HORIZON-HLTH-2023-IND

Project No. 101136424

The first **E**uropean **D**igital **Health Technology Assessment** framework co-created by all stakeholders in the European Health Ecosystem

Deliverable 2.3

Cybersecurity; DHTs, the EHDS and EDiHTA

WP 2 – Data security and privacy policy requirements for EDiHTA

Authors	Angela Lanna, Oleg Agafonov Berg, Serena Elizabeth Marshall (DNV)
Lead participant	DNV
Delivery date	02 April 2025
Dissemination level	Public
Type	Report

Version 1.0

Funded by the European Union

UK Research and Innovation

Funded by the European Union (GA no. 101136424). Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union the European Health or the Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.
The UK participant is supported by UKRI grant No 10106869 (National Institute for Health and Care Excellence).
The Swiss participant is supported by the Swiss State Secretariat for Education, Research and Innovation (SERI).

Revision History

Author(s)	Description	Date
Serena Elizabeth Marshall, Angela Lanna, Oleg Agafonov Berg (DNV)	Draft Deliverable	11/03/2025
Courtney Nadeau (DNV) Alexandros Patsanis (DNV)	DNV reviewers	11/03/2025
Iga Lipska (HPI) Wija Oortwijn (RUMC)	EDiHTA Reviewers	23/03/2025
Serena Elizabeth Marshall, Angela Lanna, Oleg Agafonov Berg (DNV)	Final version	31/03/2025
Patrick Schneier (accelCH)	Formatting, formal check	02/04/2025

Contents

Partner short names

UCSC	Università Cattolica del Sacro Cuore
FPG	Fondazione Policlinico Universitario Agostino Gemelli IRCCS
RUMC	Radboud University Medical Center
OUH	Odense Universitetshospital
FCRB	Fundació de Recerca Clínic Barcelona
HCB	Hospital Clinic of Barcelona
GUF	University Hospital Frankfurt
AGENAS	The Italian National Agency for Regional Healthcare Services
AQuAS	Agencia de Calidad y Evaluación Sanitarias de Cataluña
NSE	Norwegian Centre for E- Health Research
DNV	DNV AS
DNV-IT	DNV Business Assurance Italy Srl
EHMA	European Health Management Agency
EITH	EIT Health e. V.
EITH-FR	EIT Health CLC France
EPF	European Patients' Forum
HPI	Health Policy Institute
accelCH	accelopment Schweiz AG
NICE	National Institute for Health and Care Excellence
ITMOH	Italian Ministry of Health
VV	Vestre Viken HT
PH	Szpitale Pomorskie Sp. z o.o.

Abbreviations

AI	Artificial Intelligence
AIA	Artificial Intelligence Act - Regulation (EU) 2024/1689
CRA	Cyber Resilience Act - Regulation (EU) 2024/2847
CSA	Cybersecurity Act - Regulation (EU) 2019/881
DHT	Digital Health Technology
DoA	Date of Application
EC	European Commission
EHDS	European Health Data Space
EHRs	Electronic Health Records
ENISA	European Union Agency for cybersecurity
EU	European Union
EUCC	European Union Common Criteria
EUCS	European Union Cybersecurity Certification Scheme on Cloud Services
GDPR	General Data Protection Regulation (EU) 2016/679
GPSR	General Product Safety Regulation (EU) 2023/988
HIDs	Health Information Domains
HTA	Health Technology Assessment
HTAR	Health Technology Assessment Regulation (EU) 2021/2282
ICT	Information and Communication Technology
ISO	International Organization for Standardization
IVD	In vitro diagnostic medical device
IVDR	In Vitro Diagnostic Medical Device Regulation (EU) 2017/746
mApps	Mobile applications
MD	Medical device
MDR	Medical Device Regulation (EU) 2017/745
NIS	Network and Information Systems
NIS2	Directive (EU) 2022/2555
SW	Software

Definitions

AI system	A machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments; [AIA] Art.3 (1) (European Parliament, 2024)
Consumer	Any natural person who acts for purposes which are outside that person's trade, business, craft or profession. [GSPR] Art.3 (17) (European Union, 2023)
Cybersecurity	The activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats; [CSA] Art.2(1) (European Union, 2019)
Cyber resilience	The ability to protect electronic data and systems from cyberattacks, as well as to resume business operations quickly in case of a successful attack (European Central Bank, 2025)
Digital Health Technology	System that uses computing platforms, connectivity, software, and sensors for healthcare and related uses [ISO/TR 11147:2023 §3.1] (ISO, 2023)
Directive	A directive is a legal act adopted by the EU institutions addressed to the EU Member States and, as laid down in Article 288 of the Treaty on the Functioning of the European Union, is binding as to the result to be achieved. A directive is part of the EU's secondary law, the body of law that derives from the principles and objectives set out in the EU treaties (primary law).[…] (European Union, 2022b)
Harmonised standard	European standard adopted on the basis of a request made by the Commission for the application of Union harmonisation legislation [Regulation 1025/2012 Art.2.1.c] (European Commission, 2012)
Health Technology Assessment	HTA is a multidisciplinary process that uses explicit methods to determine the value of a health technology at different points in its lifecycle. The purpose is to inform decision-making in order to promote an equitable, efficient, and high-quality health system (O'Rourke et al., 2020)
Healthcare provider	Any natural or legal person or any other entity legally providing healthcare on the territory of a Member State [Directive 2011/24/EU] Art.3(g) (European Commission, 2011)

Intended purpose	- the use for which an AI system is intended by the provider, including the specific context and conditions of use, as specified in the information supplied by the provider in the instructions for use, promotional or sales materials and statements, as well as in the technical documentation; [AIA] Art.3(12) (European Parliament, 2024) - the use for which a device is intended according to the data supplied by the manufacturer on the label, in the instructions for use or in promotional or sales materials or statements and as specified by the manufacturer in the clinical evaluation; [MDR] Art.2(12) (European Parliament, 2017a) - means the use for which a device is intended according to the data supplied by the manufacturer on the label, in the instructions for use or in promotional or sales materials or statements or as specified by the manufacturer in the performance evaluation; [IVDR] Art. 2(12) (European Parliament, 2017b)
In Vitro Diagnostic Medical Device	Any medical device which is a reagent, reagent product, calibrator, control material, kit, instrument, apparatus, piece of equipment, software or system, whether used alone or in combination, intended by the manufacturer to be used in vitro for the examination of specimens, including blood and tissue donations, derived from the human body, solely or principally for the purpose of providing information on one or more of the following: (a) concerning a physiological or pathological process or state; (b) concerning congenital physical or mental impairments; (c) concerning the predisposition to a medical condition or a disease; (d) to determine the safety and compatibility with potential recipients; (e) to predict treatment response or reactions; (f) to define or monitoring therapeutic measures. Specimen receptacles shall also be deemed to be in vitro diagnostic medical devices; [IVDR] Art.2 (2) (European Parliament, 2017b)
Legislative framework	Adopted in 2008, the new legislative framework aims to improve the internal market for goods and strengthen the conditions for placing a wide range of products on the EU market. It is a package of measures that aim to improve market surveillance and boost the quality of conformity assessments. It also clarifies the use of CE marking and creates a toolbox of measures for use in product legislation. (European Commission)
Manufacturer	Any natural or legal person who manufactures a product or has a product designed or manufactured and markets that product under his name or trademark. [Regulation (EU) 765/2008 Art.2(3)] (European Commission, 2008)
Medical Device	Any instrument, apparatus, appliance, software, implant, reagent, material or other article intended by the manufacturer to be used,

	alone or in combination, for human beings for one or more of the following specific medical purposes: - diagnosis, prevention, monitoring, prediction, prognosis, treatment or alleviation of disease, - diagnosis, monitoring, treatment, alleviation of, or compensation for, an injury or disability, - investigation, replacement or modification of the anatomy or of a physiological or pathological process or state, - providing information by means of in vitro examination of specimens derived from the human body, including organ, blood and tissue donations, and which does not achieve its principal intended action by pharmacological, immunological or metabolic means, in or on the human body, but which may be assisted in its function by such means. The following products shall also be deemed to be medical devices: - devices for the control or support of conception; - products specifically intended for the cleaning, disinfection or sterilisation of devices […][MDR] Art.2(1) (European Parliament, 2017a)
Regulation	Regulations are legal acts defined by Article 288 of the Treaty on the Functioning of the European Union (TFEU). They have general application, are binding in their entirety and are directly applicable in all European Union (EU) Member States. A regulation is part of the EU's secondary law, the body of law that derives from the principles and objectives set out in the EU treaties (primary law).[…] (European Union, 2022c)
Union Harmonisation Legislation	Union legislation listed in Annex I to Regulation (EU) 2019/1020 and any other Union legislation harmonising the conditions for the marketing of products to which that Regulation applies [GPSR Art.3(27)]

Executive summary

The EDiHTA EU Horizon Europe project will create the first EU holistic standardised framework for the assessment of digital health technologies (DHT). In EDiHTA, DHTs encompass mobile Health (mHealth), telehealth, and artificial intelligence (AI). DHTs are used by diverse groups, including the public, patients and caregivers, healthcare professionals, and health system managers, to improve or support health system functioning and to improve health outcomes. Health Technology Assessment (HTA) will be focused on DHTs at different technological readiness levels, delivered at varying territorial levels (national, regional and local) taking into account the perspectives and needs of decision-makers, including the payer/insurer, developer/manufacturer, society and hospital management. The EDiHTA project development benefits from the representation of all stakeholders in the EU Health ecosystem (HTA experts/bodies, hospitals/clinicians, technology developers and end users, including patients and notified bodies, as well scientific associations).

The objective of Task 2.2 is to identify European regulations containing cybersecurity requirements that impact DHTs and understand through a mapping process how they should be considered in the HTA process of the different DHTs.

