



Co-funded by the Horizon 2020  
Framework Programme of the European Union



**TeNDER**

## **D5.3 – First Report on the Health Record and Pathway Repository**

Work Package 5: Services Integration and Technical Validation

**affective basEd iNtegrated carE for better Quality of Life: TeNDER Project**

**Grant Agreement ID: 875325**

**Start date:** 1 November 2019

**End date:** 31 October 2022

**Funded under programme(s):** H2020-SC1-DTH-2018-2020/H2020-SC1-DTH-2019

**Topic:** SC1-DTH-11-2019 Large Scale pilots of personalised & outcome based integrated care

**Funding Scheme:** IA - Innovation action

## Disclaimer

This document contains material, which is the copyright of certain TeNDER Partners, and may not be reproduced or copied without permission. The commercial use of any information contained in this document may require a license from the proprietor of that information. The reproduction of this document or of parts of it requires an agreement with the proprietor of that information. The document must be referenced if used in a publication.

The TeNDER consortium consists of the following Partners.

*Table 1 – Consortium Partners List*

No	Name	Short name	Country
1	UNIVERSIDAD POLITECNICA DE MADRID	UPM	Spain
2	MAGGIOLI SPA	MAG	Italy
3	DATAWIZARD SRL	DW	Italy
4	UBIWHERE LDA	UBIWHERE	Portugal
5	ELGOLINE DOO	ELGOLINE	Slovenia
6	ETHNIKO KENTRO EREVNAS KAI TECHNOLOGIKIS ANAPTYXIS	CERTH	Greece
7	VRIJE UNIVERSITEIT BRUSSEL	VUB	Belgium
8	FEDERATION EUROPEENNE DES HOPITAUX ET DES SOINS DE SANTE	HOPE	Belgium
9	SERVICIO MADRILENO DE SALUD	SERMAS	Spain
10	SCHON KLINIK BAD AIBLING SE & CO KG	SKBA	Germany
11	UNIVERSITA DEGLI STUDI DI ROMA TOR VERGATA	UNITOV	Italy
12	SLOVENSKO ZDRUZENJE ZA POMOC PRI DEMENCI - SPOMINCICA ALZHEIMER SLOVENIJA	SPO	Slovenia
13	ASOCIACION PARKINSON MADRID	APM	Spain

## Document Information

<b>Project short name and Grant Agreement ID</b>	TeNDER (875325)
<b>Work package</b>	WP.5
<b>Deliverable number</b>	D5.3
<b>Deliverable title</b>	First Report on the Health Record and Pathway repository
<b>Responsible beneficiary</b>	UBI
<b>Involved beneficiaries</b>	VUB
<b>Type<sup>1</sup></b>	Report
<b>Dissemination level<sup>2</sup></b>	PU
<b>Contractual date of delivery</b>	30 September 2020
<b>Last update</b>	30 September 2020

---

<sup>1</sup> **R**: Document, report; **DEM**: Demonstrator, pilot, prototype; **DEC**: Websites, patent fillings, videos, etc.; **OTHER**; **ETHICS**: Ethics requirement; **ORDP**: Open Research Data Pilot.

<sup>2</sup> **PU**: Public; **CO**: Confidential, only for members of the consortium (including the Commission Services).

## Document History

Version	Date	Status	Authors, Reviewers	Description
v 0.00	03/12/2019	Template	Paride Criscio (DW)	Project deliverable template
v 0.01	24/04/2020	Draft	Lisa Feirabend (VUB) Paul Quinn (VUB)	Section on EHR guidelines
v 0.02	10/08/2020	Draft	Rui Alheiro, Francisco Cardoso (UBI)	Implementation section first version
v 0.03	07/09/2020	Draft	Francisco Cardoso, Bruno Silva (UBI)	Data models and authorisation sections
v 0.04	18/09/2020	Draft	Annelore Hermann (UPM)	General review
v 0.05	18/09/2020	Draft	Ricardo Vitorino	Conclusion and final review
V 0.06	23/09/2020	Draft	Panagiotis Karkazis (MAG), Paschalis Bizopoulos (CERTH)	Peer review
V 0.07	28/09/2020	Draft	Ricardo Vitorino (UBI)	Final corrections, Executive Summary
V0.07	30/09/2020	Final	Gustavo Hernández (UPM)	Final review

## Acronyms and Abbreviations

Acronym/Abbreviation	Description
API	Application Programming Interface
AuthN	Authentication
AuthZ	Authorisation
CBeHIS	Cross Border eHealth Information Services
CEF	Connecting Europe Facility
CRUD	Create, Read, Update and Delete
CSIRT	Computer Security Incident Response Team
DAO	Data Access Object
DSM	Digital Single Market
EC	European Commission
eHDSI	eHealth Digital Services Infrastructure
EHR	Electronic Health Record
eID	electronic IDentification
eIDAS	electronic IDentification, Authentication, and trust Services
EIF	European Interoperability Framework
eEIF	eHealth EIF
EIS	European Interoperability Strategy
ENISA	European Union Agency for Cybersecurity
EU	European Union
FHIR	Fast Healthcare Interoperability Resources
GDPR	General Data Protection Regulation
HAPI	HL7 Application Programming Interface
HL7	Health Level 7
HLS	High-Level Services
HTTP	Hypertext Transfer Protocol
ICT	Information and Computer Technology
IHE	Integrating the Healthcare Enterprise
JPA	Java Persistence API
JSON	JavaScript Object Notation
MVC	Model-View-Controller

Mx	Month (where x defines a project month e.g. M8)
NCP	National Contact Point
NIF	National Interoperability Framework
ReEIF	Refined eHealth European Interoperability Framework
REST	Representational State Transfer
TeNDER	affecTive basEd iNtegrateD carE for betteR Quality of Life
TFEU	Treaty on the Functioning of the European Union
Tx.x	Task
WG	Working Group
WPx	Work Package

## Contents

<b>Disclaimer</b> .....	<b>2</b>
<b>Document History</b> .....	<b>4</b>
<b>Acronyms and Abbreviations</b> .....	<b>5</b>
<b>Contents</b> .....	<b>7</b>
<b>List of Figures</b> .....	<b>8</b>
<b>List of Tables</b> .....	<b>8</b>
<b>Executive Summary</b> .....	<b>9</b>
<b>1. Introduction</b> .....	<b>10</b>
<b>1.1 European Guidelines on EHRs</b> .....	<b>10</b>
<b>1.2 EU Recommendation on European EHR exchange format</b> .....	<b>12</b>
<b>1.3 European Interoperability Framework and eHealth</b> .....	<b>21</b>
<b>1.4 Data Protection in Connection to EHR</b> .....	<b>25</b>
<b>2. Implementation</b> .....	<b>28</b>
<b>2.1 HAPI FHIR Server</b> .....	<b>29</b>
<b>2.2 HAPI Model Objects</b> .....	<b>31</b>
<b>2.3 Authorisation and data access</b> .....	<b>35</b>
<b>3. Conclusions</b> .....	<b>38</b>

## List of Figures

Figure 1 – ReEIF Model .....	22
Figure 2 – ReEIF Alignment Model.....	23
Figure 3 – EHR architecture regarding HAPI FHIR implementation .....	28
Figure 4 – HAPI FHIR running in Maggioli’s cloud .....	30
Figure 5 – Database organisation of resources.....	31
Figure 6 – JSON format of Practitioner resource in HAPI FHIR .....	32
Figure 7 – JSON format of a Patient resource in HAPI FHIR.....	33
Figure 8 – JSON format of a Device resource in HAPI FHIR.....	34
Figure 9 – Authorising READ Operations in HAPI FHIR .....	35

## List of Tables

Table 1 – Consortium Partners List .....	2
Table 2 – Principles of access to and cross-border exchange of electronic health data .....	14
Table 3 – Recommended interoperability specifications - Table A.....	18
Table 4 – Recommended interoperability specifications – Table B.....	19
Table 5 – ReEIF interoperability levels .....	22
Table 6 – HAPI FHIR Sample Operations .....	29



## **Executive Summary**

This deliverable presents the necessary conditions for TeNDER to adapt to the European regulation for data exchanging.

Under the scope of WP5 (whose purpose is to integrate the services and technically validate them), the present document aims at describing the structure consisting of the Electronic Health Records (EHR), i.e. the database that stores the medical profile extend information available from physical, medical and behavioural activity. It includes the security and interoperability aspects in addition to the authentication and operations required.

The report starts by analysing the European guidelines on EHRs and the recommendations on exchange formats. Concrete requirements and recommendations are presented, following the outcomes of the previous deliverables D1.1 and D1.2, to ensure that the information flow will securely access data from patients, from/to the system and from/to the health professionals.

Afterwards, it reports on the first results achieved with the concrete implementation of an open-source solution called HAPI FHIR, that complies with the recommendations and guidelines defined here, namely about the server deployment and features, its data model organisation, as well as its authorisation and data access tools.

Further developments are required to ensure that TeNDER complies with EU regulation on data access and security. The outcomes of the testing activities, and the compliance reports will be demonstrated both in D5.4 and D5.5, as well as reported in the integrated deliverables from WP6 with the rest of the results of the pilots performed during the project.

## 1. Introduction

The main goal of WP5 is the delivery of the TeNDER Pilot platform for pilot's execution. Task 5.1 (European Interoperable Health Record and Pathway Gathering) will implement the necessary conditions to ensure adherence to the European regulation for data processing on the basis of existing Electronic Health Record (EHR) systems. The present section is part of the related deliverable to Task 5.1, namely the First Report on the Health Record and Pathway repository and will set out the relevant rules and guidance on EHRs on the European level. On the basis of this information, the TeNDER system will ensure that it is in line with the most up to date EHR standards, including security and interoperability aspects.

### 1.1 European Guidelines on EHRs

#### 1.1.1 Background

One of the European Commission's major priorities is "enhancing the use of digital technology through the creation of a Digital Single Market (DSM)" which was launched in 2015.<sup>3</sup> According to the Commission, "the DSM aims to open up digital opportunities to people and business, and to bring the EU's single market into the digital age."<sup>4</sup> One of the sectors included is health, "given the potential benefits that digital services have to offer citizens and enterprises in this area."<sup>5</sup>

In this regard, the European Commission, in a Communication from 2015, highlighted the sustainability challenges faced by European health systems, including an ageing population and associated rise in chronic illnesses and co-morbidities resulting in a growing demand for healthcare, increasing costs of healthcare, and inequalities and inequities in access to healthcare.<sup>6</sup> It concluded that "Member States' future ability to provide high quality care to all will depend on making health systems more resilient, [...] while remaining cost-effective and fiscally sustainable."<sup>7</sup> In particular, it strongly encouraged "cooperation between Member States on eHealth and supports them in developing and implementing cost-effective and interoperable eHealth solutions to improve health systems."<sup>8</sup>

Similarly, the Council of the European Union has, on several occasions, stressed the importance of adopting innovative approach in response to challenges related to health systems' sustainability.<sup>9</sup> In 2017, for instance, it adopted the Council conclusions on Health in the Digital Society, wherein it

<sup>3</sup> European Commission, eHealth: Digital health and care (website), see [https://ec.europa.eu/health/ehealth/home\\_en](https://ec.europa.eu/health/ehealth/home_en) (last accessed on 11 May 2020).

<sup>4</sup> European Commission, eHealth: Digital health and care (website), see [https://ec.europa.eu/health/ehealth/home\\_en](https://ec.europa.eu/health/ehealth/home_en) (last accessed on 11 May 2020).

<sup>5</sup> European Commission, eHealth: Digital health and care (website), see [https://ec.europa.eu/health/ehealth/home\\_en](https://ec.europa.eu/health/ehealth/home_en) (last accessed on 11 May 2020).

