



European Health Data Space

Harnessing the power of health data
for people, patients and innovation

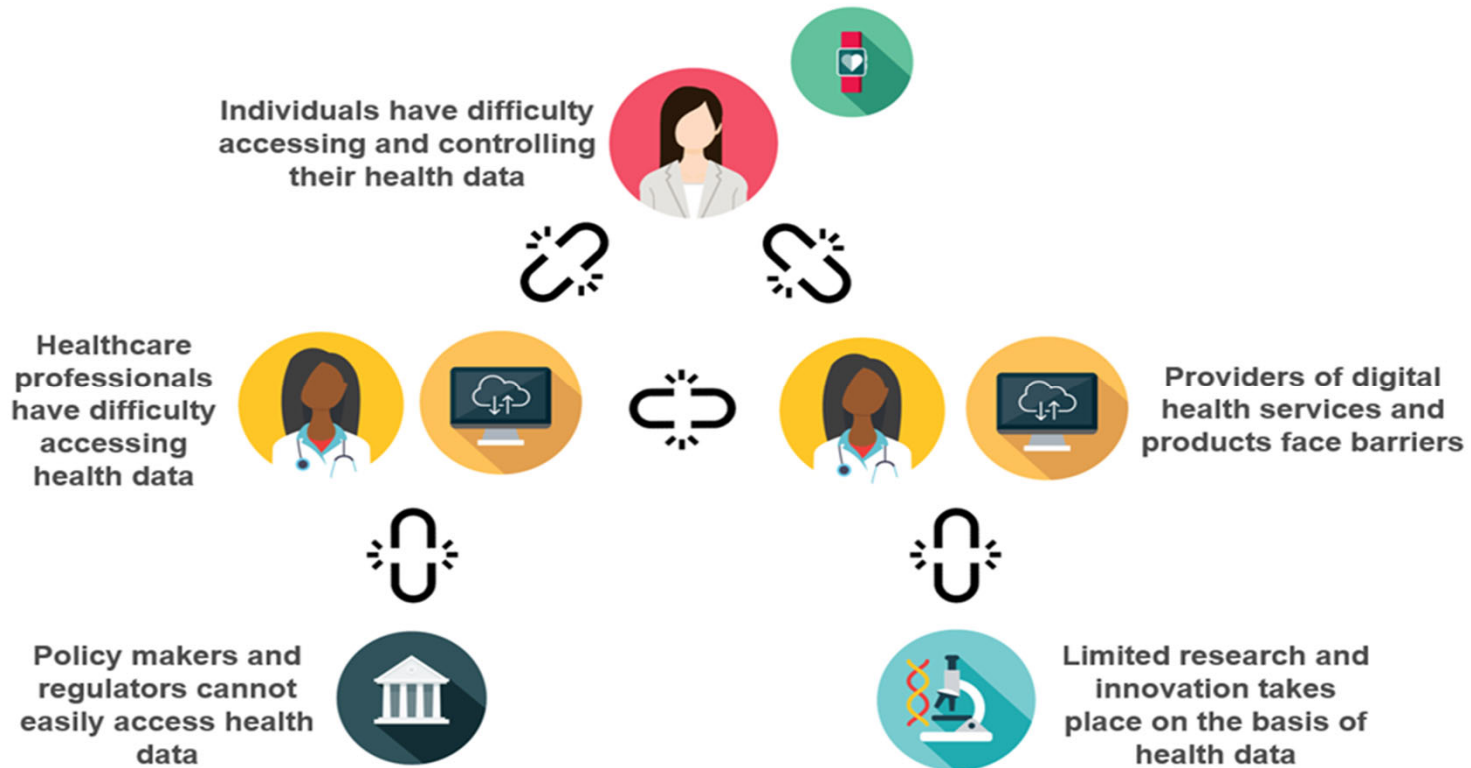
20/09/23

Skander Mabrouk – policy officer

DG SANTE – Digital Health



Main challenges in harnessing the power of health data



European Health Data Space (EHDS)

OBJECTIVES

Effective use of health data

SCOPE & EXPECTED IMPACT

Use of health data
(primary,
MyHealth@EU)

