EUI CENTRE FOR JUDICIAL COOPERATION

ROBERT SCHUMAN CENTRE

European Health Data Space – is the proposed certification system effective against cyberthreats?

Federica Casarosa – Centre for Judicial Cooperation (EUI) and visiting Fellow University of Masaryk

(supported by the ERDF project" CyberSecurity, CyberCrime and Critical Information Infrastructures Center of Excellence "(No. CZ.02.1.01 /0.0/0.0/16_019/0000822)

Funded by the European Union

European Health Data Space

Proposal for a Regulation on the European Health Data Space

(3 May 2022)

Objectives :

- creating a common space where individuals may control their health data in a trusted and secure way, including in its scope different types of health data such as electronic health records, genomics data, patient registries etc.
- enhancing the opportunities to use such data for research and innovation, still safeguarding the protection of health data.

Co-funded by the Erasmus+ Programme of the European Union

Definitions

- Article 1 (3) EHDS
  - This Regulation applies to:
    - (a)**manufacturers and suppliers of EHR systems and wellness applications** placed on the market and put into service in the Union and the users of such products;
    - (b)controllers and processors established in the Union processing electronic health data of Union citizens and third-country nationals legally residing in the territories of Member States;
    - (c)controllers and processors established in a third country that has been connected to or are interoperable with MyHealth@EU, pursuant to Article 12(5);
    - (d)data users to whom electronic health data are made available by data holders in the Union.
- Art 2 (2)
  - (n)'EHR system' (electronic health record system) means any appliance or software intended by the manufacturer to be used for storing, intermediating, importing, exporting, converting, editing or viewing electronic health records;
  - (o)'wellness application' means any **appliance or software intended by the manufacturer to be used by a natural person for processing electronic health data for other purposes than healthcare, such as well-being and pursuing healthy life-styles**;

Co-funded by the Erasmus+ Programme of the European Union

Certification scheme

- Mandatory self-certification scheme for EHR systems
  - Article 17
    - 1.Manufacturers of EHR systems shall:
      - (a)ensure that their EHR systems are in conformity with the **essential requirements laid down in Annex II and with the common specifications in accordance with Article 23**;
- Voluntary self-certification scheme for wellness applications
  - Article 31
    - 1.Where a manufacturer of a wellness application claims interoperability with an EHR system and therefore compliance with the essential requirements laid down in Annex II and common specifications in Article 23, such wellness application may be accompanied by a label, clearly indicating its compliance with those requirements. The label shall be issued by the manufacturer of the wellness application.
    - 2.The label shall indicate the following information:
      - (a)categories of electronic health data for which compliance with essential requirements laid down in Annex II has been confirmed;
      - (b)reference to common specifications to demonstrate compliance;
      - (c)validity period of the label.

Co-funded by the Erasmus+ Programme of the European Union

Security requirements

- Distinction among general requirements, requirements for interoperability and those for security
- Security requirements
  - Accesibility is linked to authentication (based on professional rights and qualifications) with possibility of limitations
  - Record of internal activity
  - Inclusion of digital signature authentication
  - Control over data retention period

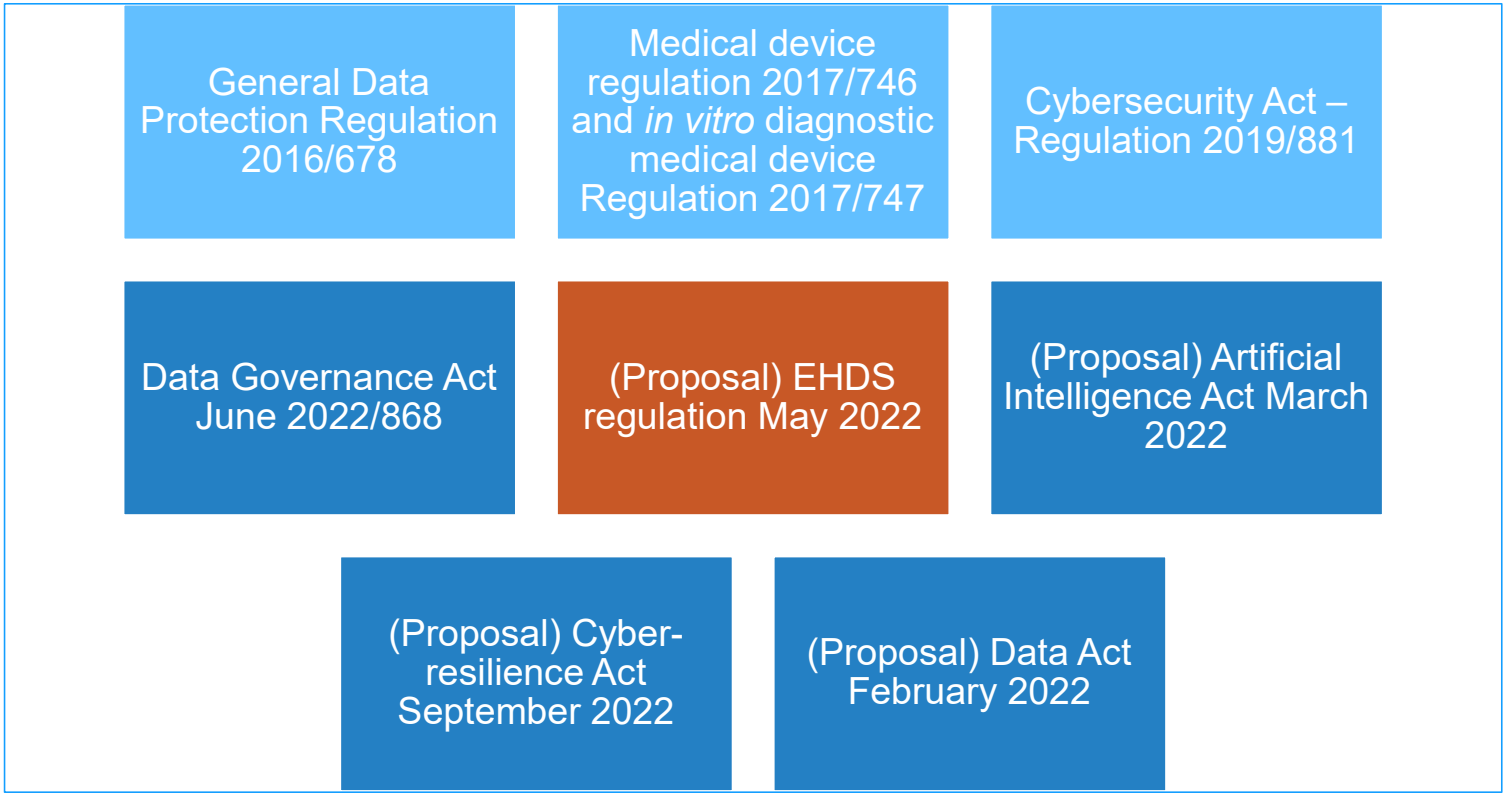
Co-funded by the Erasmus+ Programme of the European Union