<sup>6</sup> Communication from the Commission on effective, accessible and resilient health systems, COM(2015) 215 final ("Communication 2015/215"), p. 2, see [https://ec.europa.eu/health/sites/health/files/systems\\_performance\\_assessment/docs/com2014\\_215\\_final\\_en.pdf](https://ec.europa.eu/health/sites/health/files/systems_performance_assessment/docs/com2014_215_final_en.pdf) (last accessed on 27 April 2020).

<sup>7</sup> Communication 2015/215, p. 16.

<sup>8</sup> Communication 2015/215, p. 16.

<sup>9</sup> Council conclusions on Health in the Digital Society – making progress in data-driven innovation in the field of health (2017/C 440/05) ("Council Conclusions"), paras. 1, 2, see [https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52017XG1221\(01\)](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52017XG1221(01)) (last accessed on 27 April 2020).

stressed the “greater need for Member States to make their electronic health systems more interoperable in order to give citizens greater control over their health data.”<sup>10</sup>

During the mid-term review of the implementation of the DSM strategy,<sup>11</sup> the Commission considered that digital technologies could offer cost-effective tools to “help improve people’s health and address systematic challenges for healthcare systems”, thereby contributing to a patient-centred and sustainable healthcare systems.<sup>12</sup> It found that “more need[ed] to be done so that all citizens can, in full privacy and confidence, access and transfer their complete electronic health record when receiving healthcare abroad.”<sup>13</sup> The Commission set out its intention to take action in three areas:

1. citizens’ secure access to and sharing of health data across borders;
2. supporting data infrastructure to advance research, disease prevention and personalised health and care;
3. digital tools for citizen empowerment and person-centred care.<sup>14</sup>

There are a number of structures that provide a platform for collaboration and cooperation on these areas, including the eHealth Network, established under Directive 2011/24/EU (“Patients’ Rights Directive”)<sup>15</sup> and providing EU countries a forum where they “can give direction to eHealth developments in Europe by playing an important role in strategic e-Health related decision-making on interoperability and standardisation.”<sup>16</sup>

Between 20 July and 12 October 2017, the Commission conducted public consultations to “define the need and scope of policy measures that will promote digital innovation in improving people’s health and address systemic challenges to healthcare systems.”<sup>17</sup> These consultations confirmed that the relevant stakeholders considered the lack of interoperability between EHRs a major obstacle to access

<sup>10</sup> Commission Recommendation (EU) 2019/243 of 6 February 2019 on a European Electronic Health Record exchange format (“EHR Recommendation”), para. 6 see <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32019H0243> (last accessed on 27 April 2020). Also see Council Conclusions.

<sup>11</sup> See Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on a single digital market strategy for Europe, COM (2015) 192 final, see <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52015DC0192&from=EN> (last accessed on 27 April 2020).

<sup>12</sup> Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the Mid-Term Review on the implementation of the Digital Single Market Strategy, COM(2017) 228 (“Communication 2017/228”), p. 18, see <https://ec.europa.eu/transparency/regdoc/rep/1/2017/EN/COM-2017-228-F1-EN-MAIN-PART-1.PDF> (last accessed on 27 April 2020).

<sup>13</sup> Communication 2017/228, p. 18.

<sup>14</sup> Communication 2017/228, p. 19. Also see Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on enabling the digital transformation of health and care in the Digital Single Market; empowering citizens and building a healthier society, COM(2018) 233 final (“Communication 2018/233”), p. 3, see <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018DC0233> (last accessed on 27 April 2020).

<sup>15</sup> EU Directive 2011/24/EC of the European Parliament and of the Council of 9 March 2011 on the application of patients’ rights in cross-border healthcare (“EU Patients’ Rights Directive”), see <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:088:0045:0065:EN:PDF> (last accessed on 11 February 2020). Also see Recital 15, EHR Recommendation.

<sup>16</sup> European Commission, EU Cooperation (website), see [https://ec.europa.eu/health/ehealth/cooperation\\_en](https://ec.europa.eu/health/ehealth/cooperation_en) (last accessed on 11 May 2020).

<sup>17</sup> European Commission (website), [https://ec.europa.eu/info/consultations/public-consultation-transformation-health-and-care-digital-single-market\\_en](https://ec.europa.eu/info/consultations/public-consultation-transformation-health-and-care-digital-single-market_en) (last accessed on 27 April 2020).

to health data.<sup>18</sup> Standardisation of electronic health records was considered as one of the ways in which the barriers to access and sharing of data could be overcome.<sup>19</sup>

Following the public consultations, the Commission adopted its Communication “on enabling the digital transformation of health and care in the DSM; empowering citizens and building a healthier society” in 2018.<sup>20</sup> Recalling the three areas of action as identified in earlier Communications,<sup>21</sup> the Commission undertook to “adopt a Commission recommendation on the technical specification for a European electronic health record exchange format”, which should take into consideration the requirements of the GDPR.<sup>22</sup>

In 2019, the Commission adopted the EHR Recommendation that was proposed in Communication 2018/233 on a European EHR exchange format.

## 1.2 EU Recommendation on European EHR exchange format

At the outset, it is useful to note that while the EHR Recommendations and other EU rules and regulations referred therein, are directed at EU Member States, these documents can nevertheless provide useful guidance for the TeNDER consortium in the development of the TeNDER system to ensure that it is in line with the most up-to-date EHR standards, including security and interoperability aspects.

The EHR Recommendation sets out a framework for the development of a European EHR exchange format “in order to achieve secure, interoperable, cross-border access to, and exchange of, electronic health data in the Union.”<sup>23</sup> The Recommendation is a “means to promote public health, to support cooperation between the Member States, and to promote the digital single market.”<sup>24</sup> It finds its legal basis in Article 168 of the Treaty on the Functioning of the European Union (TFEU) which provides that the EU shall complement national health policy and Article 292 TFEU which sets out the Commission’s general power to issue recommendations.<sup>25</sup> Moreover, the recommendation is to be considered in light of EU Regulation 2016/679 (GDPR)<sup>26</sup> which provides for the right of citizens to access their health

---

<sup>18</sup> European Commission, Consultation: Transformation health and care in the digital single market (synopsis report), 2018 (“Consultation 2017 Report”), pp. 8, 9, see [https://ec.europa.eu/health/sites/health/files/ehealth/docs/2018\\_consultation\\_dsm\\_en.pdf](https://ec.europa.eu/health/sites/health/files/ehealth/docs/2018_consultation_dsm_en.pdf) (last accessed on 27 April 2020).

<sup>19</sup> Consultation 2017 Report, p. 10; Communication 2018/233, p. 4.

<sup>20</sup> Communication 2018/233. Also see EHR Recommendation, para. 7.

<sup>21</sup> Communication 2017/228, p. 19; Communication 2018/233, p. 3.

<sup>22</sup> Communication 2018/233, p. 7.

<sup>23</sup> EHR Recommendation, para. 1.

<sup>24</sup> Roadmap on Commission Recommendation to establish Format for a European Electronic Health Record (EHR) Exchange, Ref. Ares(2018)5986687, 22 November 2018 (“Roadmap EHR Recommendation”), p. 2, see <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/1999-European-Electronic-Health-Record-EHR-Exchange-Format> (last accessed on 28 April 2018).

<sup>25</sup> Articles 168, 292, Treaty on the Functioning of the European Union (“TFEU”), 26 October 2012, *OJ C 326*, 26.10.2012, see <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:12012E/TXT> (last accessed on 28 April 2020). Also see Roadmap, p. 2.

<sup>26</sup> EU Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (“GDPR”), see <https://eur-lex.europa.eu/eli/reg/2016/679/oj> (last accessed on 11 February 2020).

data as well as the Directive 2011/24/EU (“Patients’ Rights Directive”)<sup>27</sup> which provides that citizens have the right to access healthcare in any country.<sup>28</sup>

The EHR Recommendation notes that the lack of interoperability of EHRs across the EU leads to “fragmentation and a lower quality of cross-border healthcare provision.”<sup>29</sup> The Commission stated that “digitising health records, and creating systems that enable them to be securely accessed by citizens and securely shared within and between the different actors in the health system is an important step towards integrating digital technologies into health and care approaches.”<sup>30</sup> It further noted “[t]hat integration requires electronic health records, to be interoperable across the Union whereas currently many of the formats and standards in electronic health record systems [...] used across the Union are incompatible.”<sup>31</sup>

Accordingly, to “achieve secure, interoperable, cross-border access to, and exchange of, electronic health data”, the EHR Recommendation sets out a framework which includes:

- (a) a set of principles that should govern access to and exchange of electronic health records across borders in the Union;
- (b) a set of common technical specifications for the cross-border exchange of data in certain health information domains, which should constitute the baseline for a European health record exchange format;
- (c) a process to take forward the further elaboration of a European electronic health record exchange format.<sup>32</sup>

It is useful to note here that the EHR Recommendation, in connection to national regulations on electronic health systems, provided that “existing national specifications for electronic health record systems may continue to apply in parallel with a European electronic health record exchange format”.<sup>33</sup>

### 1.2.1 Access to and security of EHRs

The EHR Recommendation emphasised that “new technologies for health should support citizens to become active agents of their own health journey.”<sup>34</sup> For that reason, health information systems should be citizen-centric according to the Commission, “including making these systems more accessible to users, in particular to persons with disabilities, according to the accessibility requirements laid down by Directive (EU) 2016/2102”.<sup>35</sup>

It further urges Member States to ensure that EHR systems “meet high standards for the protection of health data and the security of network and information systems on which [EHR] systems rely, to

<sup>27</sup> EU Directive 2011/24/EC of the European Parliament and of the Council of 9 March 2011 on the application of patients’ rights in cross-border healthcare (“EU Patients’ Rights Directive”), see <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:088:0045:0065:EN:PDF> (last accessed on 11 February 2020).

<sup>28</sup> Roadmap, p. 2.

<sup>29</sup> Recital 11, EHR Recommendation.

<sup>30</sup> Recital 8, EHR Recommendation.

<sup>31</sup> Recital 8, EHR Recommendation.

<sup>32</sup> Para. 1, EHR Recommendation.

<sup>33</sup> Recital 19, EHR Recommendation.

<sup>34</sup> Recital 9, EHR Recommendation.

<sup>35</sup> Recital 9, EHR Recommendation, referring to Directive (EU) 2016/2102 of the European Parliament and of the Council of 26 October 2016 on the accessibility of the websites and mobile applications of public sector bodies, see <http://data.europa.eu/eli/dir/2016/2102/oj> (last accessed on 8 May 2020).

avoid data breaches and minimise the risks of security incidents.”<sup>36</sup> Moreover, it clarified that “Member States should ensure that citizens and their healthcare professionals have online access to their [EHRs] using secure electronic identification means”, thereby taking note of the security framework established by Regulation (EU) No. 910/2014 (“Electronic Identification Regulation”).<sup>37</sup> According to the Commission, “the use of secure electronic identification and authentication means provided for in [the] Regulation [...] (eIDAS) should enhance access, security and trust in electronic health record systems.”<sup>38</sup>

The Electronic Identification Regulation “lays down the conditions under which recognised electronic identification means, falling under a notified electronic identification scheme of a Member State, may be used by citizens to gain access to online public services from abroad, including access to health services and health data” and “[i]t also lays down rules for trust services such as electronic signatures, electronic seals and electronic registered delivery services, to securely manage and exchange health data by minimising the risk of possible tampering and misuse.”<sup>39</sup> In its annexes, it sets out requirements for, among others, qualified certificates for electronic signatures (Annex I, II) and for qualified certificates for website authentication (Annex IV). It is useful to note here that while the scope of the Regulation is broader than EHR’s, it serves as guidance for the use of secure electronic identification means as referred to in the EHR Recommendation.

