 Art. 23; EHDS Art. 44
Supply chain security	Disclosure of key third-party dependencies; risk management for each	NIS2 Art. 21
Data exchange security	Encrypted, mutually authenticated channels for all EEHRxF exchanges	TLS 1.3; ENISA cryptographic standards; GDPR Art. 32; NIS2 Art. 21;
Testing and certification	Independent security testing before go-live; recognised certification	GDPR Art. 32; ISO/IEC 27001 / 27799

4.1 Core Cybersecurity Requirements

4.1.1 Governance and Compliance

The Contractor must demonstrate compliance with applicable EU cybersecurity and data-protection legislation applicable to the solution; standards are recommended ways of evidencing that compliance, not legal requirements in themselves. Applicable legislation and standards may include,

- GDPR (Articles 25, 32, 33, 34): Data protection by design and by default; security measures including encryption and access controls; incident notification
- NIS2 Directive: Cybersecurity risk management, incident reporting, asset management, and supply chain security for essential and important entities (healthcare providers are listed in Annex I, sector “Health”; the obligations reach vendors through the Contracting Authority’s

supply-chain security duty under Article 21(2)(d), and directly where the vendor is itself in scope; cited at Directive level, national transposition to be confirmed)[79]

- Medical Device Regulation (MDR) and In-Vitro Diagnostics Regulation (IVDR): Cybersecurity requirements for networked and software-driven health technologies (MDR Annex I, points 17.2 and 17.4; IVDR Annex I, points 16.2 and 16.4; applicable where the product or component is a medical device)[80]
- Cyber Resilience Act (CRA, Regulation (EU) 2024/2847): Essential cybersecurity requirements and vulnerability-handling duties for manufacturers of products with digital elements, including EHR software that is not itself a medical device (products covered by the MDR or IVDR are excluded from the CRA); the EHDS Regulation also amends the CRA. The reporting obligations for actively exploited vulnerabilities and severe incidents apply from 11 September 2026 and the remaining obligations from 11 December 2027[81]
- Data Act (Regulation (EU) 2023/2854), where the Contractor is a provider of a data processing service: the safeguards against international and third-country governmental access to non-personal data held in the Union (Article 32; see Data Exchange Security below) and the switching provisions in Section 3.4.9
- AI Act: If the system incorporates AI components for clinical decision support or diagnostics. that qualify as high-risk AI systems, Article 15 requires an appropriate level of accuracy, robustness and cybersecurity, including measures against AI-specific attacks such as data poisoning, model poisoning and adversarial examples[82]. Beyond that legal baseline, distinct "AI-security" clauses (e.g., robustness against adversarial attack, data-poisoning prevention) are treated as recommended rather than compulsory in this guidance: the expert survey split 8-to-4 in favour of making them mandatory, which this guidance reads as a considered openness rather than a settled consensus — see "A Note on Persistent Open Questions" below
- ISO/IEC 27001 and ISO/IEC 27799: Information security management standards (recommended, non-exclusive ways of evidencing the legal obligations above); ISO 27799 provides healthcare-specific guidance

[79] https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng (NIS2 Directive (EU) 2022/2555: Annex I, sector "Health"; Article 21(2), points (a) to (j), in particular (a) risk analysis, (b) incident handling, (c) business continuity, (d) supply chain security, (e) vulnerability handling and disclosure, (f) assessing the effectiveness of measures, (h) cryptography and encryption, (i) access control and (j) multi-factor authentication; Article 23(4), incident reporting timelines)

[80] https://eur-lex.europa.eu/eli/reg/2017/745/oj/eng (MDR, Annex I, points 17.2 and 17.4); https://eur-lex.europa.eu/eli/reg/2017/746/oj/eng (IVDR, Annex I, points 16.2 and 16.4); https://ec.europa.eu/docsroom/documents/41863 (MDCG 2019-16, Guidance on Cybersecurity for medical devices)

[81] https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng (Cyber Resilience Act, Regulation (EU) 2024/2847: Article 2(2), exclusion of products covered by the MDR and IVDR; Article 13(2) and (5); Article 14, reporting of actively exploited vulnerabilities and severe incidents, applicable from 11 September 2026; Annex I, Part I (cybersecurity requirements) and Part II (vulnerability handling, including the SBOM and a coordinated vulnerability disclosure policy); general application from 11 December 2027)

[82] https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng (AI Act, Article 15(5): technical solutions to address AI-specific vulnerabilities, including measures against data poisoning, model poisoning, adversarial examples and confidentiality attacks)

4.1.2 Risk Assessment and Threat Coverage

The Contractor **shall** provide a documented risk assessment covering confidentiality, integrity, availability, and patient safety impacts. The risk assessment **shall** explicitly address the following threat categories: supply chain failure, human error, malicious actions, system failures, and environmental disruptions, and **shall** identify controls and residual risks for each. Basis: a documented, risk-based approach is required by GDPR Article 32(1), by NIS2 Article 21(2)(a) and, for manufacturers of products with digital elements, by the CRA (Article 13(2)); for medical devices MDR Annex I, point 17.2 requires risk management including information security. The use of ISO/IEC 27005 is a recommended method, not a legal requirement.

4.1.3 Secure System Design and Development

Suppliers **shall** demonstrate "security by design and by default" principles throughout system development and deployment. This includes secure SDLC practices, protection against unauthorized access, and minimisation of attack surfaces. Special consideration must be given to interoperability components supporting EEHRxF, ensuring that data exchange interfaces do not introduce systemic vulnerabilities. Basis: GDPR Article 25 (data protection by design and by default) and, for products with digital elements, the CRA (Annex I, Part I: appropriate level of cybersecurity, secure-by-default configuration, limited attack surfaces). The secure SDLC practices listed in the clauses below are recommended good practice.

4.1.4 Access Control, Logging, and Monitoring

Systems provide reliable identification and authentication of health professionals and **shall** log every access to personal electronic health data (EHDS Annex II, points 3.1 and 3.2)[83]. Systems **should** in addition implement strong RBAC mechanisms and audit logging of administrative actions. Logging capabilities must support incident investigation and regulatory compliance. Continuous monitoring for security events and anomalies **should** be provided, either directly by the supplier or through integration with the contracting authority's security operations. Basis: EHDS Annex II, point 3 also requires tools to review and analyse the log data (or support for connecting external tools) and support for different retention periods and access rights (points 3.3 and 3.4); the technical detail of the European logging software component will be set by common specifications under Article 36. RBAC as such, logging of administrative actions and continuous security monitoring go beyond that text and are recommended practice that supports the NIS2 Article 21(2) duties of the Contracting Authority.

4.1.5 Secure Configuration and Prevention of Common Human-Error Failures

The Contractor **shall** deliver the system in a hardened configuration by default, including removal/disablement of default credentials, least-privilege access controls, secure protocol configuration, and secure remote administration settings. The Contractor **should** provide configuration documentation and a checklist for validation during acceptance testing. Basis: secure-by-default configuration is an essential requirement of the CRA (Annex I, Part I) and follows from data protection by default (GDPR Article 25(2)); the configuration documentation and acceptance checklist are recommended practice.

---

[83] https://eur-lex.europa.eu/eli/reg/2025/327/oj/eng (EHDS Regulation, Annex II, point 3, "Requirements for security and logging", points 3.1 to 3.4; see also Annex II, points 1.3 and 1.4)

4.1.6 Secure Remote Access and Supplier Maintenance Controls

If the Contractor provides remote maintenance or support, remote access **should** be strictly controlled, time-bounded, and monitored. Remote access **should** require strong authentication, explicit authorisation, and logging of all remote sessions. The Contractor **should** not enable persistent remote access pathways without the explicit written approval of the Contracting Authority. Basis: recommended practice that supports the access-control duties of NIS2 Article 21(2)(i) and the CRA (Annex I, Part I).

4.1.7 Business Continuity and Operational Resilience

The Contractor **shall** provide a business continuity and disaster recovery plan covering system outage, ransomware/malware scenarios, supply chain disruptions (including cloud/provider failures), and major infrastructure disruptions. The plan **should** define the recovery time objective (RTO)[84] and recovery point objective (RPO)[85] targets agreed with the Contracting Authority and **should** be tested at least annually (or after major architectural changes). Basis: business continuity, backup management and disaster recovery are required of essential and important entities by NIS2 Article 21(2)(c) and are flowed down contractually to the vendor; the RTO/RPO targets and the test cycle are recommended practice, to be set by the Contracting Authority.

4.1.8 Vulnerability Management and Patch Processes

ENISA highlights vulnerability management as a core procurement requirement, asking for a formal process for receiving vulnerability reports and for patches or mitigations to be deployed without undue delay, with defined timelines for critical fixes[86]. The Contractor **should** maintain a public vulnerability disclosure policy (VDP)[87], provide a software bill of materials (SBOM)[88] with every release, and commit to timely, severity-tiered remediation: critical vulnerabilities deployed without undue delay, e.g. within 48 hours and high-severity vulnerabilities within 72 hours of disclosure (a cascading service level agreement (SLA)[89] keyed to the Common Vulnerability Scoring System (CVSS)[90] score, replacing a single blanket patch timeline)[91]. Contracts **should** establish responsibilities for coordinating security updates across interconnected systems and flow these obligations down contractually to subcontractors. Basis: for manufacturers of products with digital elements, the CRA (Annex I, Part II) requires vulnerabilities to be identified and documented, including by an SBOM, and remediated without delay; security updates to be made available (free of charge unless otherwise agreed for tailor-made products); and a coordinated vulnerability disclosure policy to be in place. NIS2 Article 21(2)(e) requires vulnerability handling and disclosure from essential and important

---

[84] The maximum acceptable time to restore the system after an outage

[85] The maximum acceptable amount of data loss, measured in time

[86] https://www.enisa.europa.eu/publications/procurement-guidelines-for-the-cybersecurity-of-hospitals-and-healthcare-providers (ENISA, Procurement guidelines for the cybersecurity of hospitals and healthcare providers, July 2026, ISBN 978-92-9204-804-4, DOI 10.2824/2503342; see requirements MANAGE-01 and PLAN-05 on vulnerability handling and defined timelines for critical fixes; accessed October 2026)

[87] A published way for security researchers and users to report vulnerabilities, with defined handling times

[88] A machine-readable list of the software components in the product

[89] The contractually agreed response and fix times

[90] A standard 0 to 10 scale for rating vulnerabilities

[91] These figures are an example for the Contracting Authority to adapt: neither ENISA nor NIS2 sets a patch deadline

entities. Providing the SBOM to the Contracting Authority with each release and the severity-tiered figures are contractual recommendations.

4.1.9 Incident Response and Business Continuity

- The Contractor **shall** provide incident response procedures aligned with NIS2 reporting timelines and support coordinated incident handling with healthcare organisations. Procurement contracts **should** require documented business continuity and recovery plans, ensuring that cybersecurity incidents do not compromise patient safety or essential clinical services. Basis: incident handling and reporting under NIS2 Articles 21(2)(b) and 23(4); manufacturers of EHR systems must in addition report serious incidents under EHDS Article 44(7) and, for products within the scope of the CRA, actively exploited vulnerabilities and severe incidents under CRA Article 14.

4.1.10 Supply Chain Security

Given the dependency on third-party components and services, it is a requirement that:

- The Contractor **should** disclose key supply chain relationships and demonstrate measures to manage associated risks. This includes cloud providers, remote maintenance services, and embedded software components[92].

4.1.11 Data Protection and Privacy

- The system shall implement data protection mechanisms ensuring confidentiality and integrity of health data throughout its lifecycle, in compliance with GDPR and emerging EHDS privacy requirements[93].

4.1.12 Secure Data Exchange

- All EEHRxF-compliant data exchanges **must** occur through secure, authenticated, and encrypted channels, preventing unauthorized interception or modification[94].

4.1.13 Software Security and Updates

- The Contractor **shall** demonstrate secure software development practices and a commitment to timely vulnerability disclosure and patching, minimizing exposure to known security weaknesses[95].

[92] Basis: NIS2 Article 21(2)(d) requires essential and important entities to address supply chain security, which a procurer can only do if vendors disclose their key dependencies (a contractual recommendation); CRA Article 13(5) requires manufacturers to exercise due diligence when integrating third-party components.

[93] Basis: GDPR Articles 5(1)(f), 25 and 32.

[94] Basis: GDPR Article 32(1)(a) and NIS2 Article 21(2)(h); EHDS Annex II, point 1.4 requires interoperability and compatibility with other products to be reliable and secure, but the Regulation does not prescribe a specific protocol. The protocols named in the clauses below are recommended practice.

[95] Basis: CRA Annex I, Part II and NIS2 Article 21(2)(e); see “Vulnerability Management” in the tender clauses.

4.1.14 Testing and Certification

- The system **should** undergo independent security testing and, where available, certification, providing objective evidence of compliance with cybersecurity requirements[96].

4.2 Ready-to-Use Tender Clauses for Cybersecurity

4.2.1 Governance and Compliance

*The Contractor **shall** demonstrate compliance with,*

- *GDPR Articles 25, 32, 33 and 34 through documented data protection by design and by default principles*
- *NIS2 Directive requirements applicable to essential and important entities, flowed down contractually to the vendor (Article 21(2), as transposed nationally) including:*
  - *Risk management and security assessment procedures aligned with ISO 27005*
  - *Asset management covering hardware, software, and supply chain components*
  - *Incident response procedures supporting the NIS2 reporting timelines (early warning within [X hours, for example 24 hours] , incident notification within [X hours, for example 72 hours] and final report within one month; Article 23(4))*
  - *Third-party and supply chain security oversight*
- *Medical Device Regulation (MDR) Annex I, (17.2) and (17.4) (and, for in vitro diagnostic devices, IVDR Annex I, points 16.2 and 16.4), where the product is a medical device.*
- *Cyber Resilience Act (Regulation (EU) 2024/2847), where the product is a product with digital elements outside the scope of the MDR and IVDR: the essential cybersecurity requirements (Annex I, Part I) and vulnerability-handling requirements (Annex I, Part II), from the dates of application of the CRA*
- *AI Act Article 15[97], if the system incorporates AI components for clinical decision support or diagnostics that qualify as high-risk AI systems.*
- *ISO/IEC 27001 or equivalent certification, with healthcare-specific controls per ISO/IEC 27799 (a recommended, non-exclusive way of evidencing the obligations above; see "Compliance and Certification" below)*

4.2.2 Risk assessment and threat coverage

*The Contractor **shall**,*

- *Conduct a comprehensive risk assessment covering threats to the confidentiality, integrity, and availability (CIA) of electronic health data in accordance with ISO/IEC 27005 or equivalent methodology (the risk assessment itself is required by GDPR Article 32(1), NIS2 Article 21(2)(a) and, for products with digital elements, CRA Article 13(2); the use of ISO/IEC 27005 is recommended).*
- *Provide the Contracting Authority with:*
  - *Risk assessment report identifying key threats (e.g., unauthorized access, ransomware, data breaches, denial of service)*

[96] Basis: GDPR Article 32(1)(d) requires a process for regularly testing, assessing and evaluating the effectiveness of security measures, and NIS2 Article 21(2)(f) requires policies to assess the effectiveness of risk-management measures; independence and certification are recommended practice.