- Empower individuals to control their data
- Standardization and mandatory certification of EHR systems
- Voluntary labelling of wellness apps
- European Electronic Health Record Exchange Format

Single market for health data, data protection, free movement of people, digital goods and services

Re-use of health data
(secondary,
HealthData@EU)

- Health data access bodies
- Purposes for use and forbidden use
- Data permits, secure environments, no identification

Facilitated Research & Innovation
Better Policy Making

MEANS

Legal / Governance

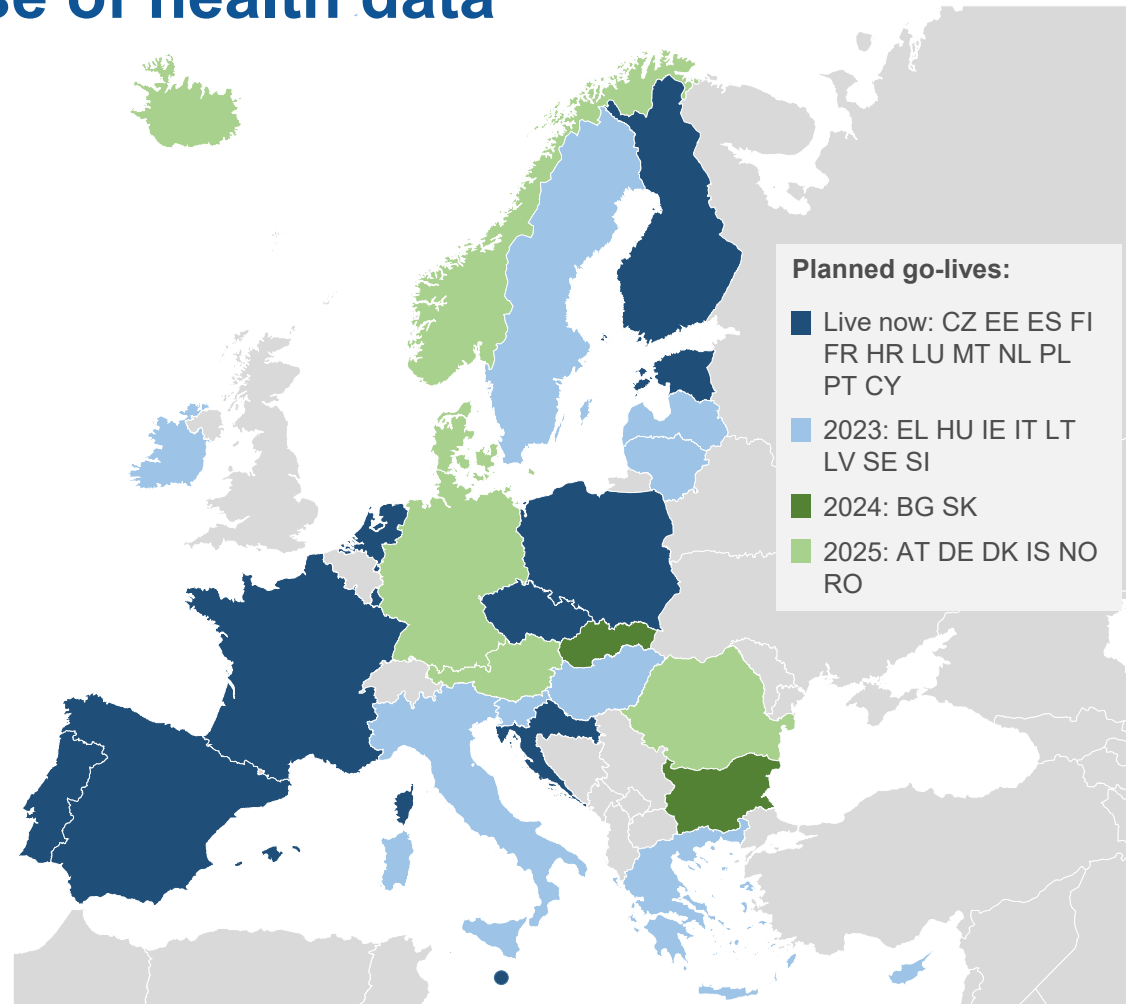
Quality of data

Infrastructure


Capacity building/digitalisation
(MFF)