### 1.2.1.1 Principles

In general, the EHR Recommendation indicates that Member States should ensure that “citizens are able to access and securely share their electronic health data across borders”. When developing solutions that will enable access to and exchange of electronic health data, the EHR Recommendation sets out the following principles that should be observed.<sup>40</sup>

*Table 2 – Principles of access to and cross-border exchange of electronic health data*

<b>Citizen-centric by design</b>	Citizens should be central to the way in which systems are designed. Such systems are to be designed to implement the principles of data protection by design and by default to meet the requirements of the GDPR.
<b>Comprehensiveness and machine-readability</b>	Electronic health records should be as comprehensive as possible in order to support health and care services throughout the Union.  Health data introduced in electronic health records should be machine-readable to the extent required by reasonable intended reuse of those data. Information should be structured and codified in the most practical way possible, with a view to making health data interoperable, including across borders.
<b>Data protection and confidentiality</b>	Electronic Health Record systems and interoperability solutions have to guarantee the confidentiality of personal health data and conform with all aspects of data protection legislation, from their design stage onward.

<sup>36</sup> Para. 2, EHR Recommendation.

<sup>37</sup> Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (“Electronic Identification Regulation”), see <http://data.europa.eu/eli/reg/2014/910/oj> (last accessed on 7 May 2020).

<sup>38</sup> Recital 13, EHR Recommendation.

<sup>39</sup> Recital 13, EHR Recommendation. Also see Article 1, Electronic Identification Regulation.

<sup>40</sup> Para. 1, Annex, EHR Recommendation.

	The fundamental right to the protection of personal data should be fully and effectively implemented, in conformity with the GDPR, including the right to transparent information, the right of access and other relevant rights listed. In particular, citizens should be able to exercise their right to access their health data by having access to their electronic health records, including across borders.
<b>Consent or other lawful basis</b>	Any processing, as defined in the GDPR, of health data must be based on the explicit consent of the citizen concerned or on any other lawful basis, pursuant to Articles 6 and 9 of the GDPR.
<b>Auditability</b>	Any processing of health data should be registered and verified for auditing purposes, using appropriate techniques, such as logging and audit trailing, to keep an accurate record of the access to electronic records, their exchange or any other processing operation.
<b>Security</b>	Pursuant to the GDPR and Directive (EU) 2016/1148 (“Network and Information Security Directive”) <sup>41</sup> appropriate technical and organisational measures must be implemented to ensure that electronic health record systems are secure. Those measures should include protection against unauthorised or unlawful processing of health data and against accidental loss, destruction or damage. Entities exchanging electronic health records should ensure that personnel dealing with electronic health records systems is properly aware of cybersecurity risks and adequately trained.
<b>Identification &amp; authentication</b>	<p>Strong and reliable identification and authentication of all involved parties is a key element to guarantee trust in exchanges of data between electronic health record systems.</p> <p>The use of notified national electronic identifications (eIDs) supports citizens’ cross-border identification and authentication to access their health data in full security and convenience, as well as the principle of ‘non- repudiation’ assuring the origin and integrity of such data. Through the mutual recognition of national electronic identification schemes, as foreseen in the Electronic Identification Regulation, citizens of one Member State may use their national electronic identifications to securely access online services provided to them in another Member State. Pursuant to Article 6 of that Regulation, online public services requiring electronic identification assurance corresponding to a certain level (‘substantial’ or ‘high’) must accept the notified electronic identification schemes of other Member States.</p>
<b>Continuity of service</b>	Continuity and availability of the electronic health record exchange service is essential to guarantee continuity of care. Any incidents or interruptions that may arise during the use of the service should be promptly addressed in accordance with defined business continuity plans.

The GDPR serves as the foundation of several of the above principles, in particular, in connection to the general need to observe data protection and confidentiality, as well as the required legal basis of data processing (in connection to the TeNDER project, likely [explicit] consent) and security (in terms of technical and organisational measures for secure processing of [health] data). The requirements of the GDPR were considered in detail in D1.1 and will therefore not be considered comprehensively

<sup>41</sup> Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (“Network and Information System Security Directive”), see <https://eur-lex.europa.eu/eli/dir/2016/1148/oj> (last accessed on 7 May 2020).

here. It is recommended that this report is read in conjunction with D1.1. In addition, some particular data protection guidance in relation to EHRs is set out in section 1.4 below.

The principle of security, in addition to referring to the GDPR, includes reference to the Network and Information System Security Directive. This Directive “lays down measures with a view to achieving a high common level of security of network and information systems within the Union so as to improve the functioning of the internal market.”<sup>42</sup>

Under this Directive, “healthcare providers, that are identified as operators of essential services by Member States and digital service providers falling in its scope, are required to take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems they use in their operations of provision of service.”<sup>43</sup>

Furthermore, such operators of essential services are also required to notify the competent national authorities or the national Computer Security Incident Response Teams (CSIRTs) about security incidents that have a “significant or substantial impact on the continuity of the services they provide.” Finally, and particularly regarding “cybersecurity for electronic health record systems, cybersecurity certification may allow the demonstration that cybersecurity requirements are fulfilled, under the relevant Union cybersecurity framework.”<sup>44</sup>

Similar to other EU rules and regulations referred to in the present report, the Directive sets out obligations for Member States. Nevertheless, there can be useful guidance in the approach taken by the EU to security measures. For instance, it includes specific guidance on security requirements and incidents notification, including digital service providers (see Articles 14, 16).

In terms of the EU’s cybersecurity framework that was referenced in the EHR Recommendation, reference is made to the 2017 Joint Communication, which provides that the Commission was “putting forward a proposal to set up **an EU cybersecurity certification framework**”.<sup>45</sup> This proposal<sup>46</sup> was considered and adopted Regulation (EU) 2019/881 on cybersecurity,<sup>47</sup> which lays down “a framework for the establishment of European cybersecurity certification schemes for the purpose of ensuring an adequate level of cybersecurity for ICT products, ICT services and ICT processes in the Union, as well as for the purpose of avoiding the fragmentation of the internal market with regard to cybersecurity certification schemes in the Union.”<sup>48</sup> It sets out this cybersecurity certification framework in Articles 46 to 65 of the Regulation. The Cybersecurity Regulation further lays down the “objectives, tasks and organisational matters relating to ENISA (the European Union Agency for Cybersecurity)”.<sup>49</sup>

---

<sup>42</sup> Article 1, Network and Information System Security Directive.

<sup>43</sup> Recital 14, EHR Recommendation.

<sup>44</sup> Recital 14, EHR Recommendation, referring to Section 2.2, Joint Communication to the European Parliament and the Council on Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, JOIN(2017) 450 final, 13 September 2017 (“2017 Joint Communication”), see <https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:52017JC0450> (last accessed on 12 May 2020).

<sup>45</sup> 2017 Joint Communication, p. 4.

<sup>46</sup> Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on ENISA, the “EU Cybersecurity Agency”, and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification (“Cybersecurity Act”), COM(2017) 477 final, 13 September 2017, see <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM:2017:477:FIN> (last accessed on 12 May 2020).

<sup>47</sup> Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (“Cybersecurity Regulation”), see <http://data.europa.eu/eli/reg/2019/881/oj> (last accessed on 12 May 2020).

<sup>48</sup> Article 1(1)(b), Cybersecurity Regulation.

<sup>49</sup> Article 1(1)(a), Cybersecurity Regulation.



### 1.2.2 Technical specifications and interoperability

The EHR Recommendation further stipulates that:

Member States should use the tools and building blocks provided by the eHealth Digital Services Infrastructure supported under the Connecting Europe Facility Program and refer to the Refined eHealth European Interoperability Framework as the common framework for managing interoperability in the eHealth domain.<sup>50</sup>

According to the EHR Recommendation, the aim of interoperability for EHRs is “to allow for the processing of information in a consistent manner between those health information systems, regardless of their technology, application or platform in a way that it can be meaningfully interpreted by the recipient.”<sup>51</sup>

The EHR Recommendation also recalls that the Member States have “taken important steps to foster interoperability” through the activities of the eHealth Network, which was established under the Patients’ Rights Directive.<sup>52</sup> “In particular, in order to facilitate the interoperability of European eHealth systems, a number of Member States participating in the eHealth Network have worked together with the Commission to build the eHealth Digital Services Infrastructure” (eHDSI).<sup>53</sup> Exchanges on ‘ePrescriptions’ through the eHDSI between several States had started and the exchange on ‘Patient Summaries’ was expected to commence shortly.<sup>54</sup> According to the Commission, “a number of tools developed for the [eHDSI] are a resource for Member States for the exchange of electronic health records.”<sup>55</sup> This could, in turn, be a useful resource for the TeNDER project as well. For more on the eHDSI, see below in section 1.2.2.2.

Furthermore, as part of achieving greater interoperability, the Commission recalled it had previously identified specific Integrating the Healthcare Enterprise profiles (“IHE profiles”), which were listed in an Annex to Commission Decision (EU) 2015/1302.<sup>56</sup> The implementations had the “the potential to increase interoperability of eHealth services and applications to the benefit of citizens and the healthcare professional community and to be eligible for referencing in public procurement.”<sup>57</sup> Providing “detailed layers of interoperability”, the EHR Recommendation indicates that “some of those profiles are already used to address specific business requirements” in the eHDSI.<sup>58</sup> Accordingly, the Commission encourages the consideration of the IHE profiles “to facilitate the exchange of healthcare information domains across borders” and proposes that such profiles could be used for, among others “patient identification, document exchange, audit trails and identity claims.”<sup>59</sup>

---

<sup>50</sup> Para. 4, EHR Recommendation.

<sup>51</sup> Recital 10, EHR Recommendation.

<sup>52</sup> Recital 15, EHR Recommendation.

<sup>53</sup> Recital 16, EHR Recommendation.

<sup>54</sup> Recital 16, EHR Recommendation.

<sup>55</sup> Recital 16, EHR Recommendation.

<sup>56</sup> Commission Decision (EU) 2015/1302 of 28 July 2015 on the identification of ‘Integrating the Healthcare Enterprise’ profiles for referencing in public procurement, see <http://data.europa.eu/eli/dec/2015/1302/oj> (last accessed on 7 May 2020). Also see Recital 11, EHR Recommendation.

<sup>57</sup> Recital 11, EHR Recommendation.

<sup>58</sup> Recital 11, EHR Recommendation.

<sup>59</sup> Section 2.2.3, Annex, EHR Recommendation.

### 1.2.2.1 Baseline for a European EHR exchange format

The EHR Recommendation further sets out a baseline for the European EHR exchange format. It states that measures should be taken “to ensure that the following health information domains [...] are part of a European [EHR] exchange format”.<sup>60</sup> These domains include:

- (a) Patient summary;
- (b) ePrescription / eDispensation;
- (c) Laboratory results;
- (d) Medical imaging and reports;
- (e) Hospital discharge reports.<sup>61</sup>

In connection to the Patient Summary, the EHR Recommendation makes reference to the eHealth Network Guideline on the electronic exchange of health data under Cross Border Directive 2011/24/EU (“eHealth Guideline on Patient Summary”),<sup>62</sup> which will be discussed below in section 1.3.1.1. In connection to the ePrescription/eDispensation, the EHR Recommendation refers to the eHealth Network Guideline on the electronic exchange of health data under Cross Border Directive 2011/24/EU (“eHealth Guideline on ePrescriptions”),<sup>63</sup> which will be discussed below in section 1.3.1.2.

The EHR Recommendation then sets out two tables containing “a set of recommended interoperability specifications for content structuring and representation”.<sup>64</sup> Table A contains the following:<sup>65</sup>

Table 3 – Recommended interoperability specifications - Table A

Table A: Content structuring and representation for health information domains for which the eHealth Network have adopted guidelines		
Health information domains	Clinical information for cross-border exchange	Content representation for cross-border exchange
Patient Summary	Structured according to the provisions in the 'GUIDELINE on the electronic exchange of health data under Cross-Border Directive 2011/24/EU Release 2 - Patient Summary for unscheduled care' adopted by the eHealth Network on 21 November 2016 (1)	Health Level Seven (HL7) Clinical Document Architecture (CDA) Release 2 (2) Level 3 and Level 1 (PDF (3)/A)
Health information domains	Clinical information for cross-border exchange	Content representation for cross-border exchange

<sup>60</sup> Para. 11, EHR Recommendation.