[97] https://artificialintelligenceact.eu/article/15/ (AI Act, Article 15, Accuracy, Robustness and Cybersecurity)

  - *Risk treatment plan documenting implemented mitigations and residual risks*
  - *Evidence that risk assessment is conducted regularly (for example annually) or upon significant system changes*
- *Implement security controls proportionate to assessed risks, with particular attention to:*
  - *Threats from external threat actors (e.g., ransomware campaigns targeting healthcare)*
  - *Threats from insider access abuse (a recognised risk in healthcare environments, where many users need legitimate access to health records)*
  - *Threats to data integrity from malicious modification or corruption*
- *Maintain a vulnerability management process aligned with NIS2, including:*
  - *Continuous monitoring for software vulnerabilities affecting the system*
  - *Release of critical security patches within the period set by the Contracting Authority in line with the severity-tiered SLA recommended under Vulnerability Management below (recommended practice; NIS2 does not specify a fixed patch-deployment deadline and the CRA requires vulnerabilities to be addressed without delay)*
  - *Testing and deployment procedures ensuring patches do not disrupt interoperability*

4.2.3 Access Control and Authentication

- *The system **shall** implement role-based access control (RBAC) or any other access-control model aligned with healthcare operational requirements (EHDS Annex II, points 3.1 and 3.4 require reliable authentication of health professionals and support for different access rights; NIS2 Article 21(2)(i) requires access control policies), including:*
  - *Distinct roles for clinicians, nurses, pharmacists, administrative staff, researchers, and patients*
  - *Granular permissions controlling which data elements each role may view, modify, or delete*
  - *Principle of least privilege: users receive minimum permissions necessary for their function*
- *For authentication the system **should** support multi-factor authentication (MFA) for all user access, with particular emphasis on administrative and privileged accounts (NIS2 Article 21(2)(j) requires essential and important entities to use multi-factor or continuous authentication where appropriate; this is flowed down contractually to the vendor)*
- *For cross-border or external access, the system **shall** integrate with eIDAS-compliant identity providers, supporting at least eIDAS assurance level "substantial" (the middle of the three eIDAS levels: low, substantial and high)[98] or must integrate eIDAS-compliant identity providers when the services for which it will be used fall under the eIDAS regulation conditions.*
  - *The system **should** support integration with national identity infrastructures where available (e.g., national digital certificates)*

[98] https://eur-lex.europa.eu/eli/reg/2014/910/oj/eng (eIDAS Regulation (EU) No 910/2014, as amended by Regulation (EU) 2024/1183: levels of assurance 'low', 'substantial' and 'high', Article 8 and Commission Implementing Regulation (EU) 2015/1502); https://ec.europa.eu/digital-building-blocks/sites/spaces/DIGITAL/pages/467110081/eIDAS+Levels+of+Assurance

- *For patient-facing interfaces, the Contractor **should** provide authentication mechanisms that balance security with usability, recognising that overly complex requirements may reduce patient engagement with personal health data*
    - *The system **should** support supporting federated authentication where patients can log in using widely used identity providers (e.g., national health or government accounts)*
- *The system **shall** maintain audit logs of all authentication events, including failed login attempts, user role changes, and escalation of privileges.*

4.2.4 Security-by-Design

- *The Contractor **shall** demonstrate that the proposed solution has been designed, developed, and maintained following "security by design and by default" principles, consistent with Articles 25 and 32 of the GDPR, the requirements of the NIS2 Directive and, for products with digital elements, the essential cybersecurity requirements of the CRA (Annex I, Part I), including the following measures, which are recommended good practice for evidencing those obligations:*
    - *A documented secure software development lifecycle (SDLC), covering threat modelling at the design stage, secure coding standards, and code review prior to release*
    - *Minimisation of the attack surface: unused ports, services, and default accounts disabled or removed before delivery*
    - *Secure-by-default configuration out of the box, such that the Contracting Authority is not required to actively harden the system after installation to reach a baseline secure state*

4.2.5 Compliance and Certification

- *The Contractor **should** provide evidence of compliance with recognised information security management standards (these standards are a recommended, non-exclusive way of evidencing the GDPR Article 32 and NIS2 Article 21 obligations, not themselves an EU regulatory requirement), including:*
    - *A valid ISO/IEC 27001 certificate (or equivalent), with a scope statement explicitly covering the system and data being procured, not a generic organisational certification that may exclude the relevant product line*
    - *ISO 27799 alignment specifically for the health-information-security controls, where the Contractor holds it*
    - *Relevant EU cybersecurity certification schemes, where available for the product category*
- *The Contractor **shall** commit, in the contract itself, to aligning with the EHDS security specifications once the relevant Implementing Acts are adopted, consistent with the future-proofing approach set out in Section 3.2.*

4.2.6 Data Exchange Security

- *All EEHRxF-compliant data exchanges **shall** use secure communication channels protecting confidentiality and integrity (GDPR Article 32(1)(a); NIS2 Article 21(2)(h)) and should use mutually authenticated channels, including:*

- *TLS 1.3 with certificate-based authentication for all network transport (TLS 1.2 accepted only as a documented, time-limited exception) (recommended; the ENISA procurement guidelines give TLS 1.3 in transit as an example of modern encryption)*[99]
- *Data at rest encrypted using algorithms compliant with ENISA-recommended cryptographic standards, with key management practices documented and auditable*
- *Certificate lifecycle management: the Contractor shall specify how certificates are issued, rotated, and revoked, and who is responsible for each step*
- *For any interoperability interface exposed to external systems (Section 3.2), the same encryption and authentication requirements apply without exception, since these interfaces are a common target for interception*

- *In compliance with Data Act Article 32, the Contractor, as provider of a data processing service, **shall** implement legal, technical and organisational safeguards, including contractual measures, to prevent international and third-country governmental access to, and transfer of, non-personal electronic health data held in the Union where this would conflict with Union law or the national law of the relevant Member State (mandated by Data Act Article 32(1)).*
- *As a recommended technical measure, the Contractor **should** use encryption whose keys are managed in the Union, by the Contracting Authority or an operator established in the Union, so that the provider alone cannot hand over readable data.*
- *The Contractor **shall** inform the Contracting Authority of any request from a third-country authority for access to its data before complying with it, unless the request serves law enforcement purposes (mandated by Data Act Article 32(5)). Personal electronic health data remain subject to the GDPR rules on transfers to third countries (Chapter V).*

4.2.7 Logging, Monitoring, and Incident Response

- *The system **shall** log every access event to personal electronic health data (mandated by EHDS Annex II, point 3.2)*[100] *and **should** log administrative actions, in line with IHE ATNA, itsHL7 FHIR-based counterpart, IHE BALP, or equivalent standards*[101]*, including:*
  - *Who accessed or modified which record, when, and from where (source system or device) (EHDS Annex II, point 3.2 requires, for every access event, the identity of the healthcare provider and of the individual who accessed the data, the categories of data accessed, the time and date of access and the origin of the data; logging of modifications and of the source device is recommended)*
  - *Administrative actions: role changes, permission escalation, configuration changes, and account creation/deletion (recommended good practice)*
  - *Log retention for a period specified by the Contracting Authority, consistent with national health-record retention rules, with logs protected against tampering or deletion by system administrators (the system must support different retention periods*

[99] https://www.enisa.europa.eu/publications/procurement-guidelines-for-the-cybersecurity-of-hospitals-and-healthcare-providers (ENISA, Procurement guidelines for the cybersecurity of hospitals and healthcare providers, July 2026, requirements GENERAL-09.01 and GENERAL-09.04 (Annex B.1): modern encryption, for example TLS 1.3 in transit, with outdated protocols disabled; accessed October 2026)

[100] https://eur-lex.europa.eu/eli/reg/2025/327/oj/eng (EHDS Regulation, Annex II, point 3, "Requirements for security and logging", points 3.1 to 3.4; see also Annex II, points 1.3 and 1.4)

[101] https://profiles.ihe.net/ITI/BALP/ (IHE ITI Basic Audit Log Patterns, FHIR AuditEvent profiles; the ATNA profile is defined in the IHE IT Infrastructure Technical Framework)

and access rights, EHDS Annex II, point 3.4; protection against tampering or deletion is recommended good practice)

- *The Contractor **shall** define an incident response process that enables the Contracting Authority to meet its own incident-reporting deadlines under NIS2 **Article 23(4)**; those deadlines bind the essential or important entity and not the Contractor, so they are flowed down by contract. The contract **should** state the incident threshold, when the clock starts and the information that the Contractor is to provide. The following deadlines are illustrative contractual deadlines, aligned with those of NIS2:*
    - *Early warning to the Contracting Authority within 24 hours of becoming aware of a significant incident*
    - *A fuller incident notification within 72 hours, including initial assessment, severity, and indicators of compromise*
    - *A final report within one month of the incident notification, including root cause and remediation taken. Separately, and without prejudice to the NIS2 timeline above, where an incident is a "serious incident" affecting the EHR system itself within the meaning of the EHDS Regulation, the Contractor, as manufacturer, shall report it to the to the market surveillance authorities of the Member States concerned immediately after establishing a causal link (or its reasonable likelihood) between the EHR system and the incident and in any event no later than three days after becoming aware of it (mandated by EHDS Article 44(7)), and **shall** notify the Contracting Authority of any such report without undue delay. Where the Contractor is the manufacturer of a product within the scope of the CRA, it must in addition report actively exploited vulnerabilities and severe incidents to its designated CSIRT and ENISA from 11 September 2026 (CRA Article 14), and should inform the Contracting Authority of such reports without undue delay*

4.2.8 Vulnerability Management

- *The Contractor **shall** maintain a public Vulnerability Disclosure Policy (VDP) and should provide a Software Bill of Materials (SBOM) with every release (supporting the vulnerability handling and disclosure duty in NIS2 Article 21) and, for products with digital elements, the CRA, Annex I, Part II, which requires an SBOM to be drawn up and a coordinated vulnerability disclosure policy to be in place), including:*
    - *Recommended severity-tiered remediation SLAs, keyed to CVSS score rather than a single blanket timeline (for example, critical vulnerabilities patched within [e.g. 48 hours] of disclosure and high-severity within [e.g. 72 hours]; the figures are illustrative and set by the Contracting Authority). This is a negotiable contractual SLA the Contracting Authority may set; neither NIS2, the CRA nor the ENISA procurement guidelines mandate a specific patch-deployment deadline (the CRA requires vulnerabilities to be addressed without delay)[102] .*
    - *Coordination of security updates across interconnected systems, with these obligations flowed down contractually to subcontractors*

[102] https://www.enisa.europa.eu/publications/procurement-guidelines-for-the-cybersecurity-of-hospitals-and-healthcare-providers (ENISA, Procurement guidelines for the cybersecurity of hospitals and healthcare providers, July 2026, ISBN 978-92-9204-804-4, DOI 10.2824/2503342; see requirements MANAGE-01 and PLAN-05 on vulnerability handling and defined timelines for critical fixes; accessed October 2026)

- *The Contracting Authority reserves the right to audit vulnerability management practices, including requesting evidence of the current SBOM and recent patch history on request.*

4.2.9 Testing, Validation, and Certification

- *For Pre-Deployment Security Testing:*
  - *Prior to deployment, the system **should** undergo independent security testing (mandated by GDPR Article 32) including:*
    - *Penetration testing simulating attacks on system interfaces and data storage*
    - *Vulnerability scanning identifying known software weaknesses*
    - *Configuration review ensuring secure default settings*
  - *Test reports **should** be provided to the Contracting Authority and remediation of identified issues should be completed before system goes live*
- *For Ongoing Security Assessment:*
  - *The Contractor **should** have regular security assessments (for example annually), performed as an external audit, that validate continued compliance with the applicable standards*
  - *The Contractor **should** provide the results to the Contracting Authority, together with remediation plans for the findings*
- *For Certification:*
  - *The Contractor **should** maintain ISO/IEC 27001 certification or equivalent (ISO/IEC 27799 for healthcare), with scope statement clearly defining what systems and data the certification covers*
  - *Certification audit reports **should** be provided to the Contracting Authority upon request*
- *The Contractor **should** maintain compliance with ISO 27001 throughout the contract term*

A consolidated, fillable checklist version for Cybersecurity is provided in Annex, Section 2 (Procurement Checklists for Cybersecurity) at the end of this document.

4.3 A Note on Persistent Open Questions

Two cybersecurity questions were deliberately **not** resolved into a single fixed rule in this version of the guidance, because the evidence base does not yet support one:

- **Mandatory vs. recommended AI-security clauses:** This guidance treats AI-security criteria as **recommended** rather than compulsory, pending further evidence of market maturity, and this should be read as a considered compromise rather than a resolved consensus. AI-related considerations beyond security are collected in Section 8.
- **Generic vs. article-specific citation for directives with variable national transposition** (principally NIS2): rather than settle this EU-wide, the guidance asks procurers to confirm the applicable national transposition directly — see Section 2.3.2, “NIS2 Directive”.

5. Minimum Procurement-Ready Criteria for Data Quality by Design

Data quality is not a compliance checkbox; it is a journey that unfolds as data move through collection, harmonisation, and reuse phases. Traditional static assessments, measuring data at a single point in time, miss critical quality gaps that emerge during transition between lifecycle stages.

5.1 Data Quality by Design Principles

The principles below are recommended practice for the capture and processing functions of the EHR system and are therefore addressed mainly to vendors. They rest on the accuracy and data-protection-by-design duties of the GDPR[103] and on the EHDS provisions on registration of data in EHR systems and rectification[104],[105]

5.1.1 Principle 1: Capture Complete, Structured Data at Point of Care

- System design should prompt clinical staff to capture relevant, complete information
- EHR interfaces should highlight required fields and fields commonly omitted
- Clinical decision support should reinforce data capture when relevant
- Avoid forcing data entry for fields clinicians perceive as irrelevant; engage clinical leadership to define truly necessary data
- Standardized coding: System should suggest standardized codes (e.g., SNOMED CT, LOINC, or the code systems prescribed by the EHDS technical specifications for the relevant priority category) rather than free-text entry, which reduces variability and improves subsequent data harmonization

Example: When entering a diagnosis, system suggests SNOMED CT concepts rather than allowing arbitrary text

This should not read as a burden placed entirely on frontline clinical staff. Two things make it more achievable in practice: management and decision-makers at the source organisation being aware of, and actively supporting, why capture quality matters upstream (not only IT or data teams); and the Contractor designing data-capture tools that fit within existing clinical workflow and the limited time clinicians actually have to document, rather than adding steps on top of it.