Legal acts (regulations and directives) included are:

- Cybersecurity Act (Regulation (EU) 2019/881) (European Union, 2024)
- NIS2 (Directive (EU) 2022/2555) (European Union, 2022b)
- Cyber Solidarity Act (Regulation (EU) 2025/38) (European Union, 2024)
- Cyber Resilience Act (Regulation (EU) 2024/2847) (European Union, 2024)

The regulatory requirements for DHTs have been identified, commencing with the precise definition of DHT in the legal acts. Once the mapping was completed, the cybersecurity requirements for the DHTs were extracted from the regulations.

These were then reviewed to link the regulatory requirement for the products to the larger context of the cybersecurity regulations within the HTA process. This review has elucidated the requirements for three distinct categories of stakeholders: healthcare providers, DHT manufacturers, and HTA bodies.

Conclusions have been drawn regarding the obligations and expectations pertaining to cybersecurity for DHTs. Additionally, any pertinent requirements for HTA bodies have been identified.

Results from this task will support the work carried out in work package 4 of the EDiHTA project, defining evidence requirements for a domain related to cybersecurity and associated regulation requirements.

We recommend that the consortium update the report as new legal acts and amendments are published.

1 Introduction

1.1 Cybersecurity threats

Cybersecurity threats and subsequent technology and data breaches have increased in prevalence, scale and sophistication. Common and damaging forms of cyberattacks include malware attacks, distributed denial-of-service attacks, ransomware, and phishing (Salama et al., 2024). Ransomware attacks alone accounted for 54% of EU analysed cyber incidents between 2021-2023 and are estimated to account for global costs exceeding EUR 250 billion by 2031 (Ifigeneia Lella et al., 2023; Morgan & Osborne, 2027). Cyberattacks target healthcare infrastructure, DHTs (including software as a medical device) and electronic health records (EHRs) as they provide a valuable target to criminals. Although cybersecurity is now recognised as critical to patient safety, it has historically been a low priority during technology development and deployment (Coventry & Branley, 2018). However, the health sector has become the most attacked industry over the last four years, with the COVID-19 pandemic catalysing this with the accelerated adoption of DHTs.

Problems arise from IT software and hardware vulnerabilities (Ifigeneia Lella et al., 2023), with reliance on unsupported old versions and an accelerated adoption of DHTs not coupled to a proportionate prioritisation of cyber prevention measures as these are costly. Cyber attackers exert pressure in two main ways: encrypting victims' data and, increasingly, leaking sensitive data. Although ransomware and exfiltration (for later blackmail/sale) offer a more immediate economic motive, there are also possibilities to infiltrate specific devices or take health services offline (without encryption). This is a standard part of hybrid warfare at this point.

1.2 Healthcare and digital technology

The digital transformation of healthcare, the high value of sensitive health data, geopolitical destabilisation, and reputational damage negatively correlating with patient trust have made healthcare an increasingly attractive target to cyber criminals. Breaches to healthcare technologies can be considered fundamentally as a risk to patient life or death if required data to determine healthcare decisions are restricted or unavailable.

The data collected by Digital Health Technologies (DHTs) can include a wide range of sensitive personal health information, such as electronic health records (EHRs), data from the Internet of Medical Things (IoMT), omics data, pharmaceutical records, radiology records, medical insurance and reimbursement claims, social media usage, environmental factors, and personal behaviour and lifestyle information. The processing of this data, along with the associated responsibilities and requirements, depends on the legal, ethical, and health context in which the data is collected.

The effects of attacks on data are magnified due to increasing health technology integration and interconnectivity, continuous monitoring, mobile consumer devices (e.g. sharing of patient reported data from DHTs to healthcare providers) and automation offering multiple attack pathways. With data increasingly available across numerous networks and stored electronically, privacy breaches now have the potential to expose the complete, detailed health records of millions of people.

Reliance on a diverse supply chain for security reemphasises the need for a secure ecosystem approach. However, funding is often prioritised towards integration of novel DHTs and not towards safeguarding them (Coventry & Branley, 2018). This changing landscape and susceptibility to attacks threatens the digital cyber resilience in healthcare, i.e. the ability of healthcare systems to succeed under varying conditions (Wiig, 2019).

1.3 Cyber resilience

Cyber resilience from the perspective of digital healthcare requires a risk management process through a holistic approach considering technologies, processes, people and cultures. Cyber security toolkits and guides provide advice for best practices to understanding risk, implementing appropriate measures and preparing for cyber incidents. The National Cyber Security Centre, for example, provides ten steps to achieving cyber protection (National Cyber Security Centre, 2021):

- Risk management
- Engagement and training
- Asset management
- Architecture and configuration
- Vulnerability management
- Identity and access management
- Data security
- Logging and monitoring
- Incident management
- Supply chain security

Cyber resilience and cybersecurity should take a product lifecycle approach, be compliant with regulations from conception, and be embedded in an organisation's culture.

Systematic approaches to cybersecurity face significant challenges from users not knowing what data is tracked and when (invisibility), having flawed or incomplete data (inaccuracy), data being stored indefinitely, data being sold (marketability), and the risk of personal information being re-identified (Algarni & Thayananthan, 2025).-Data security and protection can be considered in three data scenarios: at rest, in transit and in use. Encryption methods and query operations over encrypted data at rest, as well as protection of data in transit, are relatively well established and robust. Security can include cryptographic security, block-chain based security, authentication and authorisation and security analysis and network security. Data in use is more problematic to protect; computation is required for decryption, which can reveal the information. Techniques to mitigate risk may include trusted execution environments, homomorphic encryption, multi-party computation and differential privacy. However, even with effective implementation of a selection of protection techniques, problems can arise across the supply chain from differing computing power and speed, inconsistent connections, data heterogeneity, high costs and unauthorised access and misuse (Thapa & Camtepe, 2021).

1.4 EU coordinated action

In addition to relevant regulations and directives, the European Agency for Cybersecurity (ENISA) created the Network and Information Systems (NIS) cooperation Group workstream on Health to (i) provide coordinated guidance to the Member States and (ii) monitor the implementation of NIS provisions. ENISA support the maturing of secure systems and infrastructures to strengthen the EU Health Sector. One way they achieve this is the EU action plan on the Cybersecurity of hospitals and health. The action plan states that preparedness must take a ‘whole-of-society’ and ‘whole-of-government’ approach (Niinistö, 2024). Implementation will involve healthcare providers, the wider healthcare ecosystem, Member States and the cybersecurity community. Although the target is hospitals and health providers, there is recognition that these operate interdependently with the supply chain and ecosystem of health data users, including those that generate DHTs and medical devices. The focus of the cross-border action plan is 1) **prevention** of incidents, 2) improving cybersecurity information sharing and **detection** capabilities for faster reactions, 3) measures to **respond to** incidents and **recover** from them and 4) envisioning ways to **deter** cyber-attacks (Commission, 2025)

Emerging cybersecurity threats for 2030 are detailed in an ENISA foresight report, Figure 1, of which many are relevant (e.g. 1, 2, 4, 5, 8, 9, 10) to the healthcare ecosystem (Rossella Mattioli et al., 2023), emphasising the priority the DHT ecosystem must now place on cybersecurity:

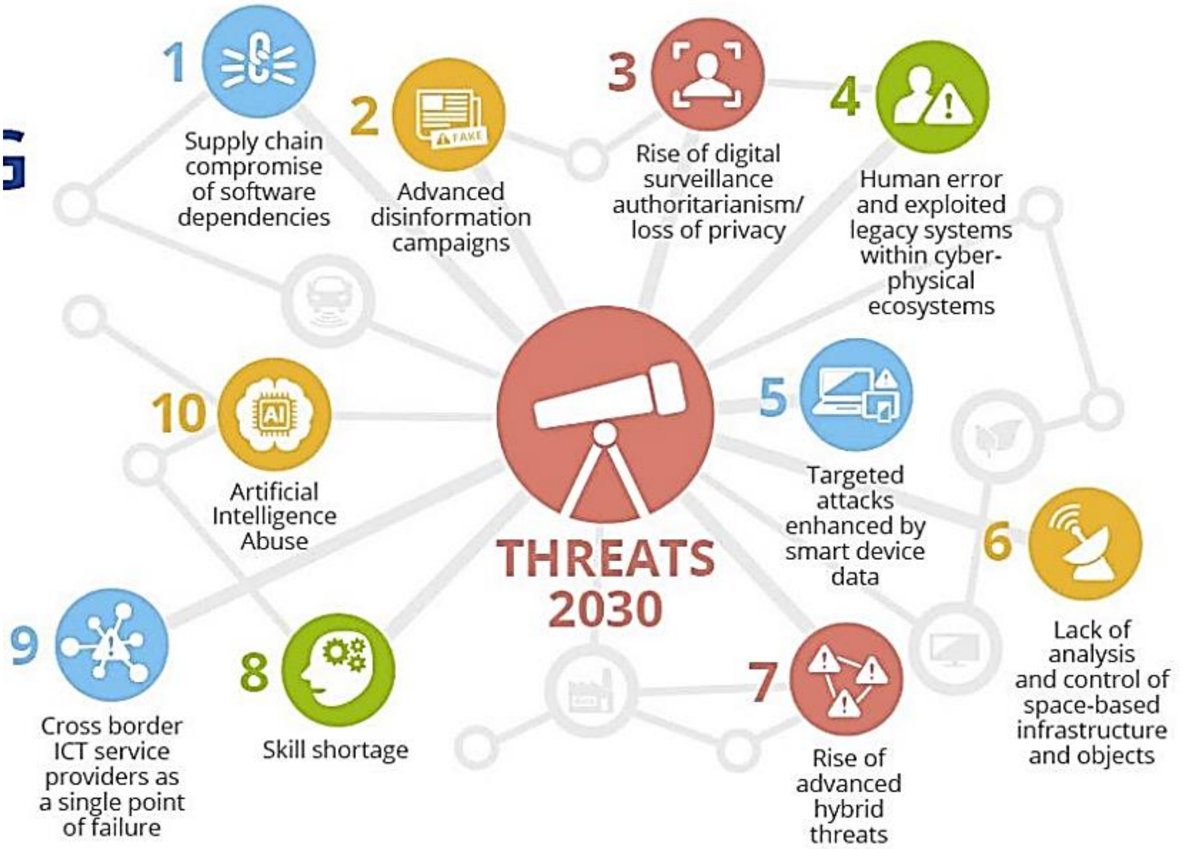

THREATS 2030
1 Supply chain compromise of software dependencies
2 Advanced disinformation campaigns
3 Rise of digital surveillance authoritarianism/ loss of privacy
4 Human error and exploited legacy systems within cyber-physical ecosystems
5 Targeted attacks enhanced by smart device data
6 Lack of analysis and control of space-based infrastructure and objects
7 Rise of advanced hybrid threats
8 Skill shortage
9 Cross border ICT service providers as a single point of failure
10 Artificial Intelligence Abuse

Figure 1: Top 10 cybersecurity threats (ENISA Foresight Report)

HTA, and the framework produced by EDiHTA, has an opportunity to define important considerations when assessing the cybersecurity of the uptake of digitally secure technologies that strengthen the healthcare ecosystem in the fight against cyber incursions.

