EU4Digital

EU4Digital: supporting digital economy and society in the Eastern Partnership

Common Guidelines for eHealth Harmonisation and Interoperability

December 2020
Version 1.0

Key terms and definitions

Term	Definition
Catalogues (to find reusable resources)	Help administrations find reusable resources (e.g. services, data, software, data models). Various types of catalogues exist, e.g. directories of services, libraries of software components, open data portals, registries of base registries, metadata catalogues, catalogues of standards, specifications and guidelines. Commonly agreed descriptions of the services, data, registries and interoperable solutions published in catalogues are needed to enable interoperability between catalogues[1]
Common harmonisation and interoperability guidelines and standards (CHIGS)	A document dedicated to the Eastern partner countries as a deliverable of eHealth stream in the project "EU4Digital: Supporting digital economy and society in the Eastern Partnership", carried out by an EY led international consortium
Common eHealth assessment framework	The defined Common eHealth assessment framework serves as a basis for preparing the set of harmonisation and interoperability guidelines and standards for the Eastern partner countries in line with relevant EU norms
Connecting Europe Facility (CEF)	A key EU funding instrument to promote growth, jobs and competitiveness through targeted infrastructure investment at European level
Digital Health	An umbrella term for a wide range of digital technologies associated with health, healthcare, living, and society to improve healthcare delivery and support personalised and precision medicine
Digital Health governance	Governance for digital health aims to strengthen the capabilities and skills needed for countries to promote, innovate and scale up digital health technologies
Digital Service Infrastructure (DSI)	A term describing foundational services that are necessary to the information technology capabilities of a modern society
Digital Single Market	A definition where the free movement of persons, services and capital is ensured and where the individuals and businesses can seamlessly access and engage in online activities under conditions of fair competition, and a high level of consumer and personal data protection, irrespective of their nationality or place of residence[2]
Digital Transformation of Health and Care	A part of Digital Single Market empowering citizens and building a healthier society
The Eastern Partnership	The Eastern Partnership is a joint initiative of the European External Action Service of the European Union together with EU, its Member States, and six Eastern European Partners governing its relationship with the post-Soviet states of Armenia, Azerbaijan, Belarus, Georgia, Moldova, and Ukraine
Eastern partner countries	The term stands for the six Eastern neighbourhood countries: Armenia, Azerbaijan, Belarus, Georgia, Moldova, and Ukraine
European Commission (EC)	A group appointed by agreement among the governments of the EU, which initiates Union action and safeguards its treaties.
eDispensation (eD)	Represents the act of electronically retrieving a prescription and giving the medicine to the patient. Once the medicine has been dispensed, a report on the items dispensed is sent to the prescriber in a structured format
eHealth Digital Service Infrastructure (eHDSI)	The term used for the generic and core services for the cross-border health data exchange under the Connecting Europe Facility financing
eHealth	The World Health Organisation defines eHealth as the use of information and communication technologies (ICT) for health[3]

1 National Interoperability Framework Observatory https://joinup.ec.europa.eu/collection/nifo-national-interoperability-framework-observatory/glossary

2 Shaping the Digital Single Market https://ec.europa.eu/digital-single-market/en/policies/shaping-digital-single-market

3 eHealth at WHO https://www.who.int/ehealth/about/en/

Term	Definition
eHDSI Member State Expert Group (eHMSEG)	Composed of Technical, Semantic or Organisation Experts according the configuration, nominated by the participating Member States. It performs the operational impact assessment
Electronic Health Record Exchange Format (EHRxF)	Seeks to facilitate the cross-border interoperability of EHR, currently being developed by EC, the recommendation released in 2019
eIDAS Network	The technical infrastructure which connects the national eID schemes
European Interoperability Framework	A part of the Communication (COM(2017)134) from the European Commission adopted on 23 March 2017. The framework gives specific guidance on how to set up interoperable digital public services. It offers public administrations 47 concrete recommendations on how to improve the governance of their interoperability activities, establish cross-organisational relationships, streamline processes supporting end-to-end digital services, and ensure that both existing and new legislation do not compromise interoperability efforts[1]
The European Interoperability Framework (EIF) principles	The fundamental behavioural aspects to drive interoperability actions. There are 12 principles relevant to the process of establishing interoperable European public services. They describe the context in which European public services are designed and implemented[1]
Electronic Health Record (EHR)	A collection of longitudinal medical records or similar documentation of an individual in digital form. This set of health information based on the principle one EHR per patient in a country
ePrescription (eP)	A tool to generate prescriptions electronically. It is generally understood as a prescriber's ability to electronically send an accurate, error-free and understandable prescription directly to a pharmacy from the point-of-care. ePrescription is also used by nurses to administer medicines and by pharmacies to review orders and manage the supply of medicines
European Reference Network (ERN)	A virtual network comprised of healthcare professionals spread around Europe. Their objective is to tackle complex or rare diseases and conditions that necessitate highly specialised treatment and a concentration of knowledge and resources[4]
EU4Digital Facility	A three-year programme promoting key areas of the digital economy and society, in line with EU norms and practices
Health Care Provider (HCP)	An individual healthcare professional or a healthcare institution licensed to provide medical care
Health Level 7 (HL7)	A framework (and related standards) for the exchange, integration, sharing, and retrieval of electronic health information. These standards define how information is packaged and communicated from one party to another, setting the language, structure and data types required for seamless integration between systems
Information Society	Describes a society where a significant degree of activity focuses on the creation, distribution, use and reuse of information. This activity takes place using what is known as information and communication technologies (ICTs)
Integrated Public Services	In the public sector context, integrated services refer to the result of bringing together government services so that citizens can access them in a single seamless experience based on their wants and needs. Integration enables public agencies to share their objectives across organisational boundaries, whereby information and services can be shared among ministries and government entities in a way that avoids data redundancy, boosts up the efficiency of internal processes and ultimately provides citizens with high quality services and improved levels of governmental interaction[1]

4 European Reference Network http://www.ern-rnd.eu/about-us/#:~:text=A%20European%20Reference%20Network%20%28ERN%29%20is%20a%20virtual,treatment%20and%20a%20concentration%20of%20knowledge%20and%20resources

Term	Definition
International Statistical Classification of Diseases and Related Health Problems, Tenth Revision (ICD-10)	The purpose of the ICD is to permit systematic recording, analysis, interpretation and comparison of mortality and morbidity data collected in different countries or areas and at different times. The ICD is used to translate diagnosis of diseases and other health problems from words into an alphanumeric code, which permits easy storage, retrieval and analysis of the data[5]
Integrating the Healthcare Enterprise (IHE)	An initiative by healthcare professionals and industry to improve the way computer systems in healthcare share information
Interoperability	The ability of different systems, organisations or countries to exchange health information and use it meaningfully. That means the participants must be able to understand and interpret the shared information correctly, which basically means using the same standards and processes to provide an eHealth service
Legislative framework	The body of policies, legislation and regulations, at national, regional and local level, governing a particular area
Logical Observation Identifiers Names and Codes (LOINC)	A terminology for laboratory and clinical observations to send clinical data electronically
Mobile health (mHealth)	The practice of healthcare supported by mobile devices
National Contact Point (NCP)	Independent organisations (Ministries, Academies of Science, Research agencies) that act as information providers to European Research Council applicants in their native language
National Contact Point for eHealth (NCPeH)	Independent organisations (Ministries, Academies of Science, Research agencies) that act as information providers to European Research Council applicants for eHealth in their native language
National eHealth Strategy (NeHS)	A national level strategy setting out a range of measures for the increased use of digital technologies to support delivery of healthcare services
OpenNCP	epSOS pilot-based component available as NCP software, available to public
Patient Summary	A standardised set of basic medical data that includes the most important clinical facts required to ensure safe and secure healthcare. This summarised version of the patient's medical data gives health professionals the essential information they need to provide care in the case of an unexpected or unscheduled medical situation (e.g. emergency or accident)
Public Key Infrastructure (PKI)	A set of roles, policies, hardware, software and procedures needed to create, manage, distribute, use, store and revoke digital certificates and manage public-key encryption
Refined eHealth European Interoperability Framework (ReEIF)	Provides a common framework of terms and methodologies that serves as a key instrument to address eHealth interoperability issues
Regulatory Authority	A public authority or government agency responsible for exercising autonomous authority over a specific area of activity in a regulatory and/or supervisory capacity. Regulatory authorities are commonly set up to enforce safety and standards, and/or to protect consumers in markets where there is a lack of effective competition
Trans European Service for Telematics between Administrations system (TESTA)	The private IP-based network of the European Union
The Systematized Nomenclature of Medicine (SNOMED)	Medical terminology covering most areas of clinical information such as diseases, procedures, pharmaceuticals etc.

5 WHO ICD-10 https://ec.europa.eu/cefdigital/wiki/display/EHSEMANTIC/WHO+ICD-10+The+International+Statistical+Classification+of+Diseases+and+Related+Health+Problems+10th+Revision?

Table of contents

About this document

The common harmonisation and interoperability guidelines and standards (CHIGS) is a document dedicated to the Eastern partner countries as a deliverable of eHealth stream in the project “EU4Digital: Supporting digital economy and society in the Eastern Partnership”, carried out by an EY led international consortium.

The present document provides a set of proposed recommendations regarding the current state of eHealth in the Eastern partner countries and current eHealth trends and directions in the EU, as well as guidelines for eHealth harmonisation and interoperability in the Eastern partner countries.

Background

eHealth as a whole, can be defined as a set of measures and capabilities supporting execution of healthcare and wellness activities with the help of information and communication technologies. Both, country-level and cross-border eHealth development and operations comprise a long-term initiative encompassing the multi-aspect approach. The common eHealth assessment framework proposed that the six Eastern partner countries are at the halfway point in relation to the EU eHealth baseline and together face common cross-border eHealth challenges. Within the EU4Digital facility we the typical view on the interoperability from legal, organisational, semantic and technical aspects has been extended to the aspects that of financial sustainability, technology meaningfulness, people skills & capability building and the reality of the stakeholder ecosystem. The document with proposed recommendations was built highlighting the importance of common region-wide actions to kick start harmonisation in the most impactful and effort-effective way by re-using the existing work from the EU space, especially in the areas, where the EU has made significant progress.

Objective of the activity

To develop the CHIGS for the Eastern partner countries, in line with relevant EU aspects in eHealth. This includes consideration of aspects like eHealth service categorisation, the functionality of eHealth systems, data exchange, cyber-security, system interoperability, health records, national legislation, and eHealth capability building.

Overall approach

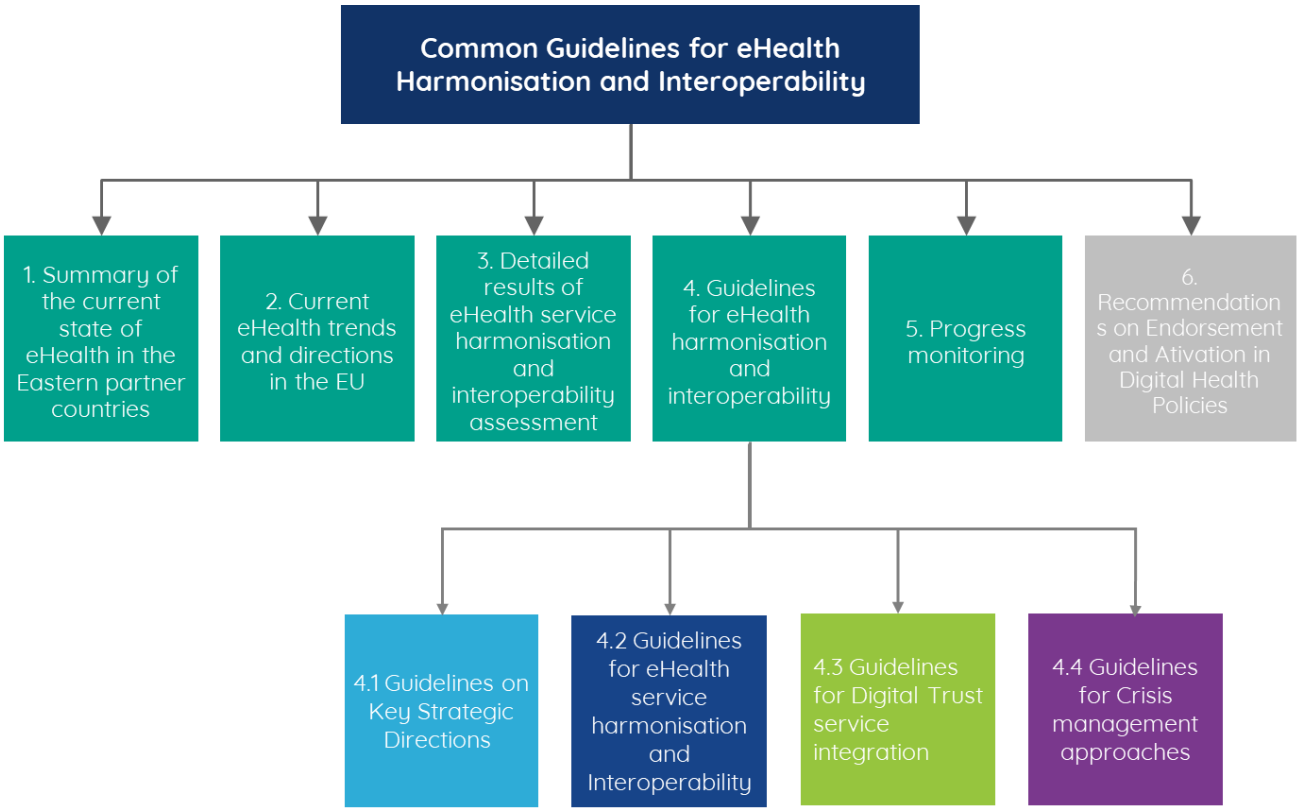
This document was developed following recommended activities provided in common eHealth assessment framework, reusing the EU developed assets and building on joint work with EU4Digital Trust & Security stream (extending and re-using of the corresponding deliverables, especially in areas of eID, data privacy, cybersecurity and data exchange infrastructure). The document was prepared for the Eastern partner countries in line with relevant EU norms – by the defined scope, priorities, and for publishing as defined. The document was prepared following clearly defined structure aiming to include proposed recommendations based on several different angles of eHealth. The CHIGS includes the summary of the current state of eHealth in the Eastern partner countries and current eHealth trends and directions in the EU, as well as common guidelines for eHealth harmonisation and interoperability, guidelines for the progress monitoring, and strong endorsement and common Eastern Partnership digital health policy.

Value delivered

The CHIGS document has been prepared for the Eastern partner countries, considering legal, organisational, semantic and technical interoperability categories and related aspects.

Summary of the common harmonisation and interoperability guidelines and standards

The following CHIGS document has been produced to ensure both, country and cross-border healthcare interoperability. Included in this document is a collection of key guidance and advice for a range of national health bodies across the Eastern partner countries. The purpose of this chapter is to introduce high-level guidelines for strategic leadership, providing the prospects for long-term success in eHealth. This set of guidelines is for use by all involved in eHealth interoperability – including healthcare providers, management and administration, and national regulatory authorities. Each guideline is of a high methodological quality and has been developed through an evidence-based process. Later in this chapter, more detailed guidelines and recommendations follow. Each detailed guideline is a result of high-level guidelines being applied to more specific individual components of eHealth interoperability. Classified by different topics these guidelines concern individual healthcare management and administration bodies.



I. High level guidelines for strategic leadership

Guidelines on Key Strategic Directions	R.1	Create, approve and regularly update a comprehensive and actionable national eHealth strategy that defines priorities, principles and activities for capturing and aggregating meaningful data
	R.2	Establish a robust financing and operational model so that project-based eHealth ecosystem matures to an interoperable health data ecosystem
	R.3	Establishing and operationalising comprehensive digital health governance model for control of data quality and useful purpose to be created
	R.4	Digital Health Architecture Development and Governance for Interoperability, reusability and integrated health data-rich services
	R.5	Strong cybersecurity capabilities and strategic thinking towards securing the data collected, stored and trusted by your citizens
	R.6	Safe and rich data can only provide health value, if it is well explored and used, a Data Usage Strategy more than ad-hoc initiatives is key to this realization
Guidelines for eHealth service harmonisation and Interoperability	R.7	Provide user-oriented eHealth services that are accessible and easy to use
	R.8	Provide multilingualism in public services
	R.9	Ensure that data collected and generated by public administrations is published as open data
	R.10	Increase transparency of Digital Services
	R.11	Develop Semantic interoperability capabilities nationally and regionally
	R.12	Enhance legal interoperability by implementing interoperability and digital checks on existing legislation
	R.13	Enhance organisational infrastructure promoting whole of the government approach and reusability
	R.14	Develop and connect to HCP information systems to the National eHealth Interoperability platform
	R.15	Digitise and integrate Healthcare sector registries and information systems to National eHealth Interoperability platform to achieve the single point of access to health information resources
	R.16	Adopt Health Information management standards and vocabularies
	R.17	Develop adequate eHealth application functionality/use cases to support patient, doctor and regulator needs
	R.18	Develop national Patient Summary eService in compliance with EU requirements for future cross-border pilot capability
	R.19	Develop national ePrescription eService in compliance with EU requirements for future cross-border pilot capability
Guidelines for Digital Trust service integration	R.20	Enhance legal maturity for the Digital Trust Services regulations
	R.21	Implement digital and interoperable by design systems and services which are aligned with defined architecture frameworks
	R.22	Enhance DSI legal interoperability including cross-border personal data movement regulation for identification of persons
	R.23	Develop DSI technical interoperability by creating/ re-using digital and interoperable by design, and aligned with defined architecture frameworks for easy Digital Trust services integration and reliable scalability
	R.24	Integrate and re-use technical interoperability capabilities for identification of Health care sector professionals and patients
	R.25	Create alternative, yet open standards based and commonly/ widely used for identification and authentication

Guidelines for Crisis management approaches	**R.26**	Embark on eHealth interoperability and public sector interoperability platforms to effectively respond to crisis
	R.27	Support rapid deployment of cloud and mobile applications, data-driven crisis experience management
	R.28	Adopt e-Learning at scale to ensure daily practice sharing and update
	R.29	Have back-up capabilities in place for crisis management mobilisation
	R.30	Establish culture and processes to support/ enable remote work

II. Guidelines on Key Strategic Directions

R.1 Create, approve and regularly update a comprehensive and actionable national eHealth strategy that defines priorities, principles and activities for capturing and aggregating meaningful data
R.1.1 Work on a two-layer National eHealth Strategy: (1) Digital Health aspects are maintained; (2) steps to ensure interoperable eHealth ecosystem
R.1.2 Conduct a comprehensiveness test to your strategy, avoiding common pitfalls (see Table 27) and ensuring external expertise and advise is used to leap-frog into new ways of doing eHealth
R.1.3 Identify and ensure that the six pillars of a solid NeHS are secured (see Table 28)
R.1.4 Conceive the NeHS in a double layer approach taking enough attention to its implementation and stakeholder involvement
R.1.5 Design 10-year strategy, 5-year programmes and annual activity plans with realistic yet progressively more ambitious targets and key performance indicators

R.2 Establish a robust financing and operational model so that project-based eHealth ecosystem matures to an interoperable health data ecosystem
R.2.1 Establish a robust operational and financing model of Digital Health to sustain the operation of the so far achieved results and continuity of the further development (creation, maintenance and update) of the Digital Health Infrastructure, Services and Capabilities. Including, the definition of the key/common criteria for funding decision making of digital health initiatives
R.2.2 Establish interdependencies between financing, data quality and interoperability implementation to create adequate incentive schema for organisations to benefit from adopting and using digital health
R.2.3 Align public funding with the interoperable ecosystem to favour its behaviours
R.2.4 Follow the widely recognised (EU and international levels) Refined eHealth European Interoperability Framework and e-accessibility specifications when planning, conducting and controlling procurements

R.3 Establishing and operationalising comprehensive digital health governance model for control of data quality and useful purpose to be created
R.3.1 Establish and operationalise Digital Health Governance, including the governance instruments to involve different stakeholders of the digital health ecosystem
R.3.2 Establish a clear link between the NeHS and the eHealth governance
R.3.3 Define aims and principles for the governance framework
R.3.4 Introduce new acts and laws establishing the principles and self-sustainability elements of the National Digital Health Agency and governance bodies and frameworks
R.3.5 Ensure that adequate capacity is allocated to the relevant authorities and technical support bodies involved in digital health governance

R.4 Digital Health Architecture Development and Governance for Interoperability, reusability and integrated health data-rich services
R.4.1 Define and establish mechanism for Digital Health Architecture and governance development, including the mechanisms for selection, prioritization and adoption of standards and common requirements on digital health capabilities, services and solutions
R.4.2 Establish eHealth architecture allowing rapid changes, for example, incorporation of new data elements as they arise. Such architecture supports portability and safe and secure development and integration of innovations
R.4.3 Build a unique identifier for patients and healthcare professionals enabling to exchange data with a full audit trail. For businesses, to provide customizable and adaptable operational systems that would ensure clinical and operational data relevance and meet business needs
R.4.4 Build upon existing rules and standards that govern access and content management. Refer to semantic and technical interoperability examples of internationally accepted rules and standards
R.4.5 While connecting with and contributing to, local, national and international health information systems, ensure continuous health information creation and collection
R.4.6 Accommodate heterogeneity across eHealth services to allow seamless information access from multiple sources
R.4.7 Establish governance and cybersecurity component in eHealth to ensure secure, safe and reliable handling of personal health and social care data
R.4.8 Introduce the Enterprise Architecture discipline to the national eHealth efforts and ensure that the overall system complexity is mapped with relevant and existing methods and IT tools