5.1.2 Principle 2: Implement Real-Time Validation

- Data entry validation should run in real time, at the point of capture, not as a downstream batch process discovered days or weeks later.

[103] https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng (GDPR, Article 5(1)(d), accuracy; Article 16, right to rectification; Article 25, data protection by design and by default)
[104] https://eur-lex.europa.eu/eli/reg/2025/327/oj/eng (EHDS Regulation, Article 13, last subparagraph: the records are to identify the health professional and the healthcare provider who registered or updated the data, and the time of registration or update; see also Annex II, point 2.4, structured entry of data with sufficient granularity to be provided in the EEHRxF)
[105] https://eur-lex.europa.eu/eli/reg/2025/327/oj/eng (EHDS Regulation, Article 6, right of natural persons to rectification of data through electronic health data access services, in line with GDPR Article 16)

- Validation feedback should be **supportive rather than punitive**: flag likely errors and missing required fields with clear, actionable messages, rather than silently rejecting entries or blocking clinical workflows.
- Validation rules should be configurable to local clinical context (e.g., paediatric vs. adult reference ranges) rather than applied as a single hard-coded rule set.
- The rationale for validation at the point of capture is not only downstream data quality: any data error entered at this point is a direct patient-safety risk, since it is the same data that immediately informs clinical decisions for that patient. Clinical staff should understand this connection explicitly, not experience validation as an arbitrary IT requirement, the Contractor's training materials should explain why the specific fields being validated matter, not only how to satisfy the validation rule.

5.1.3 Principle 3: Document and Version Data Provenance

- Every data element should carry provenance metadata: who (or which system/interface) entered or modified it, when, and from what source.

This is deliberately a "should" rather than a "shall": full provenance tracking on every single data element carries a real implementation and exchange cost, and that cost should be weighed against the actual benefit for the specific data involved. Procurers should prioritise provenance tracking for the data elements most likely to be reused, disputed, or relied on for safety-critical decisions, rather than requiring it uniformly across every field in the system. In practice, for data exchanged between organisations it is generally sufficient to identify the originating organisation (for example the hospital, laboratory or healthcare provider) and, where it is already captured, the individual source, such as the originating laboratory of a Medical Test Result or the health professional who made a manual observation; metadata that is not recorded at source (for example how a patient's telephone number was entered) should not be fabricated. As a legal floor, EHDS Article 13 provides that records identify the health professional and healthcare provider who registered or updated the data and when[106]. Which further elements warrant element-level provenance remains open for confirmation.

- Corrections should be versioned, not overwritten: the system should preserve a full, auditable history of changes to clinical data, distinguishing original entries from later corrections. Provenance and version history are also basic features of the ISO 13606 reference model for EHR communication, so ISO 13606 can serve as an established good-practice cross-check when assessing a vendor's provenance and versioning design; it is a reference, not a legal requirement and not a substitute for the EHDS technical specifications.[107]

---

[106] https://eur-lex.europa.eu/eli/reg/2025/327/oj/eng (EHDS Regulation, Article 13, last subparagraph: the records are to identify the health professional and the healthcare provider who registered or updated the data, and the time of registration or update; see also Annex II, point 2.4, structured entry of data with sufficient granularity to be provided in the EEHRxF)

[107] ISO 13606-1:2019, Health informatics — Electronic health record communication — Part 1: Reference model, https://www.iso.org/standard/67868.html (the standard specifies a means of communicating part or all of an electronic health record; its reference model, which the openEHR EHR Extract Information Model aligns with, carries audit details such as the author of content and version identifiers for record components. It does not define the internal architecture of EHR systems; accessed October 2026). ISO 13606 is a recognised good-practice reference, not a requirement of the EHDS Regulation.

- Version-control and provenance-tracking requirements should be among the highest of all design-level data-quality measures, ahead of structured coded data entry and real-time validation, and well ahead of active clinical decision-support prompting. Provenance-tracking data generates significant meta-data that will also need to be transferred, however for the adequate implementation of some EHDS rights, like the right of data elimination, this may constitute a necessity that should be progressively demanded of vendors. The checklist in Annex, Section 3 does not assign numeric weights; procurers should apply this prioritisation when deciding which items to treat as essential, favouring passive data-integrity infrastructure over more intrusive, workflow-embedded interventions.

5.1.4 Principle 4: Implement Feedback Loops for Quality Improvement

- *The Contractor **should** provide a defined mechanism through which clinical and data-management staff can report suspected data-quality issues directly to the Contractor's support team:*
    - *Reported issues should be triaged, tracked to resolution, and reported back to the Contracting Authority on a regular (at minimum quarterly) basis, consistent with the "Continuous Improvement" clause in Section 5.4.7 below.*
    - *Recurring issues should inform subsequent system updates and configuration changes, be logged.*
    - *Triage should distinguish symptoms from root causes: a reported issue that looks, on the surface, like a one-off technical defect may in fact stem from a governance or awareness gap (e.g., staff not understanding why a field matters), and a fix that only addresses the immediate symptom will not prevent recurrence. The Contractor's triage process should explicitly capture root-cause category, not only issue description and resolution.*

5.1.5 Principle 5: Support Harmonisation and Mapping Transparency

- *Where data are transformed or mapped to standardised formats (e.g., from the system's internal data model like HL7 FHIR IPS, OMOP Common Data Model to the EHDS technical specifications for a priority category), the Contractor **should** document the mapping specification in a form reviewable by the Contracting Authority's data-management staff, not only by the vendor's own engineers.*
- *Documenting the mapping once, at go-live, is not sufficient on its own: the Contractor **should** maintain governance over the mapping specification as source terminologies and target standards evolve, including a named responsible party, a defined review cadence, and a process for distributing updated mappings to the Contracting Authority when either side of the mapping changes.*
    - *Data elements that cannot be automatically mapped to a target standard; should be surfaced explicitly, rather than silently dropped or approximated, so that data managers can make an informed decision about alternative coding strategies.*
- *The Contractor **should** report the proportion of records successfully harmonised at each mapping step, to make residual data loss visible rather than assumed away.*

5.2 Multidimensional Data Quality Framework

Data quality is fitness for purpose, meaning data are of high quality if they meet the requirements of their specific use context. Data quality is multidimensional and multistakeholder, engaging clinicians, data managers, analysts, and patients.

Key Data Quality Dimensions (adapted from TEHDAS[108] recommendations):

Table 7: Data quality dimensions, definitions and implications for procurement

Dimension	Definition	Implications for Procurement
Reliability	Data consistently reflect what they were designed to measure, stable over time	Require robust data collection procedures; vendor ***should*** document data validation rules; audit trails showing consistency checks
Relevance	Data meet the needs of intended users (patients, clinicians, administrative staff)	Procure with end-user input; define data elements based on clinical workflows, not vendor convenience
Timeliness	Data are collected and available when needed for decisions; lag time between collection and use is minimized	Specify maximum acceptable latency (e.g., Medical Test Results available within specified time); require monitoring of data pipelines
Coherence	Data are consistent over time and across data holders; can be combined and compared with data from other sources	Require standardized data definitions across systems; support mapping to EHDS technical specifications for the priority categories; enable linkage across providers
Coverage	Data adequately represent the population/events of interest; no systematic gaps	For primary use, ensure data capture protocols cover all clinically necessary data domains for each patient; population-level representation is a secondary-use concern and is given for context only
Completeness	All required data elements are present for each record; no missing values	Require definitions for mandatory vs. optional data elements; specify acceptable missing-data thresholds; require capture of reasons for missing data

[108] https://tehdas.eu/app/uploads/2022/05/tehdas-european-health-data-space-data-quality-framework-2022-05-18.pdf

Accuracy	Data values are correct and correspond to the clinical/administrative reality they represent	Require validation against source documents; specify error rates or thresholds; implement correction procedures
Conformance	Data conform to defined formats and standards (the EHDS technical specifications, FHIR profiles, value sets, data models)	Require validation testing against standards; include conformance in system testing and operations

Note: A disclaimer on where this table comes from, and its limits. The eight dimensions above are adapted from the TEHDAS Joint Action's data quality framework, which, during the development of this guidance, was not seriously contested as a starting vocabulary. It is worth being explicit, though, that TEHDAS and its successor project QUANTUM[109] were built specifically to support the secondary use of health data, research, innovation, and EU-wide data quality labelling under Article 78 of the EHDS Regulation, not primary use of health data. Using it here as a shared vocabulary is reasonable, since no seriously contested alternative emerged during development of this guidance; treating it as the definitive framework for a primary-use procurement guidance would not be. For primary use, the legally relevant reference point will be the data-quality requirements for registration of personal electronic health data that the Commission is to adopt under EHDS Article 13, covering semantics, uniformity, consistency, accuracy and completeness[110]. Until then, procurers can cross-check the dimensions above against ISO/IEC 25012, a general data quality model whose characteristics (for example accuracy, completeness, consistency and currentness) overlap with them[111], and against the EHR data-quality literature (Weiskopf and Weng[112]; Kahn et al.[113]). Both papers were written for the reuse of EHR data, so they confirm the vocabulary rather than supply a primary-use framework.

The more important point sits underneath the choice of framework, and several reviewers of this guidance made it independently: **dimension importance is purpose-dependent, not universal.** An

[109] https://quantumproject.eu/

[110] https://eur-lex.europa.eu/eli/reg/2025/327/oj/eng (EHDS Regulation (EU) 2025/327, Article 13(4): by 26 March 2027 the Commission is to adopt implementing acts determining data-quality requirements, including semantics, uniformity, consistency, accuracy and completeness, for the registration of personal electronic health data in an EHR system; the acts apply from the application dates of the respective priority categories, see Article 105)

[111] https://www.iso.org/standard/35736.html (ISO/IEC 25012:2008, Software engineering – Software product Quality Requirements and Evaluation (SQuaRE) – Data quality model: 15 data quality characteristics, among them accuracy, completeness, consistency, credibility and currentness)

[112] https://pmc.ncbi.nlm.nih.gov/articles/PMC3555312 (Weiskopf NG, Weng C. Methods and dimensions of electronic health record data quality assessment: enabling reuse for clinical research. J Am Med Inform Assoc 2013;20(1):144-151)

[113] https://pmc.ncbi.nlm.nih.gov/articles/PMC5051581 (Kahn MG et al. A Harmonized Data Quality Assessment Terminology and Framework for the Secondary Use of Electronic Health Record Data. eGEMs 2016;4(1):1244)

emergency department and a geriatric ward will weight timeliness very differently; a system supporting acute decision-making cannot tolerate the latency a chronic-disease registry might accept. Procurers should treat the table above as a checklist of dimensions to consider, not a fixed weighting to apply uniformly, and should expect to state, in their own tender, which of these dimensions matter most for their specific clinical context.

On "buying" data quality: During the guidance development process, all eight dimensions above showed high consistency, and the feedback largely treated this TEHDAS-based framework as an adequate foundation rather than proposing an alternative. A more contested question, whether data quality should be specified through outcome-based KPIs, process-based capability requirements, or a hybrid of both: a hybrid approach was the single most common recommendation, but process-based and strict outcome-based approaches each retained meaningful support, and it was also argued that instead, for a risk-tiered model scaling required data-quality levels to the clinical risk of the use case. This guidance therefore **retains the hybrid framing below as the least contested of the three, not as a demonstrated consensus**. The Contractor should propose, for each dimension in Table 7, a measure, a target and a reporting interval linked to the purpose of the data, and the Contracting Authority should set the target values in the tender according to the clinical risk of the use case.

Furthermore, rather than treating outcome-based, process-based, and hybrid as three competing options to choose between, it is more useful to think of vendor evidence as needing all three of the following, together:

- A documented data quality **process** is actually in place (not merely claimed), this is the process-based half.
- That process is explicitly **linked to the specific purpose** the data will serve, expressed as concrete KPIs, data quality is not an abstract property, and a completeness or accuracy figure is only interpretable against the KPI it is meant to support.
- Evidence that the **results** meet those KPIs, the outcome-based half, but only meaningful once the first two conditions establish what the result should be judged against.

A vendor able to show only results, with no visibility into the process that produced them, is not more trustworthy than one who can only describe process; procurers evaluating vendor data quality claims should ask for both, tied to the purpose the data is actually procured for.

5.3 Understanding Data Quality Across the Data Lifecycle

Data Quality is Context-Specific: The definition of "quality" shifts depending on where data are in their lifecycle and what purpose they serve.

Stage 1 is the focus of the criteria in this guidance: quality at the point of capture and its preservation when the data are exchanged in the EHDS formats. Stages 2 and 3 are shown for context, to explain why the meaning of "quality" changes with the purpose; they are not procurement criteria in this guidance.

Who is expected to do what at Stage 1? Data quality at the point of care is a shared result. The vendor or manufacturer is expected to provide the capability: *structured capture with required fields and standard coding, real-time validation, provenance and version history, and export of the data in the EHDS formats without loss (Principles 1 to 3)*. The operator, that is the hospital or other

Contracting Authority, is expected to use and configure that capability: *it defines the mandatory data set and the local validation rules, trains and supports its staff, monitors the data quality it actually obtains and acts on the findings (Principle 4 and the Data Quality Governance clauses)*. A procurer should ask the vendor what the system can do and should keep for itself what only the operator can do.

Stages 2 and 3 are nice-to-have in this guidance. Harmonisation, population-level quality and secondary-use quality are explained so that a procurer understands why the meaning of "quality" changes with the purpose. They are not criteria for the EHR system by default, and a population-level notion such as representativeness has no meaning for a single patient or a single hospital.

5.3.1 Stage 1: Point of Care (Primary Use of Health Data)

- **Purpose:** Informing clinical decisions for individual patients
- **Completeness:** Did the clinician capture all relevant information needed to make a sound medical decision?
    - Example: For an oncology patient starting chemotherapy, completeness requires pathology results, molecular markers, comorbidities, and renal/liver function tests—all available before treatment planning.
- **Timeliness:** Are Medical Test Results, Medical Imaging Study and related Imaging Report content, and specialist input available at the moment the care decision is being made, not days later?