<sup>61</sup> Para. 11& Section 2.1, Annex, EHR Recommendation.

<sup>62</sup> eHealth Network, Guideline on the electronic exchange of health data under Cross Border Directive 2011/24/EU, Release 2, Patient Summary for unscheduled care, 21 November 2016 (“eHealth Guideline on Patient Summary”), see

[https://ec.europa.eu/health/sites/health/files/ehealth/docs/ev\\_20161121\\_co10\\_en.pdf](https://ec.europa.eu/health/sites/health/files/ehealth/docs/ev_20161121_co10_en.pdf) (last accessed on 7 May 2020).

<sup>63</sup> eHealth Network, Guideline on the electronic exchange of health data under Cross Border Directive 2011/24/EU, Release 2, ePrescriptions and eDispensations, 21 November 2016 (“eHealth Guideline on ePrescriptions”), see [https://ec.europa.eu/health/sites/health/files/ehealth/docs/ev\\_20161121\\_co091\\_en.pdf](https://ec.europa.eu/health/sites/health/files/ehealth/docs/ev_20161121_co091_en.pdf) (last accessed on 8 May 2020).

<sup>64</sup> Section 2.2, Annex, EHR Recommendation.

<sup>65</sup> Section 2.2, Annex, EHR Recommendation.

ePrescription/ eDispensation	Structured according to the provisions in the 'GUIDELINE on the electronic exchange of health data under Cross-Border Directive 2011/24/EU Release 2 – ePrescriptions and eDispensations' adopted by the eHealth Network on 21 November 2016 (4)	Health Level Seven (HL7) Clinical Document Architecture (CDA) Release 2 (2) Level 3 and Level 1 (PDF (3)/A)
(1)	<a href="https://ec.europa.eu/health/sites/health/files/ehealth/docs/ev_20161121_co10_en.pdf">https://ec.europa.eu/health/sites/health/files/ehealth/docs/ev_20161121_co10_en.pdf</a>	
(2)	<a href="http://www.hl7.org/implement/standards/product_brief.cfm?product_id=7">http://www.hl7.org/implement/standards/product_brief.cfm?product_id=7</a>	
(3)	Portable Document Format.	
(4)	<a href="https://ec.europa.eu/health/sites/health/files/ehealth/docs/ev_20161121_co091_en.pdf">https://ec.europa.eu/health/sites/health/files/ehealth/docs/ev_20161121_co091_en.pdf</a>	

The reference under note 2 in the above table is to HL7 International and the “HL7 Version 3 Clinical Document Architecture (CDA®)” (“HL7 CDA”) which is “a document mark-up standard that specifies the structure and semantics of “clinical documents” for the purpose of exchange between healthcare providers and patients. It defines a clinical document as having the following six characteristics: 1) Persistence, 2) Stewardship, 3) Potential for authentication, 4) Context, 5) Wholeness and 6) Human readability.”<sup>66</sup> According to the website, “a CDA can contain any type of clinical content -- typical CDA documents would be a Discharge Summary, Imaging Report, Admission & Physical, Pathology Report and more.”<sup>67</sup> Also see below reference to Health Level Seven Fast Healthcare Interoperability Resources (“HL7 FHIR®”).

Table B contains the following recommended interoperability specifications: <sup>68</sup>

Table 4 – Recommended interoperability specifications – Table B

Table B: Content structuring and representation for other health information domains		
Health information domain	Clinical information for cross-border exchange	Content representation for cross-border exchange
Laboratory results	Enable cross-border exchange according to the clinical information structure currently used by the sender electronic health record system, while common clinical information structures for cross-border exchange are developed and agreed.	For laboratory results, medical imaging reports and hospital discharge reports
Medical imaging and reports		Health Level Seven (HL7) Clinical Document Architecture (CDA) Release 2 Level 3 or Level 1 (PDF (1)/A)
Hospital discharge reports		For medical imaging Digital Imaging and Communications in Medicine (DICOM)
(1) Portable Document Format.		

Looking to the future, the EHR Recommendation encourages that “refinement of the exchange format should consider the possibility offered by resource driven information models” and, in this regard, makes reference to the Health Level Seven Fast Healthcare Interoperability Resources (“HL7 FHIR”).<sup>69</sup> According to the website, the “FHIR is a standard for health care data exchange, published by HL7®”<sup>70</sup>

<sup>66</sup> HL7 International Website, Product Brief, see [http://www.hl7.org/implement/standards/product\\_brief.cfm?product\\_id=7](http://www.hl7.org/implement/standards/product_brief.cfm?product_id=7) (last accessed on 8 May 2020).

<sup>67</sup> HL7 International Website, Product Brief, see [http://www.hl7.org/implement/standards/product\\_brief.cfm?product\\_id=7](http://www.hl7.org/implement/standards/product_brief.cfm?product_id=7) (last accessed on 8 May 2020).

<sup>68</sup> Section 2.2, Annex, EHR Recommendation.

<sup>69</sup> Section 3, Annex, EHR Recommendation, referring to <http://hl7.org/fhir/> (last accessed on 8 May 2020).

<sup>70</sup> HL7 FHIR (release 4) Website, Home, see <http://hl7.org/fhir/> (last accessed on 8 May 2020).

and “a platform specification that defines a set of capabilities use across the healthcare process, in all jurisdictions, and in lots of different contexts.”<sup>71</sup>

Both the HL7 FHIR and the HL7 CDA might be useful tools for the TeNDER project to consider and take guidance from.

#### 1.2.2.2 *The eHealth Digital Services Infrastructure*

According to the Commission, “in the context of exchanging electronic health records, the eHealth Network plays a valuable role in further developing the European electronic health record exchange format, by using it for the eHealth Digital Services Infrastructure and promoting its use for exchanges between healthcare providers at national level.”<sup>72</sup>

The eHDSI (or eHealth DSI) “is the initial deployment and operation of services for cross-border health data exchange” which is funded by the Connecting Europe Facility (CEF).<sup>73</sup> The “eHDSI sets up and starts deploying the core and generic services [...] for Patient Summary and ePrescription” and “[t]he generic services are the necessary implementation of data exchange at country level, the core services at EU level” and “these together enable the provision of Cross Border eHealth Information Services (CBeHIS).”<sup>74</sup> “Through 'core services', the European Commission is providing a common ICT infrastructure and crosscutting services (terminology, interoperability etc.) to EU countries.”<sup>75</sup> EU countries “can then set up 'generic services' to connect national eHealth systems through 'National Contact Points for eHealth (eHealth NCPs)', with financial assistance from the Connecting Europe Facility (CEF).”<sup>76</sup>

The eHDSI website contains a starting toolkit which includes detailed information on the eHDSI systems and data flow which might be useful to review in the context of the TeNDER project.<sup>77</sup>

<sup>71</sup> HL7 FHIR (release 4) Website, Getting started, see <http://hl7.org/fhir/modules.html> (last accessed on 8 May 2020).

<sup>72</sup> Recital 17, EHR Recommendation.

<sup>73</sup> eHDSI Website, eHDSI Mission, Governance and Communities, see <https://ec.europa.eu/cefdigital/wiki/display/EHOPERATIONS/eHealth+DSI+Operations+Home> (last accessed on 8 May 2020).

<sup>74</sup> eHDSI Website, eHDSI Mission, Governance and Communities, see <https://ec.europa.eu/cefdigital/wiki/display/EHOPERATIONS/eHealth+DSI+Operations+Home> (last accessed on 8 May 2020).

<sup>75</sup> European Commission Website, EU Cooperation, see [https://ec.europa.eu/health/ehealth/cooperation\\_en](https://ec.europa.eu/health/ehealth/cooperation_en) (last accessed on 11 May 2020).

<sup>76</sup> European Commission Website, EU Cooperation, see [https://ec.europa.eu/health/ehealth/cooperation\\_en](https://ec.europa.eu/health/ehealth/cooperation_en) (last accessed on 11 May 2020).

<sup>77</sup> eHDSI Website, eHDSI Starting Toolkit, eHDSI systems and data flow, see <https://ec.europa.eu/cefdigital/wiki/display/EHOPERATIONS/eHDSI+STARTING+TOOLKIT#eHDSISTARTINGTOOLKIT-eHDSISystemsandDataFlow> (last accessed on 8 May 2020).

### 1.3 European Interoperability Framework and eHealth

In 2010, the Commission introduced a Communication ‘towards interoperability for European public services’ (“2010 Communication”),<sup>78</sup> which introduced “the European Interoperability Strategy (EIS) and the European Interoperability Framework (EIF) for European public services, two key elements in the Digital Agenda” which, together, promoted “interoperability among public administrations.”<sup>79</sup> Noting that since the 2010 Communication, “the European interoperability framework has served as a reference throughout the Union and beyond, and was the basis of most national interoperability frameworks (NIFs) and strategies”, in 2017, the Commission issued a new Communication on the implementation of the EIF (“2017 Communication”).<sup>80</sup> The 2017 Communication was meant to update the EIF “to take on board new or revised interoperability requirements that arise from Union policies and programmes as well as from public administrations, while taking into account technological developments and trends.”<sup>81</sup>

Building on from the EIF and tuning it more specifically to the domain of health, the eHealth EIF (or “eEIF”) was developed in 2013, following a the eEIF study.<sup>82</sup>

Following the development of the first eEIF, a refinement thereof was provided in 2015 through the Antilope Project,<sup>83</sup> which aimed at creating, validating and disseminating “a common approach for testing and certification of eHealth solutions and services in Europe.”<sup>84</sup> Based on the output from the Antilope Project, the eHealth Network adopted the Refined eHealth European Interoperability Framework (ReEIF) in 2015, which aimed to “to present a common refined framework for managing interoperability and standardisation challenges in the eHealth domain in Europe.”<sup>85</sup>

#### 1.3.1 The Refined eHealth European Interoperability Framework

The ReEIF “offers a framework of terms and methodologies for reaching a common language, a common starting point, for the analysis of problems and the description of eHealth solutions throughout Europe” and is a refinement of the eEIF.<sup>86</sup> The ReEIF, “provides, among other things, an overview of possibly relevant use cases and appropriate links to the existing and available profiles from the major international consortia in the area of standardisation and interoperability” and

<sup>78</sup> Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions Towards interoperability for European public services, COM(2010) 744 final, 16 December 2010, see <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2010:0744:FIN> (last accessed on 11 May 2020).

<sup>79</sup> Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions on the European Interoperability Framework – Implementation Strategy, COM(2017) 134 final, 23 March 2017 (“2017 Communication”), p. 3, see <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:52017DC0134> (last accessed on 11 May 2020).

<sup>80</sup> 2017 Communication, p. 3.

<sup>81</sup> 2017 Communication, p. 3.

<sup>82</sup> Deloitte (on behalf of the European Commission), eHealth European Interoperability Framework, 14 February 2013, see <https://op.europa.eu/s/n6dg> (last accessed on 11 May 2020).

<sup>83</sup> eHealth Network, Refined eHealth European Interoperability Framework, 23 November 2015 (“ReEIF”), p. 7, see [https://ec.europa.eu/health/sites/health/files/ehealth/docs/ev\\_20151123\\_co03\\_en.pdf](https://ec.europa.eu/health/sites/health/files/ehealth/docs/ev_20151123_co03_en.pdf) (last accessed on 11 May 2020).

Also see <https://www.antilope-project.eu/front/index.html>.

<sup>84</sup> See <https://www.antilope-project.eu/front/index.html>.

<sup>85</sup> ReEIF, *supra* note 72.