2 Objective and Scope

The objective of WP2 is to provide the regulatory context within which the EDiHTA framework needs to be operationalised (informing WP3 and WP4), utilising analysis of national and EU policies to support the development of the EDiHTA framework through:

- Review of policy implications on data protection work (see deliverable 2.1)
- Identification of decision structures related to EHDS (see deliverable 2.4)
- Identify the correlations and challenges between the conformity assessment under the MDR and AI Act and HTA processes (see deliverable 2.2)

This deliverable supports the identification of regulatory requirements that define a DHT under assessment, understanding when and why they apply and focusing on the cybersecurity aspects of the regulatory requirements.

The objective of task 2.2, the scope of this report, is to understand and map the DHTs and their requirements towards the EU cybersecurity acts, as well as the impacts for different stakeholder groups, through review of the legal acts on cybersecurity.

3 Methodology

3.1 Review criteria

Objective of the deliverable: Identify any cybersecurity requirement that might have an impact on the HTA process.

To identify the implications of cybersecurity on DHTs, a four-tiered approach was utilised:

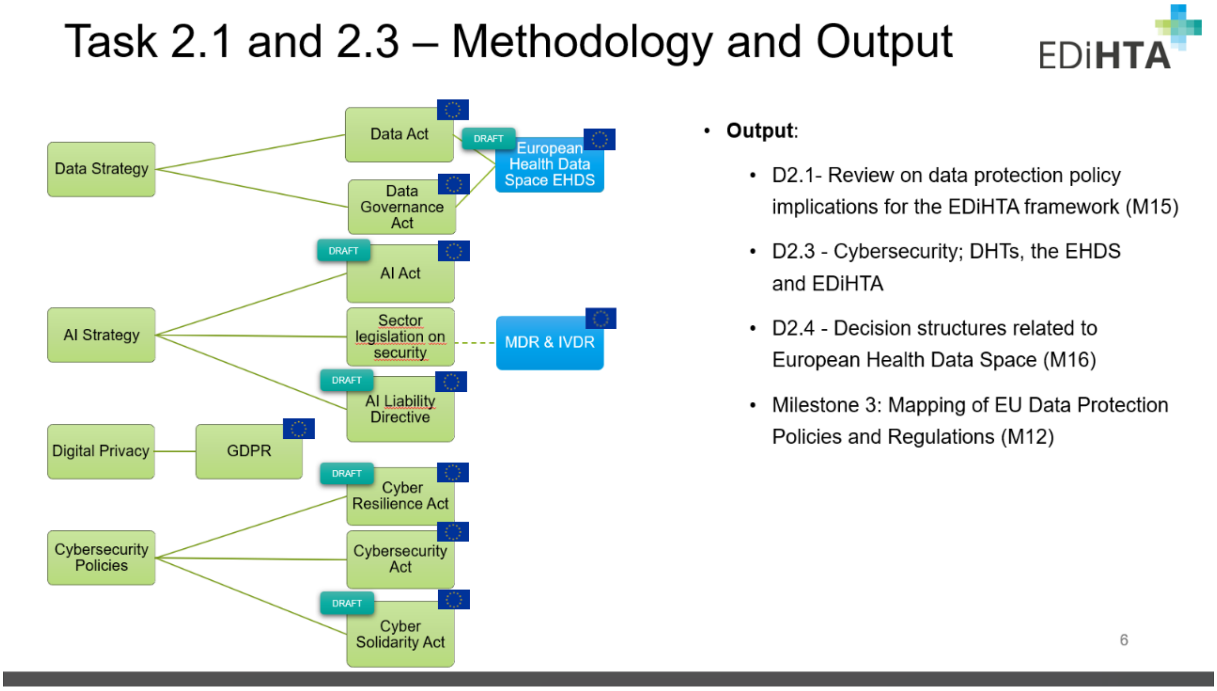
1. An initial mapping of the interconnection within coverage of the EU regulations that might apply to DHTs in the context of HTA
2. A systematic approach to each DHT type to understand features and subsequent legislative requirements
3. An assessment of the cybersecurity component of regulations and cybersecurity-specific EU legislation. This review was conducted systematically, first identifying the legislation, version and amendment date, then understanding the scope, applicability to a DHT or users, linking to other legislations that may horizontally impact (Ensuring definitions align) and reviewing the impact for EDiHTA through:
4. A consideration of the relevance of these three stakeholders responsible for implementing and assessing cybersecurity measures in the DHT and EDiHTA context.
   - **Manufacturers**: generically identified as the entities that place the product (DHT) on the market under its own responsibility (according to the regulations identified in the above paragraphs).
     Refer to definition as in Regulation (EU) 765/2008 Art.2(3) 'manufacturer' shall mean any natural or legal person who manufactures a product or has a product designed or manufactured and markets that product under his name or trademark. In the context of this review, providers, as per the AI act, are understood as manufacturers.
   - **Healthcare providers** as defined in Article 3, point (g), of Directive 2011/24/EU of the European Parliament and of the Council (14) *[i.e. 'healthcare provider' means any natural or legal person or any other entity legally providing healthcare on the territory of a Member State]*
   - **HTA Bodies:** as per EMA's website, *"Health technology assessment body - A public organisation that provides recommendations on the medicines and other*

> *healthcare interventions that can be paid for or reimbursed. These organisations look at the relative effectiveness and cost-effectiveness of medicines that have been authorised.* (European Medicines Agency)*"*

The results from this work can then be used to support the work of WP4 and inform the development of a cybersecurity assessment domain in the EDiHTA framework.

3.2 Initial mapping

At the beginning of the project, the regulations to be reviewed in the cybersecurity sector were identified as in Figure 3: initial mapping of regulation coverage versus digital health technologies. Most of the identified regulations were still unpublished.



Task 2.1 and 2.3 – Methodology and Output

EDiHTA

- **Output**:
  - D2.1- Review on data protection policy implications for the EDiHTA framework (M15)
  - D2.3 - Cybersecurity; DHTs, the EHDS and EDiHTA
  - D2.4 - Decision structures related to European Health Data Space (M16)
  - Milestone 3: Mapping of EU Data Protection Policies and Regulations (M12)

6

Figure 2: Initial mapping of cybersecurity regulations

Over the past year, the regulatory framework has steadily evolved, leading to the cybersecurity regulations as outlined in 5 Cybersecurity Acts **Error! Reference source not found.**

3.2.1 List of legal acts considered for review on cybersecurity

Regulation Short Name	Name	Status
Cybersecurity Act (CSA)	Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)	Published

Regulation Short Name	Name	Status
NIS2	Consolidated text: Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS2 Directive)	Published
Cyber Solidarity Act	REGULATION (EU) 2025/38 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 19 December 2024 laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cyber threats and incidents and amending Regulation (EU) 2021/694 (Cyber Solidarity Act)	Published
Cyber Resilience Act (CRA)	Regulation (EU) 2024/2847 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) No 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act)	Published

Table 1: regulations on cybersecurity

3.2.2 Other Acts, without a specific review in the context of cybersecurity.

Regulation Short Name	Name	Status
HTA	Regulation (EU) 2021/2282 of the European Parliament and of the Council of 15 December 2021 on health technology assessment and amending Directive 2011/24/EU	Published

Table 2: HTA Regulation (European Parliament, 2021).

Regulation Short Name	Name
EHDS	Regulation (EU) 2025/327 of the European Parliament and of the Council of 11 February 2025 on the European Health Data Space and amending Directive 2011/24/EU and Regulation (EU) 2024/2847 (Text with EEA relevance
Data Act	Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act)
Data Governance Act	Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act)
GDPR	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

Table 3: EU acts not included in the review on cybersecurity

3.3 Directives and Regulations

In the context of the review, the word regulation has to be read as any legal act adopted by the EU and constitutes part of the EU's secondary law. For the sake of definitions, we can briefly summarise:

- A directive is a legal act adopted by the EU institutions addressed to the EU Member States, and it is binding as to the result to be achieved. The national authorities of each EU Member State determine the form and the methods they use to incorporate the directive into their national law (formally known as 'transposition'), within 2 years of the directive's adoption. Infringement proceedings apply if a Member State does not transpose (European Union, 2022b).
- Regulations are legal acts, are binding in their entirety and are directly applicable in all EU Member States. A regulation is directly applicable in all Member States. This means that it applies immediately as the norm in all Member States, without needing to be transposed into national law (European Union, 2022c).

Complete descriptions and definitions are available on EUR-lex in the section for Summaries of EU legislation (https://eur-lex.europa.eu/homepage.html).

4 Cybersecurity and DHTs

To gain a deeper understanding of the topic we are exploring, we need to address two fundamental questions:

- what is a DHT from a regulatory perspective?
- what is cybersecurity?

We will describe a DHT with elements that link it to relevant regulation and its requirements, and we will examine the current regulatory framework for cybersecurity.

Our sources include mainly EU acts, official EU websites and international standards. We would refer to international standards only when EU references are incomplete, unclear or not exhaustive.