R.5 Strong cybersecurity capabilities and strategic thinking towards securing the data collected, stored and trusted by your citizens
R.5.1 Create a sub-strategy of the NeHS, within the framework of existing national cybersecurity guidance and the overall NeHS objectives
R.5.2 Define a sectorial governance model for cybersecurity in articulation with national governance
R.5.3 Ensure interoperability definitions and standards are dictated and audited by an authoritative institution
R.5.4 Introduce enterprise architecture training to technical staff and ensure it is meaningful to the mapping of healthcare reality
R.5.5 Establish good collaboration with national trust service providers and overseeing ministries, to ensure that access to health information is provided via secure architecture solutions

R.6 Safe and rich data can only provide health value, if it is well explored and used, a Data Usage Strategy more than ad-hoc initiatives is key to this realization
R.6.1 Prepare and approve the Health Data Law, clarifying roles, responsibilities and potential usage, and securing FAIR principles are to be put in place
R.6.2 Create, curate and maintain the National Health Data Dictionary and Data Cycle Policy
R.6.3 Defend core values for health data usage, through proactive use of instruments such as policy, funding and incentive programs
R.6.4 Foster interface between health sector and data science fields
R.6.5 Promote interoperable solutions, and internationally recognised data standards and terminologies

III. Guidelines for eHealth service harmonisation and Interoperability

R.7 Provide user-oriented eHealth services that are accessible and easy to use
R.7.1 Ensure the availability of multiple channels in accessing public services
R.7.2 Ensure the existence of a single point of contact in order to hide internal administrative complexity and facilitate user's access to public services
R.7.3 Establish mechanisms that involve users in analysis, design, assessment and further development of public services
R.7.4 Initiate the implementation of once-only principle and relevant-only principle for data collection

R.8 Provide multilingualism in public services
R.8.1 When establishing new public services use information systems and technical architectures that provide options for multilingualism
R.8.2 Decide on the level of multilingualism support in public services based on the expected end-users' needs

R.9 Ensure that data collected and generated by public administrations is published as open data
R.9.1 Publish the public data as open data unless certain restrictions apply

R.10 Increase transparency of Digital Services
R.10.1 Ensure internal visibility and availability of external interfaces for public services – opening up specifications of digital health services
R.10.2 Foster transparency-by-design especially relevant for systems requiring consent or that use/formulate algorithms for actions

R.11 Develop Semantic interoperability capabilities nationally and regionally
R.11.1 Perceive data and information as public assets that are appropriately generated, collected, managed, shared, protected and preserved
R.11.2 Put in place an information management strategy to avoid fragmentation and duplication, and to ensure meaningful use of data. Management of metadata, master data and reference data should be prioritised
R.11.3 Support the establishment of sector-specific and cross-sectoral communities that aim to create open information specifications and semantic dictionaries, and encourage the relevant communities to share their results on national and international platforms

R.12 Enhance legal interoperability by implementing interoperability and digital checks on existing legislation
R.12.1 Implement 'Interoperability checks' which could be used to screen legislation to identify any barriers to interoperability
R.12.2 Implement the 'digital check' on legislation to establish the public service and consider data protection requirements

R.13 Enhance organisational infrastructure promoting whole of the government approach and reusability
R.13.1 Apply the whole-of-government approach to interoperability e.g. reusability of infrastructures and services
R.13.2 Implement the processes for appropriately generating and/or collecting data and information which would be perceived as a public asset
R.13.3 Implement the processes for appropriately managing, sharing, protecting data and information
R.13.4 Implement the long-term preservation policy for information usage, especially for information that is exchanged across the borders
R.13.5 Implement the policy for transparency assurance
R.13.6 Design the processes which would help to monitor the implementation of relevant standards and specifications and check the compliance and the interoperability
R.13.7 Document business processes using commonly accepted modelling techniques
R.13.8 Implement the service (level) management plan or similar including the definition of functions, roles and responsibilities of the minimum required processes (i.e. incident, problem, change, configuration, and service level management) and support organisation
R.13.9 Implement the control measures to ensure that all users are assigned only with the necessary rights for performing their specific duties on the systems and services; and that these rights are revised and can be revoked as necessary
R.13.10 Implement the in-country disaster recovery plan
R.13.11 Ensure the continuity and availability of service (set of SLAs)

R.14 Develop and connect to HCP information systems to the National eHealth Interoperability platform
R.14.1 Define common requirements for the HCP IS including clinical processes and resource management use cases
R.14.2 Implement local, University and Regional hospitals medical information systems based on the defined common requirements
R.14.3 Aid in integrating the HCP IS to the National eHealth Interoperability platform
R.14.4 Define interoperability checks and HCP IS compliance audits ensuring that HCP systems are able to integrate with the National eHDSI for initial solution validation as well as periodic checks

R.15 Digitise and integrate Healthcare sector registries and information systems to National eHealth Interoperability platform to achieve the single point of access to health information resources
R.15.1 Continue development towards optimisation of Health Care sector electronic Registers and information system by raising the same common security and functionality standards to inhouse or licenced systems for clinical process and resource management systems
R.15.2 Define a semantic interoperability roadmap and progressively adopt SNOMED CT and other relevant terminologies
R.15.3 Implement and optimise the use of information systems in public health processes

R.16 Adopt health information management standards and vocabularies
R.16.1 Based on the eHDSI Semantic Services Specifications, it is recommended to use coding systems such as ICD-10, ICD-9-CM, SNOMED-CT, LOINC, ATC and EDQM Standard Terms
R.16.2 Establish officially defined or at least of consolidated systems/services to perform transcoding

R.16 Adopt health information management standards and vocabularies
R.16.3 Establish controlled vocabularies (e.g. terminologies or taxonomies) to express valid value sets of coded concepts
R.16.4 Ensure availability of information on the description of the dataset including content, syntax and format in the directive of ePrescriptions and eDispensations as well as Patient Summary for unscheduled care
R.16.5 Ensure information is always provided in a way that the essential original semantics (meaning and expressiveness of sensible information) as imposed by the data-producer are preserved and understandable to the data-consumer

R.17 Develop adequate eHealth application functionality/use cases to support patient, doctor and regulator needs
R.17.1 Establish the technical implementation of services, for example, Directive Patient Summary for unscheduled care
R.17.2 Implement attributes for identification, authentication and authorisation of the HCP (prescriber and dispenser) and the patient. The eHDSI Identity Management Specification suggests collecting biometric characteristics such as retina pattern, fingerprints, iris pattern, voice, face image and handwriting, etc. In addition, the identification, authentication and authorisation methods should be applied based on the business case defined by common information security and data protection policies and regulations
R.17.3 Implement common/ interoperable components for electronic identification, and trusted access of HCPs. The eHDSI Identity Management Specification suggests implementing unique identifiers for the authentication of the HCPs. Authentication process should use, if available, national interoperability gateways
R.17.4 Implement mechanisms of identification and authentication of the patient. The eHDSI Identity Management Specification suggests implementing unique identifiers for the authorisation of the patient. Patient authentication can also proceed with demographic data and/or via country's interoperability portal/gateway

R.18 Develop national Patient Summary eService in compliance with EU requirements for future cross-border pilot capability
R.18.1 The Patient Summary dataset should include a mandatory field for *National Healthcare Patient ID*
R.18.2 The dataset should include a mandatory field for *Given Name*, *Family Name/Surname* and *Date of Birth*
R.18.3 The dataset should include a mandatory field for *Country of Residence*
R.18.4 The dataset should include a mandatory field for *Date of Last Update*[6]

R.19 Develop national ePrescription eService in compliance with EU requirements for future cross-border pilot capability
R.19.1 The dataset for ePrescription (patient identification) mandatory fields should include Given Name, Family Name/Surname, Date of Birth, Regional/National Health ID
R.19.2 The dataset should include the mandatory fields (HP prescriber identification) such as *Given Name*, *Family Name/Surname*, *HP ID Number*, *Profession*, *Specialist*
R.19.3 The dataset should include the mandatory fields (Prescription data) such as *Prescription ID*, *Prescription Item ID*, *National/Regional Medical Product Code*, *Active Ingredient*, *Strength of the Medical Product, Medical Product Package, Pharmaceutical Dose Form, Number of Packages, Posology, Prescription Date of Issue*
R.19.4 The dataset should include the mandatory fields (Dispensed medicine dataset - patient identification) such as *Given Name, Family Name/Surname, Regional/National Health ID*

[6] EU guidance on Patient Summary PS Use Case - eHealth DSI Operations - CEF Digital (europa.eu)

R.19 Develop national ePrescription eService in compliance with EU requirements for future cross-border pilot capability
R.19.5 The dataset should include the mandatory fields (Dispensed medicine dataset - HP dispenser identification) such as *Given Name, Family Name/Surname, Pharmacist ID Number, Dispenser Facility Address*
R.19.6 The dataset should include the mandatory fields (Dispensed medicine data) such as *Dispensed Medicine ID, Prescription ID, Prescription Item ID, Active Ingredient, Strength of the Medicinal Product, Medicinal Product Package, Pharmaceutical Dose Form, Number of Packages, Date of the Dispensed Medicine Event*

IV. Guidelines for Digital Trust service integration

R.20 Enhance legal maturity for the Digital Trust Services regulations
R.20.1 Regulatory clarification of the purpose between the electronic signatures and the electronic seals
R.20.2 Regulatory clarification on the specific requirements for the mechanisms used to achieve the qualified status of digital trust services
R.20.3 Measures should be defined to protect the identifiable personal information contained in the digital trust services, especially qualified digital signatures, from misuse in activities like behaviour profiling without prior user consent
R.20.4 Adoption of internationally accepted standards for information security management and process quality
R.20.5 Performing regular audits of the digital trust services infrastructure and processes using internationally accepted standards
R.20.6 Measures should be defined to ensure the protection of identifiable personal information and their accepted use, especially in the context of widespread cross-border transfer of identifiable personal information between EU member states and the Eastern partner countries

R.21 Implement digital and interoperable by design systems and services which are aligned with defined architecture frameworks
R.21.1 Improve the resilience against cyber-attacks
R.21.2 Deploy endpoint and network-based intrusion detection systems
R.21.3 Integrate security events and information monitoring solutions for the TSP IT ecosystem
R.21.4 Perform regular vulnerability assessments and penetration tests

R.22 Enhance DSI legal interoperability including cross-border personal data movement regulation for identification of persons
R.22.1 Establish regulation for free cross-border movement of personal information between the Eastern partner countries and the EU (eID and eSignature regulations)
R.22.2 Establish legal certainty for identity authentication (eID and eSignature regulations)
R.22.3 Establish legal certainty for foreigners' identification (eID and eSignature regulations)

R.23 Develop DSI technical interoperability by creating/ re-using digital and interoperable by design, and aligned with defined architecture frameworks for easy Digital Trust services integration and reliable scalability
R.23.1 Integrate/ re-use public sector interoperability capabilities for eID and eSignature

R.24 Integrate and re-use technical interoperability capabilities for identification of Health care sector professionals and patients
R.24.1 Establish identity authentication legal certainty for health professionals (data integrity, authenticity and non-repudiation principles) by integrating/ re-using existing public sector infrastructures
R.24.2 Establish common eID-based access services (the connection between eID and healthcare professional ID) by integrating/ re-using existing public sector infrastructures
R.24.3 Establish legal certainty of identity authentication for patients (data integrity, authenticity and non-repudiation principles) by integrating/ re-using existing public sector infrastructures
R.24.4 Establish common eID-based access services (the connection between eID and patient ID) by integrating/ re-using existing public sector infrastructures

R.25 Create alternative, yet open standards based and commonly/ widely used for identification and authentication	
R.25.1 Define the attributes for identity authentication of healthcare specialists (prescriber and dispenser):	**R.25.1.1** eID
	R.25.1.2 Secret data such as passwords or Pin-Codes
	R.25.1.3 ID card, passport, authentication token, certificate, cryptographic keys
	R.25.1.4 Biometric characteristics such as retina pattern, fingerprints, iris pattern, voice, face image, handwriting, etc.
R.25.2 Define the attributes for identity authentication of patient:	**R.25.2.1** eID
	R.25.2.2 Secret data such as passwords or Pin-Codes
	R.25.2.3 ID card, passport, authentication token, certificate, cryptographic keys
	R.25.2.4 Biometric characteristics such as retina pattern, fingerprints, iris pattern, voice, face image, handwriting, etc.

V. Guidelines for Crisis management approaches

R.26 Embark on eHealth interoperability and public sector interoperability platforms to effectively respond to crisis	
R.26.1 Use the existing digital health platforms:	**R.26.1.1** Provide basic eHealth services, e.g. ePrescription, eReferrals, electronic image sharing services
	R.26.1.2 Connect healthcare professionals via corporate collaboration tools for online and video consultations
	R.26.1.3 Establish AI Chatbots for patient triaging
	R.26.1.4 Ensure that both real-time and historical data is provided to healthcare professionals
R.26.2 Deploy communication channels to enforce patient adherence	
R.26.3 Use AI-driven triage and proximity tracing apps:	

R.27 Support rapid deployment of cloud and mobile applications, data-driven crisis experience management	
R.27.1 Establish epidemic experience management, monitoring and reporting via digital channels:	**R.27.1.1** Establish channels for checking and reporting health status
	R.27.1.2 Implement call centre assistance
	R.27.2.1 Use AI to identify populations at risk
	R.27.2.2 Improve emergency response time

R.27 Support rapid deployment of cloud and mobile applications, data-driven crisis experience management	
R.27.2 Implement predictive analytics for emergency response and recovery:	R.27.2.3 Integrate analysis of big amounts of data into existing crisis management centre
	R.27.2.4 Implement long-term predictive planning based on data collection
R.27.3 Implement data-driven crisis management enablement for planning, resource deployment and response to citizens	

R.28 Adopt e-Learning at scale to ensure daily practice sharing and update
R.28.1 Enhance e-learning strategies
R.28.2 Mobilise national e-learning platforms
R.28.3 Strengthen digital learning delivery

R.29 Have back-up capabilities in place for crisis management mobilisation	
R.29.1 Prioritise the critical services	
R.29.2 Deliver models for mission-critical services:	R.29.2.1 Cross-reference mission-critical services with technological stock
	R.29.2.2 Establish work models for remote, hybrid and on-site services
R.29.3 Crisis management centre mobilization:	R.29.3.1 Establish the crisis command centre integrated with hospitals and health systems
	R.29.3.2 Mobilise resources and assets, i.e. staff and procedures
	R.29.3.3 Crisis management centre mobilisation ensuring an omnichannel integration of the relevant data sources (HCP's medical and asset administration systems) to be visible from a single node
	R.29.3.4 Establish dashboards and analytics to determine capacities and demands (beds, theatres, diagnostics and financing)
R.29.4 Ensure clinical workforce and vital analysis and resource planning:	R.29.4.1 Establish an action plan to reduce non-critical services and optimise virtual care delivery
	R.29.4.2 Optimise processes to let the medical professionals focus on their jobs
	R.29.4.3 Refine schedules, procedures and infrastructures
	R.29.4.4 Establish predictive analytics for modelling workforce needs and vital resources and supplies using Cloud-based tools e.g. Microsoft azure stack

R.30 Establish culture and processes to support/ enable remote work	
R.30.1 Ensure technology readiness, analysis, setup and adoption:	R.30.1.1 Identify organisations' technological readiness and gaps
	R.30.1.2 Identify technological solutions which could be developed rapidly
R.30.2 Design the new smart working model:	R.30.2.1 Develop and establish a virtual model of operations, remote collaboration tools, communications and training
	R.30.2.2 Execute smart working labour contracts to turn a crisis response into a structural smart working
R.30.3 Create training manuals:	R.30.3.1 Prepare the training material for workforce working remotely
	R.30.3.2 Provide communications to formalise the guidelines and inform employees
	R.30.4.1 Use digital tools for smart working with critical processes

R.30 Establish culture and processes to support/ enable remote work	
R.30.4 Draft guidelines:	**R.30.4.2** Determine and mitigate the barriers and risks to large scale workforces working remotely
R.30.5 Begin analysis and benchmarking:	**R.30.5.1** Analyse mission-critical services to ensure quality and continuity during remote working
	R.30.5.2 Prioritise smart working best practices

1 Summary of the current state of eHealth in the Eastern partner countries

The cross-country analysis of eHealth in the Eastern partner countries provides information regarding eHealth legislation and governance, infrastructure and services, funding mechanisms and involvement in the international communities as well as the key findings and insights for each country. Data collected by December 2019.

1.1 eHealth legislation and governance

Currently, none of the Eastern partner countries has formally adopted the national eHealth strategy (NeHS). However, from the earlier time, Armenia and Azerbaijan have approved roadmaps, Belarus, Georgia have approved concepts in different kinds of legal acts, all the countries recognise the need for dedicated eHealth strategy. Moldova and Ukraine are currently in the drafting phase of the eHealth strategies.

Countries that have partially approved the NeHS (having roadmaps and concepts) apply with international standards of eHealth to a different extent (e.g. HL7 and SNOMED are defined in most of the Eastern partner countries).

While Ukraine is the only Eastern partner country that has a legal term of eHealth within the health care legislative framework, the rest of the Eastern partner countries have initiated eHealth legislation – it is either in the approval phase (Armenia, Belarus) or drafting phase (Moldova), however, Georgia has a separate EHR regulation and is planning to have an eHealth definition in the future and Azerbaijan has a digital roadmap where eHealth is mentioned.

Only Georgia and Ukraine have defined eHealth architectural model formally approved. Nevertheless, it is planned to be included in Moldavian NeHS legal framework.

Personal medical information in Eastern partner countries is regulated under the Personal Data Protection Laws without a separate health data regulation. Regarding the data protection regulation compliance to the EU GDPR, only Georgia is mostly in compliance with the EU standards and Armenia and Moldova are in the process of synchronization. However, none of them currently have regulation as strict as GDPR.

Georgia stands out as the only country in the Eastern partner countries that have adopted regulations enabling Patient Summary services (as part of EHR regulations). Also, such document has been drafted by the Ministry of Health in Ukraine too, however, the rest of the Eastern partner countries highlight the priority to create the policy, but currently do not have these regulations.

All of the Eastern partner countries have adopted regulations for the ePrescription service except for Azerbaijan and Moldova.

The governance model with key participants in the eHealth sector is partially defined in the region (Armenia, Belarus, Georgia, Ukraine) as a part of the concept and roadmap documents. Moldova is planning to adopt the definition of the eHealth governance model (main roles and participants) in the NeHS in the future.

Ministries of Health in the Eastern partner countries are typically the responsible bodies for eHealth governing and issuing policies and regulations. Institutions under the ministries are typically the responsible bodies for the execution of eHealth development programs and projects, with exception of MD and GE, where the execution and operation have appeared to be within the Ministry of Health.

1.2 eHealth infrastructure and services

Three out of six Eastern partner countries have been re-using (Armenia, Georgia, Ukraine) or are planning to re-use (Azerbaijan and Moldova) some elements of their public sector (incl. national or regional levels) of IT infrastructure for eHealth services and eHealth IT solutions, including eGovernment services that of eGov portals, eID and eSignature for eHealth digital enablement.

eHealth services are implemented to a different level in the Eastern partner countries. Patient Summary services are operating nationwide in Armenia and Georgia, whereas in the other Eastern partner countries there is no such service implementation yet.

Meanwhile, ePrescription service is implemented in Belarus and Ukraine. In Georgia, ePrescription is used only in Tbilisi area (plans to be implemented nationwide in 2020 were held back by the COVID-19 outbreak with next steps to be decided) while it is running in a pilot phase in Armenia. The number of ePrescriptions issued in 2018 and the first half of 2019 in Belarus was approx. 10,5 million, in Georgia approx. 700 000 and in Ukraine approx. 4 million (from April of 2019 to August 2019).

National patient and health care professionals' portals (with access to EHR) operate in Armenia and Georgia. In Moldova, a health care professionals' portal is operational, whereas a patient portal is not implemented. Azerbaijan is currently in the development of the national patient portal.

The integration of national or private pharmacies information systems with eHealth information systems exists in Belarus, Georgia and Ukraine as they have implemented an ePrescription service, which fulfils prescription and dispensation functionality as well as helps for pharmaceutical reimbursement purposes, in Ukraine, it is available for the reimbursed medicine but planned support for other medicines by 2020.

During our analysis the importance of common vocabulary and semantics became apparent, for example, the name e-Referral in one of the countries refers to a service, which is primarily operated by the Social Service (in this case in a role of a health insurance provider) under Ministry of Health and used to verify whether a patient case is eligible for financial coverage by the social insurance/ financing scheme rather than the use of one HCP to refer a patient to another HCP for consultation, lab test or for further health care service provision, which would be typically understood to carry by its main purpose medical information (as usual would be typical practice in the EU or HL7 terms) rather than administrative HCP-to-Payor interaction.

1.3 Funding and incentives mechanisms for eHealth

Funding in eHealth development and operation in the Eastern partner countries is rather scarce. None of the Eastern partner countries has explicit and validated sustainable funding models to develop and operate the eHealth domain. The operation, maintenance and continuous development of eHealth services, as well as the expansion of IT solutions, are typically funded by with international organisations' funds (i.e. USAID, World Bank etc.), sometimes by the state budget or private funds.

Notably, Belarus has two out of three ongoing projects funded by the state budget and one project funded by the World Bank that relates to the development of the eHealth domain and further development of IT solutions in eHealth till 2022. Ukraine has support from USAID Health Reform Support till 2023 and together with the strongly developed ecosystem of private-sector vendors of eHealth services (HIS/ EMR) for HCPs thus taking over the direct burden from the state in development of HCP-level eHealth solutions and enabling market competition (with the condition if the HCP procurement processes are observed and vendor ICT anti-lock in measures applied).