5.3.2 Stage 2: Data Harmonisation

- **Purpose:** Preparing data for aggregation and analysis across organisations or for research cohorts
- **Completeness:** Are all required data elements present for each record, regardless of how they were captured at the source?
    - Example: of 100 patients identified at the source system, only 80 had a captured blood-pressure reading. A harmonised dataset should reflect that same 80/100 completeness rate, regardless of whether the original reading was entered as a structured field or as free text, unstructured text can, in principle, be mapped via NLP extraction, which simply adds an additional quality-control step (did the extraction correctly and completely capture what was written) rather than making the reading unmappable outright. Whether a value can be mapped at all is a separate, semantic question, whether the mapped value correctly and consistently represents what was actually captured, addressed below.
- **Timeliness:** How quickly do clinical updates flow from source systems into harmonised data warehouses? If data are updated weekly, the harmonised dataset may already be outdated for real-time research. This depends on two separate things: how quickly the source system itself updates, and how quickly the mapping pipeline that harmonises it runs. A source system with real-time updates is no guarantee of a real-time harmonised dataset if the mapping pipeline behind it is under-resourced or run as an infrequent batch job, procurers should ask about both.
- **Conformance:** Do the data structures match standardised formats? (IPS, FHIR resources, OMOP tables, etc.)

5.3.3 Stage 3: Secondary Use and Reuse (Research, AI, Public Health)

- **Purpose:** Training algorithms, conducting epidemiologic studies, generating evidence
- **Completeness**: Is the dataset representative of the population and variables needed for training a robust, generalizable model?
    - Example: If an AI model for heart failure prediction is trained on 2019 data before newer therapies became available, is not representative of today's patient population and treatment landscape, not because records are missing, but because the population the model was trained on has since shifted. This is a distinct failure mode from completeness (missing values within existing records) and should be checked separately.
- **Timeliness**: Does the data reflect current clinical practice and treatment landscapes, or is it temporally obsolete?
- **Validity**: Are the data accurate and unbiased, or do they contain systematic errors that would propagate into algorithms? (e.g., missing data disproportionately affecting certain demographics)

5.4 Ready-to-Use Tender Clauses for Data Quality

5.4.1 Data Quality Dimensions

*The Contractor **should** implement a data quality framework addressing the following dimensions, adapted to the phases of the data lifecycle (a recommended framework operationalising data-quality good practice; the Commission has not yet adopted the data-quality requirements foreseen under EHDS Article 13(4), which remain pending):*

- ***Completeness:** all clinically required data elements are present for each patient record. Sample threshold: e.g., ≥95% completeness for the defined mandatory field set at the point of capture [specify % and field set].*
- ***Accuracy:** data values correctly represent clinical or administrative reality at the time of entry, with a documented, monitored error rate. [specify acceptable error rate]*
- ***Timeliness:** data are available in the record within a clinically appropriate time of the event occurring. [specify maximum acceptable lag, e.g., hours for Medical Test Results, minutes for vital signs]*
- ***Conformance:** data captured conform to the structural and terminology standards this guidance requires for primary use (EEHRxF/HL7 FHIR profiles, and standard vocabularies such as SNOMED CT and LOINC, per Section 3).*
- ***Reliability:** the system returns the same, stable value for the same underlying clinical fact regardless of when, how, or by which authorised user it is queried — a record should not appear to disagree with itself.*
- ***Relevance:** data captured directly supports the clinical workflow and decision-making needs of the care team at the point of care, rather than being collected for an unspecified future purpose.*
- ***Coherence:** data is internally consistent within a single patient's record, and consistent with data received about the same patient from other systems the patient has been treated in (e.g., no contradictory allergy status between two integrated systems).*
- ***Coverage:** all clinically necessary data domains are captured for the patient's care episode (e.g., a complete medication list alongside vitals and diagnoses, not a partial record), a matter*

of breadth for this patient's record, not population-level sampling, which is a secondary-use concern addressed separately.

5.4.2 Data Quality Governance

*The Contractor **should** designate a Data Quality Officer or team responsible for:*

- *Developing and maintaining data quality policies and procedures*
- *Monitoring data quality metrics*
- *Investigating and remediating data quality issues*
- *Reporting data quality status to the Contracting Authority*

5.4.3 Contracting Authority Obligations as a Health Data Holder (Article 60 EHDS)

Under Article 60 of the EHDS Regulation, hospitals and clinics are placed under an obligation to provide requested electronic health data to Health Data Access Bodies within three months. A hospital can only meet that obligation if the procured system is functionally ready to support it, which is why a Contracting Authority may wish to add the optional readiness clauses below. They concern secondary use, which is outside the scope of the criteria in this guidance, and are given for context only; Chapter IV of the EHDS Regulation applies from 26 March 2029, with some provisions following in 2031[114].

- *The commissioned system **should** enable the Contracting Authority to fulfil its obligations as a Health Data Holder, including the preparation, consolidation, and timely export of datasets for Health Data Access Bodies, without imposing unjustified additional technical costs on the Contracting Authority (mandated by EHDS Article 60).*
- *The system **should** support pseudonymisation and anonymisation in accordance with the state of the art, such that prepared data packages can be transferred securely to the isolated secure processing environments established under the EHDS (supporting the Health Data Holder duties in EHDS Article 60).*
- *The Contractor **should** report [e.g., quarterly] the time needed to prepare and export a test dataset of [specify size] and the share of records that pass the pseudonymisation or anonymisation checks, so that the Contracting Authority can assess whether it could meet the three-month deadline under Article 60.*
- *Where datasets made available for secondary use contain intellectual property or trade secrets, the system should support secure identification and flagging of such data, consistent with the safeguards required under Article 52 of the EHDS Regulation.*

5.4.4 Data Quality Monitoring and Reporting

*The Contractor **should**:*

- *Implement automated data quality monitoring covering the dimensions listed above*
- *Generate data quality reports [specify frequency, e.g., monthly] including:*
  - *Completeness metrics (% of records with required fields populated)*
  - *Accuracy metrics (% of sampled records validated against source documentation)*

[114] https://eur-lex.europa.eu/eli/reg/2025/327/oj/eng (EHDS Regulation, Article 105, dates of application: Chapter IV on secondary use applies from 26 March 2029, with some provisions applying from 26 March 2031)

- *Timeliness metrics (average lag time from data entry to availability in Patient Summary)*
- *Conformance metrics (% of documents exported in the EHDS priority-category formats successfully validating against FHIR profiles)*
- *Establish Service Level Agreements (SLAs) for each metric with acceptable ranges*
- *Alert the Contracting Authority within [specify duration e.g. 72 hours] if any metric falls outside acceptable range*

5.4.5 Data Quality by Design

*System design **should** support data quality through:*

- *Real-time validation of data entry with supportive (not punitive) error handling*
- *Clinical decision support prompting complete capture of relevant data*
- *Structured data entry using standard coding systems (e.g., SNOMED CT, LOINC, or the code systems prescribed by the EHDS technical specifications)*
- *Data provenance tracking (who entered data, when, from what source)*
- *Version control preserving data corrections and auditable change history*
- *Explicit recording of the reason for absence (for example with the HL7 Data Absent Reason value set) where a required section of an EEHRxF document has no entries, so that missing data can be told apart from data not yet collected*

5.4.6 Interoperability and Harmonisation

When data are exported to standard formats (e.g. EEHRxF/HL7 FHIR IPS, OMOP Common Data Model):

- *The Contractor **should** document mapping specifications showing source-to-standard-concept transformations*
- *The Contractor **should** monitor mapping completeness and report % of records successfully harmonized*
- *The Contractor **should** provide data managers visibility into unmappable data and alternative coding strategies*

5.4.7 Continuous Improvement

*The Contractor **should** conduct quarterly reviews of data quality metrics with the Contracting Authority, identifying trends, root causes of quality degradation, and improvement opportunities. The Contractor should implement Contracting-Authority-approved improvements with progress tracked in subsequent reports.*

A consolidated, fillable checklist version for Data Quality is provided in Annex, Section 3 (Procurement Checklists for Data Quality) at the end of this document.

6. Minimum Procurement-Ready Criteria for Embedding Usability and User-Centred Design

Investments in technology, even technically excellent technology, often fail to deliver value if end-users cannot or will not adopt them. This chapter gives recommended practice for the usability, accessibility and user-centred design of EHR systems and for health professionals. The EHDS provisions on these topics are general[115], so the criteria below are phrased as "should", and standards such as EN 301 549[116] are recommended ways of meeting them rather than legal requirements in themselves. "Shall" is used only where a cited legal provision mandates the point.

6.1 Technology Adoption Framework: UTAUT and Beyond

The Unified Theory of Acceptance and Use of Technology (UTAUT)[117][118] provides a research-backed framework for understanding why individuals adopt or resist new technologies. It identifies four core factors predicting behavioural intention to use a system:

Table 8: UTAUT adoption factors and their implications for procurement

Factor	Definition	Implications for Procurement
Performance Expectancy	User's perception that the system will help them perform their job better and achieve their goals	Define success in terms users value (faster diagnosis, safer medication management, better patient outcomes); measure and communicate benefits
Effort Expectancy	User's perception that the system is easy to use and requires minimal effort to learn	Require user-centered design (usability testing, intuitive interfaces); provide comprehensive training and support
Social Influence	User's perception that important others (colleagues, supervisors) think they should use the system	Engage clinical leadership; plan implementation with champions; create peer learning and support

[115] https://eur-lex.europa.eu/eli/reg/2025/327/oj/eng (EHDS Regulation (EU) 2025/327, Article 4: the electronic health data access services and the proxy services are to be easily accessible for persons with disabilities, vulnerable groups and persons with low digital literacy; Article 12, health professional access services: personal electronic health data are to be presented in a user-friendly manner in the electronic health records to allow for easy use by health professionals)

[116] ETSI EN 301 549 V3.2.1 (2021-03), "Accessibility requirements for ICT products and services", https://www.etsi.org/human-factors-accessibility/en-301-549-v3-the-harmonized-european-standard-for-ict-accessibility.

[117] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3375136

[118] https://en.wikipedia.org/wiki/Unified_theory_of_acceptance_and_use_of_technology

Facilitating Conditions	User's belief that organizational and technical infrastructure support system use	Provide training, helpdesk support, access to resources; minimize workflow disruptions during implementation

Beyond UTAUT, additional factors specific to healthcare contexts influence adoption:

- Alignment with clinical workflows: Does the system fit how clinicians actually work, or does it require workarounds?
- Equity and access: Are all user populations (different clinical roles, digital literacy levels, languages) supported?
- Trust in data: Do clinicians trust the quality and relevance of data presented by the system?

6.2 Ethical Principles and Human Rights Considerations in Digital Health

Beyond usability, procurements should reflect the ethical principles and human rights relevant to digital health technologies. At European level, the main reference point is the set of 16 European Ethical Principles for Digital Health[119], proposed during the French Presidency of the Council of the EU and approved by the eHealth Network in January 2022[120]. The principles are not legally binding, but they give procurers and vendors a shared European vocabulary for the ethical requirements that a digital health solution should meet.

The 16 principles are grouped in four ethical dimensions:

- Base digital health on humanistic values (principles 1–4): digital health should complement and optimise, not replace, face-to-face care; individuals should be informed about the benefits and limits of digital tools and how they work; and, where AI is used, reasonable efforts should be made to make it explainable and free of discriminatory bias.
- Enable individuals to manage their digital health and data (principles 5–8): individuals should be involved in shaping the frameworks that govern digital health and their data, be able to retrieve their health data in a commonly used format, be informed how and for what purpose their data have been or may be accessed, and be able to grant access and exercise their rights, including the right to object.

[119] French Presidency of the Council of the European Union / French Ministry of Health, European Ethical Principles for Digital Health, January 2022, https://sante.gouv.fr/IMG/pdf/220131_european_ethical_principles_for_digital_health_fr_eng.pdf. A summary of the four dimensions and the 16 principles is also published by the Council of Europe: https://www.coe.int/en/web/human-rights-and-biomedicine/access-to-digital-spaces-to-understand-and-use-health-services/-/highest_rated_assets/nTmcJLi8P0UU/content/european-union-european-ethical-principles-for-digital-health.

[120] Agence du Numérique en Santé, Digital Health actions and initiatives under the French Presidency of the Council of the EU, 2022, https://esante.gouv.fr/sites/default/files/media_entity/documents/french-presidency-pfue-2022_en.pdf. The principles were proposed by the French Presidency and approved by the eHealth Network (the network of Member State authorities responsible for digital health) in January 2022.

- Make digital health inclusive (principles 9–12): digital health should be accessible to all, including people with disabilities or low literacy; intuitive and easy to use; supported by training; and backed by human communication support where needed.
- Implement eco-responsible digital health (principles 13–16): environmental impacts should be identified and measured, eco-design best practices applied, equipment re-used and recycled, and a commitment made to reduce the ecological footprint.

These principles are not procurement requirements in themselves, but several of the tender clauses in Section 6.4 put them into practice, in particular those on accessibility, inclusive design, training and support, and control over personal data. Section 6.4.7 ties the data-protection and non-discrimination points to the legal provisions that apply (GDPR and the AI Act).

6.3 Involving End-Users: Needs Assessment and Pilot Stages

End-users should be involved at two stages: when needs are assessed, before the requirements are written, and again at the pilot stage, before a solution is rolled out widely. A vendor's self-declaration is not sufficient evidence of usability at either stage (see Usability Testing above). What "pilot" means depends on what is being acquired, so this guidance distinguishes three situations:

- Needs assessment ahead of a new procurement. Before specifications are written, find out who will use the system and how they work today. Example methods: focus groups with clinicians, nurses and administrative staff; a structured survey of clinical staff on their expectations and pain points; walkthroughs or observation of current workflows.
- Piloting a full EHR replacement. Test the new system with a limited unit, such as a ward, a department or a clinic, before organisation-wide rollout, using realistic scenarios and with a defined duration and success criteria. Example methods: scenario-based testing with end-users; structured feedback surveys and short interviews at fixed points; a small group of super-users who collect and pass on issues.
- Piloting an incremental update or extension to an existing, already deployed EHR. Many providers will buy compliance-related updates rather than a new system, and end-user involvement is still needed, scaled to the change. Before the update, show users what will change and whether it is visible to them at all; after installation in a test environment or in a limited unit, confirm that workflows are unchanged or improved and that nothing has become harder to use. Example methods: a short demonstration or simulation with a sample of users; a brief survey or feedback round after a limited release.