For the definition of DHT, as the EDiHTA definition was commencing in parallel while progressing with this task of the project, we have referred to a definition used in an ISO document.

ISO/TR 11147:2023(en) Health informatics — Personalized digital health — Digital therapeutics health software systems (ISO, 2023).

3.1

digital health technology

DHT

system that uses computing platforms, connectivity, software, and sensors for healthcare and related uses

Note 1 to entry: These technologies span a wide range of uses, from applications in general wellness to applications as a medical device. They include technologies intended for use as a medical product, in a medical product, or as an adjunct to other medical products (devices, drugs, and biologics). They can also be used to develop or study medical products. (FDA-NIH Biomarker working group, 2025)

The definition of a DHT is very wide and encompasses several types of products, with a computing platform, connectivity and software and can have different purposes, including health purpose or a wellness purpose. In practice, the DHT product is defined by its features and intended purpose.

Union harmonisation legislation for placing products on the market uses the same pattern to define the products regulated by the European Acts: features and/or purpose. Features and/or purpose will guide us to understand which EU legislation applies to DHTs.

The legal definition of cybersecurity is:

> ***Cybersecurity*** means the activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats; [Cybersecurity Act Regulation (EU) 2019/881, Art.2.1]

The digital transformation and the increased prevalence of connected and interconnected healthcare and wellness products has shifted the focus of the union harmonisation legislation from the safety of a product to the security of the product. The definition of cybersecurity shifts the focus from physical attributes of the product to the security that comes with the intangible attribute of the product (software and connections).

EU has recently launched a series of regulated initiatives targeted to cybersecurity. EU created a safety net for cybersecurity that also ensures cyber resilience.

A definition of cyber resilience is available in the European Central Bank website:

> ***Cyber resilience*** refers to the ability to protect electronic data and systems from cyberattacks, as well as to resume business operations quickly in case of a successful attack. (European Central Bank, 2025).

With a broader context, as in the Directive (EU) 2022/2557 on the resilience of critical entities, ‘resilience’ means *a critical entity’s ability to prevent, protect against, respond to, resist, mitigate, absorb, accommodate and recover from an incident* [Art. 2.2 (European Union, 2022a)].

The two concepts together aim to create a protection for products, services, networks, information systems, processes and then to create a system that ensures that, when the protection fails, there is a system that allows response, recovery and the continuity of the systems.

4.1 DHTs as products in the European market

It is essential that market access regulations and regulations for HTA (forming the basis for reimbursement and pricing in some cases) remain well-linked.

An initial review, at the beginning of EDiHTA, tried to identify the interconnection within coverage of the EU regulations that might apply to DHTs in the context of HTA. At that time, with the landscape of cybersecurity in terms of regulations still very vague and unknown, the DHTs could be mapped in the venn diagram in Figure 3.

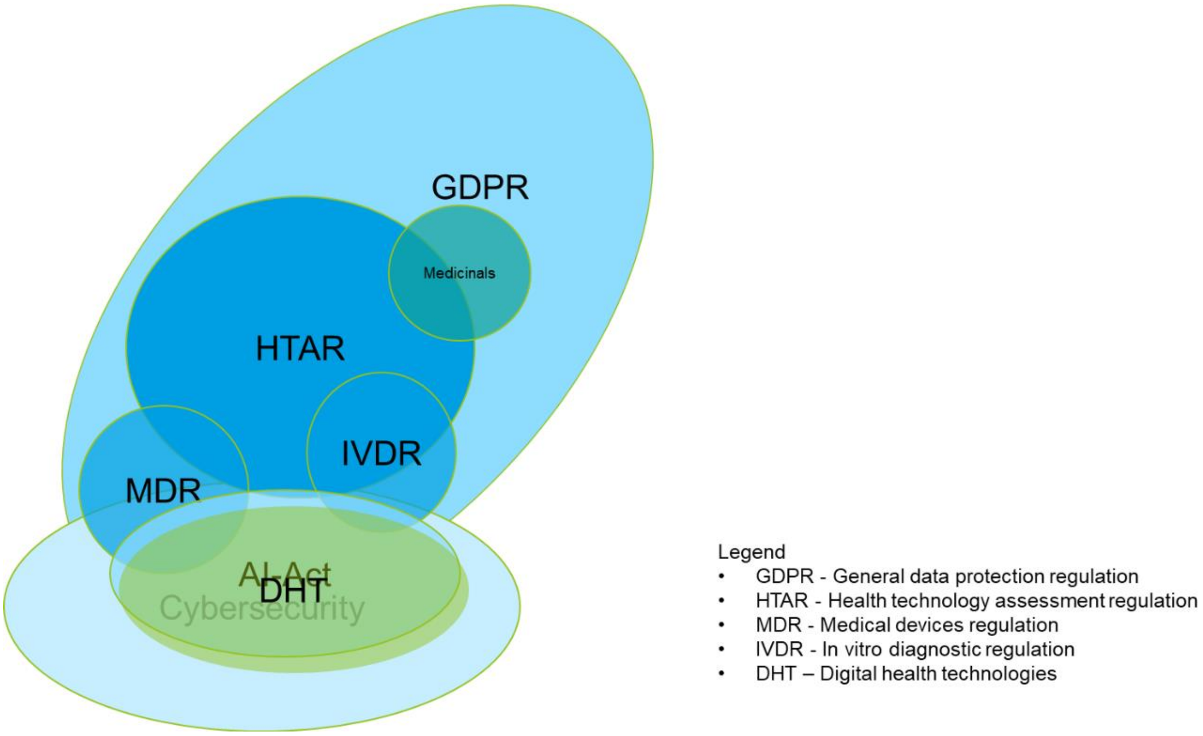

GDPR
Medicinals
HTAR
IVDR
MDR
AI Act
DHT
Cybersecurity
Legend
• GDPR - General data protection regulation
• HTAR - Health technology assessment regulation
• MDR - Medical devices regulation
• IVDR - In vitro diagnostic regulation
• DHT – Digital health technologies

Figure 3: initial mapping of regulation coverage versus digital health technologies

A glance at the interconnections and the placement of the DHTs in this context immediately shows how the DHTs might be related to many requirements and most of them would be shared with the cybersecurity space and the medical devices or in vitro devices space, as well with a shared space of requirements for the AI regulations.

The rapidly evolving regulatory framework in the digital and cybersecurity context shapes a new view on the legislation.

All the Union harmonisation legislation for placing products on the market have identified different legislative requirements for DHTs. To be made available onto the EU market, a DHT must be safe, effective, and now also secure.

The space that in the initial review of the EU legislative frameworks was identified as a grey area, i.e. an area not covered by specific regulations, is now clearly embraced by the Cyber Resilience Act. With the publication of the Cyber Resilience Act, all DHTs have a cybersecurity compliance framework to refer to.

4.1.1 Legislative requirements

The legislative requirements that apply to DHTs depend on their features and/or their intended purpose and include:

- Medical devices/in vitro devices: according to (EU) 2017/745 MDR or (EU) 2017/746 IVDR (European Parliament, 2017a, 2017b).
- AI systems: according to (EU) 2024/1689 AIA (Artificial Intelligence Act) (European Parliament, 2024).
- Any other DHT: Cyber resilience act regulation (EU) 2024/2847 (European Union, 2024)
- DHT intended for consumers: General Product Safety Regulation (EU) 2023/988 (European Union, 2023).

How to understand when a DHT falls under a legislative framework and which?

4.1.1.1 MDR

When the **definition of medical device** is applicable

[MDR] Art.2(1) '*medical device' means any instrument, apparatus, appliance,* ***software,*** *implant, reagent, material or other article intended by the manufacturer to be used, alone or in combination, for human beings for one or more of the following specific medical purposes:*

- *diagnosis, prevention, monitoring, prediction, prognosis, treatment or alleviation of disease,*
- *diagnosis, monitoring, treatment, alleviation of, or compensation for, an injury or disability,*
- *investigation, replacement or modification of the anatomy or of a physiological or pathological process or state,*
- *providing information by means of in vitro examination of specimens derived from the human body, including organ, blood and tissue donations,*
- *and which does not achieve its principal intended action by pharmacological, immunological or metabolic means, in or on the human body, but which may be assisted in its function by such means.*
- *The following products shall also be deemed to be medical devices:*
- *devices for the control or support of conception;*
- *products specifically intended for the cleaning, disinfection or sterilisation of devices […]*

Or

When the **definition of accessory for a medical device** is applicable

[MDR] Art.2 (2) '*accessory for a medical device' means an article which, whilst not being itself a medical device, is intended by its manufacturer to be used together with one or several particular medical device(s) to specifically enable the medical device(s) to be used in accordance with its/their intended purpose(s) or to specifically and directly assist the medical functionality of the medical device(s) in terms of its/their intended purpose(s);*

4.1.1.2 IVDR

When the **definition of in vitro diagnostic medical device** is applicable

[IVDR] Art.2 (2) '*in vitro diagnostic medical device' means any medical device which is a reagent, reagent product, calibrator, control material, kit, instrument, apparatus, piece of equipment, software or system, whether used alone or in combination, intended by the manufacturer to be used in vitro for the examination of specimens, including blood and tissue donations, derived from the human body, solely or principally for the purpose of providing information on one or more of the following:*

(a) concerning a physiological or pathological process or state;
(b) concerning congenital physical or mental impairments;
(c) concerning the predisposition to a medical condition or a disease;
(d) to determine the safety and compatibility with potential recipients;
(e) to predict treatment response or reactions;
(f) to define or monitoring therapeutic measures.