The Eastern partner countries neither have dedicated research funds to support eHealth research programmes nor provide incentives or funding to the private sector for the development of eHealth applications and services, and research in eHealth. Similarly, none of the Eastern partner countries provides funding mechanisms or initiatives to support the use of eHealth services among citizens.

1.4 Involvement in international communities

The involvement of the Eastern partner countries in international eHealth interoperability communities is rather low. All the countries are engaged with WHO, however, there is low involvement with the HL7 community (Belarus, Georgia[7] and Ukraine planned) and Central European Initiative (CEI) (Belarus, Ukraine, Moldova). Ukraine is also involved in the EIP on AHA activities.

However, the countries are interested in getting different eHealth practice examples and are engaged in the analysis of existing models in the EU.

7 HL7 International, https://www.hl7.org/about/yellowpages/index.cfm?membership_type_code_gomembers=GPU&co_fullname=georgia&Submit=Search

2 Current eHealth trends and directions in the EU

The development and implementation of eHealth solutions in healthcare systems is a national competence. However, current eHealth trends and directions in the EU outline some sharable practices and recommendations for tackling various eHealth-related issues. Through coordinated actions and digital alignment, some aspects of interoperability and quality standards can be addressed at the EU level.

The EU provides three fundamental documents, described in **Table 1**, that currently shape the efforts towards research and development, interoperability and harmonization, and eHealth implementation projects.

Table 1: Fundamental eHealth development documents provided by the EU

The EU documents:
Digital Single Market Strategy[8]
eHealth Network multi-annual workplan form 2018-2021 (MWP 18-21)[9]
Communication on Digital Transformation of Health and Care (2018)[10]

The need for interoperability and harmonisation in the healthcare system is growing. However, since the publication of the cross-border care directive (DIRECTIVE 2011/24/EU), there is also a growing legal imperative for cooperation. As communications and digital markets are regulated at the EU level the Digital Single Market strategy acts as a powerful enabler influencing cooperation in the areas of eHealth and Digital Transformation. The Digital Single Market strategy has already initiated ongoing support actions, namely EU4digital, and also with regards to eHealth it has meant important energy towards standardization of digital healthcare.

The MWP 18-21 together with the Joint Action (eHAction[11]) identify four areas of work: patient empowerment; innovative use of data (big data); enhancing continuity of care (the development of the eHDSI), including the addition of new healthcare domains; overcoming implementation challenges.

Finally, the communication on Digital Transformation of Health and Care 2018, layout the priorities to follow in the coming years. The EU Member States and the European Commission (EC) prepared the foundation for the first Recommendation on the European Electronic Health Record exchange format (EHRxF)[12]. Based on the EHRxF, the eHealth Network approved important recommendations on the interoperability ecosystem[13] and funding criteria. This, for the first time, linked funding of projects and structural funds to interoperability solutions and harmonization efforts. This also set the basis for directing the EU funding to the future development of a Multi-Annual Financial Framework (MFF 2021-2027)[14]. The three recent tendencies of focus from the European Commission which deserve special attention, became: Genomics[15], Artificial Intelligence and the European (Health) Data Space.

2.1 eHealth legislation and governance

The two pieces of legislation that relate to eHealth are the DIRECTIVE 2011/24/EU on the application of patients' rights in cross-border healthcare[16], and the General Data Protection Regulation (GDPR). Together these

8 The DSM Strategy, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52015DC0192

9 The MWP 2018-2021 of the eHealth Network, https://ec.europa.eu/health/sites/health/files/ehealth/docs/ev_20171128_co01_en.pdf

10 The Communication on enabling the digital transformation of health and care in the Digital Single Market; empowering citizens and building a healthier society, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A233%3AFIN

11 The Joint Action to support the eHealth Network, is running from June 2018 to June 2021, coordinated by SPMS, Portugal and is named eHAction, http://ehaction.eu/

12 Commission Recommendation on a European Electronic Health Record exchange format (C (2019)800) of 6 February 2019, https://ec.europa.eu/digital-single-market/en/news/recommendation-european-electronic-health-record-exchange-format

13 eHealth Network Guidelines on an interoperable ecosystem for digital health and investment programmes for a new/updated generation of digital infrastructure in Europe, https://ec.europa.eu/health/sites/health/files/ehealth/docs/ev_20190611_co922_en.pdf

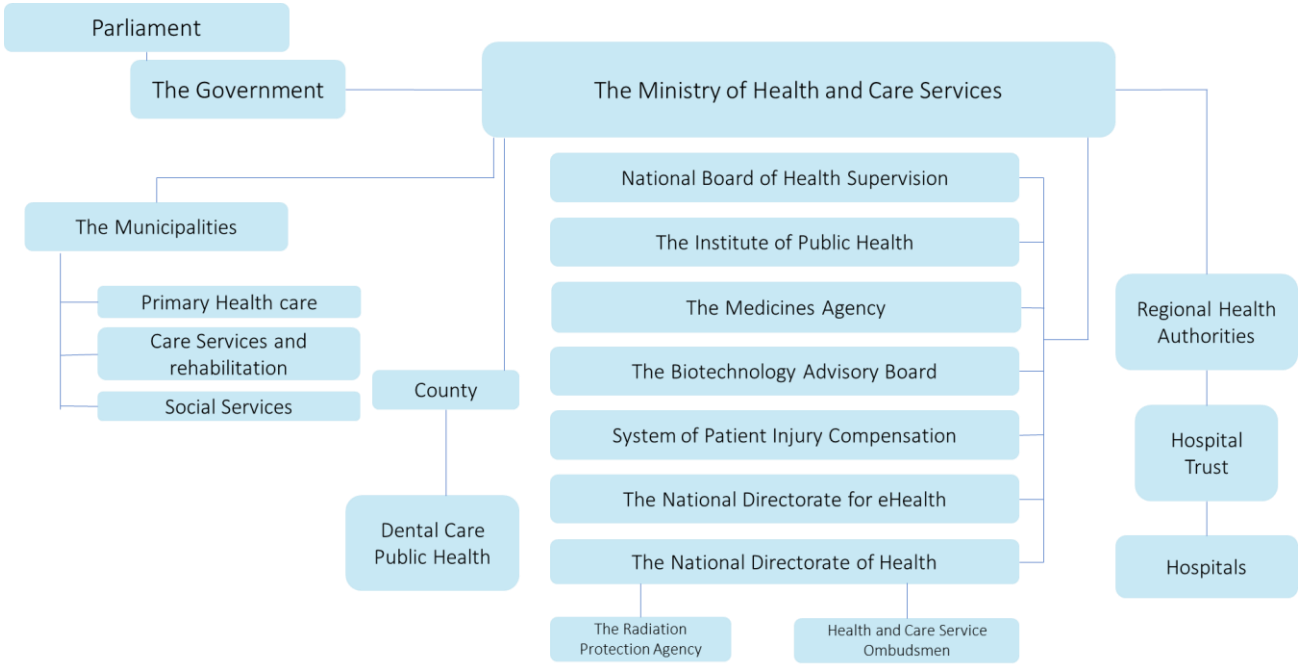
14 European Commission Multiannual financial framework, https://ec.europa.eu/info/strategy/eu-budget/documents/multiannual-financial-framework_en

15 European '1+ Million Genomes' Initiative https://ec.europa.eu/digital-single-market/en/european-1-million-genomes-initiative

16 Cross-border healthcare directive, or DIRECTIVE 2011/24/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 9 March 2011 on the application of patients' rights in cross-border healthcare, https://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:088:0045:0065:EN:PDF

legislations provide the EU citizens with the right to health data portability. This means that interoperability is no longer an optional effort derived from member states and organizations, but indeed a necessary and compulsory path enabling the member states to fully provide their citizens with the right to data portability. DIRECTIVE 2011/24/EU dedicates the whole article 14º to eHealth and places great importance on the use of electronic means. To achieve the objectives of the DIRECTIVE 2011/24/EU, the eHealth Network has been established[17] as the highest policy level body for eHealth in the EU. In October 2019, the role of the eHealth Network was revised and enlarged[18] with subgroups to look at certain topics, usually temporary. In terms of future trends, discussions exist regarding the governance of new initiatives such as the European Health Data Space, or new eHDSI services.

Figure 1: Example of Norwegian Healthcare System Organisation[19]



Many examples of well-organised healthcare governance systems can be seen across Europe. One of them is the Norwegian healthcare system, illustrated in **Figure 1**. Here, the Ministry of Health and Care Services is in charge of the regulation and supervision of the healthcare system. However, many tasks are delegated to various subordinate agencies, such as the Institute of Public Health and the Medicines Agency. In such a system, health data are collected in various types of medical registries, but overall supervision and monitoring provided by the National Board of Health Supervision. This is a good example of inter-sectoral cooperation.

2.2 eHealth infrastructure and services

Currently, in the EU, eHealth infrastructure at the European or cross-border level is composed of two blocks: not specific to health infrastructures and health-specific ones. The infrastructure block that is not specific to health defines eHealth elements such as trust services like the eIDAS Network in relation to the Connecting Europe Facility (CEF) eID building block[20], to share personal digital identity services, or TESTA network, the

17 Implementing Decision of 22 December 2011 providing the rules for the establishment, the management and the functioning of the network of national responsible authorities on eHealth (2011/890/EU), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32011D0890

18 Implementing Decision of 22 October 2019 providing the rules for the establishment, the management and the functioning of the network of national authorities responsible for eHealth, (2019/1765/EU) and repealing Implementing Decision 2011/890/EU (notified under document C (2019) 7460) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019D1765

19 Norwegian Health Services in a Comparative Perspective How to measure a health system's performance http://helsetjenesteforskning.org/wp-content/uploads/2018/03/lindahl.pdf

20 The Connecting European Facility eID Building Block primarily supports the Member States in the roll-out of the eIDAS Network (the technical infrastructure which connects national eID schemes). CEF eID is a set of services (including software, documentation, training and support) provided by the European Commission and endorsed by the Member States, which helps public administrations and private

fundamental network for data exchange between public administrations, a dedicated VPN system for connecting public administration at a national level with different commission services[21]. These are used by healthcare systems in their architecture for offering the eHealth Services. The health-specific block defines the eHealth Digital Service Infrastructure (eHDSI) under the CEF program and is composed of two sections, described in **Table 2**.

Table 2: eHealth Digital Service Infrastructure building block sections

eHDSI sections:
Infrastructure providing services for the European Reference Networks (ERNs)[22]
Infrastructure providing Cross-Border eHealth Information Services for the exchange of ePrescriptions, also known as, ePrescription/eDispensation and Patient Summary exchange (CEF eHDSI)[23]

The infrastructure providing the CBeHIS currently supports the ePrescription/eDispensation and the Patient Summary exchange. For more detailed information on this matter, there is extensive documentation online in the CEF eHDSI portal and wiki[24] These services are offered in a non-centralized architecture, where the main component is the OpenNCP, that serves as an opensource broker to directly transfer information between countries. The OpenNCP is a software installed on the national level, where the National Contact Point for eHealth (NCPeH) takes the organisational responsibility for it. To other OpenNCPs, the software is exposed via TESTA network. In preparation for the first countries going live with the OpenNCP, some crucial elements have been discussed and actioned including the governance model[25], the roadmap and the calendar of going live, as well as the organizational framework, and the eHDSI Member State Expert Group responsible for eHealth operations. Future trends and challenges regarding the OpenNCP use in CBeHIS include the architecture upgrade, the inclusion of trust services and development of common semantic work.

The creation of eHealth cross-border services in the Eastern partner countries, using the model and artefacts created in the EU is an opportunity to quickly upgrade the level of interoperability. Paying attention to the efforts made to achieve the harmonised procedures, as well as technical deployments, and especially cooperation and articulation initiatives, it becomes clear that joined international work is required to achieve success. Finally, leapfrogging to a more advance sharing of health data is possible if the Eastern partner countries learn from mistakes as well as existing challenges and create their solutions in a more capable, well-governed yet flexible manner.

2.3 Funding and incentive mechanisms for interoperability

In practice, funding and incentive mechanisms are key enablers of interoperability and harmonization. A brief overview of the financial instruments and programmes proposed under the EU's next multi-annual financial framework (MFF) 2021-2027 illustrates that there may be some opportunities for funding for non-EU countries. The specific opportunities will need to be analysed in due time. One of the most powerful incentive mechanisms for eHealth deployment is political determination and the force of law.

Service Providers to extend the use of their online services to citizens from other European countries, https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eID

21 The TESTA network service – which stands for Trans European Services for Telematics between Administrations – provides a European backbone network for data exchange between a wide variety of public administrations, https://ec.europa.eu/isa2/solutions/testa_en

22 Details about EU European Reference Networks, https://ec.europa.eu/health/ern_en

23 The eHealth Digital Service Infrastructure (eHDSI or eHealth DSI) is the initial deployment and operation of services for cross-border health data exchange under the Connecting Europe Facility (CEF). eHDSI sets up and starts deploying the core and generic services, as defined in the CEF, for Patient Summary and ePrescription. The generic services are the necessary implementation of data exchange at country level, the core services at EU level. These together enable the provision of Cross Border eHealth Information Services (CBeHIS). https://ec.europa.eu/cefdigital/wiki/display/EHOPERATIONS

24 Details about CBeHIS, https://ec.europa.eu/cefdigital/wiki/display/EHOPERATIONS

25 The governance model was adopted by the eHealth Network, https://ec.europa.eu/cefdigital/wiki/display/EHOPERATIONS/eHDSI+GOVERNANCE?preview=/35210447/41287688/ev_20161121_co06_en.pdf

Table 3: Incentives for interoperability

Incentive trends:
The US “meaningful use” initiative
The Netherlands initiative
Mandatory integration with central services
EU initiative – eHealth Network approved the recommendation on guidelines for digital health and investment programmes interoperable eco-system

Both the US “meaningful use” and the Netherlands initiatives, described in **Table 3**, serve not just as incentives for interoperability and eHealth harmonization but support healthcare process transformation. The downside is that these initiatives are very expensive and once started difficult to terminate. Mandatory integration with central services and the EU Initiative is cheaper for the governments. Both initiatives are generally for critical services such as ePrescription/eDispensation because of the higher demand for such service. However, services like Patient Summary do not have such high demand and the incentives are less likely to be effective.

2.4 Interoperability challenges and emerging technologies

Improved interoperability across various health settings is a high priority not only for healthcare providers and policymakers but for patients too. Both public and private sectors have been working across the industry to first establish and then to improve efficient health information exchange. However, to achieve optimal healthcare and improved patient health outcomes, several challenges, described in **Table 4**, are yet to overcome.

Table 4: Interoperability challenges in healthcare

eHealth interoperability challenges:
Standardisation and common digital identification of professionals, common recognition of professional categories, their respective roles and system permissions
Standards associated with mHealth APPs
Standards adoption in the area of wearables and devices, and how these link – send and receive data – to EHRs in the local, regional or national in nature
Detailed definition of the initial five domains of the Electronic Health Record Exchange Format (EHRxF), and their implementation
Identification of interoperability standards associated with the cybersecurity platforms, genomic data exchange, and transfers of bulk or large volumes of health data
The wide adoption of Semantic Interoperability standards, namely common terminologies such as SNOMED CT, LOINC, and hybrid solutions like SNOMED-FHIR aggregates or SNOMED-LOINC mapping tables; or semantic standards for imaging reports (for example, LOINC-RadLex). This is especially important for the three new domains under the EHRxF

Regarding the EHRxF the recommendation of the European Commission was published in February 2019, and the call for a Common Support Action (CSA) on the maturation of the EHRxF has already been answered and the project involving a consortium with 33 institutions from 22 member states has been approved. On the European level, the EHRxF defines five health information domains: Patient Summary, ePrescription/eDispensation, Laboratory Results, Medical Imaging and Reporting and Hospital Discharge Reports. In order to overcome the semantic challenges, the Common Semantic Strategy[26] has been approved by the eHealth Network. Finally, although the eHealth Network has done some relevant work on mobile health (mHealth), guidelines or recommendations have not yet been finalised. In April 2020 the first version of a Common Toolkit for Mobile applications has been released to support contact tracing in the EU’s fight against

26 Common semantic strategy for health in the European Union, https://ec.europa.eu/health/sites/health/files/ehealth/docs/ev_20190611_co242_en.pdf

COVID-19[27]. The toolkit constitutes the first common EU level position on mHealth solutions. More profound work on mHealth interoperability and harmonization is being conducted under the mHealth-HUB project[28].

2.5 Genomics, AI, the European health data space and personalised medicine

Precision medicine, now often referred to as personalized medicine, can be understood as personal customization of care. Data-driven analytics looking at genomic and other "omics" data, combined with smart drug design will offer a precise dosage and indications dyad that will fit each person's needs more accurately than current therapies. Personalised medicine is a similar concept looking at customised healthcare provision which also includes medical devices and certain care pathways and protocols. To be able to implement these features, healthcare systems must master genomics (and other "omics", including proteomics, metabolomics, and transcriptomics), use of artificial intelligence algorithms for data analysis and then personalised application of data-driven models. For all these data-driven technologies large volumes of data are needed. Several emerging healthcare trends in the EU have been noted in **Table 5**.

Table 5: Emerging healthcare trends in the EU

The EU trends:
Genomic data sharing projects
Development of AI for health, frameworks, research projects, as well as ethical reflection
Road-mapping towards a common European (Health) Data Space (EHDS)

These trends mean multi-member states collaboration efforts, and pooling of resources in order to generate large amounts of data. The challenge is that small countries struggle to create such datasets. Even larger countries like Germany, France or Poland, are too small compared to the US and China. In the case of rare diseases, only pooling cases in the whole EU can have the capacity to create large enough datasets for genomic-based decisions or the AI algorithms-related training. Therefore, late in 2019, the quest for the EHDS has started as part of the larger quest for the European Data Space and gained high political visibility[29]. A common EU health data space would enable secure access to different kinds of health data (Electronic Health Records, Genomic data, lifestyle/behavioural) for healthcare, research and innovation purposes, but also policymaking. Healthcare is benefiting from the AI, which can provide support for diagnosis and treatment of diseases, contributes to personalized medicine, supports doctors in keeping up to date with an increasing body of scientific literature, supports the development of robots for the patient and elderly care and is even being explored for providing advice to patients. However, AI also brings new challenges to the existing ethical, regulatory and liability rules. Work on liability implications of the AI and other emerging technologies[30] as well as ethical guidelines for trustworthy AI development[31] has been produced by the European Commission and is useful for any country reflection upon these issues.

2.6 Useful and sharable practices and proposed recommendations

Table 6: Legal sharable eHealth practices in the EU

EU sharable practices: legal
The existence of a common legal background, provided by the DIRECTIVE 2011/24/EU, and the General Data Protection Regulation (GDPR) in that it set the rights for the EU citizens to (health) data portability, creates the needs but also enables eHealth interoperability

27 Mobile applications to support contact tracing in the EU's fight against COVID-19 https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_en.pdf

28 The European mHealth Hub is an EC-funded project, under the action "Establishing EU mHealth Hub including evidence for the integration of mHealth in the healthcare systems" (Grant Agreement No 737427), https://mhealth-hub.org/

29 The mission letter of Commissioner-designate for Health, https://ec.europa.eu/commission/sites/beta-political/files/mission-letter-stella-kyriakides_en.pdf

30 Liability for Artificial Intelligence https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeetingDoc&docid=36608

31 Ethics guidelines for trustworthy AI https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai

EU sharable practices: legal
The eHealth Network established[32] in 2011 is the highest policy level body for eHealth in the EU. its scope was amplified in October 2019. The Network works in temporary sub-groups following a Multi-Annual Workplan
Liability and ethical consequences of AI in healthcare are explored benefiting from the EU-wide approach since the AI is likely to be used in more than one country

Table 7: Organisational sharable eHealth practices in the EU

EU sharable practices: organizational
Funding and incentive mechanisms, especially those that link funding to adherence and compulsory utilization of standards, can be technically verifiable to promote harmonization and interoperable solutions implementation in the real world
The governance model for the eHDSI that includes all stakeholders and has different levels of decision-making, allow sharing best practices between eHealth agencies, as well as, reinforces processes like testing and auditing to ensure high quality of cross-border services

Table 8: Semantic sharable eHealth practices in the EU

EU sharable practices: semantic
Common Semantic Strategy which joins efforts towards cross-learning and mutual benefits where the semantic maturity can be obtained as it remains to be an obstacle in primary and secondary use of healthcare data

Table 9: Technical sharable eHealth practices in the EU

EU sharable practices: technical
A decentralized architecture for health data sharing is not only politically more acceptable but is less likely to have a problem associated with the “single point of failure” problem
The OpenNCP is a good example of a jointly built, jointly maintained and jointly used Open Source Software. It serves very important breakage functions
Common guidelines for an exchange format of all health information domains (similar to the EHRxF) are very useful as they facilitate not only the cross-border exchange but also serve as a benchmark and a referential document to promote internal, regional and local, interoperability

Table 10: Current eHealth trends and directions proposed recommendations

Proposed recommendations:
Create legal stability via international protocols on health data sharing, and cross-border services
Follow-up AI in health developments and ongoing initiatives in the EU, and explore ethical and liability implications in each country by localizing the debates
Create a stable policy body for strategic alignment, harmonization and that promotes health sector interoperability in the Eastern partner countries. It should interact with the EU eHealth Network
Devise incentive mechanisms that use clear and verifiable criteria and condition funding to real-world implementation of interoperable solutions and promote harmonization efforts
Devise a governance model, dedicated to cross-border services, that encourages both cooperation and procedural rigour
Adopt the EU EHRxF and create a multi-country group of interoperability experts to follow up the work and promote harmonization efforts in the Eastern partner countries as it matures in the EU
Develop an Open Source community of technicians from different countries and built joint technological artefacts, these will serve a function as technical and cultural approximators

32 Commission Implementing Decision of 22 December 2011 providing the rules for the establishment, the management and the functioning of the network of national responsible authorities on eHealth (2011/890/EU), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32011D0890

3 Detailed results of eHealth service harmonisation and interoperability assessment

3.1 Common assessment results for the eastern partner countries

Assessment aspects

The common eHealth assessment framework supports the model of effective communications between different healthcare environments via electronic means. This model together with terms and methodologies offers a foundation for reaching a common language and starting point, for eHealth implementation. This model is also important for the analysis of problems and the description of eHealth solutions throughout Europe. It was designed to serve as a set of standards enhancing interoperability in eHealth across the Eastern partner countries. This model is a construct of several principles and criteria described in detail throughout the following subchapters. Healthcare services and administrations in the Eastern partner countries have been thoroughly assessed against these principles and criteria described in **Table 11**. The results identify gaps of eHealth infrastructure in the Eastern partner countries.