MyHealth@EU: primary use of health data

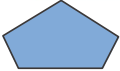


- *Currently 12 Member States are live*
- *The number of connected Member States will grow rapidly in the years ahead - there are plans for most Member States and EEA countries to join MyHealth@EU until 2025.*
- *Currently there are 2 services:*
 - **Patient Summary**
 - **ePrescription**
- *This is being expanded to include*
 - **Medical images**
 - **Laboratory results**
 - **Discharge reports**

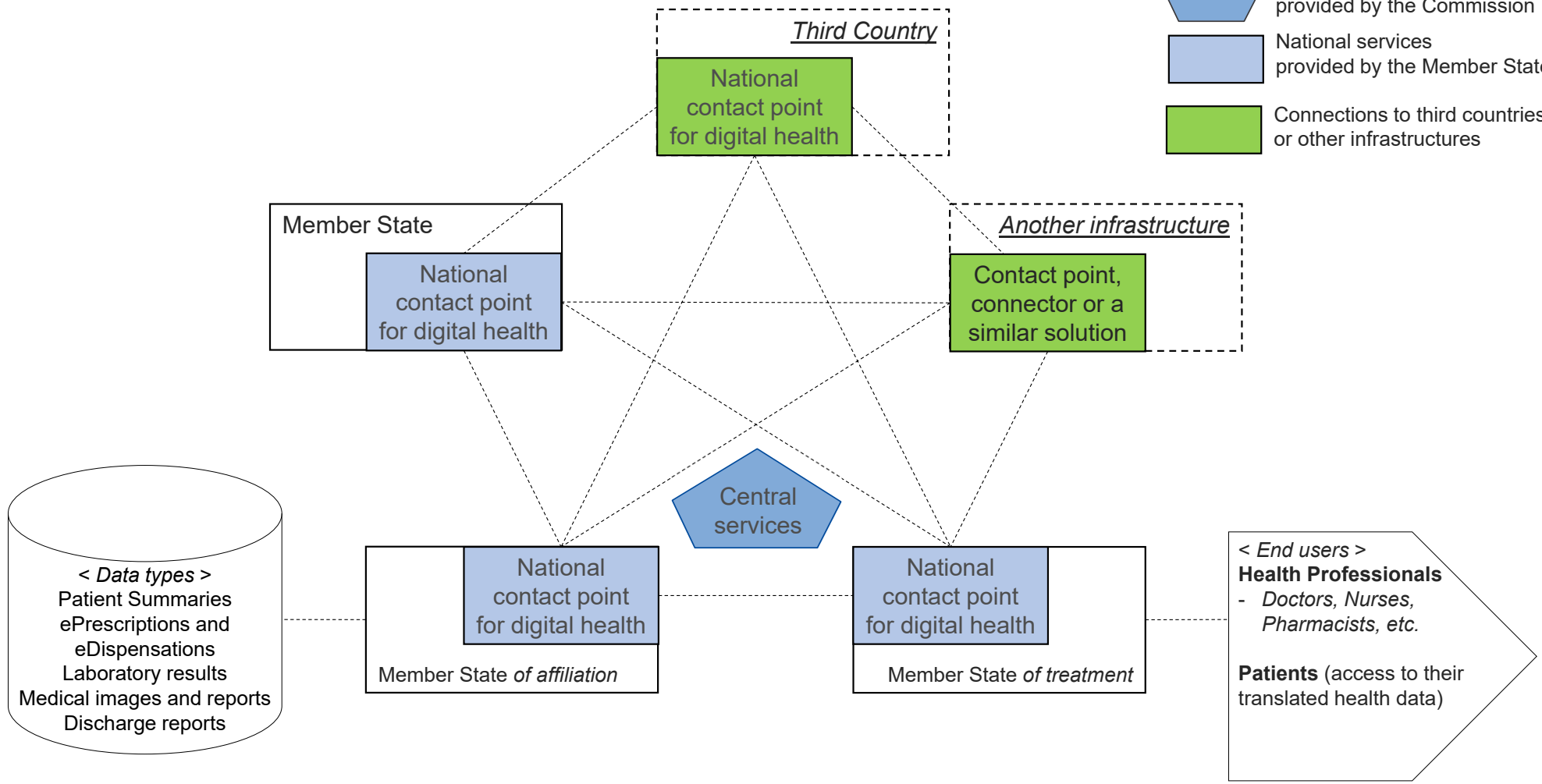


MyHealth@EU High-Level Architecture in the proposed EHDS regulation



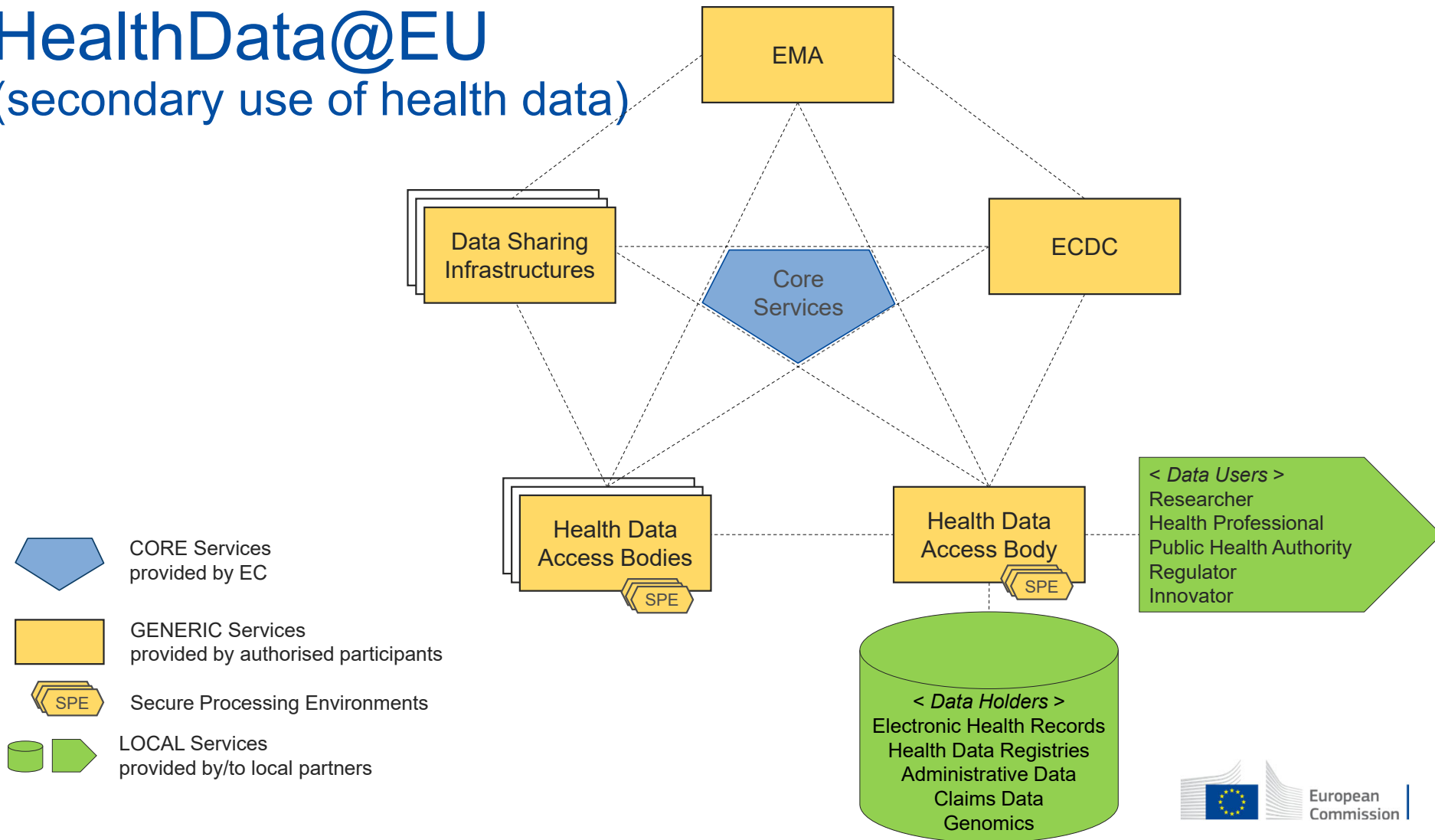
My Health @ EU
eHealth Digital Service Infrastructure
A service provided by the European Union