Standards provided by the Commission

- **Art 23 Common specifications**
  - 1. The Commission shall, by means of implementing acts, adopt common specifications in respect of the essential requirements set out in Annex II, including a time limit for implementing those common specifications. […]
  - 3. The common specifications may include elements related to the following:
    - (a) datasets containing electronic health data and defining structures, such as data fields and data groups for the representation of clinical content and other parts of the electronic health data;
    - (b) coding systems and values to be used in datasets containing electronic health data;
    - (c) other requirements related to data quality, such as the completeness and accuracy of electronic health data;
    - (d) technical specifications, standards and profiles for the exchange of electronic health data;
    - (e) requirements and principles related to security, confidentiality, integrity, patient safety and protection of electronic health data;
    - (f) specifications and requirements related to identification management and the use of electronic identification.

Co-funded by the Erasmus+ Programme of the European Union

Coordination with other legislative acts



Co-funded by the Erasmus+ Programme of the European Union

Cyber-resilience Act

Regulation addressing (art. 1)

- rules for the placing on the market of **products with digital elements** to ensure the cybersecurity of such products;
- essential requirements for the design, development and production of products with digital elements, and obligations for economic operators in relation to these products with respect to cybersecurity;
- essential requirements for the vulnerability handling processes put in place by manufacturers to ensure the cybersecurity of products with digital elements during the whole life cycle, and obligations for economic operators in relation to these processes;
- rules on market surveillance and enforcement of the above-mentioned rules and requirements.

Co-funded by the Erasmus+ Programme of the European Union

Cyber-resilience Act

Interaction with EHDS regulation:

"(31) **Regulation [European Health Data Space Regulation proposal] complements the essential requirements laid down in this Regulation.** The **electronic health record systems ('EHR systems')** falling under the scope of Regulation [European Health Data Space Regulation proposal] which **are products with digital elements within the meaning of this Regulation should therefore also comply with the essential requirements set out in this Regulation.** Their manufacturers should demonstrate conformity as required by Regulation [European Health Data Space Regulation proposal]. To facilitate compliance, manufacturers may draw up a single technical documentation containing the elements required by both legal acts. […]"

Co-funded by the Erasmus+ Programme of the European Union

Comparison between EHDS Cyber-resilience act

- Security requirements
  - Accesibility is linked to authentication (based on professional rights and qualifications) with possibility of limitations
  - Record of internal activity
  - Inclusion of digital signature authentication
  - Control over data retention period

- Distinction between security requirements and vulnerability handling requirements
- Security requirements
  - risk based taking into account CIA triad
  - Ensure data minimization
  - Resilience against DoS attack
  - Avoid network effects
  - Security by design including mitigation measures
  - Record of internal activity
  - Updates (including automatic ones)
- Vulnerability handling requirements
  - Risk based
  - Tests and security updates to be carried out (free for users)
  - Information sharing (in particular with third party components' manufacturers)

Co-funded by the Erasmus+ Programme of the European Union

Cyber-resilience Act

Art 24 Conformity assessment

1. The manufacturer shall perform a conformity assessment of the product with digital elements and the processes put in place by the manufacturer to determine whether the essential requirements set out in Annex I are met. The manufacturer or the manufacturer's authorised representative shall demonstrate conformity with the essential requirements by using one of the following procedures:

(a) the internal control procedure (based on module A) set out in Annex VI; or

(b) the EU-type examination procedure (based on module B) set out in Annex VI followed by conformity to EU-type based on internal production control (based on module C) set out in Annex VI; or

(c) conformity assessment based on full quality assurance (based on module H) set out in Annex VI.

Co-funded by the Erasmus+ Programme of the European Union

Cyber-resilience Act

Art 24 Conformity assessment

4. Manufacturers of products with digital elements that are classified as EHR systems under the scope of Regulation [the European Health Data Space Regulation] **shall demonstrate conformity with the essential requirements laid down in Annex I of this Regulation using the relevant conformity assessment procedure as required by Regulation** [Chapter III of the European Health Data Space Regulation].

Self-assessment of conformity

Art 26 (1) EHDS Reg. : “The EU declaration of conformity shall state that the manufacturer of the EHR system has demonstrated that the essential requirements laid down in Annex II have been fulfilled.”

Co-funded by the Erasmus+ Programme of the European Union

Thank you!
Questions?

Contact: federica.casarosa@eui.eu

Co-funded by the Erasmus+ Programme of the European Union