The depth of involvement should scale to the size and complexity of the change, in line with the proportionality note under User Research and Engagement above.

6.4 Ready-to-Use Tender Clauses for User-Centered Design

6.4.1 User Research and Engagement

*The Contractor **should** demonstrate commitment to user-centered design through:*

- *Documented user research identifying needs, goals, and workflows of intended users (clinicians, nurses, patients, administrative staff)*
- *Engagement of clinical advisors throughout development, with documented meeting summaries*
- *Feedback from representative end-users during needs assessment or design and pilot phase, with evidence of incorporation into design decisions*
- *Participation in the needs-assessment and pilot activities described in the section on involving end-users, with the pilot duration, scope and success criteria defined in the Contract*

Note: the depth of documented user research expected here should scale to the size and complexity of the procurement. Requiring the same formal, extensively documented research programme from a small clinic procuring a modest add-on module as from a national EHR tender risks excluding capable SME vendors who would otherwise be a strong fit, without a corresponding gain in quality. Contracting Authorities should specify what counts as sufficient evidence for their specific procurement, rather than defaulting to the most extensive documentation standard in every case. Contracting Authorities should, when applicable, promote consortium-friendly procedures and even signal incentives for that, so as to stimulate companies to work more together, apply together and create solutions together.

6.4.2 Usability Testing

*The Contractor **should** provide at minimum, either a live demonstration or scenario-based test during the tender process, or documented evidence of prior user-testing results; formal certification remains an accepted, though not mandatory, alternative. In either case, the following should be provided:*

- *Sample size and participant selection documented*
- *Tasks and scenarios reflecting real-world use*
- *Evidence, from end-user scenarios or a pilot, that the system supports the workflows that the Contracting Authority has described, without workaround*
- *Success metrics (e.g., "95% of participants able to complete key task within 5 minutes")*
- *Results documented with evidence of design iterations addressing identified usability issues*
- *Final usability test results provided to Contracting Authority prior to deployment*

A vendor's self-declaration alone should not be accepted as evidence of usability. For the design of the testing, ISO 9241-11 (usability defined as effectiveness, efficiency and satisfaction) and ISO 9241-210 (human-centred design of interactive systems) are recommended references[121].

6.4.3 Accessibility Compliance

*The Contractor **should** make sure that the system complies with:*

[121] https://www.iso.org/standard/63500.html (ISO 9241-11:2018, Ergonomics of human-system interaction, Part 11: Usability: Definitions and concepts); https://www.iso.org/standard/77520.html (ISO 9241-210:2019, Part 210: Human-centred design for interactive systems)

- *EN 301 549 (European accessibility standard for ICT products and services) at Level AA minimum*
- *WCAG 2.1 Level AA, or a later version such as WCAG 2.2 (Web Content Accessibility Guidelines)*
- *Specific accommodations for users with visual, hearing, mobility, or cognitive disabilities*

Note: EN 301 549 and WCAG 2.1 AA are recommended accessibility standards, not themselves mandated by EHDS or the other regulations in this guidance's scope; EHDS's own, narrower accessibility provisions are Article 4(5), on access-service accessibility, and Article 12, on user-friendly presentation for health professionals[122]. The version of EN 301 549 harmonised under the Web Accessibility Directive is V3.2.1, which refers to WCAG 2.1; ETSI published V4.1.1 in September 2026, so a tender should state which version applies[123].

6.4.4 Inclusive Design

*The Contractor **should** make sure that system design supports diverse users:*

- *Multiple language support for primary EU languages + [local languages]*
- *Culturally appropriate terminology and concepts*
- *Readability suitable for users with varying education and digital literacy levels*
- *Training and support accessible to diverse user populations*
- *Support for the user groups identified by the Contracting Authority, including different clinical roles*
- *An intuitive interface that users can learn to use with the training and support provided, and human communication support where needed*

6.4.5 Training and Support

*The Contractor **should** provide:*

- *Tailored training for different user roles (clinician, administrative, IT)*
- *Multiple training modalities (in-person sessions, video tutorials, written guides, helpdesk)*
- *"Train the trainer" program enabling the organisation to scale training to all staff*
- *Helpdesk support available [enter hours/week e.g. 168/week] for [X months] post-implementation with target response time [Y hours] and 24/7 when emergency or around the clock clinical services are provided.*
- *Documented FAQ and knowledge base addressing common questions and issues*

---

[122] https://eur-lex.europa.eu/eli/reg/2025/327/oj/eng (EHDS Regulation (EU) 2025/327, Article 4: the electronic health data access services and the proxy services are to be easily accessible for persons with disabilities, vulnerable groups and persons with low digital literacy; Article 12, health professional access services: personal electronic health data are to be presented in a user-friendly manner in the electronic health records to allow for easy use by health professionals)

[123] https://digital-strategy.ec.europa.eu/en/policies/web-accessibility-directive-standards-and-harmonisation (European Commission: EN 301 549 V3.2.1 harmonised on 18 August 2021 under the Web Accessibility Directive, Implementing Decision (EU) 2021/1339; WCAG 2.2, published 5 October 2023, was not yet used in a harmonised version at the time of consultation);
https://www.etsi.org/deliver/etsi_en/301500_301599/301549/04.01.01_60/en_301549v040101p.pdf (ETSI, EN 301 549 V4.1.1, published September 2026; accessed October 2026)

- *Support for the Contracting Authority's implementation plan, by working with its clinical leadership and clinical champions and by providing peer-learning and support materials for staff*
- *An implementation plan that minimises disruption to clinical workflows*

6.4.6 Feedback Mechanisms and Continuous Improvement**

*The Contractor **should**:*

- *Establish feedback mechanisms during implementation (user surveys, focus groups, office hours)*
- *Monitor adoption metrics (% of users, frequency of use, feature utilisation, error rates)*
- *Address usability issues according to a severity scale agreed in the contract (for example, critical = clinical-safety impact or inability to complete a clinical task without a workaround), with separate times for response, workaround and final fix, and acceptance criteria for closing each issue*
- *Conduct post-implementation user satisfaction surveys at 3, 6, and 12 months*
- *Engage with users on an ongoing basis to identify and prioritise improvements*
- *State the expected benefits of the system in terms that users value (for example faster diagnosis, safer medication management, better patient outcomes), and agree with the Contracting Authority how these benefits are measured and reported after go-live*
- *Show clinicians the source and the time of the data presented by the system, and report data quality measures to the Contracting Authority (see the clauses on Data Quality Monitoring and Reporting)*

6.4.7 Human Rights Alignment

*The Contractor **should** design and operate the system in line with the following human rights principles:*

- Data protection: The Contractor should provide functions that give users control over their personal data, and transparent, understandable privacy information *(mandated by GDPR Articles 12–14 and 25)*
- Non-discrimination: For any algorithmic component that qualifies as a high-risk AI system under the AI Act (e.g., an MDR-classified clinical decision-support tool, per Article 6(1)), the Contractor should conduct a conduct bias assessment; document and monitor for differential impact across populations *(mandated by AI Act Article 10)*; for other algorithmic components. *This is recommended good practice rather than a regulatory requirement*
- Transparency: The Contractor should ensure that the system lets users understand what data are collected, how they are used, and who has access *(mandated by GDPR Articles 12–14)*
- User control: the Contractor should implement mechanisms allowing users to access, correct, and restrict sharing of personal data *(mandated by GDPR Articles 15–18 and 21)*

A consolidated, fillable checklist version for User-Centered Design is provided in Annex, Section 4 (Procurement Checklists for User-Centered Approach) at the end of this document.

7. Innovative Procurement Approaches

Traditional procurement instruments (open tenders with fixed specifications) may be suboptimal for procuring solutions requiring innovation, co-design with users, or where requirements are not fully defined at the outset. The European Union has developed flexible procurement instruments designed to foster innovation while maintaining public sector accountability. This chapter is informational: it describes instruments that already exist in EU public procurement law and does not set requirements of its own. Examples that touch on secondary use (analytics infrastructure, data harmonisation) are given for context only, because the criteria in this guidance concern primary use. Article references are to Directive 2014/24/EU[124]. This chapter can be complemented by much more specific readings and online materials. There are also courses on Innovative Procurement that staff of the Contracting Authority should consider taking to prepare for its adequate use.

7.1 Overview of Innovative Procurement Instruments

The table below compares the four instruments at a glance; the detailed sections that follow give the full process, advantages, disadvantages, and guidance on when to use each one.

Table 9: Comparison of the four innovative procurement instruments

Instrument	Best for	Commitment to purchase	Time and effort
Competitive Dialogue	A complex, one-off purchase where the technical approach isn't fully defined yet	Yes, at the end of the dialogue	Heavier than Open Procedure; multiple dialogue rounds before a single tender is submitted
Innovation Partnership	Genuinely novel EEHRxF work with no market-ready solution, where you may also want to buy what gets developed	Optional, phase by phase — can stop without purchasing	Significant, ongoing commitment across development phases; higher than Competitive Dialogue
Public Procurement of Innovation (PPI)	Deciding which instrument to use in the first place — an umbrella decision frame, not a procedure itself	Depends on the instrument ultimately chosen	No procedural shortcut of its own; effort is whatever the chosen instrument requires
Pre-Commercial Procurement (PCP)	A genuinely unsolved problem where no workable solution exists anywhere on the market yet	None — R&D only; a separate procurement (e.g., PPI) follows if a	Longest time horizon of the four; no guarantee of a usable outcome

[124] https://eur-lex.europa.eu/eli/dir/2014/24/oj/eng (Directive 2014/24/EU on public procurement: Article 30, competitive dialogue; Article 31, innovation partnership; the Directive is transposed into national law, so national rules and applicable thresholds need to be checked)

		solution proves viable	

7.2 Competitive Dialogue (Article 30, Procurement Directive 2014/24/EU[125])

Purpose: Engage with potential vendors through structured dialogue to jointly define requirements and solutions before finalising technical specifications.

Process:

- The Contracting Authority publishes a contract notice describing its needs and requirements without a fully fixed technical specification.
- Selected candidates are invited into a structured dialogue, conducted in successive stages, to develop one or more suitable technical, legal, or financial solutions.
- The Contracting Authority may progressively reduce the number of solutions discussed by applying the published award criteria, until it can identify the solution(s) capable of meeting its needs.
- Once the dialogue is declared closed, participants submit their final tenders based on the solution(s) presented during the dialogue.

Advantages for EEHRxF Procurement:

- Allows discussion of interoperability standards and data quality approaches before specifications are locked
- Lets procurers draw directly on vendor knowledge to shape realistic, market-tested requirements, rather than guessing at specifications in isolation. The procedure itself needs substantial procurement and technical expertise, so external expert support is a prerequisite where in-house capacity is limited, and the conditions of Article 26(4) of Directive 2014/24/EU must be met.
- Reduces the risk of a tender attracting no compliant bids, or bids that technically comply but fail to deliver a workable solution, because requirements are stress-tested with the market before being finalised.

Disadvantages:

- More time-intensive and costly than open procedure
- Requires procurement staff time and process discipline to run well; without it, dialogue can drift without converging on a specification.
- Places a higher burden on bidders (multiple dialogue rounds), which can discourage smaller vendors from participating unless the process is actively designed to keep it proportionate.

When to Use:

[125] https://eur-lex.europa.eu/eli/dir/2014/24/oj/eng (Directive 2014/24/EU on public procurement)

Complex IT systems with interoperability components where technical approach is not fully defined; need for vendor innovation or creative solutions.

7.2.1 How and When to Launch a Competitive Dialogue

The Open Procedure remains viable where substantial internal technical expertise already exists; Competitive Dialogue or Innovation Partnership are preferred where it does not.

- **Before launching:** confirm internally that requirements genuinely cannot be fully specified in advance — Competitive Dialogue is a heavier process than the Open Procedure and is not justified for straightforward, well-understood purchases.
- **Resourcing:** assign a named evaluation panel with the technical capacity to engage substantively across multiple dialogue rounds; this is where organisations with thin internal expertise most often struggle, and where external technical advisory support is most valuable.
- **A lower-effort complementary route:** where an organisation lacks the capacity to run a full Competitive Dialogue or Innovation Partnership, this guidance's survey respondents independently and repeatedly proposed a **national or EU-wide catalogue of pre-vetted, EEHRxF-compliant services** as a complementary instrument — a lighter-weight route that does not replace Competitive Dialogue for genuinely novel requirements but can shortcut it for more standard ones.
- **External resources:** national e-procurement portals typically publish worked Competitive Dialogue case studies and procedural templates; procurers should consult their national portal before drafting a dialogue-based contract notice from scratch.

7.3 Innovation Partnership (Article 31, Procurement Directive 2014/24/EU)[126]

Purpose: Establish long-term partnership where vendor develops new solutions alongside the contracting authority, with procurement of developed solutions built into the contract.

Process:

- A single procedure (no separate re-tendering step) combining competitive-dialogue-style negotiation with an R&D phase and an option to purchase the resulting solution.
- The Contracting Authority sets out the need for an innovative product, service, or works that cannot be met by solutions already available on the market and structures the partnership in successive phases with intermediate targets.
- The Contracting Authority may terminate the partnership, or reduce the number of partners, at the end of each phase against the agreed targets, before committing to purchase.

Advantages for EEHRxF Procurement:

- Avoids the two-step “develop then separately re-tender” problem: the vendor that develops a solution can, if it meets the agreed targets, be the vendor that supplies it, without a second competitive procedure.

[126] https://eur-lex.europa.eu/eli/dir/2014/24/oj/eng (Directive 2014/24/EU on public procurement)

- Well suited to genuinely novel EEHRxF integration work — for example, harmonisation tooling or cross-border analytics infrastructure — where no market-ready solution yet exists.

Disadvantages:

- Significant commitment of procurer time and technical resource across multiple phases; not suited to organisations seeking a quick or low-effort route to market.
- Carries genuine development risk — unlike buying an existing product, the partnership may not produce a solution that meets the agreed targets, and the Contracting Authority should plan for that possibility.

When to Use: Need for pioneering solutions combining EEHRxF with other innovations (e.g., AI-supported data harmonization, patient-centered data access platforms, cross-border analytics infrastructure).

7.4 Public Procurement of Innovation (PPI)

Purpose: Public procurement of innovative solutions where the Contracting Authority acts as an early adopter of innovative solutions that are not yet available on a large-scale commercial basis, using existing procedures such as Competitive Dialogue, Innovation Partnership and other flexible approaches. The European Commission uses “innovation procurement” for the wider field that covers both PPI and Pre-Commercial Procurement (PCP)[127].