-  CENTRAL services provided by the Commission
-  National services provided by the Member States
-  Connections to third countries or other infrastructures

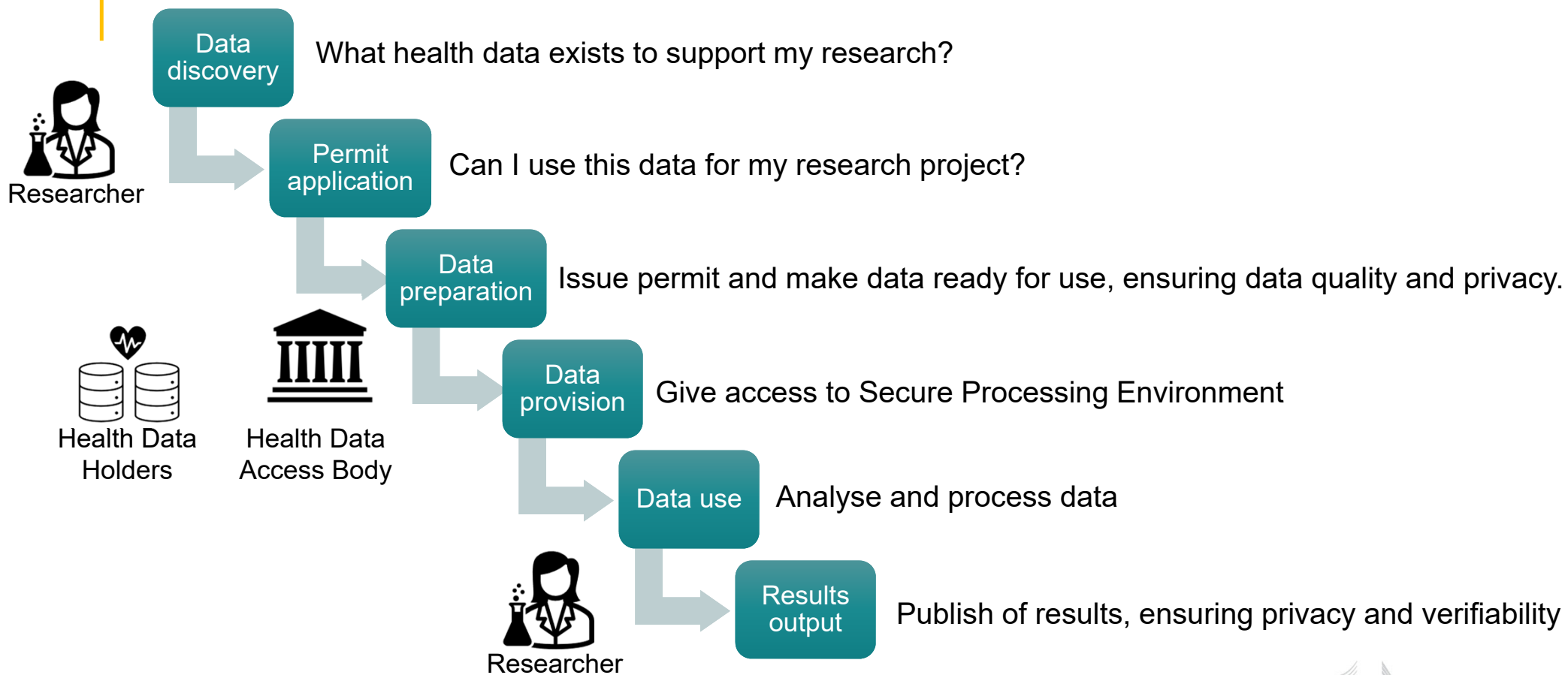


HealthData@EU

(secondary use of health data)



Overview of a generic data access approval process for secondary use under EHDS proposal



Primary use: expected benefits



Empower people...
... to have better control over their own health data
... to easily share with health professionals



Leading to...
... increased data sharing
... better health outcomes
... savings for patients and insurers by reducing unnecessary tests



Enable health professionals to have access to relevant health data
Translation functions as part of MyHealth@EU services



Better diagnosis and treatment
improved patient safety and continuity of care
Less manual data input