Table 11: Description of common eHealth assessment framework principles and criteria

Common eHealth assessment framework:	
EIF Principles	Is a set of principles intended to establish general behaviours of interoperability
EIF Layers	Is a construct of aspects of interoperability that need to be addressed when designing European public services
DSI Criteria	Is a combination of levels of interoperability designed to guide digital service infrastructure
eHDSI Criteria	Are the criteria designed to enable the cross-border healthcare services and data exchange
eHDSI Building Blocks	Is a collection of standards required for setup and start of eHealth services such as Patient Summary and ePrescription
eHealth Service: Patient summary	Represents European eHealth service enabling cross-border healthcare visits, where the healthcare professionals will have access to patient's medical background and history
eHealth Service: ePrescription	Represents European eHealth service enabling the patient being abroad to dispense the equivalent medication that was prescribed in the home country
Data Elements: Patient Summary	Is a set of data elements considered to be essential for Patient Summary to be an optimised and legal eHealth service
Data elements: ePrescription	Is a set of data elements considered to be essential for ePrescription to be an optimised and legal eHealth service

Alignment with the common eHealth assessment framework principles and criteria

The analysis framework based on the ReEIF model displays the overall level of interoperability in the Eastern partner countries. The results are illustrated in **Figure 2** and key gaps in alignment with the ReEIF are identified in **Table 12**.

- The best scoring has been observed in the **Data Elements: ePrescription** as several of the Eastern partner countries have ePrescription service meeting the mandatory EU dataset requirements.
- It has also been revealed that **eHealth Service score: Patient Summary** have the lowest score. The analysis shows that s0me countries are lacking regulation enabling Patient summary services in the Eastern partner countries and data sharing between the countries.

Figure 2: Assessment results based on ReEIF model

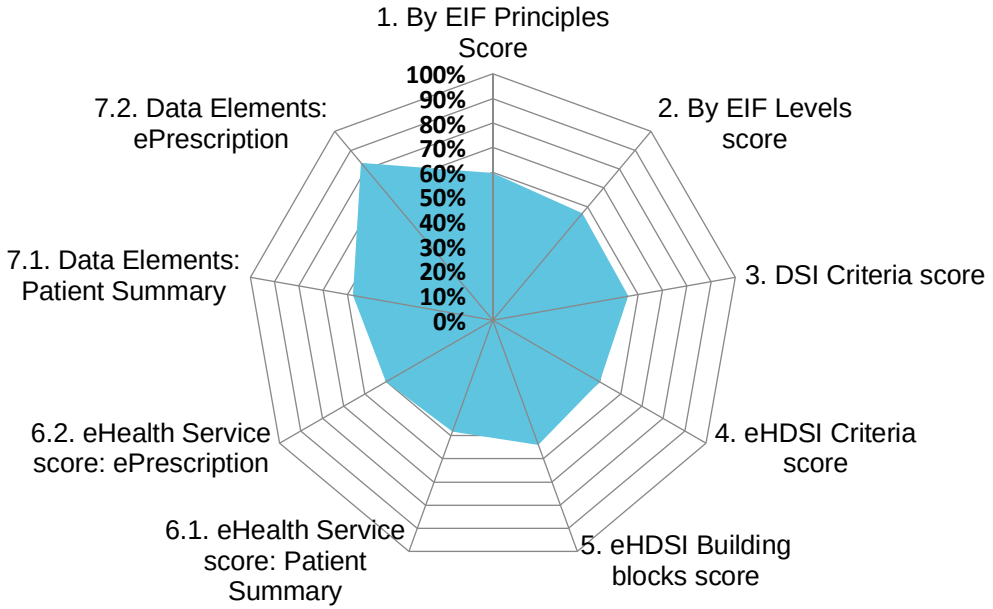


Table 12: Key findings in the alignment with the ReEIF model

1. By EIF Principles Score	**60%**
2. By EIF Levels score	**57%**
3. DSI Criteria score	**56%**
4. eHDSI Criteria score	**50%**
5. eHDSI Building blocks score	**54%**
6.1. eHealth Service score: Patient Summary	**48%**
6.2. eHealth Service score: ePrescription	**50%**
7.1. Data Elements: Patient Summary	**58%**
7.2. Data Elements: ePrescription	**83%**
	57%

3.2 Results of alignment with European Interoperability Framework principles

Assessment aspects

Each of the Eastern partner countries has been assessed in relation to the European Interoperability Framework (EIF) principles. The EIF principles is a set of 12 fundamental behavioural aspects, outlined in **Table 13**, driving interoperability actions relevant to the process of establishing interoperable public services. The 12 underlying principles describe the context in which European public services are designed and implemented. Efficient interoperability actions play an important role in the implementation of eHealth framework and services and are highly recommended for consideration in the Eastern partner countries.

Table 13: Description of EIF principles

EIF principles[33]:	
Subsidiary and proportionality	Ensures that the EU undertakes only necessary and more effective actions than the same ones taken at the national level
Openness	Ensures public data availability for use and reuse
Transparency	Enables visibility of public administration, availability of interfaces with internal information systems and protection of personal data
Reusability	Ensures reusability of IT solutions, information and data
Technological neutrality and data portability	Allows access and reuse of public services and data, irrespective to specific technologies or products allowing data portability
User-centricity	Ensures that users' needs are considered. Multi-channel service delivery and a single point of contact are available, and users' feedback is taken into consideration
Inclusion and accessibility	Ensures that everyone has access and can make use of public services
Security and privacy	Ensures that public authorities provide a secure and trustworthy environment for citizens; public administrations guarantee citizens' privacy
Multilingualism	Ensures that public services are available in the language of the expected end-users
Administrative simplification	Ensures streamlined and simplified administrative processes
Preservation of information	Ensures long term accessibility of the records
Assessment of effectiveness and efficiency	Ensures the evaluation of various technological solutions to confirm the effectiveness

Alignment with the EIF principles

The assessment results based on the EIF principles revealed the current state of interoperability in healthcare system existing in the Eastern partner countries. The results are illustrated in **Figure 3** and key gaps in alignment with the EIF principles are identified in **Table 14**.

- **Security and Privacy** principle is a well-established area due to the national electronic services operating in all Eastern partner countries. Most of these countries also follow local data privacy regulations to guarantee the citizen's privacy and confidentiality. However, the security of cross-border digital services requires a more harmonised action, as such interoperability is beneficial but increases surface attack area.
- In comparison, **Multilingualism** and **User-centricity** demonstrate the biggest gap in the alignment with the EIF principles. The analysis shows that countries scored the lowest in these areas due to the limited availability of channels for accessing public services and lacking multilingualism in public services.

33 The New European Interoperability Framework, https://ec.europa.eu/isa2/sites/isa/files/eif_brochure_final.pdf

Figure 3: Assessment results based on the EIF Principles

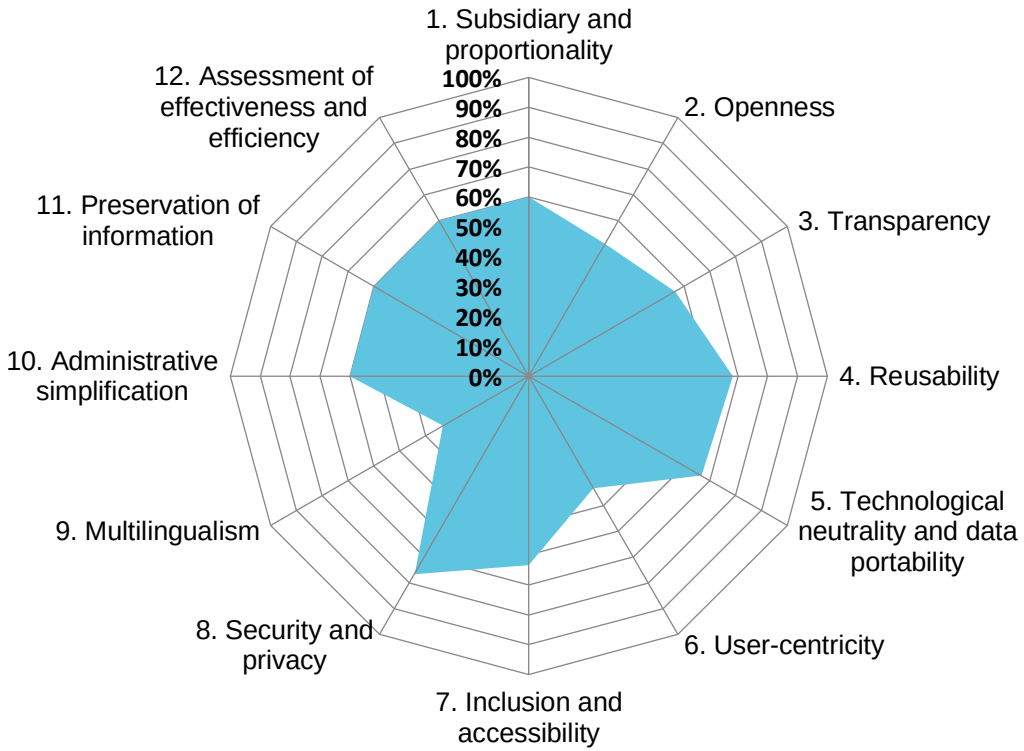


Table 14: Key findings in the alignment with the EIF Principles

1. Subsidiary and proportionality	**60%**
2. Openness	**51%**
3. Transparency	**57%**
4. Reusability	**68%**
5. Technological neutrality and data portability	**67%**
6. User-centricity	**43%**
7. Inclusion and accessibility	**63%**
8. Security and privacy	**77%**
9. Multilingualism	**33%**
10. Administrative simplification	**60%**
11. Preservation of information	**60%**
12. Assessment of effectiveness and efficiency	**60%**
	58%

3.3 Results of alignment with the European interoperability layers

Assessment aspects

Interoperability model used in this analysis applies to all digital public services, including eHealth, and is considered as an integral part of the interoperability-by-design paradigm. This model includes interoperability governance, integrated public service governance as well as four layers of interoperability (legal, organisational, semantic and technical) with wider definitions provided in **Table 15**. The concept of the interoperability agreement is that of an inter-organizational agreement around the duties and responsibilities of a given interoperable link (e.g. who maintains datasets and their value definition, and change process for a given data change).

Table 15: Description of interoperability layers

Interoperability layers:	
Interoperability governance	Is a background layer describing decisions on interoperability frameworks, institutional arrangements, organisational structures, roles and responsibilities, policies, agreements and other aspects of ensuring and monitoring interoperability at the national and EU levels
Integrated public service governance	Is a cross-cutting component of the four layers of interoperability. It oversees organisational structures and roles and responsibilities for the delivery and operation of public services, service level agreements, establishment and management of interoperability agreements, change management procedures and plans for business continuity and data quality
Legal interoperability	Is a layer ensuring that organisations operating under different legal frameworks, policies and strategies can work together
Organisational interoperability	Is a layer describing the way organizations and administrations public and/or private align their business processes, responsibilities and expectations to achieve commonly agreed and mutually beneficial goals
Semantic interoperability	Is a layer ensuring that the format and the meaning of exchanged data and information is understood between the exchanging parties
Technical interoperability	Is a layer describing the applications and infrastructures linking systems and services

Alignment with the European interoperability layers

The analysis results of alignment with the European interoperability layers are illustrated in **Figure 4**, which display the latest interoperability model in the Eastern partner countries. Key gaps in alignment with the interoperability layers are identified in **Table 16**.

- **Integrated public service governance** scored highest as most of the countries have separate agencies responsible for eGovernance.
- However, **Semantic interoperability** was identified as the least mature aspect. Large differences between the countries have been identified, as well as misalignments with HL7 definitions.
- **Legal interoperability** was another least mature aspect of European interoperability in the Eastern partner countries. It is believed this is mainly due to the lack of implemented systems which would identify any barriers of interoperability in organisations operating under different legal frameworks.

Figure 4: Assessment results based on the European Interoperability Layers

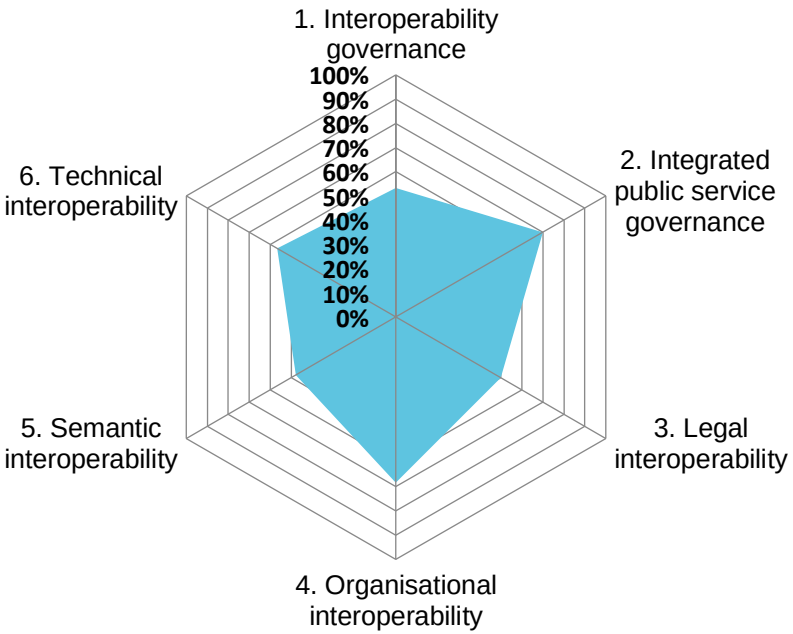


Table 16: Key findings in the alignment with the European Interoperability Layers

1. Interoperability governance	**53%**
2. Integrated public service governance	**70%**
3. Legal interoperability	**50%**
4. Organisational interoperability	**68%**
5. Semantic interoperability	**48%**
6. Technical interoperability	**57%**
	58%

3.4 Results of alignment with the criteria of Digital Service Infrastructure

Assessment aspects

A detailed cross-border Digital Service Infrastructure (DSI) assessment has been conducted in the Eastern partner countries. The attention was drawn to the services enabling cross-border interactions between the healthcare providers and between healthcare providers and citizens. The criteria assessed serve as enablers for any digital healthcare service and are based on EIF principles and layers. These criteria, described in **Table 17**, are important as they access the basis of the country's eGovernance landscape and give the context for further eHealth focused assessment part.

Table 17: Description of DSI criteria

Digital Service Infrastructure criteria:	
Legal	Ensures that organisations operating under different legal frameworks, policies and strategies can work together
Organisational	Refers to how public administrations align their business processes, responsibilities and expectations to achieve commonly agreed and mutually beneficial goals
Semantic	Ensures that the precise format and meaning of exchanged data and information is preserved and understood throughout exchanges between parties
Technical	Covers the applications and infrastructures linking systems and services including interface specifications, interconnection services, data integration services, data presentation and exchange, and secure communication protocols

National DSI assessment

The results of this assessment are illustrated in **Figure 5** and key gaps in alignment with the DSI criteria are identified in **Table 18**.

- **Technical** infrastructure scored highest due to the existence of technological solutions for public sector services even though they often lack legal base to fully replace paper in processes.
- **Organisational** infrastructure scored lowest, in general, due to lack of clarity of the governance approach in defining DSI governance and management processes and responsibilities.

Figure 5: Assessment results based on the DSI criteria

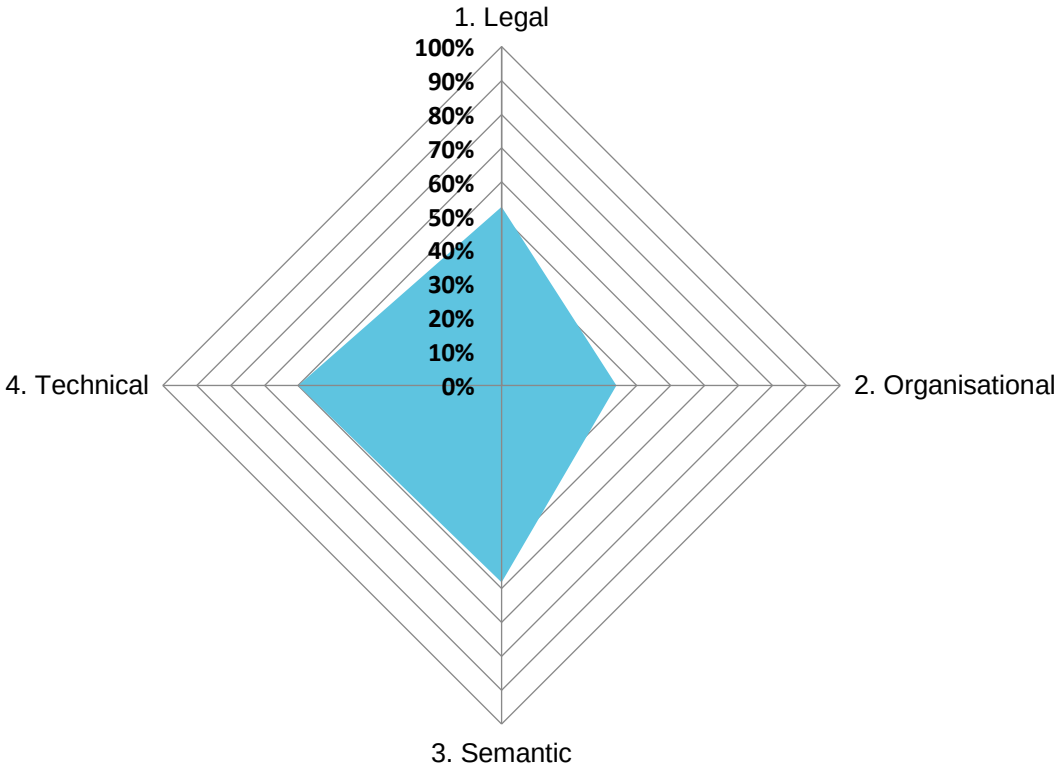


Table 18: Key findings in the alignment with DSI criteria

1. Legal	**53%**
2. Organisational	**34%**
3. Semantic	**58%**
4. Technical	**60%**
	51%

3.5 Results of alignment with the eHDSI criteria

Assessment aspects

The eHealth Digital Service Infrastructure (eHDSI or eHealth DSI) can be defined as services and infrastructures using ICTs that enable cross-border healthcare services and health data exchange. eHDSI principles set up and establish the core and generic services for Patient Summary and ePrescription. The generic services are the necessary implementation of data exchange at the country level, the core services - at the EU level and across the Eastern partner countries. These together enable cross-border healthcare services.

The healthcare services and the health data exchange have been assessed in the Eastern partner countries against the eHDSI criteria, described in **Table 19**. The criteria evaluate legal and regulatory, policy, information, applications and IT infrastructure. This assessment helped to identify the current digital service infrastructure and further eHealth needs.

Table 19: Description of eHDSI criteria

eHDSI criteria:	
Legal and regulatory	Legal and regulatory constraints
Policy	Information exchange and collaboration agreements
Information	Defining structure and coding of information
Applications	Transport and exchange services and integration in healthcare systems
IT infrastructure	Generic communication protocols

Alignment with the eHDSI criteria

The assessment results are illustrated in **Figure 6** and key gaps in alignment with the eHDSI criteria are identified in **Table 20**.

- The **Application** dimension scored highest as most of the countries have basic ePrescription services running. The EHR use cases are implemented or in preparation to implement.
- The aspects of **Policy** scored lowest due to the lack of defined processes and responsibilities to drive the health care system to transform to digital. It was observed that the Eastern partner countries still heavily rely on paper-based processes.

Figure 6: Assessment results based on eHealth Digital Public Service Infrastructure

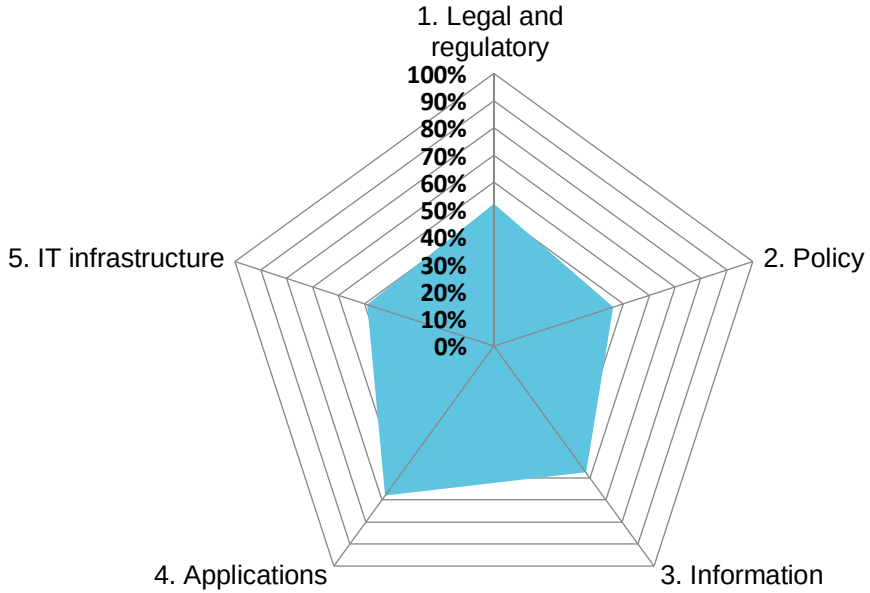


Table 20: Key findings in the alignment with the eHealth Digital Public Service Infrastructure

1. Legal and regulatory	**52%**
2. Policy	**46%**
3. Information	**58%**
4. Applications	**68%**
5. IT infrastructure	**49%**
	55%

3.6 Results of alignment with eHDSI building blocks

Assessment aspects

The eHDSI building blocks, described in **Table 21**, were designed according to the eHDSI principles to help build stronger technical, functional and operational eHealth infrastructure. The assessment involved healthcare systems, public services and administrations to better understand the level of interoperability across the Eastern partner countries.