Process:

- The Contracting Authority selects whichever instrument — Competitive Dialogue, Innovation Partnership, or a well-specified Open Procedure with innovation-friendly award criteria — best fits the specific requirement, rather than treating PPI as a single fixed procedure of its own.

Advantages for EEHRxF Procurement:

- Gives procurers a decision framework rather than a single tool: start from the need, then choose the lightest procedure capable of meeting it.

Disadvantages:

- As an umbrella category rather than a distinct procedure, it offers no procedural shortcut of its own — the procurer still has to make (and justify) a specific instrument choice

When to use:

[127] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52021XC0706(03) (European Commission, Guidance on Innovation Procurement, C(2021) 4320 final, published in the Official Journal on 6 July 2021: innovation procurement covers pre-commercial procurement and the public procurement of innovative solutions, the latter using existing procedures such as competitive dialogue and innovation partnership)

- As a starting frame for procurement strategy discussions, before narrowing down to Competitive Dialogue, Innovation Partnership, PCP, or an innovation-friendly Open Procedure.

7.5 Pre-Commercial Procurement (PCP)

Purpose: Commission vendor to develop new solutions (not yet market-ready) addressing specified needs, with no guarantee of procurement.

Process: Structured as R&D services procurement, falling outside the scope of Directive 2014/24/EU only where the conditions of **Article 14** and recital 47 of that Directive are met (the benefits do not accrue exclusively to the contracting authority, or the service is not wholly remunerated by it, with risks and benefits shared at market conditions and the intellectual property rights arranged accordingly); otherwise the Directive applies[128]. It is typically run in phases (solution exploration, prototyping, and original development/first product testing) with multiple vendors competing in parallel through early phases. No commitment to purchase the resulting solution at commercial scale; PCP funds the R&D phase only, with a separate procurement process (e.g., PPI) potentially following if a solution proves viable.

Advantages for EEHRxF Procurement:

- Allows genuinely early-stage exploration — for example, novel approaches to cross-border data harmonisation — where no vendor yet has a workable solution, without the Contracting Authority committing to buy an unproven result.
- Running several vendors in parallel through early phases spreads technical risk and surfaces multiple candidate approaches before any purchasing decision is made.

Disadvantages:

- Longest time horizon of the instruments in this section, with no guarantee that any resulting solution reaches commercial maturity or is ultimately procured.
- Requires separate follow-on procurement (e.g., PPI) to actually acquire a resulting solution at scale, adding a further procedural step.

When to use:

- Genuinely unsolved problems — where the Contracting Authority cannot yet specify a solution because a workable one does not yet exist anywhere on the market — rather than as a route to a faster or cheaper standard procurement.

7.6 Digital Tools Across the Procurement Life Cycle

Contracting authorities should run the procedure itself on an established e-procurement tool, that is, a platform on which the procedure is published, communications are exchanged, tenders are

[128] Directive 2014/24/EU of the European Parliament and of the Council of 26 February 2014 on public procurement, Article 14 and recital 47, http://data.europa.eu/eli/dir/2014/24/oj; Commission Communication COM(2007) 799 final, “Pre-commercial Procurement: Driving innovation to ensure sustainable high quality public services in Europe”.

received and evaluated, dialogue or negotiation stages are run and the contract is formulated online, in line with the European Commission's work on e-procurement.[129] Electronic communication is already the rule for procedures under Directive 2014/24/EU, but in practice the full life cycle is not yet fully digital. This recommendation is deliberately generic, and the guidance does not name platforms.

Tools for market mapping (acknowledged, not recommended). A different category of software helps procurers map the supplier market and identify vendors with particular characteristics. Such a tool was demonstrated at Workshop 4 and appears to have potential, but it is not an e-procurement platform, the market for such tools is still immature and the evidence gathered is too limited to recommend or rank specific products. This guidance therefore acknowledges that these tools exist and does not recommend them. Any reference to specific products would be illustrative and non-exhaustive and would soon be outdated, so none is given here.

Both categories belong to a wider set of digital tools that can support the whole life cycle, from mapping market opportunities to following up the contract and collecting performance feedback. The Procurement Process Map in Annex, Section 5 shows where they fit.

[129] Directive 2014/24/EU, Article 22(1): Member States are to ensure that all communication and information exchange under the Directive, in particular electronic submission, is performed by electronic means; the tools used must be non-discriminatory, generally available and interoperable with the ICT products in general use, and the Article lists limited exceptions (for example specialised tools or protection of especially sensitive information). See also the European Commission's overview of digital procurement (eSubmission, eAccess, eInvoicing, the European Single Procurement Document and eCertis; eForms notices are published on Tenders Electronic Daily): https://commission.europa.eu/funding-and-tenders/tools-public-buyers/digital-procurement_en (accessed October 2026).

8. Considerations for AI-Enabled Solutions

AI has become more prominent, and AI-related regulation, namely the AI Act and, for AI used for medical purposes, the MDR, has become more relevant to the purchase of EHR systems. It is added here deliberately with a light-touch: it does not aim to be comprehensive, it sets no requirements of its own, and it identifies some of the relations between AI components and the four core pillars, so that a procurer knows what to look for when a solution incorporates AI.

AI Act and the MDR already cover much of the associated risk for AI with a medical purpose. This chapter therefore contains no strong recommendations. The chapter is about how a procurer can prepare for compliance and check that the vendor is ready.

8.1 Considerations

- **Discovery first.** Which rules apply depends on whether AI is present and what it does. The procurer's practical task is to find out which AI components the solution contains, what they do (for example clinical decision support, diagnostics, documentation or ambient notetaking, or coding assistance), whether the vendor treats them as medical devices, and where they sit in the data flow.
- **Compliance is for the vendor to demonstrate.** The procurer does not have to verify AI Act compliance independently. The procurer asks the vendor to state which AI Act and MDR obligations it considers apply, in which role (provider or deployer), and what evidence supports that position. How AI tools used in clinical settings are classified and regulated is still being worked out in several Member States.
- **AI and the exchange format.** When an AI function that is part of the EHR system produces or processes content in an EEHRxF priority category, for example by drafting a discharge report, the result should be representable in the EEHRxF specification for that category, so that AI-generated or AI-processed data does not fall outside the structure and coding the exchange format requires. This is a consideration for AI inside the EHR system. It is not a requirement for separate AI tools that sit on top of an existing system and do not produce priority-category data; requiring those to produce the exchange format would be too limiting for the market.
- **Visibility of AI-generated content.** Where AI generates or influences clinical content, it should be possible to tell that AI was involved, so that its role in a care decision can be traced. The AI Act's transparency rule for AI-generated content (Section 2.3) is relevant here.
- **Security of the AI component**. AI components need the same cyber resilience as any other component, including protection of the algorithm and its data (Chapter 4). AI-specific attacks are treated there as a recommended topic.
- **Ethics, bias and transparency.** Bias, differential impact and transparency towards users are touched on in the ethical principles and human-rights considerations in Section 6.2. How non-discrimination is defined and evidenced is still an open question.

8.2 Moderate Recommendations

Where a solution incorporates AI, require the vendor to disclose which AI components are present, how they are used and which regulatory category the vendor assigns to each (for example medical device, high-risk AI system, or neither), with the supporting documentation. Basis: the AI Act and the MDR, cited at Regulation level.

Sample clause: *The Contractor **should** provide, with its tender, a list of the AI components included in the solution, stating for each its purpose, whether it processes or generates data in an EEHRxF priority category, the regulatory category the Contractor assigns to it under the AI Act and the MDR, and the supporting evidence (for example a declaration of conformity or a summary of the technical documentation). The Contractor **should** notify the Contracting Authority before adding or materially changing an AI component during the term of the Contract.*

Where an AI component of the EHR system generates or processes data in an EEHRxF priority category, how the output is represented in the EEHRxF specification for that category, and how the vendor tests and validates that representation, need further work before a procurement requirement can be formulated. Until then, a procurer may ask the vendor to demonstrate how the output is represented in the EEHRxF specification for that category. This is not asked of separate tools that do not produce priority-category data.

Annex

This Annex collects the checklists and reference material that support the main chapters.

- **Sections 1–4** are the evaluation checklists for Interoperability, Cybersecurity, Data Quality and the User-Centered Approach;
- **Section 5** is the Procurers Readiness Checklist;
- **Section 6** is the Vendors Readiness Checklist;
- **Section 7** lists the reference standards, regulations and tools.

Section numbers cited in the Annex (for example “Section 3.3” or “Section 4”) refer to the main body of this guidance, unless written as “Annex, Section n”. The checklist items are recommended practice and evidence requests, not legal requirements in themselves: where a legal provision mandates a point it is cited, and a procurer may turn any item into a requirement in its own tender (see Section 1.2). The checklists point back to the chapter each item comes from and do not repeat its tender clauses.

1. Procurement Checklists for Interoperability

The four checklists below consolidate the “require evidence of” items from the worked examples in Section 3.3 (Patient Summary, Electronic Prescription, Electronic Dispensation, Medical Test Results and Discharge Report), in one place, in a format usable directly during vendor evaluation. For each item, mark whether the evidence provided is Present, Partially Present, or Absent, rather than treating vendor evidence as a simple yes/no.

Medical Imaging Study and related Imaging Report is covered at reference depth in Section 3.3.5 and has no checklist in this version. The items are recommended evidence requests, not legal requirements in themselves; where a provision of the EHDS Regulation mandates a point, it is cited. Items that ask about readiness signals (experience of MyHealth@EU-based exchange, xShare participation) are optional indicators, and their absence should not by itself disqualify a vendor (Section 3.2.5). Where an item refers to the Xt-EHR logical models, these are the reference models available today; the regulatory definition of the logical models will be set by the implementing act under Article 15 of the EHDS Regulation (Section 3.1.2).

1.1 Patient Summary (EHR / GP System)

Requirement	Present	Partial	Absent
HL7 FHIR-based interfaces with a published CapabilityStatement, stated HL7 FHIR version(s) and a demonstration of a Patient Summary export conforming to the HL7 FHIR IPS Implementation Guide			
Patient Summary elements required by the applicable specification, to the extent the system holds them, available as discrete, coded data, not only as narrative or PDF, with narrative and structured content coexisting			
Awareness of and roadmap toward the forthcoming HL7 Europe Patient Summary (EPS) specification (publication expected by the end of 2026), not only the international IPS			
Documented mapping of the system’s data model to the logical information model for the Patient Summary (currently the Xt-EHR model; the regulatory model will be set by the Article 15 implementing act)			
Support for the Value Sets speciifed for the Patient Summary based on SNOMED CT, ATC, LOINC and other code systems as applicable, with documented mapping of local codes to the reference terminologies			
The system processes data originating from MyHealth@EU Patient Summary exchange, or data generated by it is used in such exchange (which runs			

through the Member State's national contact point), in at least one Member State (a readiness signal, not a pass/fail criterion)			
Full patient-summary-history portability, including API access, with no vendor lock-in (no feature that prohibits, restricts or places an undue burden on authorised export; EHDS Annex II)			
Readiness Label/Signal present or participation (e.g. xShare Label or other)			
Any health-app quality label held (for example Label2Scale or other)			
Contractual commitment keeps the system compliant with the EHDS Implementing Acts and common specifications as adopted, with defined scope, conditions and pricing method for this category			

1.2 Electronic Prescription / Electronic Dispensation (Pharmacy or e-Prescribing System)

Requirement	Present	Partial	Absent
HL7 FHIR-based interfaces with a working MPD implementation, stating the supported HL7 FHIR version(s) (R4 and/or R5)			
Structured, linked prescription-to-dispense data, including partial and declined dispenses			
Medicinal products identified with the designated product coding (SNOMED GPS, EMA PMS identifier or national coding system; ATC as a non-binding classification), with documented local-registry mapping			
UCUM-coded dosage units			
Structured dosage instructions alongside free-text instructions			
Experience of MyHealth@EU-based exchange for this category in at least one Member State, with the MPD implementation tested against the MyHealth@EU cross-border profiles (a readiness signal, not a pass/fail criterion)			
Full prescription/dispense-history portability, including API access, with no vendor lock-in (no feature that prohibits, restricts or places an undue burden on authorised export; EHDS Annex II)			

Readiness Label/Signal present or participation (e.g. xShare Label or other), specifically for this category			
Any health-app quality label held (for example Label2Scale or other), specifically for this category			
Contractual commitment to keep the system compliant with the EHDS Implementing Acts and common specifications as adopted, with defined scope, conditions and pricing method for this category			

1.3 Medical Test Results, including Laboratory Report and Other Diagnostic Results and Related Reports (LIS)

Requirement	Present	Partial	Absent
HL7 FHIR-based interfaces with a published CapabilityStatement, stated HL7FHIR version(s) with a migration path, a HL7 FHIR REST API			
Structured export of every result element, independent of the PDF report			
Narrative and structured content coexist: the laboratory's interpretive commentary is available as structured data, not only as free text or an attachment			
Demonstrated mapping to the logical information model for Medical Test Results (currently the Xt-EHR Laboratory Report model)			
HL7 Europe Laboratory Report FHIR IG support			
LOINC- or NPU-coded results, with a documented local-code mapping process			
SNOMED CT for qualitative/microbiology findings; UCUM for units			
MyHealth@EU readiness: pilot participation, export aligned with the MyHealth@EU Laboratory Report specifications, or testing in a National Contact Point for eHealth (NCPeH) environment (a readiness signal, not a pass/fail criterion)			
Readiness Label/Signal present or participation (e.g. xShare Label or other) (where available)			
Any health-app quality label held (for example Label2Scale or other)			

Contractual commitment to keep the system compliant with the EHDS Implementing Acts and common specifications as adopted, with defined scope, conditions and pricing method for this category			

1.4 Hospital Discharge Report (EHR)

Requirement	Present	Partial	Absent
HL7 FHIR-based interfaces: stated HL7 FHIR version(s) with a migration path, a HL7 FHIR REST API			
Mapping to the logical information model for the Discharge Report (currently the Xt-EHR model)			
HL7 Europe Hospital Discharge Report (HDR) Implementation Guide support			
MyHealth@EU readiness: pilot participation, export aligned with the MyHealth@EU Hospital Discharge Report specifications, or testing in a National Contact Point for eHealth (NCPeH) environment (a readiness signal, not a pass/fail criterion)			
SNOMED CT, ICD-10, LOINC, ATC and UCUM support, with documented mapping of local codes			
Narrative, structured sections and optional attachments are produced together, with no key diagnoses or medications held only in a PDF or in free text			
Structured medications, diagnoses, procedures, and devices' usage			
Structured care plans and discharge recommendations			
Patient data portability with no vendor lock-in (no feature that prohibits, restricts or places an undue burden on authorised export; EHDS Annex II)			
Readiness Label/Signal present or participation (e.g. xShare Label or other)			
Any health-app quality label held (for example Label2Scale or other)			
Contractual commitment to keep the system compliant with the EHDS Implementing Acts and common specifications as adopted, with defined			

scope, conditions and pricing method for this category			

2. Procurement Checklists for Cybersecurity

Use the checklists below to evaluate vendor proposals and contracts, phase by phase. For each item, mark whether it is Present, Partially Present, or Absent, rather than treating evidence as a simple yes/no. The items are recommended practice; a procurer may turn any of them into a requirement in its own tender.