Specimen receptacles shall also be deemed to be in vitro diagnostic medical devices.

or

When the **definition of accessory for an in vitro diagnostic medical device** is applicable

[IVDR] Art.2 (4) ‘*accessory for an in vitro diagnostic medical device’ means an article which, whilst not being itself an in vitro diagnostic medical device, is intended by its manufacturer to be used together with one or several particular in vitro diagnostic medical device(s) to specifically enable the in vitro diagnostic medical device(s) to be used in accordance with its/their intended purpose(s) or to specifically and directly assist the medical functionality of the in vitro diagnostic medical device(s) in terms of its/their intended purpose(s).*

For both MDR and IVDR the definition of the DHT is by their purpose.
In MDR, "Intended purpose" means the use for which a device is intended according to the data supplied by the manufacturer on the label, in the instructions for use or in promotional or sales materials or statements and as specified by the manufacturer in the clinical evaluation."
According to Regulation (EU) 2017/746 – IVDR, "Intended purpose" means the use for which a device is intended according to the data supplied by the manufacturer on the label, in the instructions for use or in promotional or sales materials or statements or as specified by the manufacturer in the performance evaluation."
When considering the requirements of the Regulation (EU) 2021/2282 on health technology assessment (HTAR), all the DHTs that will be involved, are covered by MDR (or IVDR). However, the HTAR does not address any cybersecurity requirement for the assessment of health technologies; hence, it is excluded from the review in this task.

4.1.1.3 AI Act

When the **definition of AI system** is applicable
[AIA] Art.3 (1) ‘*AI system’ means a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments;*

It is to be noted that an AI system falls under the AI Act even if it is not a medical device. An AI system that is not a high-risk AI System still needs to comply with the AI Act.

For the AI Act, the definition is targeted on features and on purpose, where the feature is "machine based", and the purpose is "designed to". (European Law Institute, 2024).

4.1.1.4 Cyber Resilience Act

When the product is not regulated by MDR, IVDR or AI Act, the DHT is identified by features only and the applicable regulation is the Cyber Resilience Act (CRA).

In November 2024 the CRA was published and, with a transitional period until 11 December 2027, any product containing a "digital element" shall be compliant to the regulation and complete a Conformity Assessment before it is placed on the market. The Act also applies penalties in case of non-compliance to the regulation.

Product with digital elements *means a software or hardware product and its remote data processing solutions, including software or hardware components being placed on the market separately* [Art.3(1)].

For DHTs, the CRA applies to products with digital elements. The CRA requires that products placed on the market are cyber secure. The type of conformity assessment is defined by the type of the product.

[CRA] Annex III - Important products with digital elements that might fit more the definition of a DHT are*: […] Class I […] Personal wearable products to be worn or placed on a human body* *that have a health monitoring (such as tracking) purpose and to which Regulation (EU) 2017/745 or (EU) No 2017/746 do not apply, or personal wearable products that are intended for the use by and for children*.

4.1.1.5 General Product Safety Regulation:

A DHT would fall under the General Product Safety Regulation (GPSR) when none of the above would be applicable. Moreover, whenever a product with digital elements (corresponding to the definition as in CRA) is also a GPSR product, then CRA requirements also apply.
This makes the GPSR applicable only to a limited number of DHTs.

When the **definition of product** is applicable:
[GPSR] Art.3 (1) *'**product**' means any item, whether or not it is interconnected to other items, supplied or made available, whether for consideration or not, including in the context of providing a service, which is intended for consumers or is likely, under reasonably foreseeable conditions, to be used by consumers even if not intended for them*;

AND

[GPSR] Art.3 (17) '***consumer***' *means any natural person who acts for purposes which are outside that person's trade, business, craft or profession*;

Any DHT intended for a consumer would fall under the GPSR, if not a medical device. The requirements shift the obligations of the manufacturer from the GPSR to the CRA, as stated in the Cyber Resilience Act, Article 11.

In GPSR, the product is identified by purpose: *"which is intended for consumers".*

Note:

Directive 2014/53/EU on radio equipment (RED) has been intentionally not considered, even if one of the EDiHTA pilot cases is telemedicine, because the complete system for telemedicine would need to comply to the requirements on the Regulations above, while only components of the system will need to comply with the RED directive. The cybersecurity compliance is, for the scope of the project only addressed to the system as a whole and the essential requirements in Article 3 of the Directive do not address specifically to cybersecurity. CRA will then be applicable to the products covered by the 2014/53/EU.

In conclusion, a DHT might have one or more applicable regulations, as simplified in Figure 4. DHTs and their applicable legislative framework.

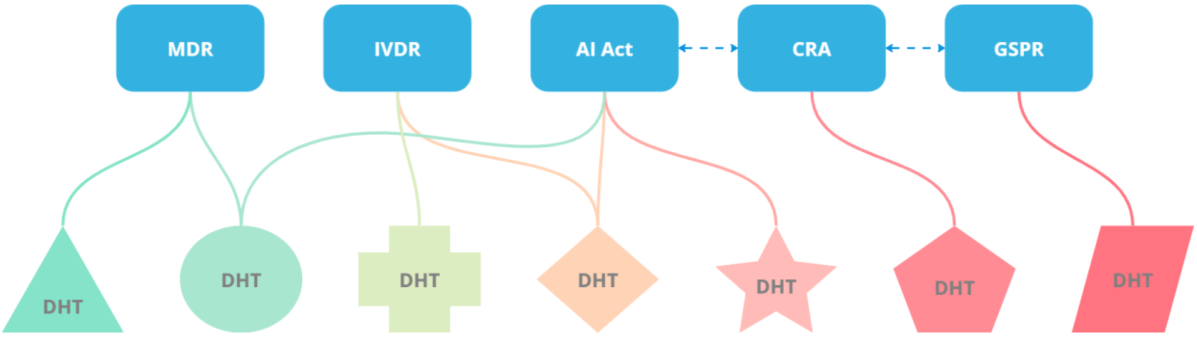


Figure 4. DHTs and their applicable legislative framework

4.1.2 Cybersecurity Requirements

The above regulations refer to implicit or explicit requirements for cybersecurity, whether the word cybersecurity is mentioned or not.

In the next paragraph, how the cybersecurity requirements are addressed in each of the included regulations will be examined.

4.1.2.1 MDR

[MDR] "Annex I.II.14

Construction of devices and interaction with their environment

14.2. *Devices shall be designed and manufactured in such a way as to remove or reduce as far as possible: […] (d) the risks associated with the possible negative interaction between software and the IT environment within which it operates and interacts*;

[…]

14.5. *Devices that are intended to be operated together with other devices or products shall be designed and manufactured in such a way that the interoperability and compatibility are reliable and safe*

17. *Electronic programmable systems — devices that incorporate electronic programmable systems and software that are devices in themselves […] 17.4. Manufacturers shall set out minimum requirements concerning hardware, IT networks characteristics and IT security measures, including protection against unauthorised access, necessary to run the software as intended*.

18. *Active devices and devices connected to them […] Devices shall be designed and manufactured in such a way as to protect, as far as possible, against unauthorised access that could hamper the device from functioning as intended.*

4.1.2.2 IVDR

[IVDR] "Annex I.II.13

13*. Construction of devices and interaction with their environment […] 13.2. Devices shall be designed and manufactured in such a way as to remove or reduce as far as possible:(d) the risks associated with the possible negative interaction between software and the IT environment within which it operates and interacts;*

[…]

13.5. *Devices that are intended to be operated together with other devices or products shall be designed and manufactured in such a way that the interoperability and compatibility are reliable and safe.*

[…]

16. *Electronic programmable systems — devices that incorporate electronic programmable systems and software that are devices in themselves […] 16.4. Manufacturers shall set out minimum requirements concerning hardware, IT networks characteristics and IT security measures, including protection against unauthorised access, necessary to run the software as intended.*

MDR and IVDR are the oldest regulations in the Union Harmonisation Legislation and the first to be published within the context analysed in EDiHTA. Requirements for cybersecurity are presented in terms of actions: software/IT environment, interoperability and compatibility and protection and unauthorised access. Notably, the current requirements do not include any recovery actions in case of failure–a limitation that needs to be addressed. Risk Management process should ensure that this risk is identified and that the risk control measure can prevent and mitigate the consequence.

4.1.2.3 AI Act

[AIA] Article 15 "*Accuracy, robustness and cybersecurity*

1.*High-risk AI systems shall be designed and developed in such a way that they achieve an appropriate level of accuracy, robustness, and cybersecurity, and that they perform consistently in those respects throughout their lifecycle. […]*

5.*High-risk AI systems shall be resilient against attempts by unauthorised third parties to alter their use, outputs or performance by exploiting system vulnerabilities.*

The technical solutions aiming to ensure the cybersecurity of high-risk AI systems shall be appropriate to the relevant circumstances and the risks.

The technical solutions to address AI specific vulnerabilities shall include, where appropriate, measures to prevent, detect, respond to, resolve and control for attacks trying to manipulate the training data set (data poisoning), or pre-trained components used in training (model poisoning), inputs designed to cause the AI model to make a mistake (adversarial examples or model evasion), confidentiality attacks or model flaws.

The AI Act establishes stringent contextual requirements for cybersecurity, mandating that organisations address activities that could compromise the system's functionality while implementing processes that include both prevention and control measures. Additionally, the Act stipulates that providers of high-risk AI systems must implement a comprehensive quality management system and maintain a robust risk management process. The confluence of these requirements ensures that appropriate cybersecurity measures are in place.

The publication of the Cyber Resilience Act has changed the fulfilment of requirements of Article 15 of the AI Act for high-risk systems. Compliance with cybersecurity requirements can now be achieved through Annex I of the CRA, and the possibility exists to compile a singular technical documentation for compliance, provided that the notified body for AI possesses the requisite competencies as the notified bodies of the CRA.

4.1.2.4 Cyber Resilience Act

[CRA] *Annex I ESSENTIAL CYBERSECURITY REQUIREMENTS*

Part I Cybersecurity requirements relating to the properties of products with digital elements

(1) Products with digital elements shall be designed, developed and produced in such a way that they ensure an appropriate level of cybersecurity based on the risks.