<sup>86</sup> ReEIF, p. 4.

presents three tools: “a refined model for interoperability, a template for the description of high-level use cases, and a glossary of terms and definitions.”<sup>87</sup>

The refined eHealth EIF model builds on the original EIF model and sets out a total of six main levels (in contrast to the four original EIF main levels).<sup>88</sup>

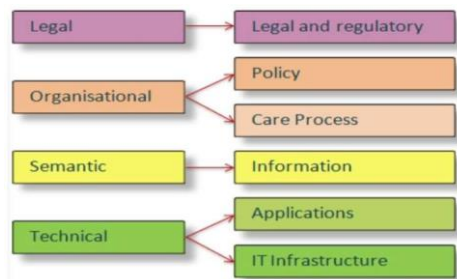


Figure 1 – ReEIF Model

The ReEIF then explains the six interoperability levels in more detail.<sup>89</sup>

Table 5 – ReEIF interoperability levels

<b>Legal and regulatory</b>	On this level, compatible legislation and regulatory guidelines define the boundaries for interoperability across borders, but also within a country or region.
<b>Policy</b>	On this level, contracts and agreements between organisations have to be made. The purpose and value of the collaboration must be set. Trust and responsibilities between the organisations are formalised on the Policy level. In governance documents the governance of collaboration is anchored.
<b>Care process</b>	After the organisations have agreed to work together, specific care processes are analysed and aligned, resulting in integrated care pathways and shared workflows. This level handles the tracking and management of the workflow processes. The shared workflow prescribes which information is needed in order to deliver the integrated care.
<b>Information</b>	This level represents the functional description of the data model, the data elements (concepts and possible values) and the linking of these data elements to terminologies that define the interoperability of the data elements.
<b>Applications</b>	On this level, agreements are made about the way import and export of medical information are handled by the healthcare information systems. The technical specification of how information is transported is at this level (communication standards). The information systems must be able to export and import using these communication standards.  Another aspect in this level is the integration and processing of exchanged information in user-friendly applications.
<b>IT infrastructures</b>	The generic communication and network protocols and standards, the storage, backup, and the database engines are on this level. It contains all the “generic” interoperability standards and protocols.

<sup>87</sup> ReEIF, p. 7.

<sup>88</sup> ReEIF, p. 8.

<sup>89</sup> ReEIF, pp. 9, 10.

The ReEIF further includes another helpful model in connection to interoperability, namely a model that shows “alignments that are necessary on the different levels of interoperability”:<sup>90</sup>

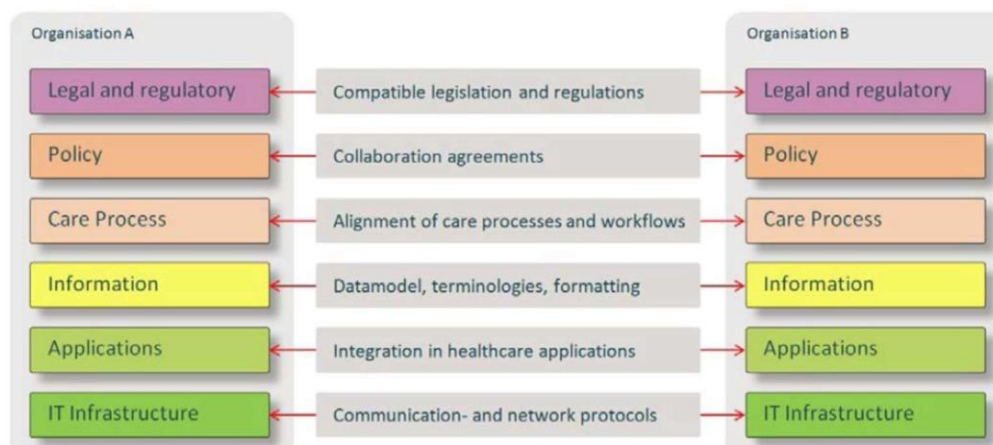


Figure 2 – ReEIF Alignment Model

The ReEIF further includes templates for high-level use cases (“the functional description of the process”) and realisation scenarios (“a translation into technical process steps”).<sup>91</sup> Furthermore, it includes a glossary of interoperability terms and definitions, noting that “interoperability starts with a shared understanding of the terms that are used”.<sup>92</sup>

In terms of the process, the ReEIF recommends that “any activity on interoperability starts with the description of the wanted outcome in terms of care processes, *i.e.* in terms of what patients and health professionals want to achieve with the interoperable solution to be created”, referring here to the utilisation of use cases.<sup>93</sup> Then, with this in mind, “the focus shifts to the content of the information, and the needed standards in terms of structure and semantics.”<sup>94</sup> At that stage, “the applications of both organisations should be aligned and an information exchanging mechanism (*e.g.* a document or a message) should be defined: containing the information needed and able to be generated and read by the applications, and meaningfully presented on the receiving side.”<sup>95</sup> “The technical pathways for these information packages need to be defined in order to communicate correctly and safely.”<sup>96</sup> The ReEIF further recommends that in the meantime, the use cases and their technical and financial consequences should be considered at a policy level between the organisations, regions or countries.<sup>97</sup> Finally, “everything should be checked against the legal and regulatory environment(s) relevant to the project.”<sup>98</sup>

#### 1.3.1.1 The eHealth Guideline on Patient Summary

This Guideline, issued by the eHealth Network in 2016, starts with setting out a use case for sharing of patient summaries on a cross-border scale, as previously set out in the Patients’ Rights Directive.<sup>99</sup>

<sup>90</sup> ReEIF, p. 10.

<sup>91</sup> ReEIF, pp. 11 to 14.

<sup>92</sup> ReEIF, p. 14, referring to Appendix C of the ReEIF.

<sup>93</sup> ReEIF, p. 14.

<sup>94</sup> ReEIF, p. 14.

<sup>95</sup> ReEIF, p. 14.

<sup>96</sup> ReEIF, p. 14.

<sup>97</sup> ReEIF, p. 14.

<sup>98</sup> ReEIF, p. 14.

<sup>99</sup> eHealth Guideline on Patient Summary, p. 5.

The following definition is provided “a Patient Summary is an identifiable ‘dataset of essential and understandable health information’ that is made available ‘at the point of care to deliver safe patient care during unscheduled care [and planned care] with its maximal impact in the unscheduled care’; it can also be defined at a high level as: ‘the minimum set of information needed to assure Health Care Coordination and the continuity of care’.”<sup>100</sup>

Regarding authorisation, authentication and identification, it provides that “implementation of the patient dataset implies that each Member State has addressed enabling activities such as” the provision of an official ID number, maintaining electronic registers of health professionals and agreed levels of authentication of citizens and health professionals.<sup>101</sup>

The content of the patient summaries is set out in Section 4 of the guidelines and includes “Patient Administrative Data and Patient Clinical Data.”<sup>102</sup>

While it is indicated that “Member States are free to choose the technical implementation of their Patient Summary dataset”, “the format of the document for [cross-border] exchange should be based on standards and profiles as agreed by” the eHealth Network.<sup>103</sup> More specifically, “[t]he cross-border specification is described in section 5, which also refers to supporting requirements and other relevant documentation.”<sup>104</sup>

#### 1.3.1.2 The eHealth Guideline on ePrescriptions

This Guideline was also issued by the eHealth Network in 2016, and also starts with a use case, taken from the Antilope project.<sup>105</sup> It applies “to the implementation of interoperable electronic prescription services across Member States, in order to facilitate the recognition and delivery of prescriptions issued in another Member State.”<sup>106</sup>

It contains an overview of the “fields for the dataset”, the data elements which “are taken from Implementing Directive 2012/52/EU and Draft International Standard DIS 175233 published in June 2016.”<sup>107</sup> Furthermore, “for cross-border exchange, the format of the document for exchange will be the CEF specification, as shown in Annex B.5.”<sup>108</sup> It also emphasises that “Member States shall ensure that communication of identifiable personal health data is subject to secure communication and end-to-end security measures.”<sup>109</sup>

---

<sup>100</sup> Section 2, Article 2, eHealth Guideline on Patient Summary.

<sup>101</sup> Section 2, Article 5, eHealth Guideline on Patient Summary. Also see, Section 3, Article 5, eHealth Guideline on Patient Summary.

<sup>102</sup> Section 2, Article 10, eHealth Guideline on Patient Summary. Also see, Section 3, Article 10, eHealth Guideline on Patient Summary.

<sup>103</sup> Section 2, Article 13, eHealth Guideline on Patient Summary. <sup>104</sup>

Section 2, Article 13, eHealth Guideline on Patient Summary. <sup>105</sup>  
eHealth Guideline on ePrescriptions, p. 5.

<sup>106</sup> Section 2, Article 1, eHealth Guideline on ePrescriptions.

<sup>107</sup> Section 2, Article 10, eHealth Guideline on ePrescriptions.

<sup>108</sup> Section 2, Article 14, eHealth Guideline on ePrescriptions.

<sup>109</sup> Section 2, Article 15, eHealth Guideline on ePrescriptions.



## 1.4 Data Protection in Connection to EHR

While the requirements of the GDPR were considered in detail in D1.1 (and this report should be considered in conjunction with D1.1), there was a specific guidance document that considered data protection in connection to EHRs. This will be briefly considered below.

In 2007, the Article 29 Data Protection Working Party (“Art. 29 WP”), adopted a working document on the processing of personal data relating to health in EHRs (“Working Document”).<sup>110</sup> While the Working Document was issued in relation to Directive 95/46/EC (the precursor to the GDPR),<sup>111</sup> and while it mostly relates to the development of EHR systems on the national level, it nevertheless contains relevant guidance that is useful in connection to the TeNDER project.

The Working Document intended to set out “the data protection preconditions for establishing a nation-wide EHR system, as well as the applicable safeguards”.<sup>112</sup> While acknowledging the potential benefits of EHR systems, the Working Document also cautioned, stating that “from a data protection point of view the fact has to be stressed that EHR systems additionally have the potential not only to process more personal data (e.g. in new contexts, or through aggregation) but also to make a patient’s data more readily available to a wider circle of recipients than before.”<sup>113</sup> According to Art. 29 WP, it was important to consider this new “risk scenario” and its related dangers.<sup>114</sup>

Art. 29 WP stressed that in collecting data in the context of EHRs, data controllers should comply with all the general data protection principles and take into consideration the specific requirements for processing special categories of data, which includes health data (for detailed description of both see D1.1).<sup>115</sup> The Art. 29 WP was of the opinion that “all data contained in medical documentation, in electronic health records and in EHR systems should be considered to be ‘sensitive personal data’.”<sup>116</sup> As a result, processing is generally considered prohibited, unless one of the legal bases of Article 9(2) of the GDPR applies. In the context of the TeNDER project, this is generally going to be explicit consent (Article 9(2)(a) GDPR – also see for further details D1.1).

The Working Document further sets out a number of recommended safeguards that should be considered when developing EHR systems in order to guarantee the data protection rights of patients:<sup>117</sup>

*Table 6 – Art. 29 WP Recommendations for safeguards in EHR systems*

<b>Respecting self-determination</b>	The patient’s self-determination concerning when and how his data are used should have a significant role as a major safeguard. In view of the varying damage potential of different types of health information, categories of use cases should be discerned with different degrees of the possibility to exercise self-determination. It should in principle always be possible for a patient to prevent
--------------------------------------	--

<sup>110</sup> Article 29 Data Protection Working Group (“Art. 29 WG”), Working document on the processing of personal data relating to health in electronic health records (EHR), WP 131, 15 February 2007 (“Working Document”), see [https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp131\\_en.pdf](https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp131_en.pdf) (last accessed on 25 May 2020).

<sup>111</sup> Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, see <http://data.europa.eu/eli/dir/1995/46/oj> (last accessed on 25 May 2020).

<sup>112</sup> Working Document, p. 4.

<sup>113</sup> Working Document, p. 4.

<sup>114</sup> Working Document, p. 4.

<sup>115</sup> Working Document, pp. 6, 7.

<sup>116</sup> Working Document, p. 7.