EU-wide standards for EHR systems



Easier market access in other Member States
Increased competition

Secondary use: expected benefits



Assist policy makers and regulators in accessing relevant health data



Better and faster decision-making
More resilient health systems
Safer medical technologies



Facilitate access to health data for innovators in industry



Greater opportunities for research and innovation
More innovative medical products



Make available health data for researchers



Greater opportunities for research and innovation

Individuals: strengthened **security**

Primary use

- Builds upon EU-cybersecurity legislation
- Security/interoperability criteria for EHR systems + CE marking
- Security audits for the MyHealth@EU (primary use) infrastructure
- Strong authentication for patient and health professionals
- Only persons entitled to access the data can get access to individual's data

Secondary use

- Data processed in secure processing environments, compliant with high standards of privacy and (cyber)-security.
- No personal data can be downloaded
- Users cannot identify individuals
- Audits of participants in HealthData@EU

Legislative process

- **Commission proposal** for EHDS Regulation: adopted on 3 May 2022 (COM(2022)197)
- **Council:** started examination under the FR Presidency (05/2022); Progress Report under the CZ Presidency (12/2022); second compromise text under the SE Presidency (1st half 2023); work continues under ES Presidency (2nd half 2023)
- **European Parliament:** shared competency of ENVI and LIBE committees

EHDS: requirements for EHR systems

- Mandatory **self-certification scheme** for electronic health records systems that process one or more priority categories of electronic health data
- The Commission shall, by means of **implementing acts**, adopt **common specifications** for EHR systems in respect of the essential requirements. The common specifications may include elements related to:
 - **security, confidentiality, integrity, patient safety and protection of electronic health data**
 - specifications and requirements related to **identification management** and the use of **e-identification**.
- Where common specifications covering interoperability and security requirements of **medical devices** or **high-risk AI systems** falling under other acts impact **EHR systems**, the adoption of these specifications shall be preceded by a consultation with the **EHDS Board**.

EHDS: requirements for EHR systems

- Section 3 of Annex II of the EHDS Regulation proposal is about the **essential security requirements for electronic health records systems**. The requirements are:
- Design that ensures safe and secure processing of health data, preventing unauthorised access
- For systems designed to be used by health professionals:
 - Supporting the use of information on professional rights and qualifications as part of the **access control mechanisms** (e.g. role-based access control)
 - Providing sufficient **logging mechanisms**, at least the following on each access event/group of events: a) identification of the individual who accessed the data, b) identification of the individual, c) categories of data accessed, d) time and date of access, and e) origins of data
- Including tools to **allow persons to restrict health professionals' access to their personal data**; including mechanisms to allow access to the data in **emergency situations**, while ensuring that the access is **strictly logged**

Thank you



© European Union 2020

Unless otherwise noted the reuse of this presentation is authorised under the [CC BY 4.0](https://creativecommons.org/licenses/by/4.0/) license. For any use or reproduction of elements that are not owned by the EU, permission may need to be sought directly from the respective right holders.



Health and the **NIS Directive**

- Under the **NIS2 Directive** (revised Network and Information Systems Directive), **healthcare** is identified as a **critical sector**. The NIS2 Directive:
 - obliges entities to strengthen security requirements
 - introduces stringent supervisory measures
 - imposes strict reporting obligations in case of incidents

Health and the EU Cybersecurity Act

- The EU's Cybersecurity Act contains a **cybersecurity certification framework**. This framework provides EU-wide certification schemes as a comprehensive set of **rules, technical requirements, standards and procedures**.
- It will attest that ICT products and services that have been certified in accordance with such a scheme comply with specified requirements.
- The first scheme under development is the one on Common Criteria, targeting ICT products such as hardware and software products and components. This could become **relevant for the health sector**.

Health and the **Cyber Resilience Act**

- The **Cyber Resilience Act** is focused on products with digital elements. It stipulates that **EHR systems** under the scope of the **EHDS** Regulation shall demonstrate conformity with the essential requirements of the Cyber Resilience Act (Art. 24). These essential requirements include:
 - cybersecurity-by-design
 - risk assessments
 - encrypting relevant data
 - mitigation of denial of service attacks
 - coordinated vulnerability disclosure