Alignment with eHDSI building blocks

The assessment results are illustrated in **Figure 7** and key gaps in alignment with eHDSI building blocks are identified in **Table 22**.

- The assessment showed that the **National registries and information systems from other public administration domains** scored highest as most of the countries have rather mature resident, foreigner and business entity registries at the national level.
- The assessment also showed that **HCP Information Systems**, as well as **Health Care Sector Registries and Information Systems**, show lowest maturity levels, which reflect the low digitisation of the hospital processes and integration with the national eHealth systems.

Table 21 Description of eHDSI building blocks

Building blocks and definitions		
1. eHealth Interoperability Platform - A platform allowing eHealth services to be used in an interoperable way on a national level	**1.1. Health Data Access** - A private and secure way of accessing the citizen's electronic health data record	**1.1.1. Patient Portal** - A private and secure online portal providing access to eHealth services to the citizens **1.1.2. Healthcare Professional Portal** - A private and secure online platform providing healthcare providers with access to eHealth services e.g. EHR, ePrescription and Patient Summary **1.1.3. Pharmacist Portal** - A private and secure online platform providing pharmacists with eHealth services e.g. ePrescription **1.1.4. Data Analytics and Open Data APIs** - Computing interface for health data analysis and management
	1.2. eHealth Services - Services using ICTs that can improve prevention, diagnosis, treatment, monitoring and management of illnesses, e.g. Patient Summary and ePrescription	**1.2.1. eHealth Service Catalogue** - Information package helping healthcare administrative services to comply with European standards **1.2.2. Patient Summary** - A standardised set of basic medical data that includes the most important clinical facts required to ensure safe and secure healthcare. This summarised version of the citizen's medical data gives health professionals the essential information they need to provide care in the case of an unexpected or unscheduled medical situation (e.g. emergency or accident) **1.2.3. ePrescription** - A tool to generate prescriptions electronically. It is generally understood as a prescriber's ability to electronically send an accurate, error-free and understandable prescription directly to a pharmacy from the point-of-care. ePrescription is also used by nurses to administer medicines and by pharmacies to review orders and manage the supply of medicines **1.2.4. Electronic Health Record (EHR)** - A collection of longitudinal medical records or similar documentation of an individual in digital form. This set of health information based on the principle one EHR per citizen in a country **1.2.5. Medical Imaging** - Different imaging modalities and processes used for diagnostic and treatment purposes
	1.3. Data and Documents Storage - Data and document storage using information technology to improve citizen-centred care and digital health	**1.3.1. eHealth Reference Catalogue** - Centrally stored authorised eHealth documentation and information about all eHealth-related activities **1.3.2. EHR Data** - Includes all medical information related to the particular citizen **1.3.3. Patient Summary Data** - Information regarding the citizen's health required for medical emergencies or clinical encounters while travelling **1.3.4. ePrescription Data** - Information regarding patient's valid prescriptions and dispensations log of medicinal products **1.3.5. Laboratory Reports** - Laboratory reports database **1.3.6. PACS** - A medical imaging technology providing storage and access to images from multiple modalities

Building blocks and definitions		
		1.3.7. HCP Registry - An authorised central source of registered HCP **1.3.8. Patient Registry** - An authorised central source of patients registered with HCP **1.3.9. Healthcare Specialist Registry** - An authorised central source of registered healthcare specialists
2. HCP Information Systems - HCP used information systems that can improve prevention, diagnosis, treatment, monitoring and management of illnesses	**2.1. University HCP IS** - Health information systems available for University HCPs	
	2.2. National/ Regional HCP IS - Health information systems available on a national/regional level	
	2.3. Local/ Other HCP IS - Health information systems available on a local level	
3. Healthcare Sector Registries and Information Systems - Authorised healthcare systems and platforms designated for reliable health-related information collection and storage	**3.1. Specialists Registry** - An authorised platform providing the list of healthcare professionals, usually focused around specific specialisation, diseases and conditions	
	3.2. Health Insurance IS - Information systems designated for smooth healthcare insurance management	
	3.3. Pharmacy IS - Pharmacy information systems that have many different functions to maintain the supply and organisation of medicinal products	
	3.4. Drug Registry - An authorised online platform providing the list of controlled substance prescriptions	
	3.5. Patient Visit On-line Booking - An online platform for booking patient appointments with HCP	
	3.6. Registry of Insured - An online platform enabling HCP to identify insured citizens	
	3.7. Clinical Decision Support IS - The health information technology system designed to provide healthcare professionals with clinical decision support	
	3.8. HCP Licencing IS - Information systems assisting HCP with licensing standards, rules and laws	
	3.9. SNOMED - Medical terminology covering most areas of clinical information such as diseases, procedures, pharmaceuticals etc.	
	3.10. Public Health IS - A combination of vital and health statistical data from multiple sources, used to derive information about the health needs, health resources, use of health services, and outcomes of use by the people in a defined region or jurisdiction	
4. National Interoperability Platform - A platform responsible for advancing connectivity and interoperability of healthcare services	**4.1. Identification Services** - Services enabling the identification of citizens and healthcare providers	
	4.2. Access to eHealth portal/eHealth services via the common eGovernment services gateway catalogue - An authorised secure and monitored access to eHealth portal/eHealth services	
	4.3. Data Exchange Platform - Platform where data can be shared between different computer programs	
5. National Registries and Information Systems from other public administration domains -	**5.1. Resident Registry** - An authorised electronic database of people living in the country on a long-term basis	
	5.2. Foreigner Registry - An electronic database for registered non-native residents	
	5.3. Business Entity Registry - An electronic database for registered businesses	

Building blocks and definitions	
Administrative public data repository electronic database	**5.4. Social/Health Insurance IS** - Information systems for social /healthcare insurance management.
	5.5. Address Registry - An authorised central electronic database of validated addresses
	5.6. Disability Registry - An authorised central electronic database for those who may need disability-related assistance

Figure 7: Assessment results based on the eHDSI Building Blocks Criteria

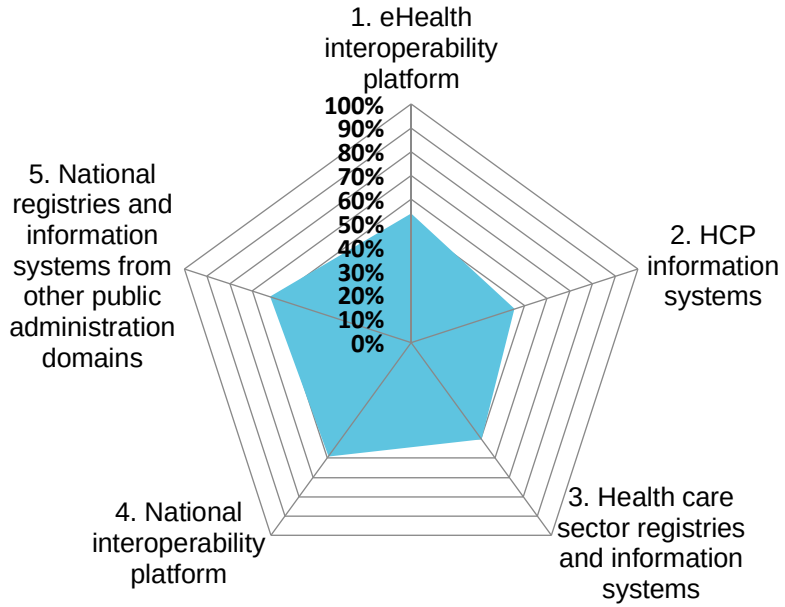


Table 22: Key findings in the alignment with the eHDSI Building Blocks Criteria

1. eHealth interoperability platform	**54%**
2. HCP information systems	**46%**
3. Health care sector registries and information systems	**50%**
4. National interoperability platform	**59%**
5. National registries and information systems from other public administration domains	**62%**
	54%

3.7 Results of alignment with eHealth service criteria: ePrescription and Patient Summary

Assessment aspects

The eHDSI is looking to facilitate the cross-border exchange of health data between the EU countries in a secure, efficient and interoperable way which could also be followed in the Eastern partner countries. The ePrescription and the Patient Summary are the services enabling the patient to get their medications electronically and in case of emergency, while travelling, doctors can give better care by accessing the patient's past health records. This assessment was conducted to understand the current state in the Eastern partner countries regarding such eHealth services as ePrescription and Patient Summary. The basis for data exchange between a wide variety of public administrations has been assessed to evaluate the level of performance, security and interoperability.

- ePrescription enables patients to obtain their medications abroad. This process is enabled by the online transfer of electronic prescription from the country of residence where the patient is affiliated, to the country of travel.
- Patient Summary provides doctors with information on important health-related aspects of a travelling patient, for example, allergies, current medications, previous illness, surgeries, etc. Patient Summary is part of EMR and is designed to provide doctors with the essential information about the patient in their language.

The eHealth Service Criteria, described in **Table 23**, was designed to facilitate the analysis of ePrescription and Patient Summary services in the Eastern partner countries. The criteria carefully assess the systems and services currently in use and describe their interoperable applications with the focus on trust, security and national methods of enhancing continuity of care and ensuring access to safe and high-quality healthcare.

Table 23: Description of eHealth service criteria

eHealth service criteria: ePrescription and Patient Summary	
Legal and regulatory	Interoperability aspect covering various legal certainties and regulations as part of eHDSI identity management specification. For example, this includes regulation of patient consent, DSI compliance with European security and privacy legislation and directives or equivalent, guaranteed authenticity of a document by its issuer etc.
Policy	Interoperability aspect combining both, eHDSI identity management specifications and eHDSI interoperability specifications. It defines the governance model of active entities of eHealth DSI with their tasks and positions in eHealth DSI environment and standardised sets of privileges that are assigned to each role. The policy ensures appropriate awareness and training for healthcare professionals regarding the service. This interoperability also ensures that control mechanisms (e.g. security audit) exist, data is shared in a way that all information provided by data-producer is visible to data-consumer etc.
Care process	Interoperability aspect responsible for the existence of care processes to share documents, to store documents, to create and manage audit logs. It also covers maintenance processes for code systems used and ensures that documentation of medical data exchanged is fully traceable, reconstructable and seamless
Information	Interoperability aspect responsible for coding systems used, the existence of officially defined systems/services for transcoding and the existence of controlled vocabularies. It also ensures that the information provided is understandable to the data consumer and the description of the dataset including content, syntax and format is available
Applications	Interoperability aspect ensuring the existence of the technical implementation of services. It also ensures authentication and identification of the HCP and the patient
IT infrastructure	Interoperability aspect ensuring data accessibility for HCPs through a unified portal, level of integration between service IS and pharmacy IS, strict end-to-end encryption duty in medical data exchange and level of integration between service IS and HCP IS
ePrescription use case	Interoperability aspect ensuring that all aspects of ePrescription are fully implemented and optimised. For example, the information about the drugs prescribed and prescriptions issued is provided on a patient portal
Patient Summary	Interoperability aspect ensuring that all aspects of Patient Summary are fully implemented, optimised and available for full use. For example, it ensures that patient summary is

eHealth service criteria: ePrescription and Patient Summary	
	regularly reviewed and updated, accessible to the patient and the patient can make appropriate changes to it

Alignment with eHealth service criteria

The results of ePrescription use case assessment are illustrated in **Figure 8** and Patient Summary use case assessment results are illustrated in **Figure 9**. Key ePrescription gaps in alignment with the eHealth Service Criteria are identified in **Table 24** and key Patient Summary gaps are presented in **Table 25**.

- **Policy** aspect of eHealth Service Criteria has scored highest in the ePrescription use case assessment. ePrescription in all of the Eastern partner countries has established control policy and control mechanisms (e.g. security audit).
- After the assessment of ePrescription use case, the lowest scores have been identified in **Information** and **Applications** domains. This was due to the limitations of the ePrescription use case implementations and the integration into the common country eHealth Digital Services Infrastructure.
- Patient Summary has scored highest in the **Policy** aspect of eHealth Service Criteria as defined processes exist for Patient Summary service in most of the Eastern partner countries.
- Patient Summary scored lowest in **Information** and **Applications** domains due to the lack of Patient summary service implementations in most of the Eastern partner countries.

Figure 8: Assessment results based on the eHealth Service Criteria: ePrescription

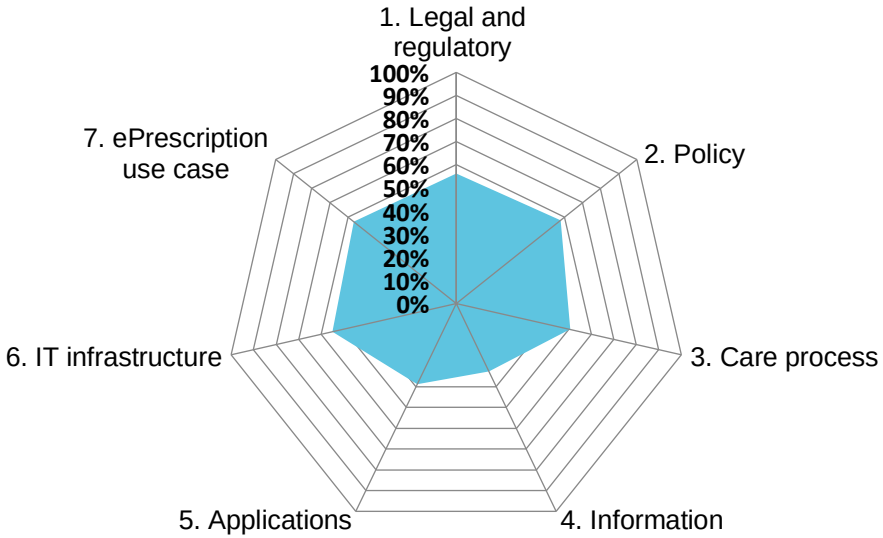


Table 24: Alignment with eHealth Service Criteria: ePrescription; and the Average Score

1. Legal and regulatory	**56%**
2. Policy	**58%**
3. Care process	**51%**
4. Information	**33%**
5. Applications	**39%**
6. IT infrastructure	**55%**
7. ePrescription use case	**57%**
	50%

Figure 9 Assessment results based on the eHealth Service Criteria: Patient Summary

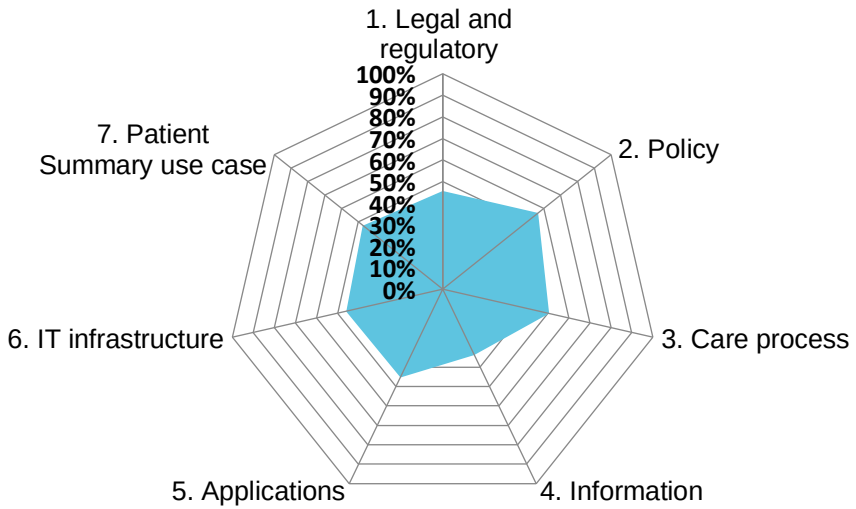


Table 25 Key findings in the alignment with the eHealth Service Criteria: Patient Summary

1. Legal and regulatory	**56%**
2. Policy	**58%**
3. Care process	**51%**
4. Information	**33%**
5. Applications	**39%**
6. IT infrastructure	**55%**
7. ePrescription use case	**57%**
	50%

4 Common guidelines for eHealth harmonisation and interoperability in the Eastern partner countries

4.1 Guidelines on key strategic directions

Thinking of eHealth and its strategic directions, defined in **Figure 10**, around health data help to make it more understandable, concrete and focused because any new system or digital service, involves data and information management. The key strategic directions have been defined in order to help with achieving harmonised eHealth development in the Eastern partner countries.

Figure 10: Overview of key strategic directions of interoperability in healthcare sector

4.1.1. Guidelines for comprehensive and actionable National eHealth Strategy

The eHealth services, systems, projects and initiatives in many countries have been developing rapidly. However, it has become evident that in order to achieve interoperable eHealth integration, planning and orchestration of different elements and efforts, described in **Table 26**, is the key.

Table 26: Summary of key elements and efforts to consider before eHealth implementation

Key elements and efforts to consider:
Cost containment, especially the maintenance of often underestimated costs
Truly interoperable national level systems
Trust and security services
Sense of “holistic” experience by both professional users (doctors, nurses, etc) and citizens (i.e. patients)

Why the National eHealth Strategy is fundamental for harmonization and interoperability?

Without a sense of targets and priorities, the long road to a fully interoperable and harmonised eHealth ecosystem can be discouraging and lacking focus. A stepwise approach oriented by an actionable strategy will help identify priorities and gradual pace towards interoperability. Therefore, the National eHealth Strategy (NeHS) became fundamental in achieving harmonisation and interoperability in eHealth. Risk planning and

mitigation strategies, described in **Table 27**, will add guarantees to the strategy in case countries lose focus in the process. This also may help gain more political traction and needed support for eHealth implementation.

Table 27: The summary of commonly observed NeHS mistakes

Areas of mistakes:	The NeHS commonly observed mistakes to avoid:	
1. Capacity management	Listing all eHealth areas for implementation, when there is no available budget or capacity. In practice, it is important to consider:	a) Financial capacity
		b) Given time period
		c) Organisational capacity to produce meaningful work in a selected area
		d) The technical basis to make meaningful use of technology
2. National vision	Listing various projects for implementation without considering the national vision. National objectives to be attained by fostering eHealth capacity	
3. National level strategy	The NeHS formulated not at the national level may not reflect the national perspective	
4. Stakeholders	Not considering the full complexity of stakeholders' environment and their different interests. Thus, stakeholders' involvement and communication are critical in the development of the NeHS	
5. Healthcare system complexity	Not considering the full complexity of the healthcare system. For example, the NeHS is a strategy for the public healthcare units but may not consider processes and systems used by pharmacies and/or private healthcare providers	
6. Ministries	Not foreseeing the engagement with ministries such as education, defence and justice, which normally cover aspects such as:	a) Training and capacity building,
		b) Military healthcare
		c) Prisons' healthcare

Digital versus eHealth

Digital health is an umbrella term for a wide range of digital technologies associated with healthcare. It focuses on health living, and society to improve healthcare delivery and support personalised and precision medicine. Digital health dedicates efforts in creating and securing the right governmental standing point for eHealth. Although, digital health strategy is needed in all countries, including the Eastern partner countries, considering the degree of digital health maturity, the focus should be on achieving solid eHealth foundations. A digital health strategy needs to consider aspects like mHealth, AI usage, digital tools for patients, road-mapping for digital inclusion and looking at the start-up ecosystems of small and medium-sized enterprises, or data economy. In contrast, the NeHS is more comprehensive and actionable, if it sets concrete priorities and identifies achievable targets. However, these should not be handled all at once because of a potential scarcity of resources and future issues which may need time to mature before they can be identified and fixed.

The NeHS should be comprehensive

The NeHS should be comprehensive and capture all trends in eHealth, eventually outlining reflections on digital health newest dimensions. However, to be successfully implemented, the NeHS needs realistic perspective and, in its structure, avoid commonly observed mistakes, see **Table 27**.

NeHS pillars for the Eastern partner countries

The six pillars of the NeHS have been proposed to better explain the substance of the NeHS and encourage its development in the Eastern partner countries. Although others may be identified, these six pillars, identified in **Table 28**, are deemed to be essential for successful strategy endorsement.

Table 28: Summary of the NeHS pillars for the Eastern partner countries

NeHS pillars for the Eastern partner countries:
Strong interoperability culture
Harmonization with the EU eHealth and Digital Single Market
A whole-of-government approach to health cybersecurity strategy
One strong national institution responsible for digital health, containing a cybersecurity specialized unit

NeHS pillars for the Eastern partner countries:
A large, multi-stakeholder group, capable of involving, encouraging and mobilizing all parts of the health system around cybersecurity efforts
International cooperation and outlook culture

Strong interoperability culture

The culture of interoperability is not just a careful observation and implementation of the presented guidelines. It requires certain behaviours and a particular mindset, i.e. it requires a model/ leader demonstrating the interoperability values. It is suggested that the government and the public bodies, as well as healthcare providers and industry at large, should act and think in an interoperable manner. For example, healthcare services and other organisations should be able to operate in interdependency. This is the key to achieving a better integrated healthcare, which is the ultimate goal of using technology in health.