<sup>117</sup> Working Document, pp. 13 to 21.

	disclosure of their medical data, documented by one health professional during treatment, to other health professionals, if they so choose.
<b>Identification and authentication of patients and health care professionals</b>	<p>Reliable identification of patients in EHR systems is of crucial importance. If health data were used which relate to the wrong person as a result of incorrect identification of a patient the consequences would in many cases be detrimental. Moreover, the special sensitivity of health data requires that no access is possible for unauthorised persons. Reliable access control depends on reliable identification and authentication.</p> <p>For health care professionals it will be necessary to develop an identification and authentication system, which proves not only identities but additionally also the role in which a healthcare professional acts electronically.</p>
<b>Authorisation for accessing EHRs in order to read and write in EHR</b>	<p>Data in EHR systems are confidential medical records. Thus, the essential principle concerning access to an EHR must be that – apart from the patient himself – only those healthcare professionals/ authorised personnel of healthcare institutions who presently are involved in the patient’s treatment may have access. There must be a relationship of actual and current treatment between the patient and the healthcare professional wanting access to his EHR record.</p> <p>It should also be considered which categories of health care professionals/ institutions at which level have access to EHR-data.</p>
<b>The use of EHR for other purposes</b>	<p>The acceptance of EHR systems by the citizens will depend on their trust in the confidentiality of the system.</p> <p>The reason for legitimate access to data in an EHR should correspond to the main purpose of any EHR system, i.e. successful medical treatment by better information.</p>
<b>Organisational structure of an EHR system</b>	<p>In the context of discussing different organisational alternatives for storing data in an EHR system the following main alternatives are usually mentioned:</p> <ul style="list-style-type: none"> <li>• EHR as a system furnishing access to medical records kept by the health care professional, who has the obligation to keep records on the treatment of his patients – this is often called “decentralised storage”, or</li> <li>• EHR as a uniform system of storage, to which medical professionals have to transfer their documentation; this is often called “centralised storage”;</li> <li>• a third alternative could be to enable the data subject to be “master” of his own medical records by offering him storage of patients’ medical data as a special e-service under the patient’s control, possibly even including the power to decide what goes into an EHR.</li> </ul>
<b>Categories of data stored</b>	<p>In light of the principle of data minimisation, the legitimacy of EHR systems will also depend on an adequate solution of choosing the ‘right’ categories of data and the ‘right’ length of time for storing information in an EHR.</p> <p>The fact that it is possible to discern different categories of health data which require quite different degrees of confidentiality suggests that it might be generally useful to create different data modules within an EHR system with different access requirements. Particularly sensitive data could also be better protected by storage in separate modules with especially strict conditions for access.</p>
<b>International transfer of medical records</b>	<p>Electronic availability of medical data in EHR systems can considerably enhance diagnostic or treatment facilities by making use of medical expertise available only in foreign medical institutions. If possible, such data should be transferred to countries outside the European Union/European Economic Area only in anonymised or at least pseudonymised form.</p>

	Any processing – especially the storage – of EHR data should take place within jurisdictions applying the [GDPR] or an adequate data protection legal framework
<b>Data security</b>	<p>The legal framework for setting up an EHR system would have to foresee the requirement of implementing a series of measures of a technical and organisational nature appropriate for avoiding loss or unauthorised alteration, processing and access of data in the EHR system. Integrity of the system must be guaranteed by making use of the knowledge and instruments representing the present state of the art in computer science and information technology.</p> <p>Privacy enhancing technologies (PETs) should be applied as much as somehow possible in order to promote personal data protection. Encryption should not only be used for transfer but also for storage of data in EHR systems. All security measures should be constructed in a user-friendly way to broaden their application. The necessary costs should be seen as an investment into the fundamental rights compatibility of EHR systems, which will be one of the most important prerequisites if EHR systems are to become a success.</p> <p>Although many of the safeguards discussed above already contain elements of data security, the legal framework concerning security measures should especially foresee the necessity of:</p> <ul style="list-style-type: none"> <li>• the development of a reliable and effective system of electronic identification and authentication as well as constantly up-dated registers for checking on the accurate authorisation of persons having or requesting access to the EHR system;</li> <li>• comprehensive logging and documentation of all processing steps which have taken place within the system, especially access requests for reading or for writing, combined with regular internal checks and follow up on correct authorization;</li> <li>• effective back-up and recovery mechanisms in order to secure the content of the system;</li> <li>• preventing unauthorised access to or alteration of EHR data at the time of transfer or of back up storage, e.g. by using cryptographic algorithms;</li> <li>• clear and documented instructions to all authorized personnel on how to properly use EHR systems and how to avoid security risks and breaches;</li> <li>• a clear distinction of functions and competences concerning the categories of persons in charge of the system or at least involved in the system with a view to liability for shortcomings;</li> <li>• regular internal and external data protection auditing.</li> </ul>
<b>Transparency</b>	It seems evident, that an EHR has high potential for medical treatment but in principle also for misuse by unauthorised access. Public opinion and the individuals will therefore call for extra transparency concerning the content and the functioning of an EHR system in order to be able to trust in the system.
<b>Liability issues</b>	Any EHR system must also guarantee that the possible infringements of privacy which are caused by storing and furnishing medical data in an EHR system are adequately balanced by liability for damages caused e.g. by incorrect or unauthorised use of EHR data.
<b>Control mechanisms for processing data in EHR</b>	Considering the special risk scenario created by the establishment of EHR systems effective control mechanisms for evaluating the existing safeguards are necessary. The complexity of the information contained in an EHR together with the multitude of possible users may call for new procedures concerning the access rights of data subjects.

## 2. Implementation

This document refers to the first report of the results of T5.1, which is responsible for the implementation of the European regulation for data exchanging, based on existing EHR systems. This database will store the medical profile, extending information available from physical, medical and behavioural activity, to allow the information securely flowing from patients, to the system and to the health professionals.

With this subsystem aiming at managing and organising patient information that is provided by a series of different low-level subsystems, HL7 FHIR has been chosen as the standard specification for data exchange. FHIR is a next generation standards framework created by HL7, and stands for “Fast Healthcare Interoperability Resources”, leveraging the latest web standards and applying a tight focus on implementation. FHIR solutions are built from a set of modular components called “Resources”, which can be easily assembled into working systems that solve real-world clinical and administrative problems, being suitable for use in a wide variety of contexts, such as mobile phone apps, cloud communications, EHR-based data sharing, server communication in large institutional healthcare providers, and much more.

In order to achieve this goal, an instance of HAPI FHIR Server<sup>118</sup> is being integrated, an open-source and complete implementation of the HL7 FHIR standard for healthcare interoperability in Java. HAPI has been designed to provide a flexible way of adding FHIR capability to applications, allowing different types of clients to connect to this server (cf. figure below).



Figure 3 – EHR architecture regarding HAPI FHIR implementation.

The HAPI Server’s implementation of the FHIR standard provides an HTTP API to perform CRUD (create, read, update and delete) operations on the database, supporting different deployment schemes and relational databases. Initial tests are being done with HAPI’s R4 version (since the latest is branded as unstable) and PostgreSQL v12.0 relational database (but others can be used, maintaining the structural integrity equal to the guidelines and examples provided in their documentation). The server has modules developed by the HAPI community that implement an assortment of functionalities and allow users to interact with the server with relative ease, which will support the other High-Level Subsystems (HLS) in TeNDER.

HAPI FHIR provides a built-in mechanism for connecting to FHIR REST servers. The HAPI RESTful client is designed to be easy to set up and to allow strong compile-time type checking wherever possible. A client has been set up as a proof of concept, using Java with Spring Framework, configured to use Apache Tomcat applicational server, and organised as a Model-View-Controller (MVC) pattern. At the moment of writing this deliverable, the proof of concept implemented a Controller with three endpoints described in the table below.

<sup>118</sup> HAPI FHIR – <https://hapifhir.io/> . Checked in September 2020.

Table 6 – HAPI FHIR Sample Operations

METHOD	ENDPOINT	PARAMETERS	RESPONSE
GET	/patient/all	<p><b>name</b> - String - person name, surname</p> <p><b>location</b> - A server defined search that may match any of the string fields in the Address, including line, city, district, state, country, postalCode, and/or text</p> <p><b>orgId</b> - The id of the organisation that is the custodian of the patient record</p> <p><b>gender</b> - gender of a patient</p> <p><b>idRelatedPatient</b> - All patients linked to the given patient id</p> <p><b>isActive</b> - Whether the patient record is active</p> <p><b>phoneNumber</b> - A value in a phone contact</p> <p><b>isDeceased</b> - This patient has been marked as deceased, or as a death date entered</p> <p><b>email</b> - A value in an email contact</p> <p><b>identifier</b> - A patient identifier (it can be a social security number, passport id, something unique!)</p>	<p>Bundle Resource (example: <a href="https://www.hl7.org/fhir/R4/bundle-example.json.html">https://www.hl7.org/fhir/R4/bundle-example.json.html</a>)</p>
POST	/patient	<p><b>Patient Resource</b> (example: <a href="https://hl7.org/FHIR/patient-example.json.html">https://hl7.org/FHIR/patient-example.json.html</a>)</p>	<p>Receives the same resource as it was entered</p>
PUT	/patient/{id}	<p><b>id</b> – String</p>	<p>Receives the updated resource</p>

Despite being a proof of concept compliant with eHealth standards and EC reference architectures and guidelines, there are other considerations to be included for this tool:

- The data sources are scattered in multiple formats like sensors, files and databases, so different clients need to be configured.
- The data to be collected not only contains private data, but it also reflects sensitive data, so explicit consent should be provided by patients and caregivers when submitting information to the platform.
- The overall architecture of the TeNDER platform is not yet concluded, and therefore this solution shall be adapted along the project's lifetime.

## 2.1 HAPI FHIR Server

The HAPI FHIR Server is the full implementation of the FHIR standard, which currently supports two options for its implementation:

1. Using the plain server configuration to create a FHIR server endpoint against an arbitrary data source, which could be a database of your own design, for example.
2. Opting for the HAPI JPA (Java Persistence API) Server which is a project that contains a fully implemented contained FHIR server, supporting all standard operations (read/create/delete/etc).

The HAPI JPA Server has the following components:

- **Resource Providers:** A RESTful server Resource Provider is provided for each resource type in a given release of FHIR. Each resource provider implements a @Search method implementing the complete set of search parameters defined in the FHIR specification for the given resource type. The resource providers also extend a superclass which implements all the CRUD operations
- **HAPI DAOs:** The Data Access Objects (DAOs) actually implement all of the database business logic related to the storage, indexing, and retrieval of FHIR resources, using the underlying JPA API.
- **Hibernate:** The HAPI JPA Server uses the JPA library, implemented by Hibernate. No Hibernate specific features are used, so the library should also work with other providers (e.g. EclipseLink) but it is not tested regularly with them.
- **Database:** The RESTful server uses an embedded Derby database but can be configured to integrate with any database engine supported by Hibernate.

The experimentation and testing performed with HAPI FHIR have been targeting version R4 of FHIR, although the team has been experimenting and keeping up with newer versions (R5) and will upgrade towards this more recent version(s) as soon as its stability and performance meet the project's requirements.