2.1 Planning Phase

Requirement	Present	Partial	Absent
Applicable cybersecurity frameworks identified (GDPR, NIS2, EHDS Annex II, MDR/IVDR, CRA, and AI Act Article 15 where the system is AI-enabled)			
EEHRxF data domains (the priority data categories and the data elements they contain) and security objectives (confidentiality, integrity, availability and traceability of that data) defined			
Required standards for encryption, authentication, audit logging specified (logging and authentication of health professionals are required by EHDS Annex II; the standards named in the tender are recommended)			

2.2 Tender Preparation

Requirement	Present	Partial	Absent
Security-by-design clause included			
ISO 27001/27799[130] or equivalent considered as a tender requirement (recommended, not mandated by law)			
Encryption and authentication standards defined			
Audit logging requirements specified			
Documented risk assessment required (ISO/IEC 27005 or equivalent), covering confidentiality, integrity, availability and patient-safety impacts			
Business continuity and disaster recovery plan required, with RTO/RPO [specify] and a test frequency [specify, e.g. at least annually]			

[130] ISO/IEC 27001, Information security management systems – Requirements; ISO 27799:2025, Health informatics – Information security controls in health based on ISO/IEC 27002, https://www.iso.org/standard/84647.html.

Secure-by-default configuration (no default credentials, least privilege) and controlled, time-bounded, logged remote maintenance access required			

2.3 Evaluation Phase

Requirement	Present	Partial	Absent
Supplier ISO 27001 certification validity verified (within scope for this system)			
Evidence of secure development lifecycle (SDLC) policy reviewed			
Incident response plan reviewed for alignment with NIS2 timelines (early warning within 24 hours, notification within 72 hours, final report within one month; NIS2 Article 23(4))			
References from existing customers provided and checked for security track record			

2.4 Contracting Phase

Requirement	Present	Partial	Absent
Severity-tiered patch deployment timelines defined (CVSS-based cascading SLA), for example [48 hours] for critical and [72 hours] for high-severity vulnerabilities (illustrative figures; neither NIS2 nor ENISA sets a patch deadline)			
Incident reporting aligned with NIS2 (early warning within 24 hours, notification within 72 hours, final report within one month; Article 23(4))			
Public Vulnerability Disclosure Policy (VDP) and Software Bill of Materials (SBOM) required with every release			
Continuous oversight via periodically reported Key Risk Indicators (KRIs), with a Corrective Action Plan (CAP) and specific deadlines (recommended)			
Subcontractor flow-down of cybersecurity requirements, with disclosure of key third-party dependencies and, where the Contracting Authority so decides, exclusion of designated High-Risk Vendors (HRVs)			

Secure Switching and Exit Plan for securing data and systems at contract end			
Safeguards against international and third-country governmental access to non-personal electronic health data held in the Union (Data Act Article 32), including who holds the encryption keys and in which jurisdiction, and a duty to inform the Contracting Authority of third-country access requests			
Access control and logging aligned with EHDS Annex II: authentication of health professionals, logging of every access to personal electronic health data, retention periods and access rights			

2.5 Implementation Phase

Requirement	Present	Partial	Absent
Security testing completed and documented before system deployment			
Hardened configuration validated at acceptance testing (no default credentials, least privilege, remote-access controls) and the business continuity and disaster recovery plan tested			
Conformance validation confirms alignment with standards			
Security logs configured and operational			
Incident response procedures tested			

2.6 Operation Phase

Requirement	Present	Partial	Absent
Incident management monitored and logged			
Security updates (patches) tracked and applied timely			
Regular (for example annual) security assessments completed			
Vendor maintains ISO 27001 or equivalent certification			
Supply chain security reviewed for third-party risks			

3. Procurement Checklists for Data Quality by Design

Use the following checklists to evaluate vendor proposals and contracts, phase by phase. For each item, mark whether it is Present, Partially Present, or Absent, rather than treating evidence as a simple yes/no. The items are recommended practice for data quality at the point of care (primary use).

3.1 Planning Phase

Requirement	Present	Partial	Absent
Data quality objectives defined, aligned with intended use			
Stakeholders responsible for data quality identified (clinical staff, data governance, IT, quality management)			
Data quality governance established: ownership, responsibilities, and escalation path defined			

3.2 Tender Preparation

Requirement	Present	Partial	Absent
Required data elements and their definitions specified			
Data quality dimensions that matter most for the intended purpose stated in the tender (from the eight: reliability, relevance, timeliness, coherence, coverage, completeness, accuracy, conformance)			
Acceptable completeness levels specified for defined fields			
Maximum acceptable timeliness lag specified			
Conformance to data standards specified (the EHDS technical specifications for the priority categories and the standard vocabularies they prescribe, as applicable)			
Vendor required to document data quality assurance processes (validation rules, quality checks, error handling)			
Vendor required to provide a current data quality metrics baseline			
Data-quality-by-design features required, with provenance tracking (who entered data, when, from what source) and version-controlled corrections as the highest priorities, followed by real-time validation			

at entry and structured, coded entry (ISO 13606 can serve as a good-practice cross-check for provenance and versioning)			

3.3 Evaluation Phase

Requirement	Present	Partial	Absent
Evidence of vendor's data quality framework requested and reviewed			
References from existing customers checked specifically for data quality experience			
Data quality assurance mechanisms and reporting evaluated			
Quality metrics and SLAs defined and included in the proposal			

3.4 Contracting Phase

Requirement	Present	Partial	Absent
Data quality metrics and acceptable ranges specified in the contract			
Data quality reporting requirements included [specify frequency, e.g. monthly or quarterly]			
Remediation procedures defined for when metrics are not met			
Warranty period specified: vendor warrants data quality meets specified standards for [specify] months post-implementation			

3.5 Implementation Phase

Requirement	Present	Partial	Absent
Baseline data quality assessment conducted before go-live			
Migrated/imported data quality compared against acceptable thresholds			
Data quality gaps and remediation plans documented			
Mapping specifications documented and monitored, with visibility of unmappable data and the percentage of records successfully harmonised			

3.6 Operation Phase

Requirement	Present	Partial	Absent
Automated data quality checks and monitoring dashboards implemented			
Regular data quality reports generated, tracking adherence to SLAs			
Quarterly review of data quality metrics with the Contracting Authority, identifying trends, root causes of degradation and improvement actions			
Quality-degradation escalation process in place, with vendor response time [specify]			
Periodic data quality audits conducted [specify frequency, e.g. at least annually] with independent review			

4. Procurement Checklists for User-Centered Approach

User-centered procurement shifts focus from: "What can the technology do?" to: "How will real users work with this technology, and what support do they need?". Use the table below to evaluate vendor proposals and contracts, step by step. For each item, mark whether it is Present, Partially Present, or Absent, rather than treating evidence as a simple yes/no. The items are recommended practice; a procurer may turn any of them into a requirement in its own tender.

4.1 Step 1: Understand User Needs and Workflows (Pre-Procurement)

Requirement	Present	Partial	Absent
End-users engaged early: interviews/focus groups held with clinicians, patients, administrative and IT staff, and underrepresented groups, before tender specifications are written			
Current workflows mapped: how clinicians currently capture, access, and share health information			
Pain points identified: what is difficult about current processes, what errors occur, what time is wasted			
Success defined in user terms, not only technical terms (e.g., “clinician can access relevant Patient Summary within <5 seconds”, not only “system delivers data in FHIR format”)			

4.2 Step 2: Translate User Needs into Procurement Requirements

Requirement	Present	Partial	Absent
Usability requirements defined measurably: learnability, efficiency, error tolerance, satisfaction targets			
User-centered design practices required of the vendor: user research, clinical advisor involvement, usability testing, iterative design			
Inclusive design planned for: EN 301 549 compliance (version stated in the tender), multi-language and terminology support, training accessible to varying digital literacy			
Human-rights-aligned design addressed: transparent privacy information and user control over personal data (GDPR Articles 12–18, 21 and 25) and, for high-risk AI components, bias assessment (AI Act Article 10), and accessibility as a practical minimum of non-discrimination (WCAG)			

4.3 Step 3: Evaluate Vendor Proposals for User-Centeredness

Requirement	Present	Partial	Absent
Usability evidence required: reference-site interviews, usability testing results, UI mockups/prototypes reviewed with sample clinical staff (a vendor's self-declaration alone should not be accepted; the depth of evidence is scaled to the size and complexity of the procurement)			
Training and support plans assessed: training approach, ongoing support channels, process for identifying and addressing usability issues			
Pilot and feedback mechanisms included: pre-deployment pilot option, in-implementation feedback channel, contractual provision to address critical post-implementation usability issues, with a response time [specify]			

4.4 Step 4: Support Implementation and Adoption

Requirement	Present	Partial	Absent
Training tailored to different user roles and skill levels, with accessible materials (written, video, in-person), including a train-the-trainer programme			
Workflow disruption minimised: implementation timeline coordinated with clinical schedules			
Feedback loops created: regular surveys, focus groups, or office hours during the first months post-implementation			
Equity addressed: user groups struggling with adoption identified and given targeted support			

4.5 Step 5: Monitor Adoption and Iterate

Requirement	Present	Partial	Absent
Adoption metrics tracked: % active users, frequency of use, feature utilisation, error rates and support ticket patterns			
Regular user satisfaction assessments conducted (e.g., at 3, 6, and 12 months)			

Continuous improvement process in place with the vendor to address usability barriers as use patterns emerge			

5. Procurers Readiness Checklist

Use this checklist to confirm that your organisation is ready before, and while, it procures systems, services or components supporting EEHRxF adoption. It covers organisational readiness, requirements definition and procurement strategy, followed by a step-by-step Procurement Process Map and the most common pitfalls. It does not repeat the tender clauses in Sections 3–6 or the evaluation checklists in Annex, Sections 1–4: it points to them at the step where they are needed.

5.1 Procurement Readiness Self-Assessment

Before launching a procurement, use the following checklist to help verify that your are ready. For each item, mark whether it is Present, Partially Present, or Absent, rather than treating readiness as a simple yes/no.

5.1.1 Organisational Readiness

Requirement	Present	Partial	Absent
Clinical leadership (physicians, nurses, quality directors) engaged and supportive			
Internal technical capacity assessed honestly: does the organisation have staff who can evaluate cybersecurity, data quality, and usability claims without external help?			
Budget secured for the full lifecycle, not only the initial purchase: implementation, training, and ongoing compliance monitoring			

5.1.2 Requirements Definition

Requirement	Present	Partial	Absent
Current state documented: existing systems, data flows, pain points			
Compulsory regulatory baseline identified for this specific use case (Section 2.3) — bound to the actual solution being procured, not copied wholesale from a previous tender			
End-users (clinicians, administrative staff, patients as relevant) consulted on needs before requirements are drafted, not only at evaluation stage			

5.1.3 Procurement Strategy

Requirement	Present	Partial	Absent
Procurement instrument selected (open procedure, competitive dialogue, etc.)			

E-procurement tool identified for the online stages of the procedure			
Procedure choice matched to internal technical expertise (Section 7.2.1, “How and When to Launch a Competitive Dialogue”): Open Procedure only where strong in-house expertise exists, Competitive Dialogue or Innovation Partnership otherwise, with the applicable Article 26(4) ground documented where a Competitive Dialogue is used			
Evaluation panel confirmed and technically resourced before the tender is published, not assembled after bids arrive			

5.2 Procurement Process Map with EEHRxF Considerations

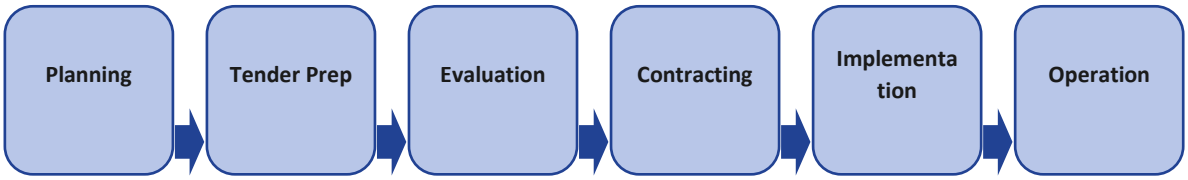


Figure 5: Phases of the procurement process, from planning to operation

Planning Phase

- Complete the Procurement Readiness Self-Assessment above
- Identify which of the four core dimensions (Sections 3–6: Interoperability, Cybersecurity, Data Quality, Usability) are in scope for this specific solution
- Select the procurement procedure (Section 7)
- Plan to run the online stages of the procedure on an established e-procurement tool (Section 7.6); market-mapping tools may be consulted but are not recommended

Tender Preparation

- Draft technical specifications using the ready-to-use tender clauses in Sections 3–6, adapted to this use case, together with the evaluation checklists in Annex, Sections 1–4 to define the evidence requested
- Confirm compulsory regulatory elements (Section 2.3) and any applicable additional elements (Section 2.4)
- Draft evaluation criteria and weighting, including the verification standards set out in set out in Sections 3–6 (e.g., live demonstration or documented evidence for usability, per Section 6)

Evaluation Phase

- Score bids against the pre-published criteria; request supporting evidence (test reports, certifications, live demonstrations) rather than accepting self-declaration alone
- Where used, run Competitive Dialogue or Innovation Partnership stages per Section 7

Contracting Phase

- Embed the ready-to-use tender clauses directly into the contract, not only the tender documentation
- Confirm continuous oversight and reporting mechanisms are contractually binding (Key Risk Indicators, Corrective Action Plan, data-quality SLAs, per Section 4 and Section 5)
- Confirm a Switching and Exit Plan is in place before signature, not negotiated after go-live (Section 2.3.5; Section 3.2.4, Section 3.4.9)