Harmonization with the EU eHealth and Digital Single Market

When defining the NeHS in the Eastern partner countries, it is suggested to pay attention to the EU recommendations and guidelines for eHealth and Digital Single Market. For example, projects in the Eastern partner countries aiming to interoperate with or be funded by the EU, need to constitute the minimum denominator for interoperability to exist. This may include the common language and shared understanding of the image of information systems in healthcare. A combination of these behaviours constitutes harmonisation with the EU.

A whole-of-government approach to health cybersecurity strategy

A whole-of-government approach to eHealth is needed. Experience has shown that it is not possible to progress to sophisticated levels of maturity without significant cross-sectorial involvement. It is suggested for the government to get involved to stabilise the costs and avoid fragmentation of the nation. Increased usage of digital services in the healthcare system increases the need for cybersecurity. For example, digital services in a healthcare working environment often are used for personal reasons. It is becoming no longer possible for the healthcare personnel working long hours to be fully segregated from interacting digitally with the external networks. The government involvement in using generic frameworks, introducing education towards secure digital use and adopting lessons learned from other sectors is key.

One strong national institution responsible for digital health

Chapter 4.1 describes more arguments for whether a country should have a digital health institution. Evidence shows that countries and regions in the EU with mature eHealth infrastructure have such institutions. As can be anticipated, a strong agency responsible for digital health becomes a key institutional force and drive the NeHS implementation.

A large, multi-stakeholder group

Likewise, a larger multi-stakeholder group involvement is important and constitutes part of governance.

International cooperation and outlook culture

International cooperation and outlook culture development are suggested in the Eastern partner countries as a strategic innovation and gathering of future perspectives in preparation for future versions of the NeHS.

NeHS needs to be actionable

What makes the strategy actionable, is its capacity to link its main goals and initiatives with concrete lines of activities and then commit these in the timelines of five to ten years, considering the right set of principles and stakeholders. A yearly action plan should be approved together with the strategy document approval and endorsed by the relevant agencies (government, public institutes or important stakeholders). This is the best way to link the NeHS strategic contents with the necessary activities. Such action plan should have yearly hallmarks identified and ideally, quarterly defined progress goals. These should be discussed and agreed together with the available budget (public funds, a mix of public and private funds or other sources of financing). Key performance indicators can be created for each activity or initiative to measure process as well as outcome indicators or intended results. If the strategy is designed with a consideration of its plans, annual targets, budget and actors, it will be more realistic. It is recommended exploring all that needs to be achieved and how that could positively impact healthcare. Also, important to anticipate financing opportunities, mapping existing reality and potential challenges. This allows estimating the “duration” of a truly comprehensive yet actionable strategy.

Table 29: Proposed recommendations for the NeHS

R.1 Create, approve and regularly update a comprehensive and actionable national eHealth strategy that defines priorities, principles and activities for capturing and aggregating meaningful data
R.1.1 Work on a two-layer National eHealth Strategy: (1) Digital Health aspects are maintained; (2) steps to ensure interoperable eHealth ecosystem
R.1.2 Conduct a comprehensiveness test to your strategy, avoiding common pitfalls (see Table 27) and ensuring external expertise and advise is used to leap-frog into new ways of doing eHealth
R.1.3 Identify and ensure that the six pillars of a solid NeHS are secured (see Table 28)
R.1.4 Conceive the NeHS in a double layer approach taking enough attention to its implementation and stakeholder involvement
R.1.5 Design 10-year strategy, 5-year programmes and annual activity plans with realistic yet progressively more ambitious targets and key performance indicators

4.1.2. Guidelines for establishing a robust financing and operational model

Robust financing model

To ensure the sustainability of current operations and further development of Digital Health it is necessary to establish a robust financing model. Thus, it is important that the government provides incentives and uses different financing instruments to support healthcare providers. The purpose of making the financial means available is to fund the new generation of digital infrastructure among healthcare providers that would ensure interoperability between healthcare systems at the national and cross-border levels.[34] To ensure continuity of health care sector development, a robust funding strategy is required.

Public funding

Public funding is used to support the establishment or further development of an interoperable ecosystem for digital health, particularly used by healthcare professionals and healthcare providers. Also, public funding is used to enable patient access to their managed health data, firstly on the national level and opening up for the cross-border eHealth services in the later stages.

New healthcare financing models

From the healthcare financing models perspective, the fee-for-service model has been predominant historically, where fewer data (and even fewer health data) is needed to process claims. Payment is made based on the number of services provided, not the quality. However, nowadays, there are more complex and more sophisticated healthcare financing models, where the clinical outcome is the focus. This meaning that healthcare payment model is value-based, and its focus is rewarding healthcare providers based on the quality of care and treatment. This model helps to cut the costs attributed to unnecessary, inefficient services and uncoordinated care which create a burden on the whole healthcare system. Comprehensive financing models support changes in healthcare organisations and enhance preventative medicine. All healthcare financing models require large volumes of data about each case. Health data needs to be interoperable and certain healthcare systems need to be integrated to make it possible to improve healthcare in multiple facilities and measure outcomes in an equally disperse manner.

Procurements in healthcare

National authorities should refer to the Refined eHealth European Interoperability Framework for public procurements and when formulating tender documents proposals. Procurements should comply with e-accessibility specifications widely recognized at the European and international levels. This does not exclude compliance with already existing national regulations. It is recommended to consult relevant catalogues of standards, specifications and guidelines at the EU and national levels, in accordance with national interoperability framework and relevant domain-specific interoperability frameworks, when procuring and developing ICT solutions.[35]

34 eHealth Network Guidelines on interoperable eco-system for digital health and investment programmes, https://ec.europa.eu/health/sites/health/files/ehealth/docs/ev_20190611_co922_en.pdf

35 New European Interoperability Framework, https://ec.europa.eu/isa2/sites/isa/files/eif_brochure_final.pdf

Table 30: Proposed recommendations for robust financing and operational model

R.2 Establish a robust financing and operational model so that project-based eHealth ecosystem matures to an interoperable health data ecosystem
R.2.1 Establish a robust operational and financing model of Digital Health to sustain the operation of the so far achieved results and continuity of the further development (creation, maintenance and update) of the Digital Health Infrastructure, Services and Capabilities. Including, the definition of the key/common criteria for funding decision making of digital health initiatives
R.2.2 Establish interdependencies between financing, data quality and interoperability implementation to create adequate incentive schema for organisations to benefit from adopting and using digital health
R.2.3 Align public funding with the interoperable ecosystem to favour its behaviours
R.2.4 Follow the widely recognised (EU and international levels) Refined eHealth European Interoperability Framework and e-accessibility specifications when planning, conducting and controlling procurements

4.1.3. Guidelines for establishing digital health governance

Governance of digital health can be described as a set of rules, principles and actors, and their interrelations in fostering, implementation and use of digital technology in health. Digital health governance additionally includes the adoption, organisation and follow-up processes of the NeHS, as described in **Chapter 2.1**. An effective and modern governance framework should be formatted to uphold certain values and principles, described in **Table 31**.

Table 31: Digital health governance framework values and principles

Governance framework values and principles:
Maintain sustainability and long-term perspective
Inclusiveness-by-design
Patient engagement
Data-driven collaboration
Explicit processes and bodies for engaging national stakeholders
Security and privacy by design and default
Ecosystem view of digital health

Governance bodies

Several digital health governance bodies are required to provide direction and coordination of eHealth development. They protect individuals by assuring an oversight and accountability in various aspects relating to the use of ICTs.

Digital health governance framework

A good governance framework and design highly depend on a central “actor” – a Digital Health Agency. In practice, the Ministry of Health assign or create a dedicated eHealth function in an organization, or by expanding the mandate of an existing one to incorporate the functions of a national digital health agency. The central elements of the governance processes should focus on defending the principles already outlined. Above all, such governance should have built-in mechanisms that ensure it sets the pace so that digital health adoption can happen quickly. Different elements, described in **Table 32**, should be involved in a comprehensive Digital Health governance framework.

Health data element

It is recommended establishing an agency, or a competency centre that would be responsible for the use of health data. This element should have the capacity to aggregate and manage the secondary use of data at the national level. Typically, it is directly linked to the National Health Data Strategy, as will be later discussed in **Chapter 4.1.6**. Such element is important in defining processes and purposes for which data is collected, processed, qualified and stored or destroyed.

Governance framework aspects

The establishment of a governance framework involves the outline of the capacity, principles, decision-making mechanisms, strategy planning and follow-up, value creation and value capture, and budget-related matters. It is also important to decide who regulates and measures outcomes achieved and captures value creation. Finally, a circular strategy "plan-act-do-evaluate" is key to ensure that in the long run, in case of the government change or other decision-making factors, eHealth can still evolve. In practical terms, new acts and laws should be introduced creating the main element – the National Digital Health Agency – developing its main functions and selecting its main collaborators. The governmental act(s) should be further specified to adopt strategies, as well as elements of the governance framework. Finally, operationalised governance is very dependent on pragmatic thinking, and administrative support. Administrative staff and their capacity are key to success, together with regular meetings, well-set agendas, and prepared policy materials. Designing and setting in motion such mechanics may benefit from initial external help, but it should start running by its own in year two or three.

Table 32: Summary of elements describing Digital Health governance framework elements

Digital health governance framework elements:
A ministerial representative for eHealth/digital health
National Digital Health Agency (with roles to eHealth strategy, direct dependency to Ministry of Health and other governmental sectors, and active role in semantics and technical interoperability setting – potentially with contributions from other entities e.g. universities and other competent centres)
National Data Protection Authority
National or Sectorial Cybersecurity Agency
National agency responsible for eID, eventually looking at eIDAS node, and harmonization of other trust services
Authority or organization as the NCP for eHealth cross-border services
National Medical Drug-Device Agency or equivalent
National Public Health Authority
National Public Sector Interoperability Authority (to ensure collaboration with other public and private sector domains). Healthcare sector is not alone in going digital and collaboration and re-use of existing capabilities and infrastructures is key

Table 33: Proposed recommendations for Digital health governance

R.3 Establishing and operationalising comprehensive digital health governance model for control of data quality and useful purpose to be created
R.3.1 Establish and operationalise Digital Health Governance, including the governance instrument to involve different stakeholders of the digital health ecosystem
R.3.2 Establish a clear link between the NeHS and the governance
R.3.3 Define aims and principles for the governance framework
R.3.4 Introduce new acts and laws establishing the principles and self-sustainability elements of the National Digital Health Agency and governance bodies and frameworks (e.g. alternative financing models by creating data services)
R.3.5 Ensure that adequate capacity is allocated to the secretariat and technical support bodies involved in digital health governance

4.1.4. Guidelines for digital health architecture development and governance

The emerging field of digital health is the intersection of medical informatics, public health and business. To enhance health services through the information technology-based systems, clear digital health architecture must be defined together with evident governance inputs. Defining and establishing a mechanism for digital health architecture development and growing government support is highly recommended before undertaking any steps towards the development of the eHealth ecosystem. As a course of action should follow the inclusion of a mechanism for selection, prioritization and adoption of standards and common requirements on digital health capabilities, services and solutions.

eHealth digital service infrastructure building blocks

To strengthen eHealth architecture, illustrated in **Figure 11**, and facilitate the delivery of digital healthcare service across borders, as a reasonable approach, it has been proposed to use a combination of building blocks enabling and enhancing interoperability in digital health. In general, a building block is a self-contained, interoperable and replaceable unit encapsulating an internal structure, thus it enables more complex digital health service infrastructures to function properly. Based on eHealth DSI model for cross-border data exchange, several eHDSI building blocks, summarised in **Table 34**, have been developed.

Table 34: Summary of key eHDSI building blocks

The key eHDSI building blocks:
eHealth Interoperability Platform
HCP Information Systems
Healthcare Sector Registries and Information Systems
National Interoperability Platform
National Registries and Information Systems from Other Public Administration Domains

eHealth interoperability platform

eHealth interoperability platform is a modular interoperability platform that integrates core eHealth services for managing and exchanging patient-related medical data across various institutions and systems on a national and international levels. The platform incorporates eHealth services together with eHealth data access component, data and document storage component and eHealth data exchange component. The eHealth data access is a component responsible for secure and permissioned portal area access for patients, healthcare professionals and pharmacists. It also ensures insightful analysis of administrative, financial and clinical information through data analytics and open data APIs. The eHealth services provide fast and secure method to manage medical data electronically. Agile services adapt to healthcare needs quickly. Data and document storage provide various data storage sources, for example registries and catalogues. Data storage standards allow persistence and over time, interoperability. For example, data that is standardised in terms of format, nomenclature, terminologies and definitions will be able to enter other systems. The eHealth data exchange component ensures that data structure remains unchanged at the site of collection. Information exchanged via secure and authorised means.

HPC information systems

HCP information systems are the main originators of electronic health data. They allow electronic sharing of health information among clinicians, researchers and others. Semantic and technical interoperability standards guide the management of access to such systems and the control of their contents.

Healthcare sector registries and information systems

Healthcare sector registries and information systems refers to the systems designed to manage medical data and health information at the national level. This includes systems that handle data related to the healthcare i.e. systems that collect, store, manage and transmit health data. For example, public health information system provides the electronic capture, secure storage and confidential management of public health information for health practice, research and learning purposes.

National interoperability platform

National interoperability platform is responsible for advancing interoperability and connectivity of health services via the internet and related technologies with other sectors of activity. For example, education (sharing of vaccination record for school admission), or internal administration (for medical certification to allow driving licence renewal). The platform aims to serve as a connected platform providing personalised services that span through different sectors.

National registries and information systems from other public administration domains

National registries and information systems from other public administration domains ensure customisable, adaptable and operational registries and systems meeting eGovernment needs including eHealth. It is important that registries such as, civil registry, citizen tax registry and others connect with health-related sectors, for example, e-birth registration and e-death certification. These systems provide relevant information and operational services (for example, change of home address) to support better health services and outcomes (for example, adequate homecare, or geolocated population surveillance).

eHealth governance

Strong eHealth governance actions are required towards directing and coordinating digital health development. Commonly accepted data security frameworks, assurance schemes and standards must be established for personal health and social care data handling. eHealth services and systems should perform as expected, to produce secure, safe and reliable outcomes based on governance and cybersecurity standards. eHealth governance should include the institutions within health sector, and from other governmental agencies. This links with strong and formalised governance set-up as suggested in this document.

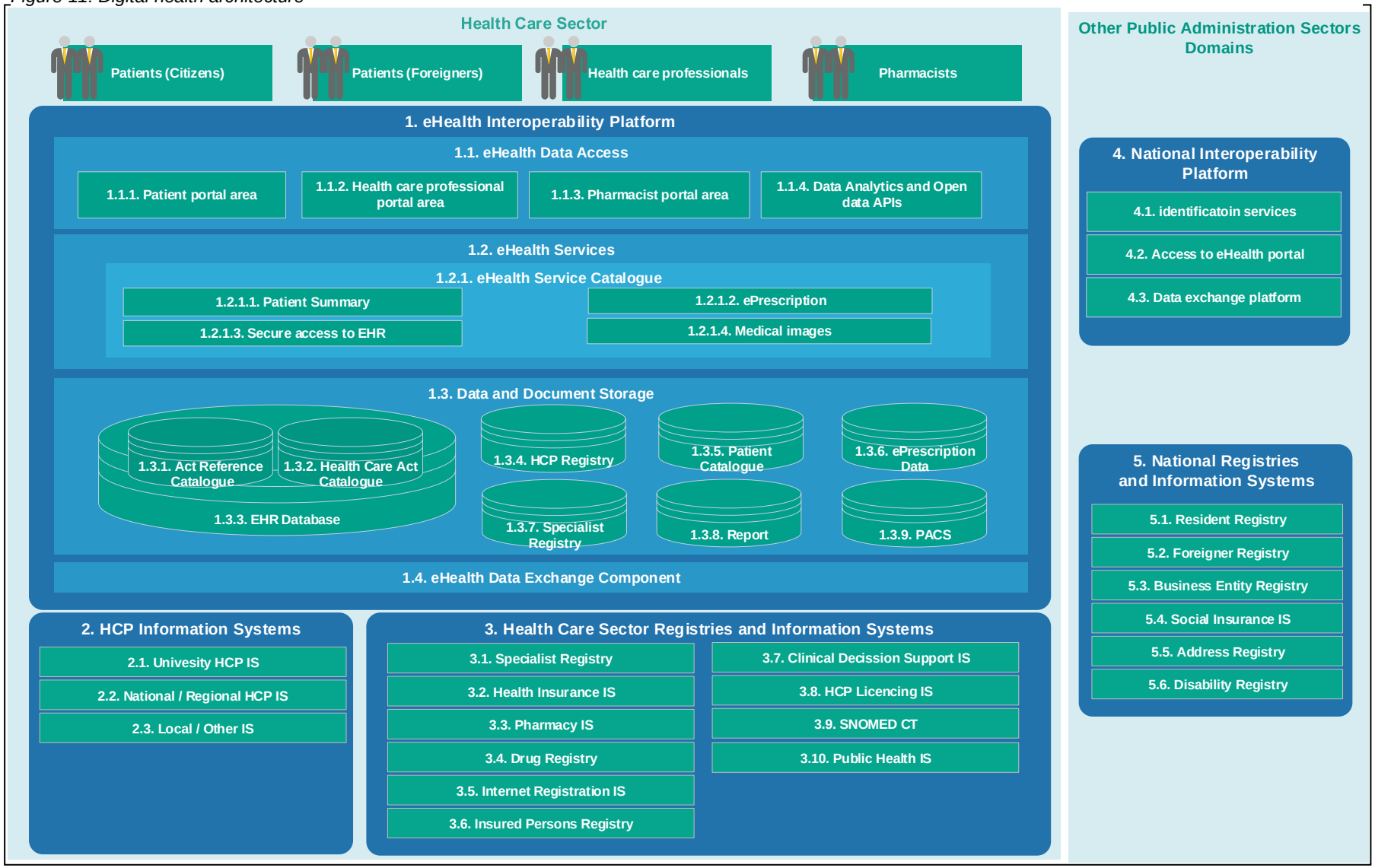
Enterprise architecture

Another element to consider is the discipline of Enterprise architecture (EA). EA links systems architecture to the organisational set-up and digital services. By mapping these together, enterprise architects can present a systemic view of interdependencies. Only through such extensive layout, new interactions and possibilities are easier to see and the interdependencies between services and digital links become obvious. EA as a discipline is also very useful for linking cybersecurity efforts and strategy to that of securing the more relevant services in healthcare and eHealth, as it becomes obvious who and what is affected when a given system or a DSI is compromised.

Table 35: Proposed recommendations for Digital health architecture development and governance

R.4 Digital Health Architecture Development and Governance for Interoperability, reusability and integrated health data-rich services
R.4.1 Define and establish mechanism for Digital Health Architecture and governance development, including the mechanisms for selection, prioritization and adoption of standards and common requirements on digital health capabilities, services and solutions
R.4.2 Establish eHealth architecture allowing rapid changes, for example, incorporation of new data elements as they arise. Such architecture supports portability and safe and secure development and integration of innovations
R.4.3 Build a unique identifier for patients and healthcare professionals enabling to exchange data with a full audit trail. For businesses, to provide customizable and adaptable operational systems that would ensure clinical and operational data relevance and meet business needs
R.4.4 Build upon existing rules and standards that govern access and content management. Refer to semantic and technical interoperability examples of internationally accepted rules and standards
R.4.5 While connecting with and contributing to, local, national and international health information systems, ensure continuous health information creation and collection
R.4.6 Accommodate heterogeneity across eHealth services to allow seamless information access from multiple sources
R.4.7 Establish governance and cybersecurity component in eHealth to ensure secure, safe and reliable handling of personal health and social care data
R.4.8 Introduce the Enterprise Architecture discipline to the national eHealth efforts and ensure that the overall system complexity is mapped with relevant and existing methods and IT tools.

Figure 11: Digital health architecture



4.1.5. Guidelines for health cybersecurity policies and strategies

Healthcare faces many challenges when trying to secure its information. For example, the unprecedented wave of new digital services, diagnostics and therapeutics, bring new changes in processes and organizational mindsets, in a long transition from paper-based services to digital healthcare.

Cybersecurity in healthcare

Healthcare must have strong cybersecurity capabilities. Individualized National Health Cybersecurity Policy and Strategy have been proposed in articulation with national trust services, and national cybersecurity strategy. Health cybersecurity policies advance when co-created with national cybersecurity frameworks and in close collaboration with national and international cross-sectorial agencies. However, these policies should be formulated by Ministries of Healthcare ensuring that the context of healthcare is present, commitment is higher, and innovation in initiatives will be more attractive.

Key aspects of a national health cybersecurity policy and strategy

The success of National Health Cybersecurity Policy and Strategy depend on the four cybersecurity enables in health, described in **Table 36**.

Table 36: Four cybersecurity enablers in health

Cybersecurity enablers:
Enforcing interoperability
Conformance assessment systems and audits
Enterprise architecture
Digital identification and other trust services

Interoperability and cybersecurity

Interoperability is an important enabler of cybersecurity because the lack of it often leads to the misuse of systems or information sharing channels. The investment in interoperable ecosystems is a security-enhancing investment in health where the use of internationally recognized standards for information systems, and electronic health records can be enhanced.