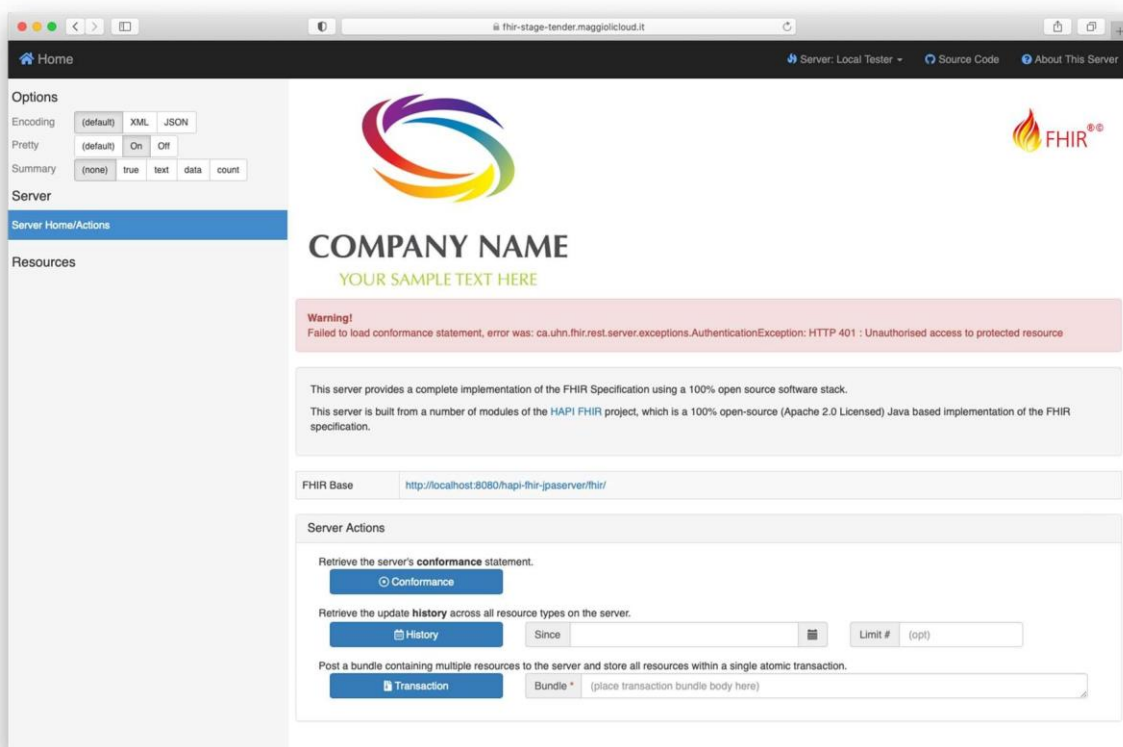


Figure 4 – HAPI FHIR running in Maggioli's cloud

The server has modules developed by the HAPI community that implement an assortment of functionalities and allow users to interact with the server with relative ease.

## 2.2 HAPI Model Objects

The database currently used is PostgreSQL v12.0, and the server's database schema is presented in the following figure. The HAPI FHIR JPA schema relies heavily on the concept of internal persistent IDs on tables, using a Java type of Long (8-byte integer, which translates to an *int8* or *number(19)* on various database platforms). Many tables use an internal persistent ID as their primary key, allowing the flexibility for other more complex business identifiers to be changed and minimising the amount of data consumed by foreign key relationships. These persistent ID columns are generally assigned using a dedicated database sequence on platforms which support sequences. The persistent ID column is generally called PID in the database schema, although there are exceptions.

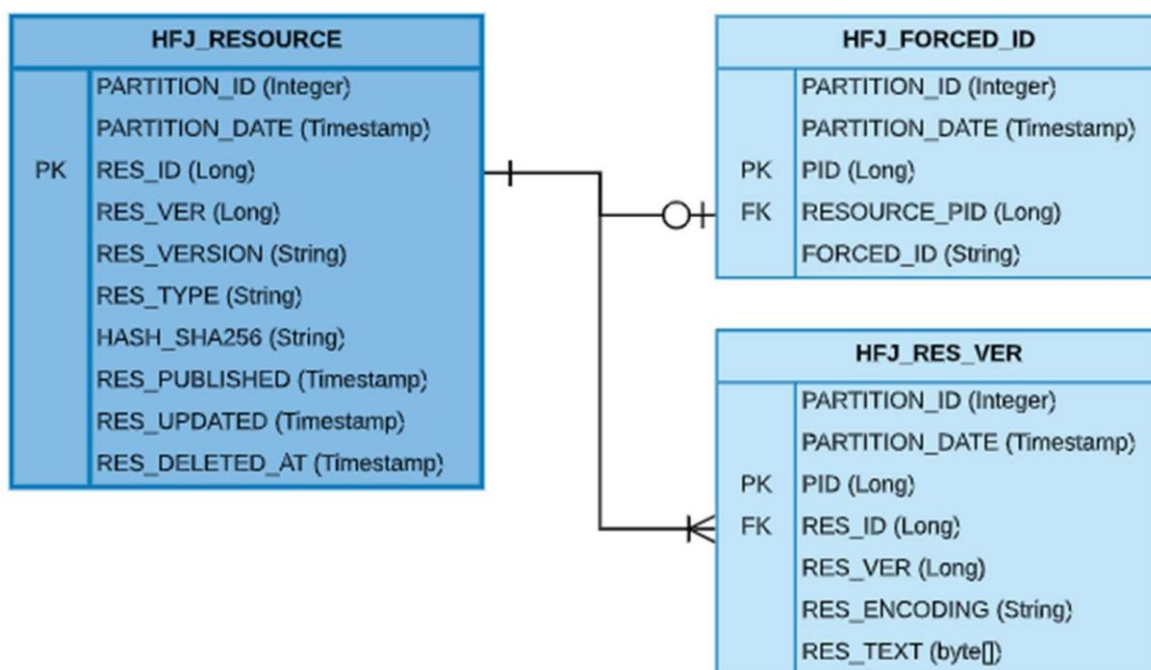


Figure 5 – Database organisation of resources

The HFJ\_RESOURCE table indicates a single resource of any type in the database. For example, the resource **Patient/1** will have exactly one row in this table, representing all versions of the resource. The HFJ\_RES\_VER table contains individual versions of a resource. If the resource **Patient/1** has 3 versions, there will be 3 rows in this table. The complete raw contents of the resource are stored in the **RES\_TEXT** column, using the encoding specified in the **RES\_ENCODING** column.

Basically, the HFJ\_RES\_VER will save the contents of the resource whilst HFJ\_RESOURCE will save a reference to the last version of a known resource. For reference, a list of all the resources can be found in the following page: <https://hl7.org/FHIR/resourcelist.html>

None of the resources have mandatory attributes, allowing flexibility and integrity regarding the HL7 standard. Taking into account the specifications and requirements from D2.1, the resources that are of bigger importance for TeNDER are the following:

- Patient
- Practitioner
- Practitioner Role
- Related Person

- Organization
- Organization Affiliation
- Healthcare Service
- Location
- Device
- Device Metric
- Appointment
- Appointment Response
- Medication Request
- Medication Administration
- Medication Dispense
- Medication Statement
- Medication
- Observation
- Condition
- Procedure
- Questionnaire
- Questionnaire Response

A few examples of these resources are demonstrated in the following figures where they are represented as JSON objects, respectively a Practitioner, a Patient and a Device:

```

{
  "resourceType": "Practitioner",
  // from Resource: id, meta, implicitRules, and language
  // from DomainResource: text, contained, extension, and modifierExtension
  "identifier": [{ Identifier }], // An identifier for the person as this agent
  "active": <boolean>, // Whether this practitioner's record is in active use
  "name": [{ HumanName }], // The name(s) associated with the practitioner
  "telecom": [{ ContactPoint }], // A contact detail for the practitioner (that apply to all roles)
  "address": [{ Address }], // Address(es) of the practitioner that are not role specific (typically home address)
  "gender": "<code>", // male | female | other | unknown
  "birthDate": "<date>", // The date on which the practitioner was born
  "photo": [{ Attachment }], // Image of the person
  "qualification": [{ // Certification, licenses, or training pertaining to the provision of care
    "identifier": [{ Identifier }], // An identifier for this qualification for the practitioner
    "code": { CodeableConcept }, // R! Coded representation of the qualification
    "period": { Period }, // Period during which the qualification is valid
    "issuer": { Reference(Organization) } // Organization that regulates and issues the qualification
  }],
  "communication": [{ CodeableConcept }], // A language the practitioner can use in patient communication
}

```

Figure 6 – JSON format of Practitioner resource in HAPI FHIR



```

{
  "resourceType" : "Patient",
  // from Resource: id, meta, implicitRules, and language
  // from DomainResource: text, contained, extension, and modifierExtension
  "identifier" : [{ Identifier }], // An identifier for this patient
  "active" : <boolean>, // Whether this patient's record is in active use
  "name" : [{ HumanName }], // A name associated with the patient
  "telecom" : [{ ContactPoint }], // A contact detail for the individual
  "gender" : "<code>", // male | female | other | unknown
  "birthDate" : "<date>", // The date of birth for the individual
  // deceased[x]: Indicates if the individual is deceased or not. One of these 2:
  "deceasedBoolean" : <boolean>,
  "deceasedDateTime" : "<dateTime>",
  "address" : [{ Address }], // An address for the individual
  "maritalStatus" : { CodeableConcept }, // Marital (civil) status of a patient
  // multipleBirth[x]: Whether patient is part of a multiple birth. One of these 2:
  "multipleBirthBoolean" : <boolean>,
  "multipleBirthInteger" : <integer>,
  "photo" : [{ Attachment }], // Image of the patient
  "contact" : [{ // A contact party (e.g. guardian, partner, friend) for the patient
    "relationship" : [{ CodeableConcept }], // The kind of relationship
    "name" : { HumanName }, // A name associated with the contact person
    "telecom" : [{ ContactPoint }], // A contact detail for the person
    "address" : { Address }, // Address for the contact person
    "gender" : "<code>", // male | female | other | unknown
    "organization" : { Reference(Organization) }, // C? Organization that is associated with the
    contact
    "period" : { Period } // The period during which this contact person or organization is valid
    to be contacted relating to this patient
  }],
  "communication" : [{ // A language which may be used to communicate with the patient about his
    or her health
    "language" : { CodeableConcept }, // R! The language which can be used to communicate with
    the patient about his or her health
    "preferred" : <boolean> // Language preference indicator
  }],
  "generalPractitioner" : [{ Reference(Organization|Practitioner|
    PractitionerRole) }], // Patient's nominated primary care provider
  "managingOrganization" : { Reference(Organization) }, // Organization that is the custodian of
  the patient record
  "link" : [{ // Link to another patient resource that concerns the same actual person
    "other" : { Reference(Patient|RelatedPerson) }, // R! The other patient or related person r
    esource that the link refers to
    "type" : "<code>" // R! replaced-by | replaces | refer | seealso
  }],
}