(2) On the basis of the cybersecurity risk assessment referred to in Article 13(2) and where applicable, products with digital elements shall:

a. be made available on the market without known exploitable vulnerabilities;

b. be made available on the market with a secure by default configuration, unless otherwise agreed between manufacturer and business user in relation to a tailor-made product with digital elements, including the possibility to reset the product to its original state;

c. ensure that vulnerabilities can be addressed through security updates, including, where applicable, through automatic security updates that are installed within an appropriate timeframe enabled as a default setting, with a clear and easy-to-use opt-out mechanism, through the notification of available updates to users, and the option to temporarily postpone them;

d. ensure protection from unauthorised access by appropriate control mechanisms, including but not limited to authentication, identity or access management systems, and report on possible unauthorised access;

e. protect the confidentiality of stored, transmitted or otherwise processed data, personal or other, such as by encrypting relevant data at rest or in transit by state of the art mechanisms, and by using other technical means;

f. protect the integrity of stored, transmitted or otherwise processed data, personal or other, commands, programs and configuration against any manipulation or modification not authorised by the user, and report on corruptions;

g. process only data, personal or other, that are adequate, relevant and limited to what is necessary in relation to the intended purpose of the product with digital elements (data minimisation);

h. protect the availability of essential and basic functions, also after an incident, including through resilience and mitigation measures against denial-of-service attacks;

i. minimise the negative impact by the products themselves or connected devices on the availability of services provided by other devices or networks;

j. be designed, developed and produced to limit attack surfaces, including external interfaces;

k. be designed, developed and produced to reduce the impact of an incident using appropriate exploitation mitigation mechanisms and techniques;

l. provide security related information by recording and monitoring relevant internal activity, including the access to or modification of data, services or functions, with an opt-out mechanism for the user;

m. provide the possibility for users to securely and easily remove on a permanent basis all data and settings and, where such data can be transferred to other products or systems, ensure that this is done in a secure manner.

Part II Vulnerability handling requirements Manufacturers of products with digital elements shall:

(1) identify and document vulnerabilities and components contained in products with digital elements, including by drawing up a software bill of materials in a commonly used and machine-readable format covering at the very least the top-level dependencies of the products;

(2) in relation to the risks posed to products with digital elements, address and remediate vulnerabilities without delay, including by providing security updates; where technically feasible, new security updates shall be provided separately from functionality updates;

(3) apply effective and regular tests and reviews of the security of the product with digital elements;

(4) once a security update has been made available, share and publicly disclose information about fixed vulnerabilities, including a description of the vulnerabilities, information allowing users to identify the product with digital elements affected, the impacts of the vulnerabilities, their severity and clear and accessible information helping users to remediate the vulnerabilities; in duly justified cases, where manufacturers consider the security risks of publication to outweigh the security benefits, they may delay making public information regarding a fixed vulnerability until after users have been given the possibility to apply the relevant patch;

(5) put in place and enforce a policy on coordinated vulnerability disclosure;

(6) *take measures to facilitate the sharing of information about potential vulnerabilities in their product with digital elements as well as in third-party components contained in that product, including by providing a contact address for the reporting of the vulnerabilities discovered in the product with digital elements;*

(7) *provide for mechanisms to securely distribute updates for products with digital elements to ensure that vulnerabilities are fixed or mitigated in a timely manner and, where applicable for security updates, in an automatic manner;*

(8) *ensure that, where security updates are available to address identified security issues, they are disseminated without delay and, unless otherwise agreed between a manufacturer and a business user in relation to a tailor-made product with digital elements, free of charge, accompanied by advisory messages providing users with the relevant information, including on potential action to be taken.*

The specific regulation on cybersecurity stipulates the prerequisites for both products and their associated cybersecurity requirements. This encompasses the necessary features of the products as well as the protocols for managing vulnerabilities. It is worth noting that this regulation uniquely acknowledges the occurrence of vulnerabilities and delineates a comprehensive list of measures that manufacturers must undertake in the event of a known vulnerability, including the dissemination of relevant information and the deployment of patches. Additionally, it is significant that the regulation addresses the concept of a bill of materials and the notion of a supply chain within software development.

4.1.2.5 General Product Safety Regulation

[GPSR] *Art. 6 - Aspects for assessing the safety of products*

1. *When assessing whether a product is a safe product, the following aspects in particular shall be taken into account: […]*

   (b) the effect on other products, where it is reasonably foreseeable that the product will be used with other products, including the interconnection of those products;[…]

   (g) when required by the nature of the product, the appropriate cybersecurity features necessary to protect the product against external influences, including malicious third parties, where such an influence might have an impact on the safety of the product, including the possible loss of interconnection.

The generic requirements that are described in GPSR are not articulated, however the publication of CRA modifies GPSR, by making it applicable also to products with digital elements, creating a continuum in requirements of both regulations, including cybersecurity.

5 Cybersecurity Acts

5.1 NIS2 DIRECTIVE (EU) 2022/2555

Short name	NIS2
Title	Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (**NIS2 Directive**)
Amendment Date	Corrigendum, OJ L 90206, 22.12.2023, p. 1 (2022/2555)
In force?	Y

The NIS2 has been in force since October 2024, and it addresses the management of cybersecurity risks on network and information systems (NIS) across critical sectors. The Directive requires Member States to define national cybersecurity strategies and to cooperate across national borders. The objective is to protect network and information systems and their users from cyber threats.

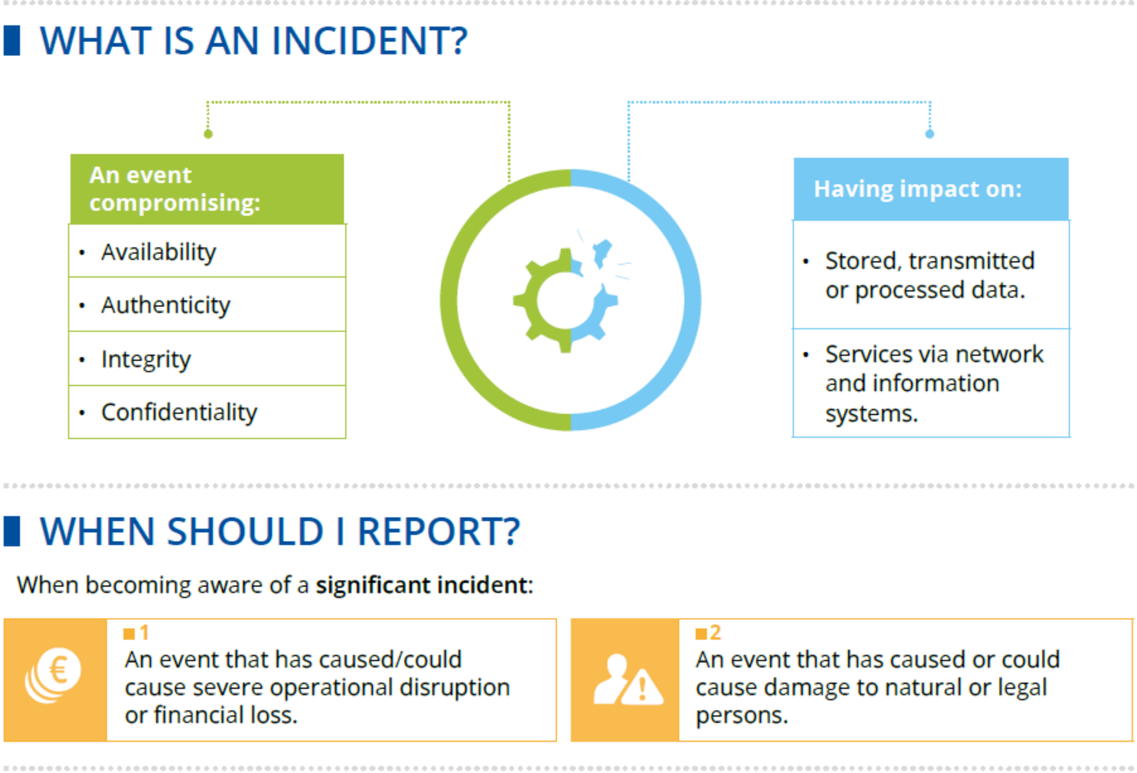
It is of interest for EDiHTA, as healthcare providers, EU reference labs and the manufacturers of medical devices (in case of emergency) are listed as high critical entities, while all manufacturers of medical devices and manufacturers of computer, electronic and optical products and manufacturers of electrical equipment are included as critical entities. Software manufacturers are not included (unless the SW is a medical device in itself). High criticality sectors, critical sectors and types of entities are listed in NIS2 Annex I and Annex II.

The requirements for the NIS2 regulation are based on prevention, risk management and incident handling. Incidents, defined as [NIS2 Art.6.6] "*an event compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems*" need to be reported. Significant incidents - whereas [NIS2 Art.23.3] *An incident shall be considered to be significant if: (a) it has caused or is capable of causing severe operational disruption of the services or financial loss for the entity concerned; (b) it has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage - needs to be reported.*

In short, the critical and high critical entities need to have in place a management system and a risk management system that is implemented:

- with policies on risk management and information security,
- capable to guarantee business continuity and manage crisis
- includes incident handling
- where supply-chain is identified and secure
- that includes training for human resources, along with access control policies and asset management
- where communications are secured also by multifactor authentication

Such requirements set in the NIS2, along with the obligation to report significant incidents and a coordinated vulnerability disclosure process, aim to guarantee a more efficient cybersecurity system across Europe.



WHAT IS AN INCIDENT?

An event compromising:

- Availability
- Authenticity
- Integrity
- Confidentiality

Having impact on:

- Stored, transmitted or processed data.
- Services via network and information systems.

WHEN SHOULD I REPORT?