Performance assessment

Without proper compliance assessment systems and audits, many of the definitions, including security requirements will not be checked and verified. Systems of national-level authorities have a certain level performance, as they dictate, determine, even legislate, but this performance needs to be checked for conformance. The “normative-reality” gap is a big problem in cybersecurity because, in case of a crisis, decision-makers tend to act based on the norms they have emitted. Actions are suggested based on system attributes and capacity, and what in theory should have worked, fails. Compliance assessments and audits, regular as well as unexpected, can help close this gap.

Architecture of systems in healthcare

A solid health system enterprise architecture and information system architecture is the only way to know, at any given time, what systems relate to each other and, more importantly, which systems support each organization’s core and non-core activities. These links are essential to understand the relative risk if an information system in the ecosystem becomes compromised. Not just data breaches, but also, system performance issues, connectivity performances and system availability can be put at risk. To name a few examples, ePrescription, eDispensation, hospital laboratory results, or lists of patients to be operated on the next day. The May 2017 WannaCry incident showed these dependencies in the worst possible way. An enterprise architecture-based healthcare system would have the information granularity to simulate such consequences not just on the information systems, but, more importantly, on the business/provider layer.

Digital authentication systems

Without strong digital authentication, authorization and eSignature, information systems and operations technology may be a subject to an unauthorized accessing. Securing systems access to the right people and for the right set of roles is key to information security. Development of nation-wide solutions of this sort is key to cyber resilience which also brings other benefits to the process and technologies, for example, support creation and sustainability of up-to-date patient, healthcare professional and organization registries/ catalogues. The Ministry of Health is probably the best institution to keep and maintain the so-called “professional attributes”

database. This is an online system providing information about the healthcare professionals their medical speciality and whether to grant or restrict certain access. These definitions are best managed by the health side, while they can be used in authentication and authorisation of digital services in joint architectures with national trust service providers.

Table 37: Proposed recommendations for cybersecurity in healthcare

R.5 Strong cybersecurity capabilities and strategic thinking towards securing the data collected, stored and trusted by your citizens
R.5.1 Create a sub-strategy of the NeHS, within the framework of existing national cybersecurity guidance and the overall NeHS objectives
R.5.2 Define a sectorial governance model for cybersecurity in articulation with national governance
R.5.3 Ensure interoperability definitions and standards are dictated and audited by an authoritative institution
R.5.4 Introduce enterprise architecture training to technical staff and ensure it is meaningful to the mapping of healthcare reality
R.5.5 Establish good collaboration with national trust service providers and overseeing ministries, to ensure that access to health information is provided via secure architecture solutions

4.1.6. Guidelines for using healthcare data

Key processes and values of healthcare data

Using healthcare data is more than implementing eHealth solutions. The National Health Data Strategy is mostly about clearly defining processes and the purpose for which data is to be collected, processed, qualified, stored and destroyed. It is equally relevant to strike a balance between primary use of healthcare data, i.e. for the direct provision of care, and secondary use, for research, public health, health management and policy. Defining the right processes and values, described in **Table 38** and **Table 39** respectively, associated with healthcare data lifecycle and core values for data usage is key.

Table 38: Summary of healthcare data processes

Healthcare data processes:	
Data collection	Aspects such as the format of data entry, form design, terminologies and clinical data models
Data processing	Algorithms, cross-validations, interoperability and data transfer/sharing, dealing with missing data points policy. Lawful processing, consent management, patient access, and cybersecurity
Data quality	Aspects of captured data quality, consistency, subject identification issues and corrupted data management
Data storage	Duration, format, retrieval criteria and access policy
Data destruction	Authorization criteria, process and traceability, legal maintenance period, equipment used, legacy systems and durable formats, data recoverability, cybersecurity, back-up policy and contingency planning

Table 39: Summary of core values for data usage

Core values for data usage:	
Maintain trust	Safe and confidential use of personal information is essential to the development of complex data analysis tools and artificial intelligence in the healthcare sector
Deliver high-quality information	The quality of information is paramount to its usefulness. The information must be reliable, up to date, independent and trustworthy for population health purposes. It is not possible to develop reliable reporting systems if there is no confidence in data quality. The validity of data collection, adequate data quality management procedures ensuring high accuracy and adequate bias identification is extremely challenging in the big data era and must be a central requirement

Efficiency through data integration and interoperability	The historical background of health information systems development based on the "project" approach, resulted in scattered and differently codified data that does not yield a complete picture of a person's health (either for clinical practice or population health). The word "system" implies a connected and organized process. In most countries, health information systems lack such cohesion, having developed in a piecemeal way, fashioned by administrative, economic or legal pressures and invariably are highly complete
Data-driven innovation in healthcare	Innovation refers to transforming healthcare operations into data-driven processes, using technology and artificial intelligence to reshape management and accountability of healthcare service delivery and public health

Healthcare innovation

Innovation and research are key in fast-changing environments and advanced analytics where AI will play a major role in the healthcare domain. Healthcare innovation in the digital era is a national health policy requirement to support all the above-mentioned core values established for the use of health data and AI.

FAIR principles

Lastly, the FAIR principles[36] of data usage, described in **Table 40**, are a particularly useful framework for the National Health Data Strategy. FAIR and Open data principles allow permanent improvement circles.

Table 40: Summary of FAIR principles for data usage

FAIR principles:	
Data is FINDABLE	Information can be uniquely and persistently identifiable
Data is ACCESSIBLE	Information can be always obtained upon appropriate authorisation and through well-defined protocols
Data is INTEROPERABLE	Information can be digitally actionable, formalised and shared in different vocabularies, and it is semantically and syntactically presentable
Data is RE-USABLE	Information is sufficient and well-described to automatically integrate with other data sources

Table 41: Proposed recommendations for using healthcare data

R.6 Safe and rich data can only provide health value, if it is well explored and used, a Data Usage Strategy more than ad-hoc initiatives is key to this realization
R.6.1 Prepare and approve the Health Data Law, clarifying roles, responsibilities and potential usage, and securing FAIR principles are to be put in place
R.6.2 Create, curate and maintain the National Health Data Dictionary and Data Cycle Policy
R.6.3 Defend core values for health data usage, through proactive use of instruments such as policy, funding and incentive programs
R.6.4 Foster interface between health sector and data science fields
R.6.5 Promote interoperable solutions, and internationally recognised data standards and terminologies

4.2 Guidelines for cross-border eHealth service harmonisation and interoperability

Many people request medical help while travelling abroad. Patient Summary has been designed to provide healthcare practitioners with patients' key medical information in case of a medical encounter. Patient Summary dataset allows collection of most relevant medical information including medical history and medical conditions. It is suggested to pay particular attention to the design of dataset for this service, as it is to capture vital medical information necessary to provide proper treatment to the patient abroad, especially when there is a language barrier between the patient and the HCP.

36 FAIR open data principles resources online, https://www.go-fair.org/fair-principles/

4.2.1. Guidelines for alignment with European Interoperability Framework principles

To improve the current state of **User-centricity** in the Eastern partner countries, as a recommendation it is proposed, remodelling public services aiming to allow citizens and businesses to freely access and benefit from these services. Users' needs and requirements should be considered and used as a guide when designing and developing public services. In addition to this, several other expectations based on EIF principles can be suggested. For example, it is important to increase the availability of multiple channels in accessing public services. Multi-channel service delivery is an important part of public service purpose as it acknowledges that service users may require an alternative channel to access the service. To improve the user experience for the citizens and businesses it is suggested introducing the Government portal and create a single point of contact for every government service. This would reduce administrative complexity and facilitate access to public services. To design new public services and to further improve existing ones it is suggested implementing mechanisms that would involve users in analysis, design and assessment of public services. For example, users' feedback should be systematically collected to allow reflection on users' needs. Finally, the implementation of once-only principle and relevant-only principle for data collection is suggested. This means that citizens and businesses should be requested to provide the information once and only relevant information. Under the legislation in force and in accordance with data protection rules, administration of public services should be able to retrieve and share data to serve the users' needs.

Table 42: Proposed recommendations for resolving identified gaps in user-centricity aspect

R.7 Provide user-oriented eHealth services that are accessible and easy to use
R.7.1 Ensure the availability of multiple channels in accessing public services
R.7.2 Ensure the existence of a single point of contact in order to hide internal administrative complexity and facilitate user's access to public services
R.7.3 Establish mechanisms that involve users in analysis, design, assessment and further development of public services
R.7.4 Initiate the implementation of once-only principle and relevant-only principle for data collection

Multilingualism should be carefully considered in the design of public services. Every citizen should be able to use public services and for them to do so public services should be available in the language the citizen speaks. To improve the current state of multilingualism in the Eastern partner countries, a balance needs to be found between the ability of public administrations to offer their services in multiple languages and the expectations of citizens and businesses to receive services in their preferred language. Therefore, it is recommended, when designing public services, to decide the number of languages available in the public services based on end-user's needs.

Table 43: Proposed recommendations for resolving identified gaps in multilingualism aspect

R.8 Provide multilingualism in public services
R.8.1 When establishing new public services use information systems and technical architectures that provide options for multilingualism
R.8.2 Decide on the level of multilingualism support in public services based on the expected end-users' needs

The concept of **Openness** relates to open government data in the context of interoperable public services. According to the EIF principles, all public data should be freely available for use and reuse by others (except when restrictions apply for protection of personal data, confidentiality and intellectual property rights). Therefore, since public administrations collect and generate huge amounts of data, public sector in the Eastern partner countries is encouraged to make public information available for access and reuse as open data.

Table 44: Proposed recommendations for resolving identified gaps in openness aspect

R.9 Ensure that data collected and generated by public administrations is published as open data
R.9.1 Publish the public data as open data unless certain restrictions apply

Several suggestions have also been made to improve the current state of **Transparency** in the Eastern partner countries. For instance, the administrative environment such as administrative rules, processes, data, service and decision-making should be visible to other public administrations, citizens and businesses. In addition, ensuring the availability of interfaces with internal information systems would facilitate the reuse of systems and data and enable these to be integrated into larger systems. Finally, public administrations hold and manage large amounts of citizens' data, by respecting the applicable local legal framework, personal data protection should be established.

Table 45: Proposed recommendation for resolving identified gaps Transparency aspect

R.10 Increase transparency of Digital Services
R.10.1 Ensure internal visibility and availability of external interfaces for public services – opening up specifications of digital health services
R.10.2 Foster transparency-by-design especially relevant for systems requiring consent or that use/formulate algorithms for actions

4.2.2. Guidelines for alignment with the European interoperability layers

To improve the current state of **Semantic interoperability** it is recommended to address both semantic and syntactic aspects of Semantic interoperability. For example, the semantic aspect includes developing vocabularies and schemata to describe data exchanges. It also ensures that data elements are understood in the same way by all communicating parties. The syntactic aspect describes the information in terms of grammar and the format that is understood throughout exchanges between the parties. Here it is suggested that data and information should be recognized as a valuable public asset. Next step for improving semantic interoperability is to draft and coordinate an information management strategy at the corporate or enterprise level. This would help to avoid fragmentation and set priorities. Countries can benefit from joining international well-established semantic organisations like SNOMED International and learn from the most developed nations on how to organise and structure semantic assets. To improve the semantic interoperability more, innovative approaches are suggested, like data-driven design, as well as linked data technologies. To ensure seamless data movement and data portability among Eastern partner countries, it is recommended to introduce standardisation efforts. Robust, coherent and universally applicable information standards and specifications are needed to enable meaningful information exchange among countries.

Table 46: Proposed recommendations for resolving identified gaps in semantic interoperability

R.11 Develop semantic interoperability capabilities nationally and internationally
R.11.1 Perceive data and information as public assets that are appropriately generated, collected, managed, shared, protected and preserved
R.11.2 Put in place an information management strategy to avoid fragmentation and duplication, and to ensure meaningful use of data. Management of metadata, master data and reference data should be prioritised
R.11.3 Support the establishment of sector-specific and cross-sectoral communities that aim to create open information specifications and semantic dictionaries, and encourage the relevant communities to share their results on national and international platforms

To improve **Legal interoperability**, it is suggested implementing a system that would ensure that organisations operating under different legal frameworks, policies and strategies, would be able to work together. Clear agreements, also, should be drafted explaining how to deal with differences in legislation across the borders. The information exchanged between Eastern partner countries should maintain the legal value across borders. Data protection legislation should be complied with in both originating and receiving countries. For legal

interoperability to exist, it is not enough to have a good national legislation. There should be a process for legislation harmonization with the EU member-states, as well as among the Eastern partner countries. This requires a policy-level operating body to function. Please see **Chapter 4.1**.

Table 47: Proposed recommendations for resolving identified gaps in legal interoperability

R.12 Enhance legal interoperability by implementing interoperability and digital checks on existing legislation
R.12.1 Implement 'Interoperability checks' which could be used to screen legislation to identify any barriers to interoperability
R.12.2 Implement the 'digital check' on legislation to establish the public service and consider data protection requirements

4.2.3. Guidelines for alignment with the criteria of Digital Service Infrastructure

To improve the current state of **Organisational** infrastructure in the Eastern partner countries, several approaches have been proposed. As discussed in the previous chapters, to achieve commonly agreed and mutually beneficial goals, public services must align their business processes, responsibilities and expectations in an organised manner. In practice, it is suggested documenting and integrating or aligning business processes and relevant information exchanged. Existing business processes or established new ones need to be defined and aligned in different administrative entities. This would help to work together more efficiently and effectively when providing public services across the Eastern partner countries. Documenting business processes in an agreed manner and with commonly accepted modelling techniques will help with business process alignment. To better understand the overall business process, public services contributing to the delivery of cross-border services should have their business processes aligned.

Public services should also aim to meet the requirements of users. To achieve user-focused organisational interoperability, it is also suggested making public services available, easily identifiable and accessible to the end-users. Relationship between service providers and service consumers must be clearly defined. For example, finding instruments to formalise mutual assistance and interconnected business processes between participating public administrations.

Table 48: Proposed recommendations for resolving identified gaps in Organisational aspect

R.13 Enhance organisational infrastructure promoting whole of government approach and reusability
R.13.1 Apply the whole-of-government approach to interoperability e.g. reusability of infrastructures and services
R.13.2 Implement the processes for appropriately generating and/or collecting data and information which would be perceived as a public asset
R.13.3 Implement the processes for appropriately managing, sharing, protecting data and information
R.13.4 Implement the long-term preservation policy for information usage, especially for information that is exchanged across the borders
R.13.5 Implement the policy for transparency assurance
R.13.6 Design the processes which would help to monitor the implementation of relevant standards and specifications and check the compliance and the interoperability
R.13.7 Document business processes using commonly accepted modelling techniques
R.13.8 Implement the service (level) management plan or similar including the definition of functions, roles and responsibilities of the minimum required processes (i.e. incident, problem, change, configuration, and service level management), and support organisation
R.13.9 Implement the control measures to ensure that all users are assigned only with the necessary rights for performing their specific duties on the systems and services; and that these rights are periodically or on a business-event basis revised and can be revoked as necessary
R.13.10 Implement the in-country disaster recovery plan

R.13 Enhance organisational infrastructure promoting whole of government approach and reusability
R.13.11 Ensure the continuity and availability of service (set of SLAs)

4.2.4. Guidelines for alignment with the eHDSI criteria

To align with **Policy** aspects in the eHDSI criteria, several approaches have been proposed. Interoperability of eServices and eHealth, in particular, is established when information is exchanged, understood and used for policy-shared purpose. Policy aspect of eHDSI is the main source of stability and interoperability security of organisations as well as the governance. To align with the policy aspect, the Eastern partner countries should ensure that contracts and agreements between organisations are made and the purpose and value of the collaboration are set. Trust and responsibilities between the organisations should be formalised on the policy level. The governance of collaboration is to be tied up in the governance documents. For more detail, see 4.1 on key strategic directions.

4.2.5. Guidelines for alignment with eHDSI building blocks

To fill the gap in alignment with the **HCP information systems**, several recommendations have been proposed. For example, health information systems available on a regional and national level benefit best practices in healthcare and healthcare data management. This is being done via systems that collect, store, manage and transmit patient's her data, support operational management systems running in hospitals and assist in healthcare policy decisions. Healthcare providers and health organisations rely on HCP information systems to handle data related to their activities. For instance, as an integrated enterprise, HCP information systems can help improve patient outcomes, inform research and influence both policy and decision making. Health information technology (HIT) is involved in HCP information systems development. Large volumes of sensitive data are being accessed, processed and maintained within HCP information systems. This raises a primary demand for security which HIT helps to ensure.

Table 49: Proposed recommendations for resolving identified HCP information systems gaps

R.14 Develop and connect to HCP information systems to the National eHealth Interoperability platform
R.14.1 Define common requirements for the HCP IS including clinical processes and resource management use cases
R.14.2 Implement local, University and Regional hospitals medical information systems based on the defined common requirements
R.14.3 Provide assistance in integrating the HCP IS to the National eHealth Interoperability platform
R.14.4 Define interoperability checks and HCP IS compliance audits ensuring that HCP systems are able to integrate with the National eHDSI for initial solution validation as well as periodic checks

Table 50: Proposed recommendations for resolving identified Healthcare sector registries and information systems gaps

R.15 Digitise and integrate Healthcare sector registries and information systems to National eHealth Interoperability platform to achieve the single point of access to health information resources
R.15.1 Continue development towards optimisation of Health Care sector electronic Registers and information system by raising the common security and functionality standards to in-house or licenced systems for clinical process and resource management systems
R.15.2 Define a semantic interoperability roadmap and progressively adopt, for example, SNOMED CT and/ or other relevant terminologies
R.15.3 Fully implement and optimise the use of information systems in public health processes

Healthcare Sector Registries and Information Systems also showed a big gap in alignment with the EU standards and practices. It is particularly important to improve the current state of healthcare sector registries and information systems, as they become increasingly critical to clinical care and hospital operations. Resources need to be prioritised appropriately and a systematic approach should be used to improve healthcare registries and information systems without causing confusion or chaos in the healthcare systems as a whole. Health

registries and information systems should be easy to understand and use by anyone in the healthcare system including patients, clinicians and public health officials.

4.2.6. Guidelines for alignment with eHealth service criteria: ePrescription and Patient Summary

Administrative procedures regarding cross-border healthcare, in achieving harmonisation, are explicitly required to ensure a high level of protection of human health. In practice, appropriate **information** on all essential aspects of healthcare is necessary to enable patients to exercise the cross-border healthcare. To help patients to make an informed choice when they seek to receive healthcare in another Eastern partner country, the country of travel should ensure that patients from other Eastern partner countries receive the relevant information on safety and quality standards as well as which healthcare providers are subject to these standards. Patients also should be provided with information on specific aspects of the healthcare providers, healthcare services they offer and the treatment options. If requested, more extensive information regarding healthcare should be provided to the travelling patients, than is already provided to the residents. One of the mechanisms for providing appropriate information to the patients is to establish national contact points within each Eastern partner country. Information that must be provided compulsorily, should be specified. Furthermore, the information should be provided in any of the official languages of the Eastern partner countries, although, may be provided in other languages as well. Cross-border healthcare does not exclude the right to the protection of personal data. Therefore, every patient has the right to access their data concerning health. For example, the information in patient's medical records, such as diagnosis, examination results, assessments by treating physicians and any treatment or interventions provided. The Eastern partner countries should adopt measures to facilitate the comprehensibility of the information to patients concerning the prescription and the instructions included on the use of the product, including an indication of active substance and dosage.

Table 51: Proposed recommendations for resolving identified gaps in Information aspect

R.16 Adopt health information management standards and vocabularies
R.16.1 Based on the eHDSI Semantic Services Specifications, it is recommended to use coding systems such as ICD-10, ICD-9-CM, SNOMED-CT, LOINC, ATC and EDQM Standard Terms
R.16.2 Establish officially defined or at least of consolidated systems/services to perform transcoding
R.16.3 Establish controlled vocabularies (e.g. terminologies or taxonomies) to express valid value sets of coded concepts
R.16.4 Ensure availability of information on the description of the dataset including content, syntax and format in the directive of ePrescriptions and eDispensations as well as Patient Summary for unscheduled care
R.16.5 Ensure information is always provided in a way that the essential original semantics (meaning and expressiveness of sensible information) as imposed by the data-producer are preserved and understandable to the data-consumer

To ensure safe and high-quality healthcare, and high level of trust and security across the Eastern partner countries, interoperable **applications** should be in place. Countries should have set standards on the data included in patients' summaries and that can be shared between health professionals to enable continuity of care and patient safety across the Eastern partner borders. Furthermore, these standards should be the foundation for effective methods which would enable the use of medical information for public health and research. Countries should develop common identification and authentication measures for both the HCP and the patient to facilitate the transferability of data in cross-border healthcare.

Table 52: Proposed recommendations for resolving identified gaps in Applications aspect

R.17 Develop adequate eHealth application functionality/ use cases to support patient, doctor and regulator needs
R.17.1 Establish the technical implementation of services, for example, Directive Patient Summary for unscheduled care
R.17.2 Implement attributes for identification, authentication and authorisation of the HCP (prescriber and dispenser) and the patient. The eHDSI Identity Management Specification suggests collecting biometric characteristics such as retina

pattern, fingerprints, iris pattern, voice, face image and handwriting, etc. In addition, the identification, authentication and authorisation methods should be applied based on the business case defined by common information security and data protection policies and regulations
R.17.3 Implement common/ interoperable components for electronic identification, and trusted access of HCPs. The eHDSI Identity Management Specification suggests implementing unique identifiers for the authentication of the HCPs. Authentication process should use, if available, national interoperability gateways
R.17.4 Implement mechanisms of identification and authentication of the patient. The eHDSI Identity Management Specification suggests implementing unique identifiers for the authorisation of the patient. Patient authentication can also proceed with demographic data and/or via country's interoperability portal/gateway

4.2.7. Meting the standard EU Patient Summary and ePrescription datasets – assessment results

Patient Summary and ePrescription together constitute electronic cross-border health services. These are examples of the many infrastructures ensuring the continuity of care across the EU countries and has the potential to be developed and fully implemented in the Eastern partner countries. The HCPs can exchange health data of citizens who are travelling abroad in the EU, in a secure, efficient and interoperable way. Patient Summary can be used in any clinical encounter. Although, it is most useful when the healthcare professional and the patient do not share the same language, or there is an unplanned encounter where no information has been previously requested. ePrescription allows the patient to have uninterrupted access to their prescribed medication while travelling in the EU. The assessment conducted in the Eastern partner countries analysed the alignment with the EU datasets of Patient Summary and ePrescription **Figure 12**. These datasets have been taken as a measure to enable electronic cross-border data exchange. For example, the EU datasets for Patient Summary and ePrescription have relatively high coverage of optional data fields. However, it has been identified that none of the Eastern partner countries operate Patient Summary services meeting the requirements of the EU dataset. It has also been observed that none of the Eastern partner countries has operating ePrescription services in place, which would fully meet the EU dataset.