Implementation Phase

- Conduct conformance and security testing before go-live (Section 3.4.7 and 3.4.8)
- Establish the data-quality baseline (Section 5) and confirm user training is delivered per the vendor's committed plan (Section 6)

Operation Phase

- Monitor the agreed KRIs, data-quality SLAs, and usability feedback mechanisms on the reporting cadence set in the contract, rather than only at renewal
- Track vendor responsiveness against the committed patch-deployment and incident-response timelines (Section 4)

5.3 Common Pitfalls and How to Avoid Them

Pitfall	Why It Happens	How to Avoid
Specifications too vague: Tender describes "interoperability" without defining what that means	Procurement staff may not have technical expertise; tendency to be concise	Invest time defining requirements clearly; engage IT technical experts; provide examples (e.g., "the system should exchange Patient Summaries conforming to the EHDS technical specification for the Patient Summary (currently expected to build on the HL7 FHIR International Patient Summary), version [specify]")
Vendor self-declaration accepted as sufficient proof of compliance	Easiest evidence for the vendor to supply, and procurement staff may not know what stronger evidence to ask for	Require live demonstration, documented prior test results, or independent certification; reserve self-declaration for low-risk, non-compulsory items only
Compulsory elements copied wholesale from a	Reusing a previous tender is faster, but a	Bind compulsory elements to this use case specifically (Section 2.3); do not include secondary-

previous, unrelated tender	District Hospital's requirements differ from a University Hospital's	use or research-specific clauses unless the use case requires them
Procurement procedure chosen before internal technical capacity is assessed	Open Procedure looks fastest on paper, so it is often the default choice regardless of internal expertise	Assess internal technical capacity first (Procurement Readiness Self-Assessment above); use Competitive Dialogue or Innovation Partnership where in-house expertise is limited (Section 7)
Contract signed without a Switching and Exit Plan	Exit terms feel like a low priority during contract negotiation, when the relationship is new and positive	Require a documented Switching and Exit Plan, with a defined transition period and switching charges disclosed before signature; for for data processing services (IaaS, PaaS, SaaS) the Data Act caps the notice period at two months and the transitional period at 30 calendar days (up to seven months only where this is technically unfeasible and justified) and bars switching charges from 12 January 2027[131] (Sections 2.3.5, 3.2.4 and 3.4.9)
Requirements set as “shall” without a legal basis, or out of proportion to the contract	A strict requirement feels safer, and the difference between what the law mandates and what is good practice is not always visible	Use “shall” only where a cited provision mandates the point; keep the rest as “should” or as scored criteria; scale the evidence asked for to the size and complexity of the contract so that capable SMEs are not excluded (Section 1.2; Section 6.4.1)

[131] https://eur-lex.europa.eu/eli/reg/2023/2854/oj/eng (Data Act, Regulation (EU) 2023/2854, Article 25(2) and (4): contracts for data processing services (cloud services in any delivery model) provide for a maximum notice period of two months for initiating switching and a mandatory maximum transitional period of 30 calendar days, which the provider may extend, with justification, to no more than seven months where it is technically unfeasible; Article 29: from 12 January 2027 providers shall not impose any switching charges, reduced charges being allowed until then)

6. Vendors Readiness Checklist

Use this checklist to prepare for procurement opportunities as a software or service vendor developing and commercialising EEHRxF-compatible solutions. It covers vendor readiness, a capability assessment template that mirrors the questions procurers typically ask, and guidance on the evidence they increasingly request. It is a self-assessment tool, not a certification, and it does not repeat the tender clauses in Sections 3–6: it points to them where relevant.

6.1 Vendor Readiness Self-Assessment

Before responding to procurement opportunities, use the following checklist. For each item, mark whether it is Present, Partially Present, or Absent, rather than treating readiness as a simple yes/no. Keep the supporting evidence ready, because procurers may ask for it.

6.1.1 Product Development

Requirement	Present	Partial	Absent
System implements core EEHRxF technical specifications for the priority categories it supports (until they are final, the reference specifications named in Section 3.1.2, such as HL7 FHIR IPS and the HL7 Europe Implementation Guides, standard vocabularies and IHE profiles)			
EHDS conformity infrastructure in place: European interoperability and logging software components, ideally tested in the EU digital testing environment as part of self-assessment or, when applicable, due to Member State requirements, CE-marked, and registered in the EU database (see Sections 3.4.7 and 3.4.8)			
Cybersecurity baseline documented: VDP, SBOM process, and patch-deployment SLAs capable of meeting the severity-tiered timelines set in the tender (the xShare example in Section 4 is [48 hours] for critical and [72 hours] for high-severity vulnerabilities)			

6.1.2 Service and Support Capability

Requirement	Present	Partial	Absent
Helpdesk established: staff trained, documentation/knowledge base developed, response time SLAs defined			
Prior user-testing evidence, or a live-demonstration capability, ready to present — self-declaration alone should not be accepted for usability claims (Section 6)			

6.1.3 Commercial Readiness

Requirement	Present	Partial	Absent
Pricing strategy defined (development cost recovery, margin, pricing model)			
Switching and Exit Plan drafted in advance: export formats, methods, and a transition timeline, with switching charges disclosed in advance; for for data processing services (IaaS, PaaS, SaaS) the Data Act provides for a notice period of at most two months, a transitional period of at most 30 calendar days (up to seven months only where technically unfeasible and justified) and no switching charges from 12 January 2027[132] (Sections 2.3.5, 3.2.4 and 3.4.9)			
Subcontractor register maintained and key third-party dependencies disclosed (and, where the Contracting Authority designates high-risk vendors, confirmed free of them)(Section 4)			

6.2 Vendor Capability Assessment Template

Procurers often request vendors to complete detailed questionnaires. This template captures key areas procurers typically evaluate; use it to prepare your answers in advance, and mark your own current state as Present, Partially Present, or Absent for each item. Procurers can use the same areas as a basis for their own supplier questionnaires, together with the evaluation checklists in Annex, Sections 1–4.

6.2.1 Company Overview

Area	Present	Partial	Absent
Company history and stability			
Years in healthcare IT market			
Financial stability (turnover, credit standing, ownership structure)			
Existing footprint in the EHDS/EEHRxF ecosystem: named reference deployments, if any			

[132] https://eur-lex.europa.eu/eli/reg/2023/2854/oj/eng (Data Act, Regulation (EU) 2023/2854, Article 25(2) and (4): contracts for data processing services (cloud services in any delivery model) provide for a maximum notice period of two months for initiating switching and a mandatory maximum transitional period of 30 calendar days, which the provider may extend, with justification, to no more than seven months where it is technically unfeasible; Article 29: from 12 January 2027 providers shall not impose any switching charges, reduced charges being allowed until then)

6.2.2 Product Capability

Area	Present	Partial	Absent
EEHRxF conformance evidence (Section 3.4.7 and 3.4.8): conformance test reports, EHDS conformity infrastructure status, EU database registration			
Priority categories supported (Patient Summary, Electronic Prescription/Electronic Dispensation, Medical Test Results, Medical Imaging Study and related Imaging Report, Discharge Report) and the specification versions implemented, with the category-level evidence listed in Annex, Section 1			
Cybersecurity posture (Section 4): certifications held, VDP/SBOM practices, patch-deployment track record, logging and authentication of health professionals per EHDS Annex II)			
Data-quality framework (Section 5): which of the eight dimensions are covered, provenance and version-control capability, monitoring and reporting capability			
Usability evidence (Section 6): prior user-testing results or live-demonstration capability, and accessibility evidence (EN 301 549, version stated)			

6.2.3 Implementation and Support

Area	Present	Partial	Absent
Implementation methodology and typical timeline, with named milestones			
Training approach and materials (see “User-Centered Design and Training” below)			
Support-tier structure and response-time commitments			
Switching and Exit Plan available on request, not only on contract signature			

6.2.4 References and Case Studies

Area	Present	Partial	Absent
Customer references (names, contacts, implementations similar to prospect)			

6.3 Vendor Guidance on Key Topics

6.3.1 Demonstrating EEHRxF Compliance

Challenge: Procurers need objective evidence that your system complies with EEHRxF standards, not just vendor claims.

Solution: Conduct and document conformance testing using recognized validation platforms:

- Complete the testing required by the EHDS Regulation (Article 40) and, as additional proof points, run conformance tests with open or national tools such as the IHE Gazelle testing platform and Inferno[133] — procurers may ask for them directly rather than accepting a compliance statement alone
- Complete testing in the EU's dedicated digital testing environment (EHDS Article 40; Sections 3.4.7 and 3.4.8), or that of the Member State where it applies, and be ready to show EU database registration status before a procurer asks
- Where you cite named vocabularies (SNOMED CT, LOINC etc), be explicit that this is illustrative, not a claim of exclusivity — procurers increasingly check for lock-in language
- Be ready to describe any experience of MyHealth@EU-based exchange and any xShare Label, Label2Scale (or similar) participation, but present them as readiness signals: procurers should not treat them as pass/fail criteria (Section 3.2.5)

6.3.2 Data Quality Framework and Monitoring

Challenge: Procurers expect vendors to articulate how data quality is assured and monitored.

Solution: Develop and document a comprehensive data quality framework:

- Be ready to speak to all eight data quality dimensions in Section 5 , not only the ones your product currently measures well
- Lead with provenance and version-control infrastructure: co-creation evidence rated this ahead of other design-level data-quality measures, so procurers are likely to ask about it directly
- If your product supports the Contracting Authority's own Health Data Holder obligations (timely export, pseudonymisation/anonymisation), say so explicitly — this is an optional readiness point on secondary use, not part of the primary-use criteria (see Section 5.4.3)

6.3.3 User-Centered Design and Training

Challenge: Procurers increasingly recognise that technology adoption depends on usability and user support; they expect evidence of user-centred design.

Solution: Document and demonstrate user-centred design practices

[133] https://www.ihe-europe.net/testing-IHE/gazelle (IHE-Europe, Gazelle testing platform: Gazelle Test Management coordinates conformity and interoperability tests for IHE profiles, for example at Connectathons and Projectathons); https://inferno-framework.github.io/ (Inferno Framework, open-source tooling for conformance tests of FHIR APIs); accessed October 2026

- Bring evidence, not assurances: documented prior user-testing results or a live-demonstration offer. Co-creation evidence shows self-declaration is trusted by almost no one on the procurer side
- Show how end-users were involved as early as the needs-assessment stage, not only during a pre-award demo — this is now the stage procurers weight most heavily and, where applicable, at the pilot stage
- Document accessibility compliance (EN 301 549, with the version stated in the tender, and WCAG 2.1 Level AA or later) with test evidence, not a checklist claim

6.3.4 Cybersecurity and Compliance

Challenge: Healthcare procurements increasingly include strict cybersecurity requirements; vendors must demonstrate compliance.

Solution: Invest in security infrastructure and communicate proactively:

- Publish a Vulnerability Disclosure Policy and provide a Software Bill of Materials with every release — both are now baseline expectations, not differentiators (for manufacturers of products with digital elements, a coordinated vulnerability disclosure policy and an SBOM are also required by the Cyber Resilience Act, Annex I, Part II, where it applies)
- Be able to commit to the severity-tiered patch-deployment timelines the tender sets (for example [48 hours] for critical and [72 hours] for high-severity vulnerabilities), and explain your process for meeting them, rather than a general “timely patching” assurance
- Prepare to report against Key Risk Indicators on an ongoing basis: procurers are moving from one-off audits to continuous oversight, and vendors who can already report this way will stand out; this is recommended practice rather than a legal requirement
- Maintain a current subcontractor register and be able to disclose your key third-party dependencies and, where the Contracting Authority designates high-risk vendors, to confirm their absence from your supply chain
- If your product contains AI components, be ready to list them, say what they do, which regulatory category you assign to each (AI Act, MDR) and what evidence supports it; the guidance asks procurers to find this out first, not to verify AI Act compliance themselves

7. Reference Standards, Regulations and Tools

This section provides a curated reference list of the key standards, regulations, and tools cited throughout this guidance, grouped by domain.

7.1 Interoperability Standards and Specifications

- HL7 FHIR (Fast Healthcare Interoperability Resources) — hl7.org/fhir
- International Patient Summary (IPS) Implementation Guide — hl7.org/fhir/uv/ips
- IHE Profiles (XDS, sIPS, ATNA) — ihe.net
- EURIDICE EU Health Data API — https://euridice.org/eu-health-data-api/
- Xt-EHR logical information models — https://www.xt-ehr.eu/fhir/models/en/
- OMOP Common Data Model — ohdsi.org
- SNOMED CT, LOINC (illustrative, non-exhaustive vocabulary examples — see Section 2.2)

7.2 Regulatory Framework

- Regulation (EU) 2025/327 (European Health Data Space Regulation)
- Regulation (EU) 2016/679 (GDPR)
- Directive (EU) 2022/2555 (NIS2 Directive)
- Regulation (EU) 2017/745 (MDR) and Regulation (EU) 2017/746 (IVDR)
- Regulation (EU) 2023/2854 (Data Act)
- Regulation (EU) 2024/2847 (Cyber Resilience Act)
- Regulation (EU) 2024/1689 (AI Act)
- Directive 2014/24/EU (Public Procurement Directive)

7.3 Information Security Standards

- ISO/IEC 27001 (Information Security Management)
- ISO 27799 (Health informatics — Information security management in health)
- ISO/IEC 27005 (Information security risk management)
- ENISA good practices for the security of healthcare services
- ENISA procurement guidelines for the cybersecurity of hospitals and healthcare providers

7.4 Data Quality Frameworks

- TEHDAS (Towards European Health Data Space) Joint Action — data quality framework, referenced throughout Section 5
- EHDS implementing acts on data quality (Article 13), pending adoption
- ISO/IEC 25012 (data quality model)
- ISO 13606 (Health informatics — Electronic health record communication)

7.5 Testing and Validation Tools

- IHE Gazelle Conformity Assessment Framework (IPS/FHIR validation)
- Inferno FHIR testing suite
- IHE testing infrastructure (XDS document exchange)
- EU digital testing environment established under Article 40 of the EHDS Regulation

7.6 Accessibility and Usability Standards

- EN 301 549 (European accessibility standard)
- WCAG 2.1 AA (Web Content Accessibility Guidelines)
- ISO 9241-11 (usability)
- ISO 9241-210 (human-centred design of interactive systems)

7.7 User Experience and Adoption Research

- Unified Theory of Acceptance and Use of Technology (UTAUT)
- Companion scientific paper: “Co-Designing Market Readiness: Utilising Innovative Procurement and Stakeholder Co-Creation to Operationalise the European Health Data Space” (see xShare D7.4 for the methodology)