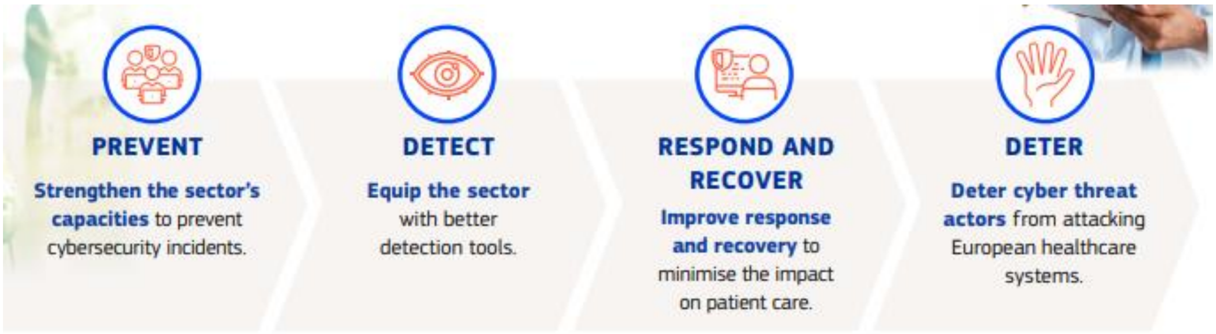
When becoming aware of a **significant incident**:

1 An event that has caused/could cause severe operational disruption or financial loss.

2 An event that has caused or could cause damage to natural or legal persons.

Figure 5: Incidents, significant incidents and reporting. (European Union Agency for Cybersecurity)

The EU Commission deployed an action plan in January 2025 called “European action plan on the cybersecurity of hospitals and healthcare providers” that is “aimed at bolstering the cybersecurity of hospitals and healthcare providers.” The plan is structured on 4 priorities (see figure below) and will be implemented during 2025-2026 (European Commission, 2025).



PREVENT

Strengthen the sector’s capacities to prevent cybersecurity incidents.

DETECT

Equip the sector with better detection tools.

RESPOND AND RECOVER

Improve response and recovery to minimise the impact on patient care.

DETER

Deter cyber threat actors from attacking European healthcare systems.

Figure 6: The four priorities of the action plan (European Commission, 2025)

5.1.1 How is EDiHTA impacted?

The NIS2 Directive (not yet transposed in all Member States) defines requirements for the healthcare providers that, *after positive recommendation* from an HTA process, adopt the technology. Hence, the HTA process should also include a pre-screening of the “recipient” that will adopt the technology and verify/check that the processes requested by the NIS2 are in place.

The interplay with manufacturers and HTA bodies for the NIS2 is about the application of the directive. When the DHT is a medical or *in vitro* diagnostic device, the elements required by the NIS2 should be verified with manufacturers, eventually through questionnaires or interviews, collecting information on cyber threats on their systems and recovery actions that they had to implement in case a cyber threat was discovered in devices already adopted by the healthcare provider or hospital.

5.2 Cyber Resilience Act (CRA)

Short name	CRA
Title	Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act).
Amendment Date	20/11/2024 (corrigendum on title)
In force?	Yes, Date of Application (DoA) 11 December 2027

Recently published, this regulation represents a significant advancement in cybersecurity for products with digital elements. It is the first to establish detailed mandatory requirements for cybersecurity in products with digital components.

All products with digital elements (see above, 4.1.1.4) will need to comply with minimum cybersecurity requirements set in Annex I of the regulation. In addition, Article 14 of this regulation sets the obligations for reporting exploited vulnerabilities with defined timelines (varying from 24 hours to 72 hours) and the obligation to submit a final report within 14 days.

Like all new legislative framework legislation, it sets the requirements and obligations for the manufacturers to have:

- a risk management system, it requires that the compliance is not limited only to the pre-market stage, but throughout the life cycle of the product, including the mandatory fixing of known vulnerabilities
- a quality management system
- technical documentation for the product
- provide instructions and information to users in a “language which can be easily understood by users and market surveillance authorities. They shall be clear, understandable, intelligible and legible.”

5.2.1 How is EDiHTA impacted?

Manufacturers of DHTs: The CRA creates a common legislative reference for the cybersecurity requirements and for handling vulnerabilities. DHTs that are medical devices or in vitro devices are excluded from the regulation [CRA Art.2.2.a], but for manufacturers, the obligation to report incidents is still applicable through NIS2.

Healthcare providers: after the date of application of CRA, healthcare providers will receive complete information to install, adopt and operate the DHT according to the instruction of the manufacturer.

The requirements set in [CRA Art.13.18] “*allow for the secure installation, operation and use of products with digital elements*” and in [Annex II] will include “*5. any known or foreseeable circumstance, related to the use of the product with digital elements in accordance with its* *intended purpose or under conditions of reasonably foreseeable misuse, which may lead to significant cybersecurity risks; […] 7. the type of technical security support offered by the manufacturer and the end-date of the support period during which users can expect vulnerabilities to be handled and to receive security updates; 8.detailed instructions or an internet address referring to such detailed instructions and information on: (a) the necessary measures during initial commissioning and throughout the lifetime of the product with digital elements to ensure its secure use; (b) how changes to the product with digital elements can affect the security of data; (c) how security-relevant updates can be installed; (d) the secure decommissioning of the product with digital elements, including information on how user data can be securely removed; (e) how the default setting enabling the automatic installation of security updates, […], can be turned off*' […] .

The regulation changes dramatically the amount of information that healthcare providers have access to and that will be able to configure its environment for correct use of the product. Also, the obligations for the manufacturers concerning vulnerabilities handling [CRA Annex I Part II] will ensure that the healthcare providers have an updated security patch whenever it is needed.

HTA bodies: the amount of information that is made available due to the requirements set in the regulation enables an assessment of the DHT to verify the suitability to the environment where it is going to be used. The compliance to the cybersecurity essential requirements [Annex I] addresses what kind of items are managed by the manufacturers. The requirements set by the regulation concerning the presence of technical documentation are then a valid support for assessment during the HTA process. It becomes then advisable that together with the information that is expected to be delivered by the manufacturer of the DHT, there is also part of the technical documentation.

5.3 Cybersecurity Act (CSA)

Short name	CSA
Title	Regulation (EU) 2019/881 of the European Parliament and of the Council Of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)
Amendment Date	Published on 7 June 2019, amended by Regulation (EU) 2025/37 [Regulation (EU) 2025/37 of the European Parliament and of the Council of 19 December 2024, amending Regulation (EU) 2019/881 as regards managed security services]
In force?	Yes, 28 June 2021 (for managed security services: after 4 February 2025)

CSA has been in force since 2021, amended by Regulation (EU) 2025/37, which adds a new type of product service to the ones already included in the first version of the regulation.

The regulation defines cybersecurity certification frameworks for certain types of products or services. The same certification framework is also recalled in the Cyber Resilience Act as a means of compliance to the CRA itself. Currently, the only developed certification scheme is the European Common Criteria (EUCC), defined in the Commission implementing regulation (EU) 2024/48. The European Union Cybersecurity Certification Scheme on Cloud Services (EUCS) and a certification scheme for 5G are currently under development. ENISA, the European Union Agency for cybersecurity, keeps the updated library of certification schemes within its European Union Cybersecurity Certification website (European Union Cybersecurity, 2024), (European Union Cybersecurity).

The certification framework introduced by the Cyber Security Act is voluntary, so it is not included in the Union harmonisation legislation, and the manufacturers of products might decide to apply the certification schemes or not. The certification framework is targeted to information and communication technology (ICT): *ICT products, ICT services, ICT processes, and managed security services* [CSA Art.1.1.b], where:

- *[CSA Art.2 (12)] 'ICT product' means an element or a group of elements of a network or information system;*
- *[CSA Art.2(13)] 'ICT service' means a service consisting fully or mainly in the transmission, storing, retrieving or processing of information by means of network and information systems;*
- *[CSA Art.2(14)] 'ICT process' means a set of activities performed to design, develop, deliver or maintain an ICT product or ICT service;*
- *[CSA Art.2'(14a)] "managed security service" means a service provided to a third party consisting of carrying out, or providing assistance for, activities relating to cybersecurity risk management, such as incident handling, penetration testing, security audits and consulting, including expert advice, related to technical support;'*

The certification framework provides three different types of assurance levels, defined by the scheme: "basic", "substantial", or "high". For the existing EUCC, a mark has been defined within the implementing act.

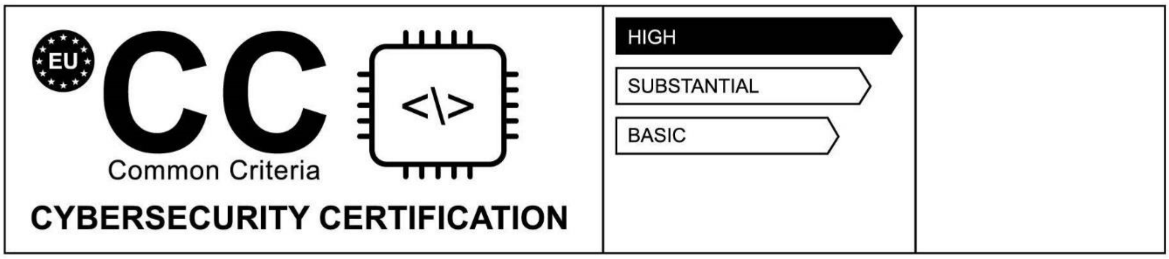


Figure 7: example of mark for EUCC with assurance level "high"

The EUCC applies after 27 February 2025 and can be used for the following products: Biometric systems; Firewalls (both hardware and software); Detection and response platforms; Routers; Switches; Specialised software (such as SIEM and IDS/IDP systems); Data diodes; Operating systems (including for mobile devices), Encrypted storage, Databases, Smart cards and secure elements included in all sorts of products, such as in passports daily used by all citizens.

5.3.1 How is EDiHTA impacted?

DHTs as finished products are not directly impacted by the Cyber Security Act. A DHT however might contain some elements that are covered by the CSA, so the control of the supply chain of the products by the manufacturers (providers) might benefit from the use of components that have a recognised and harmonised assurance level of cybersecurity.

So far, there is not a direct impact of the CSA on the stakeholders reviewed in this task.

The upcoming certification scheme will be monitored during EDiHTA for the cloud services and 5G, as they might be of interest to the HTA bodies.