```

Figure 7 – JSON format of a Patient resource in HAPI FHIR

```

"resourceType" : "Device",
// from Resource: id, meta, implicitRules, and language
// from DomainResource: text, contained, extension, and modifierExtension
"identifier" : [{ Identifier }], // Instance identifier
"definition" : { Reference(DeviceDefinition) }, // The reference to the definition for the device
"udiCarrier" : [{ // Unique Device Identifier (UDI) Barcode string
  "deviceIdentifier" : "<string>", // Mandatory fixed portion of UDI
  "issuer" : "<uri>", // UDI Issuing Organization
  "jurisdiction" : "<uri>", // Regional UDI authority
  "carrierAIDC" : "<base64Binary>", // UDI Machine Readable Barcode String
  "carrierHRF" : "<string>", // UDI Human Readable Barcode String
  "entryType" : "<code>" // barcode | rfid | manual +
}],
"status" : "<code>", // active | inactive | entered-in-error | unknown
"statusReason" : [{ CodeableConcept }], // online | paused | standby | offline | not-ready | transduc-discon | hw-discon | off
"distinctIdentifier" : "<string>", // The distinct identification string
"manufacturer" : "<string>", // Name of device manufacturer
"manufactureDate" : "<dateTime>", // Date when the device was made
"expirationDate" : "<dateTime>", // Date and time of expiry of this device (if applicable)
"lotNumber" : "<string>", // Lot number of manufacture
"serialNumber" : "<string>", // Serial number assigned by the manufacturer
"deviceName" : [{ // The name of the device as given by the manufacturer
  "name" : "<string>", // RI The name of the device
  "type" : "<code>" // RI udi-label-name | user-friendly-name | patient-reported-name | manufacturer-name | model-name | other
}],
"modelNumber" : "<string>", // The model number for the device
"partNumber" : "<string>", // The part number of the device
"type" : { CodeableConcept }, // The kind or type of device
"specialization" : [{ // The capabilities supported on a device, the standards to which the device conforms for a particular purpose, and used for the communication
  "systemType" : { CodeableConcept }, // RI The standard that is used to operate and communicate
  "version" : "<string>" // The version of the standard that is used to operate and communicate
}],
"version" : [{ // The actual design of the device or software version running on the device
  "type" : { CodeableConcept }, // The type of the device version
  "component" : { Identifier }, // A single component of the device version
  "value" : "<string>" // RI The version text
}],
"property" : [{ // The actual configuration settings of a device as it actually operates, e.g., regulation status, time properties
  "type" : { CodeableConcept }, // RI Code that specifies the property DeviceDefinitionPropertyCode (Extensible)
  "valueQuantity" : [{ Quantity }], // Property value as a quantity
  "valueCode" : [{ CodeableConcept }], // Property value as a code, e.g., NTP4 (synced to NTP)
}],
"patient" : { Reference(Patient) }, // Patient to whom Device is affixed
"owner" : { Reference(Organization) }, // Organization responsible for device
"contact" : [{ ContactPoint }], // Details for human/organization for support
"location" : { Reference(Location) }, // Where the device is found
"url" : "<uri>", // Network address to contact device
"note" : [{ Annotation }], // Device notes and comments
"safety" : [{ CodeableConcept }], // Safety Characteristics of Device
"parent" : { Reference(Device) } // The parent device
}

```

Figure 8 – JSON format of a Device resource in HAPI FHIR

At any time during the development stage of TeNDER project, it will be possible to add or discard any of these resources, thanks to the high flexibility and scalability of HAPI FHIR's implementation.

## 2.3 Authorisation and data access

HAPI FHIR does not provide a single one-size-fits-all security layer. Instead, it provides a number of useful tools and building blocks that can be built around as a part of the overall security architecture. Because HAPI FHIR's REST server is based on the Servlet API, one may use any security mechanism which works in that environment, such as:

- Authentication (AuthN) to verify that the user is who they say they are, which is typically accomplished by testing a username/password in the request, or by checking a "bearer token" in the request.
- Authorisation (AuthZ) to verify that the user is allowed to perform the given action. For example, in a FHIR application, one might use AuthN to test that the user making a request to the FHIR server is allowed to access the server, but that test might determine that the requesting user is not permitted to perform write operations and therefore block a FHIR create operation (both AuthN and AuthZ in action).
- Consent and Audit to verify that a user has rights to see/modify the specific resources they are requesting, applying any directives to mask data being returned to the client (either partially or completely), and creating a record that the event occurred.

For Authentication, the team relied on an instance of Keycloak<sup>119</sup>, the well-known open-source Identity and Access Management. Keycloak handles the user authentication and provides an authorisation token that is sent along the requests to HAPI FHIR APIs and processed by an **AuthorizationInterceptor** for permission grant validation, as described in the official website, where the following image is provided<sup>120</sup>:

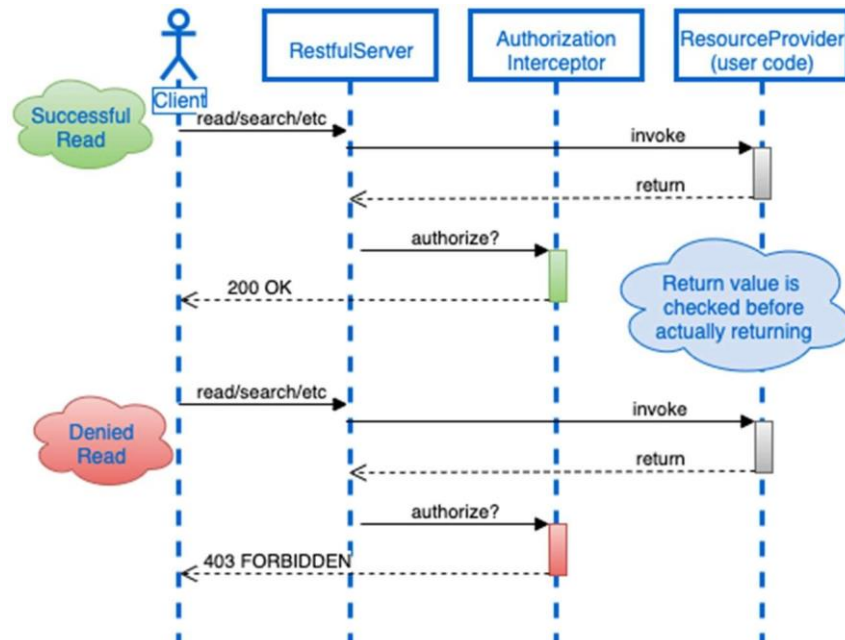


Figure 9 – Authorising READ Operations in HAPI FHIR

<sup>119</sup> Keycloak, Open-source Identity and Access Management <https://www.keycloak.org/>

<sup>120</sup> HAPI FHIR Authorization Interceptor [https://hapifhir.io/hapi-fhir/docs/security/authorization\\_interceptor.html](https://hapifhir.io/hapi-fhir/docs/security/authorization_interceptor.html)

As described in HAPI FHIR’s official website with technical documentation:

*“The AuthorizationInterceptor works by allowing you to declare permissions based on an individual request coming in. In other words, you could have code that examines an incoming request and determines that it is being made by a Patient with ID 123. You could then declare that the requesting user has access to read and write any resource in compartment "Patient/123", which corresponds to any Observation, MedicationOrder etc with a subject of "Patient/123 ". On the other hand, another request might be determined to be made by an administrator user and could be declared to be allowed to do anything”.*

An example of these authentication and authorisation flows with the existing deployment of WP5 and Maggioli’s cloud environment is demonstrated in the following screenshots below:

**(1) Retrieving Keycloak for an Access Token to retrieve information from HAPI FHIR:**

```

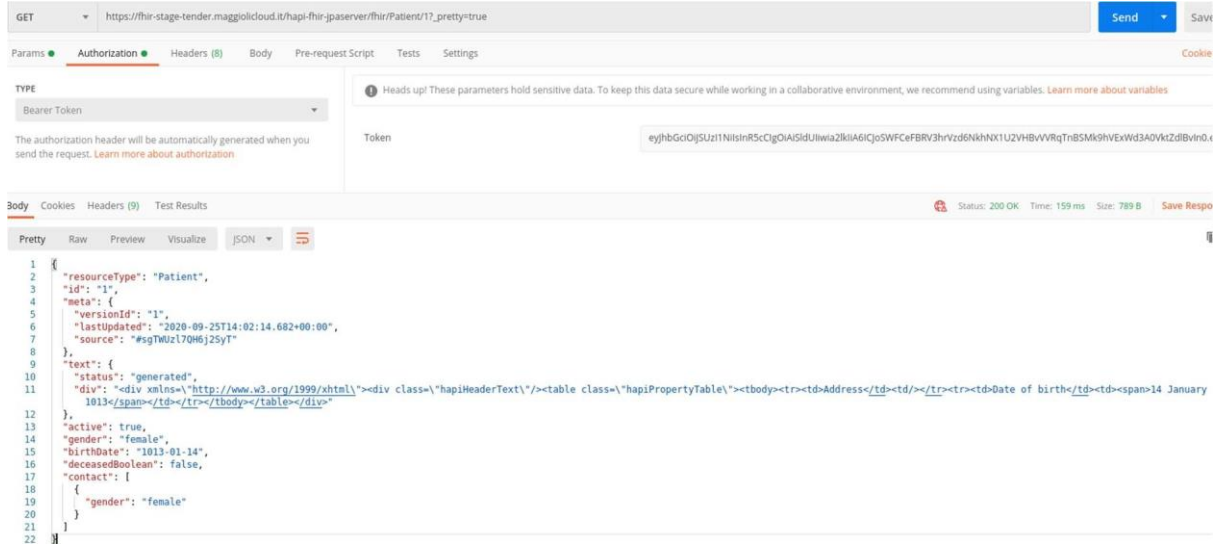
1 {
2   "access_token": "eyJhbGciOiJIUzI1NiIsInR5cCI6IWRX",
3   "expires_in": 3600,
4   "refresh_token": "eyJhbGciOiJIUzI1NiIsInR5cCI6IWRX",
5   "scope": "email openid profile"
6 }
    
```

**(2) Creating a Patient resource using the token retrieved before.**

```

1 {
2   "resourceType": "Patient",
3   "id": "1",
4   "meta": {
5     "versionId": "1",
6     "lastUpdated": "2020-09-25T14:02:14.682+00:00"
7   },
8   "text": {
9     "status": "generated",
10    "div": "<div xmlns='http://www.w3.org/1999/xhtml'><div class='hapiHeaderText'><table class='hapiPropertyTable'><tbody><tr><td>Address</td><td>1013</td></tr><tr><td>Date of births</td><td>14 January 1013</td></tr></tbody></table></div>"
11  },
12  "active": true,
13  "gender": "female",
14  "birthDate": "1013-01-14",
15  "deceasedBoolean": false,
16  "contact": [
17    {
18      "gender": "female"
19    }
20  ]
21 }
    
```

**(3) Retrieving the patient’s information with the access token (which would not be authorised without it).**



The screenshot shows a REST client interface with the following details:

- Method:** GET
- URL:** `https://fhir-stage-tender.maggiolcloud.it/hapi-fhir-jpaserver/fhir/Patient/1?_pretty=true`
- Authorization:** Bearer Token. The token value is `eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXLTJkIiwiaWF0IjoiMjAyMjA4MjQyMzY1In0=`.
- Response Status:** 200 OK, Time: 159 ms, Size: 789 B.
- Response Body (JSON):**

```
1 {
2   "resourceType": "Patient",
3   "id": "1",
4   "meta": {
5     "versionId": "1",
6     "lastUpdated": "2020-09-25T14:02:14.682+00:00",
7     "source": "#sgTmZl7Qh6j25yT"
8   },
9   "text": {
10    "status": "generated",
11    "div": "<div xmlns='http://www.w3.org/1999/xhtml'><div class='hapiHeaderText'><table class='hapiPropertyTable'><tbody><tr><td>Address</td></tr><tr><td>Date of birth</td><span>14 January
12 1013</span></td></tr></tbody></table></div>"
13  },
14  "active": true,
15  "gender": "female",
16  "birthDate": "1013-01-14",
17  "deceasedBoolean": false,
18  "contact": [
19    {
20      "gender": "female"
21    }
22  ]
23 }
```

The **AuthorizationInterceptor** examines all the client requests to determine whether "writing" operations are authorised, as well as looking at the response from the server to determine whether "reading" operations are legal, as shown in the images before. Despite causing performance implications (since the server fetches data even though users might not be authorized to read it), the mechanism protects other features in HAPI FHIR which could cause the server to show data to users who do not have permissions to do so.

### **3. Conclusions**

FHIR (Fast Healthcare Interoperability Resources) is a powerful standard for exchanging electronic health records, with a robust implementation by the open-source community. HAPI FHIR fulfils the requirements for TeNDER, namely the ones that concern data collection on patients' health status, their activities, but especially the observation of their quality of life. Throughout the project's pilots, it will be possible to assert all the capabilities of this standard, by validating the data access and usage within the different TeNDER's High-Level Services (HLS).

Further developments are required to ensure that the implementation complies with EU regulation on data access and security, as well as with the different member-states' policies and privacy laws. The outcomes of the testing activities, and the compliance with the aforementioned policies, will be demonstrated both in D5.4 and D5.5, as well as reported in the integrated deliverables from WP6 with the rest of the results of the pilots performed during the project.