Figure 12: Inclusion of the standard EU datasets of Patient Summary and ePrescription in the Eastern partner countries

Patient Summary	
Overall coverage of Patient Summary dataset	**47%**
Number of countries compatible with EU dataset	**0**

ePrescription	
Overall coverage of ePrescription	**68%**
Number of countries compatible with EU dataset	**0**

Table 53: Proposed recommendations for resolving identified gaps in Patient Summary

R.18 Develop national Patient Summary eService in compliance with EU requirements for future cross-border pilot capability
R.18.1 The Patient Summary dataset should include a mandatory field for *National Healthcare Patient ID*
R.18.2 The dataset should include a mandatory field for *Given Name*, *Family Name/Surname* and *Date of Birth*
R.18.3 The dataset should include a mandatory field for *Country of Residence*
R.18.4 The dataset should include a mandatory field for *Date of Last Update*[37]

[37] EU guidance on Patient Summary PS Use Case - eHealth DSI Operations - CEF Digital (europa.eu)

Table 54: Proposed recommendations for resolving identified gaps in ePrescription

R.19 Develop national ePrescription eService in compliance with EU requirements for future cross-border pilot capability
R.19.1 The dataset for ePrescription (patient identification) mandatory fields should include Given Name, Family Name/Surname, Date of Birth, Regional/National Health ID
R.19.2 The dataset should include the mandatory fields (HP prescriber identification) such as *Given Name*, *Family Name/Surname*, *HP ID Number*, *Profession*, *Specialist*
R.19.3 The dataset should include the mandatory fields (Prescription data) such as *Prescription ID*, *Prescription Item ID*, *National/Regional Medical Product Code*, *Active Ingredient*, *Strength of the Medical Product, Medical Product Package, Pharmaceutical Dose Form, Number of Packages, Posology, Prescription Date of Issue*
R.19.4 The dataset should include the mandatory fields (Dispensed medicine dataset - patient identification) such as *Given Name, Family Name/Surname, Regional/National Health ID*
R.19.5 The dataset should include the mandatory fields (Dispensed medicine dataset - HP dispenser identification) such as *Given Name, Family Name/Surname, Pharmacist ID Number, Dispenser Facility Address*
R.19.6 The dataset should include the mandatory fields (Dispensed medicine data) such as *Dispensed Medicine ID, Prescription ID, Prescription Item ID, Active Ingredient, Strength of the Medicinal Product, Medicinal Product Package, Pharmaceutical Dose Form, Number of Packages, Date of the Dispensed Medicine Event*

4.3 Guidelines for digital trust service integration

One of the eHealth purposes is to extend the use of public and private administrative online services from the national level to citizens from other Eastern partner countries. Digital technologies, while evolving and transforming, are leading the way to interoperable cross-border services. However, the digital landscape is becoming more and more diverse which introduces novel challenges in cross-border interoperability. This leads to some obstacles that public and private administrative services are still to overcome.

As a result, citizens, businesses and governments cannot fully benefit from digital technologies. For example, citizens miss out on innovative digital solutions during the clinical encounters, HCPs miss out on interoperable digital solutions that can help provide better healthcare, governments and other public services miss out on digital technology and new generation software that can help manage and preserve digital information more effectively. The goal now is to overcome these obstacles and challenges by providing a proper regulatory background together with a set of a cross-border Digital Service Infrastructures (DSI) and Digital Trust Services.

In order to integrate Digital Trust Services, it is important to refer to the DSI, also known as generic and reusable Building Blocks based on the European Commission recommendations. These Building Blocks provide the foundation for interoperability infrastructure which is recommended to be reused in delivery of different public services across borders and sectors. This includes eHealth services.

4.3.1. Digital trust services available in the region

Digital trust services overview

Digital trust services are key enablers for secure cross-border interoperability. These services have been adopted by the EU, and now recommended to the Eastern partner countries, to enable continuous and secure electronic interactions between the citizens, public services, authorities and businesses. The regulation on electronic identification and trust services for electronic transactions in the EU single market, or in other words the eIDAS Regulation, has been developed to support an open, sustainable and resource-efficient society. Implementing the eIDAS Regulation or equivalent in the Eastern partner countries can bring multiple benefits such as higher security and convenient online activities, for example, submitting tax declarations or remotely opening a bank account.

To extend the eIDAS Regulation views, ideas and good practices to the Eastern partner countries, it is important to understand the present existing condition of digital trust services in the region, please see the detailed report developed during by the EU4Digital Trust and Security team[38]. It is also important to understand the issues relating to the implementation of the regulation and to find ways to facilitate the cross-border digital trust services in the Eastern partner countries.

[38] Legal-and-technical-maturity-assessment-of-Trust-and-eID-services-in-Eastern-Partner-countries.pdf (eufordigital.eu)

Legal maturity of Digital Trust services

Electronic identification (eID) and electronic trust services (eTS) are reliable systems playing an important role in electronic delivery of public services. The Eastern partner countries currently offer most of the trust and eID services using compatible technologies with those deployed by the EU member states. The main differences between how the trust and eID services are delivered in the EaP and in the EU are defined by the national regulatory frameworks governing:

- trust services and digital signatures
- electronic identification
- data privacy and protection
- legal value and use case for trust services

Technical maturity of Digital Trust services

It has also been identified that the following services described in the eIDAS Regulation are widely offered in the Eastern partner countries:

- Electronic signatures - a legal concept capturing the signatory's intent to be bound by the terms of the signed document.
- Electronic seals - similar to electronic signature, ensured document origin and integrity.
- Timestamp services - a legal-binding service providing date and time reference to prove the existence and integrity of an electronic document.
- Revocation and validation services - service providing digital revocation or validation of digital documents.
- eID and Mobile ID - services that guarantee the unambiguous identification of a person.
- Preservation services - service providing data preservation and retention.
-

Gaps of Digital Trust Services integration with the eHealth services infrastructure

Even though Digital Trust services are widely available in the region, the usage in the eHealth services provision could still be improved especially in:

- Electronic signatures integration in medical documents preparation and services such as eReferral and ePrescription
- Electronic seals - similar to electronic signature, for ensuring medical document origin and integrity to be used for reporting and statistical documents provision by the HCP where the documents are prepared in batches.
- Timestamp services are to be used together with electronic seals on medical documents providing date and time reference to prove the existence and integrity of an electronic document.
- Revocation and validation services integrated into the eHDSI infrastructure for checking the integrity of medical documents received.
- eID and Mobile ID usage for identification of the HCP workers and Patients in the eHDSI.

Table 55: Proposed recommendations for identified legal maturity gaps

R.20 Enhance legal maturity for the Digital Trust Services regulations
R.20.1 Regulatory clarification of the purpose between the electronic signatures and the electronic seals including the selected use cases in the eHealth infrastructure for national eHDSI and Hospital information systems
R.20.2 Regulatory clarification on the specific requirements for the mechanisms used to identify users in the public services including eHealth, with strong endorsement to re-use the national Digital Trust Services
R.20.3 Measures should be defined to protect the identifiable personal information contained in the digital trust services, especially qualified digital signatures, from misuse in activities like behaviour profiling without prior user consent
R.20.5 Performing regular audits of the digital trust services infrastructure and processes using internationally accepted standards

R.20 Enhance legal maturity for the Digital Trust Services regulations
R.20.6 Measures should be defined to ensure the protection of identifiable personal information and their accepted use, especially in the context of widespread cross-border transfer of identifiable personal information between EU member states and the Eastern partner countries

Table 56: Proposed recommendations for identified technical maturity gaps

R.21 Implement digital and interoperable by design systems and services which are aligned with defined architecture frameworks
R.21.1 Deploy endpoint and network-based intrusion detection systems
R.21.2 Integrate security events and information monitoring solutions for the TSP IT ecosystem
R.21.3 Perform regular vulnerability assessments and penetration tests

4.3.2. Guidelines on best practices for digital trust integration in eHealth services

Digital trust integration

The integration of Digital Trust Services across the Eastern partner borders can bring new services to eHealth. eID and eSignature have been recognised as building blocks supporting DSI Legal and Technical aspects which play an important role in the digitalisation of the healthcare system. eID and eServices integration should also be an important part of eHDSI Legal and eHealth Service Application aspects by providing national and cross-border level trusted way for patients, Health care sector workers to identify themselves in the eHDSI.

Table 57: Proposed recommendations for identified DSI legal interoperability gaps

R.22 Enhance DSI legal interoperability including cross-border personal data movement regulation for Digital Trust Services
R.22.1 Establish regulation for free cross-border movement of personal information between the Eastern partner countries and the EU (eID and eSignature regulations)
R.22.2 Establish legal certainty for cross-border electronic identification (eID and eSignature regulations)
R.22.3 Establish legal certainty for foreigners' living in the country electronic identification (eID and eSignature regulations)

Table 58: Proposed recommendations for identified DSI technical interoperability gaps

R.23 Develop DSI technical interoperability by creating/ re-using digital and interoperable by design, and aligned with defined architecture frameworks for easy Digital Trust services integration and reliable scalability
R.23.1 Integrate/ re-use public sector interoperability capabilities for secure public register access.
R.23.2 Integrate eSignature into medical documents preparation processes and services such as eReferral and ePrescription
R.23.3 Re-use electronic seals ensuring medical document origin and integrity to be used for reporting and statistical documents provision by the HCP where the documents are prepared in batches
R.23.4 Timestamp services are to be used together with electronic seals on medical documents providing date and time reference to prove the existence and integrity of an electronic document.
R.23.5 Integrate revocation and validation services integrated into the eHDSI infrastructure for checking the integrity of medical documents received
R.23.6 Integrate eID and Mobile ID for identification of the HCP workers and Patients in the eHDSI.

Table 59: Proposed recommendations for identified eHDSI legal and regulatory gaps

R.24 Integrate and re-use technical interoperability capabilities for identification of Health care sector professionals and patients
R.24.1 Establish identity authentication legal certainty for health professionals (data integrity, authenticity and non-repudiation principles) by integrating/ re-using existing public sector infrastructures
R.24.2 Establish common eID-based access services (the connection between eID and healthcare professional ID) by integrating/ re-using existing public sector infrastructures
R.24.3 Establish legal certainty of identity authentication for patients (data integrity, authenticity and non-repudiation principles) by integrating/ re-using existing public sector infrastructures
R.24.4 Establish common eID-based access services (the connection between eID and patient ID) by integrating/ re-using existing public sector infrastructures

Table 60: Proposed recommendations for identified eHealth service applications gaps

R.25 Create alternative, yet open standards based and commonly/ widely used for identification and authentication	
R.25.1 Define the possible options for identity authentication of healthcare specialists (prescriber and dispenser):	**R.25.1.1** National eID
	R.25.1.2 Secret data such as passwords or Pin-Codes
	R.25.1.3 ID card, passport, authentication token, certificate, cryptographic keys
	R.25.1.4 Biometric characteristics such as retina pattern, fingerprints, iris pattern, voice, face image, handwriting, etc.
R.25.2 Define the possible options for identity authentication of a patient:	**R.25.2.1** National eID
	R.25.2.2 Secret data such as passwords or Pin-Codes
	R.25.2.3 ID card, passport, authentication token, certificate, cryptographic keys
	R.25.2.4 Biometric characteristics such as retina pattern, fingerprints, iris pattern, voice, face image, handwriting, etc.

4.4 Guidelines on crisis management approaches

Identified management issues

Covid-19 pandemic has been highly consequential for the healthcare sector globally. This outbreak teaches both public and private healthcare sectors some very important lessons for the future management of such crisis. Lessons learned globally are also applicable to the Eastern partner countries and should be taken into consideration.

After a quick examination of key processes and on-site personnel efforts to maintain healthcare sector stability during this period, two main issues have been identified:

- Government organisations lack an integrated approach ensuring continuity of critical operations during crises
- Government organisations lack digital applications needed for businesses and public services continuity

Proposed crisis management approaches

It is suggested to look for practical ways of using digital systems in healthcare to help cope with crisis management. Several key government actions linked to eHealth have been described. For example, there is a need for a rapid setup of technology infrastructures for care solutions and remote working. There is also a great need for rapid technology deployment for triage and patient management. These technology solutions, once operationalized, then need to be stabilised and optimised. Finally, to prepare for the next crisis that could happen in the future, it is suggested to prepare the digital strategy and transformation to respond the next crisis more efficiently via technology-enabled smart hospital establishment.

Table 61: Proposed recommendations for identified digital health platforms and telehealth access gaps

R.26 Embark on eHealth interoperability and public sector interoperability platforms to effectively respond to crisis	
R.26.1 Use the existing digital health platforms:	**R.26.1.1** Provide basic eHealth services, e.g. ePrescription, eReferrals, electronic image sharing services
	R.26.1.2 Connect healthcare professionals via corporate collaboration tools for online and video consultations
	R.26.1.3 Establish AI Chatbots for patient triaging
	R.26.1.4 Ensure that both real-time and historical data is provided to healthcare professionals
R.26.2 Deploy communication channels to enforce patient adherence	
R.26.3 Use AI-driven triage and proximity tracing apps:	

Table 62: Recommendations for data-driven crisis management

R.27 Support rapid deployment of cloud and mobile applications, data-driven crisis experience management	
R.27.1 Establish epidemic experience management, monitoring and reporting via digital channels:	**R.27.1.1** Establish channels for checking and reporting health status
	R.27.1.2 Implement call centre assistance
R.27.2 Implement predictive analytics for emergency response and recovery:	**R.27.2.1** Use AI to identify populations at risk
	R.27.2.2 Improve emergency response time
	R.27.2.3 Integrate analysis of big amounts of data into existing crisis management centre
	R.27.2.4 Implement long-term predictive planning based on data collection
R.27.3 Implement data-driven crisis management enablement for planning, resource deployment and response to citizens	

Table 63: Proposed recommendations for e-Learning enhancement

R.28 Adopt e-Learning at scale to ensure daily practice sharing and update
R.28.1 Enhance e-learning strategies
R.28.2 Mobilise national e-learning platforms
R.28.3 Strengthen digital learning delivery

Table 64: Proposed recommendations for crisis management mobilisation

R.29 Have back-up capabilities in place for crisis management mobilisation	
R.29.1 Prioritise the critical services	
R.29.2 Deliver models for mission-critical services, e.g. establish work models for remote, hybrid and on-site services	
R.29.3 Crisis management centre mobilisation:	**R.29.3.1** Establish the crisis command centre integrated with hospitals and health systems
	R.29.3.2 Mobilise resources and assets, i.e. staff and procedures
	R.29.3.3 Crisis management centre mobilisation ensuring an omnichannel integration of the relevant data sources (HCP's medical and asset administration systems) to be visible from a single node

R.29 Have back-up capabilities in place for crisis management mobilisation	
	R.29.3.4 Establish dashboards and analytics to determine capacities and demands (beds, theatres, diagnostics and financing)
R.29.4 Ensure clinical workforce and vital analysis and resource planning:	R.29.4.1 Establish an action plan to reduce non-critical services and optimise virtual care delivery
	R.29.4.2 Optimise processes to let the medical professionals focus on their jobs
	R.29.4.3 Refine schedules, procedures and infrastructures
	R.29.4.4 Establish predictive analytics for modelling workforce needs and vital resources and supplies using Cloud-based tools e.g. Microsoft azure stack

Table 65: Proposed recommendations for supporting remote working

R.30 Establish culture and processes to support/ enable remote work	
R.30.1 Ensure technology readiness, analysis, setup and adoption:	R.30.1.1 Identify organisations' technological readiness and gaps
	R.30.1.2 Identify technological solutions which could be developed rapidly
R.30.2 Design the new smart working model:	R.30.2.1 Develop and establish a virtual model of operations, remote collaboration tools, communications and training
	R.30.2.2 Execute smart working labour contracts to turn a crisis response into a structural smart working
R.30.3 Create training manuals:	R.30.3.1 Prepare the training material for workforce working remotely
	R.30.3.2 Provide communications to formalise the guidelines and inform employees
R.30.4 Draft guidelines:	R.30.4.1 Use digital tools for smart working with critical processes
	R.30.4.2 Determine and mitigate the barriers and risks to large scale workforce working remotely
R.30.5 Begin analysis and benchmarking:	R.30.5.1 Analyse mission-critical services to ensure quality and continuity during remote working
	R.30.5.2 Prioritise smart working best practices

5 Guidelines for the progress monitoring

As it is important to follow the guidelines, it is equally important to find the way to monitor progress towards interoperable and harmonised eHealth ecosystem. To do so, the best indicator may be the progress in several eHealth milestones, described in **Table 66**.

Table 66: Summary of eHealth milestones

Key milestones to achieve success in eHealth interoperability
Define eHealth term in the context of the national healthcare legislation
Define and establish National eHealth Strategies
Define and establish eHealth governance model
Establish common security and data privacy policy for eHealth
Define National eHealth architecture model
Organise different funding and incentives for eHealth development in a programme manner
Integration with public infrastructure achieved (e.g. interoperability platform, trust services, registers)
Launch eHealth priority services cross-border pilots (ePrescription/Patient Summary)

A break-down of these milestones with involving advances in the four layers of interoperability can be the best way to monitor progress. Involvement in international cooperation, described in **Table 67**, can help to acknowledge achievements and appropriately direct future planning.

Table 67: Proposed recommendations for involvement in international cooperation

Involvement in international cooperation:
Establish partnerships with neighbouring countries or some of the EU countries to improve the areas which, by the common eHealth assessment framework, are less developed
Look for international support and consultancy, not only for the technical tasks to build IT systems, but to conceptualize strategy, governance, and implementation plans
Participate in eHealth international conferences organised by EU eHealth Network, HL7 community or other eHealth organisations and share the national experiences as well as understand the practices in other countries and the directions sector is moving
Actively explore new topics and harmonization opportunities within both, the EU space and the international practices by engaging in international projects and inviting international experts

Table 68: Proposed recommendations for progress monitoring

Proposed recommendations:
To establish a set of milestones and break them down into quarterly intermediate milestones
To create a follow-up unit in the Ministry of Health and/or the National eHealth Agency
To work with other countries and international experts/organizations in follow-up and strategic planning

6 Strong endorsement and common Eastern Partnership digital health policy

The EU4Digital Facility in the Eastern Partnership aims to foster the harmonisation of digital markets and thereby providing tangible results to citizens in the region. The programme also aims to extend the EU Digital Single Market to the Eastern partner countries, developing the potential for the digital economy and society, to bring economic growth, generate more jobs, improve people's lives and help businesses in different areas including health. It is fundamental to show how and why harmonization and interoperability guidelines in Digital Health, described in **Table 69**, can allow faster and more integrated digital health solutions development in the region. A pack of such information serves to outline the main aspects, define prioritization schemas and communicate them to Ministry of Health and health stakeholders.

All six countries making efforts to foster their eHealth development, creates the common understanding for eHealth that drives establishment of common agenda which is an instrument to direct the resources and effort for common interoperability goals. Recognising this agenda may allow peer-to-peer pressure and support in thriving for interoperability objectives. If cross-border services are to be created, similar maturity levels have to be achieved in different interoperability dimensions and across borders. An agreement can be conceived where countries voluntarily endorse and approve each other progress, as well as the metric to define such progress. Continuous support from local governments is key and ways to ensure enduring policies and strategies should be put in place. The Eastern partners capacity to "approve and endorse" can be developed by exploring the model of the EU eHealth network with adaptations. This helps in "follow-up on commitments for change" regarding Digital Health recommendations and guidelines. Such peer-to-peer commitment is key for eHealth implementation.

Table 69: Proposed recommendations for digital health fostering

Digital health fostering:	
Formally endorse the project's key recommendations (a higher-level summary of key guideline areas) as these benefit from the highest political empowerment, namely by a high-level ministerial meeting	
It would ideally be followed by a sustainability process of on-going international collaboration on Digital Health and a further endorsement of new topics/joint positions	
Fostering a common "formalized" collaboration space for Digital Health, particularly focusing on:	Joint Semantic interoperability efforts
	Setting up and evolution of concrete real eHDSI services
	Collaboration on Public health informatics

Table 70: General recommendations for endorsement of digital health policy in the Eastern partner countries

General recommendations:	
To Ministry of Health:	To establish an informal launching meeting of high-level representatives of Ministry of Health to start a formal eHealth Network of the six countries; choose the first country to hold the chairmanship for a maximum of 2years, with the main mission to follow-up from the EU4Digital recommendations, and to set up the network functioning, and sustainability
	To create a common agenda around digital health in the region, and harmonization and interoperability of eHDSI with the EU
To EC:	Find ways to enable support to the creation and the establishment of such eHealth policy body by eventually using a similar mechanism to the joint action to support the eHealth Network.

Please find annexes provided as separate documents.