5.4 Cyber Solidarity Act

Title	Regulation (EU) 2025/38 of the European parliament and of the council of 19 December 2024 laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cyber threats and incidents and amending Regulation (EU) 2021/694 (Cyber Solidarity Act)
Amendment Date	19/12/2024
In force?	Yes

The regulation aims to strengthen the preparedness and responsiveness of EU Member States to threats and incidents. It focuses on fostering collaboration and cooperation across Member States, without imposing obligations on manufacturers or healthcare providers. The regulation establishes the following mechanisms: *[Art. 1] (a) A pan-European network of cyber hubs, known as the European Cybersecurity Alert System, to build and enhance coordinated detection and common situational awareness capabilities. (b) A Cybersecurity Emergency Mechanism to support Member States in preparing for, responding to, mitigating the impact of, and initiating recovery from significant cybersecurity incidents and large-scale cybersecurity incidents. This mechanism also supports other users in responding to significant cybersecurity incidents and large-scale-equivalent cybersecurity incidents. (c) A European Cybersecurity Incident Review Mechanism to review and assess significant cybersecurity incidents or large-scale cybersecurity incidents.*

The regulation is then deemed as not relevant for EDiHTA as there is no direct impact on the HTA process.

6 Cybersecurity aspects on HTA process

Regulations reviewed in this task of EDiHTA conclude that all DHTs are subject to at least one of the Union harmonisation legislation acts. This ensures that the DHTs need to respond to specific requirements as set in the regulations and that all the applicable legal acts setting the requirements include minimum requirements for cybersecurity.

From the perspective of conducting HTA, the evaluation of cybersecurity aspects must also include the utilisation of the DHT within the context of healthcare providers. This necessitates the assessment of product documentation (information for users and instructions for use), which, according to the reviewed regulations, always requires the manufacturer (or provider) to inform the user of the technical specifications for the environment in which the technology will be installed. Additionally, information derived from the risk management process (pertaining to both medical devices and in-vitro devices) must be included.

The intended purpose of DHTs, as defined by the manufacturer, is approved during conformity assessment by the Notified Bodies if required. The HTA process shall consider the cybersecurity aspects in relation to the full intended purpose of the technology when assessing the suitability of the DHTs. Therefore, the elements to take into consideration when assessing the cybersecurity of the DHT need to include the intended purpose and the use environment, which will include the technology requirements for networks and physical devices that will be connected to the DHT. Moreover, the instructions for use of the DHT will include the requirements for the operator and user training needed to operate and understand the technology. The use environment might also require specific cyber security requirements for the DHT to work as per its intended purpose.

7 Conclusion

The analysis has shown that the regulatory context is dynamic and subject to change. The publication of implementing acts, new regulations and amendments to the existing regulations or directives, as well as the publication of new documents in the healthcare context by ENISA, show that the landscape is evolving rapidly. Also, there is a strong commitment from the EU Commission to implement a robust supporting structure for products, users and institutions, as well as strict requirements on management processes for the organisations.

Some regulations have been published recently, and while they have entered into force, they have not yet fully reached the date of application. We are still in the transition period; therefore, many products are not yet compliant with the relevant regulations. Furthermore, harmonised standards are not yet available.

Cybersecurity compliance under the Cyber Resilience Act can be pursued through harmonised standards or via existing certification schemes under the CSA, both as alternatives to Notified Bodies assessment. This approach urges manufacturers to take more responsibility for conformity assessment and provides a faster way to comply with legislative requirements. The CRA issued at the end of 2024 provides a *de facto* interpretation of the AI Act Article 15 requirements. Conversely, the two oldest regulations that cover most DHTs – MDR and IVDR – though pioneering in many respects, still appear to lack specific context and detail regarding cybersecurity requirements. Therefore, it is advisable for the EU Commission to propose a method to ensure that all DHTs progress at a uniform pace towards cybersecurity, without additional requirements and obligations that could potentially delay the market introduction of these devices.

We advise the EDiHTA consortium to monitor, until the end of June 2026, developments in the regulatory landscape, including changes to the regulatory requirements as well as the issuance of any harmonised standards, common specifications or implementing acts that might modify the state of the art described within this report.

8 References

Algarni, A. M., & Thayananthan, V. (2025). Digital Health: The Cybersecurity for AI-Based Healthcare Communication. *IEEE Access*, *13*, 5858-5870. https://doi.org/10.1109/ACCESS.2025.3526666

Commission, E. (2025). *European action plan on the cybersecurity of hospitals and healthcare providers*. https://digital-strategy.ec.europa.eu/en/library/european-action-plan-cybersecurity-hospitals-and-healthcare-providers

Coventry, L., & Branley, D. (2018). Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. *Maturitas*, *113*, 48-52. https://doi.org/10.1016/j.maturitas.2018.04.008

European Central Bank. (2025). *What is cyber resilience?* https://www.ecb.europa.eu/paym/cyber-resilience/html/index.en.html

European Commission. *New legislative framework*. https://single-market-economy.ec.europa.eu/single-market/goods/new-legislative-framework_en

European Commission. (2008). Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93 (Text with EEA relevance). Article 765/2008. https://eur-lex.europa.eu/eli/reg/2008/765/oj/eng

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, (2011). https://eur-lex.europa.eu/eli/dir/2011/24/oj/eng

Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council Text with EEA relevance, (2012). https://eur-lex.europa.eu/eli/reg/2012/1025/oj/eng

European Commission. (2025). *European action plan on the cybersecurity of hospitals and healthcare providers*. https://digital-strategy.ec.europa.eu/en/library/european-action-plan-cybersecurity-hospitals-and-healthcare-providers

European Law Institute. (2024). *Commission Guidelines on the Application of the Definition of an AI System and the Prohibited AI Practices Established in the AI Act*. http://europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Response_on_the_definition_of_an_AI_System.pdf

European Medicines Agency. *Health Technology Assessment body*. https://www.ema.europa.eu/en/glossary-terms/health-technology-assessment-body

Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC (Text with EEA relevance.), 1-175 117 (2017a). http://data.europa.eu/eli/reg/2017/745/oj

Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU (Text with EEA relevance.), (2017b). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32017R0746&qid=1743155413456

Regulation (EU) 2021/2282 of the European Parliament and of the Council of 15 December 2021 on health technology assessment and amending Directive 2011/24/EU (Text with EEA relevance), (2021). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021R2282&qid=1743155209635

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance), 1689 (2024). http://data.europa.eu/eli/reg/2024/1689/oj

Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), (2019). http://data.europa.eu/eli/reg/2019/881

Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC ((2022a). http://data.europa.eu/eli/dir/2022/2555

European Union directives, (2022b). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=legissum:l14527

European Union regulations, (2022c). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM:l14522

Regulation (EU) 2023/988 of the European Parliament and of the Council of 10 May 2023 on general product safety, amending Regulation (EU) No 1025/2012 of the European Parliament and of the Council and Directive (EU) 2020/1828 of the European Parliament and the Council, and repealing Directive 2001/95/EC of the European Parliament and of the Council and Council Directive 87/357/EEC, (2023). https://eur-lex.europa.eu/eli/reg/2023/988/oj/eng

Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act), (2024). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R2847&qid=1739452079191

European Union Agency for Cybersecurity. *Network and Information Systems Directive 2 (NIS2) - Key topic campaign*. https://www.enisa.europa.eu/topics/awareness-and-cyber-hygiene/network-and-information-systems-directive-2-nis2

European Union Cybersecurity. *What is EU Cybersecurity Certification?* https://certification.enisa.europa.eu/index_en

European Union Cybersecurity. (2024). *Certification Library*. https://certification.enisa.europa.eu/certification-library_en

FDA-NIH Biomarker working group. (2025). *BEST (Biomarkers, EndpointS, and other Tools) Resource [Internet].* NIH. https://www.ncbi.nlm.nih.gov/books/NBK338448/

Ifigeneia Lella, Eleni Tsekmezoglou, Marianthi Theocharidou, Erika Magonara, Apostolos Malatras, Rossen Svetozarov Naydenov, Cosmin Ciobanu, & Cybersecurity, E. U. A. f. (2023). *ENISA Threat Landscape 2023*. **https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023**

ISO. (2023). Health Informatics – Personalised digital health – Digital therapeutics health software systems. In *ISO/TR 11147:2023*: International Organisation for Standardisation.

Morgan, S., & Osborne, C. (2027). *Global Ransomware Damage Costs Predicted To Exceed $265 Billion By 2031*. KnowBe4. https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/

National Cyber Security Centre. (2021). *10 Steps to Cyber Security*. Retrieved from https://www.ncsc.gov.uk/files/2021-10-steps-to-cyber-security-infographic.pdf

Niinistö, S. (2024). *Safer Together – Strengthening Europe’s Civilian and Military Preparedness and Readiness*. https://commission.europa.eu/document/5bb2881f-9e29-42f2-8b77-8739b19d047c_en

O'Rourke, B., Oortwijn, W., & Schuller, T. (2020). The new definition of health technology assessment: A milestone in international collaboration. *International Journal of Technology Assessment in Health Care*, *36*(3), 187-190. https://doi.org/10.1017/S0266462320000215

Rossella Mattioli, Apostolos Malatras, ENISA, Eve Naomi Hunter, Marco Gino Biasibetti Penso, Dominic Bertram, & Neubert, I. (2023). *Identifting Emerging Cyber Security Threats and Challenges for 2030*. https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Foresight%20Cybersecurity%20Threats%20for%202030.pdf

Salama, R., Altrjman, C., & Al-Turjman, F. (2024). 8 - Healthcare cybersecurity challenges: a look at current and future trends. In F. Al-Turjman (Ed.), *Computational Intelligence and Blockchain in Complex Systems* (pp. 97-111). Morgan Kaufmann. https://doi.org/https://doi.org/10.1016/B978-0-443-13268-1.00003-0

Thapa, C., & Camtepe, S. (2021). Precision health data: Requirements, challenges and existing techniques for data security and privacy. *Computers in Biology and Medicine*, *129*, 104130. https://doi.org/https://doi.org/10.1016/j.compbiomed.2020.104130

Wiig, S. F. Ø. S. (2019). Regulation and resilience at the macro-level healthcare system – a literature review. Proceedings of the 29th European Safety and Reliability Conference, Hannover.