Colloquium on Cybersecurity in the Health Sector
European University Institute, Robert Schuman Centre
28 April 2023

Pseudonymisation, anonymisation and secure processing environments relating to the secondary use of electronic health data in the EHDS

Dr. Richard Rak

DIGITALEUROPE

DIGITALEUROPE represents over 45,000 businesses

The voice of digitally transforming industries

- platform services
- data analytics
- software & hardware
- cybersecurity
- telecoms
- semiconductors
- cloud technology
- Digital technologies
- Digital infrastructure
- Digital health
- Digital manufacturing
- Digital commerce
- Digital finance
- Digital sustainability

41
NATIONAL TRADE ASSOCIATIONS

103
COMPANIES

DIGITALEUROPE

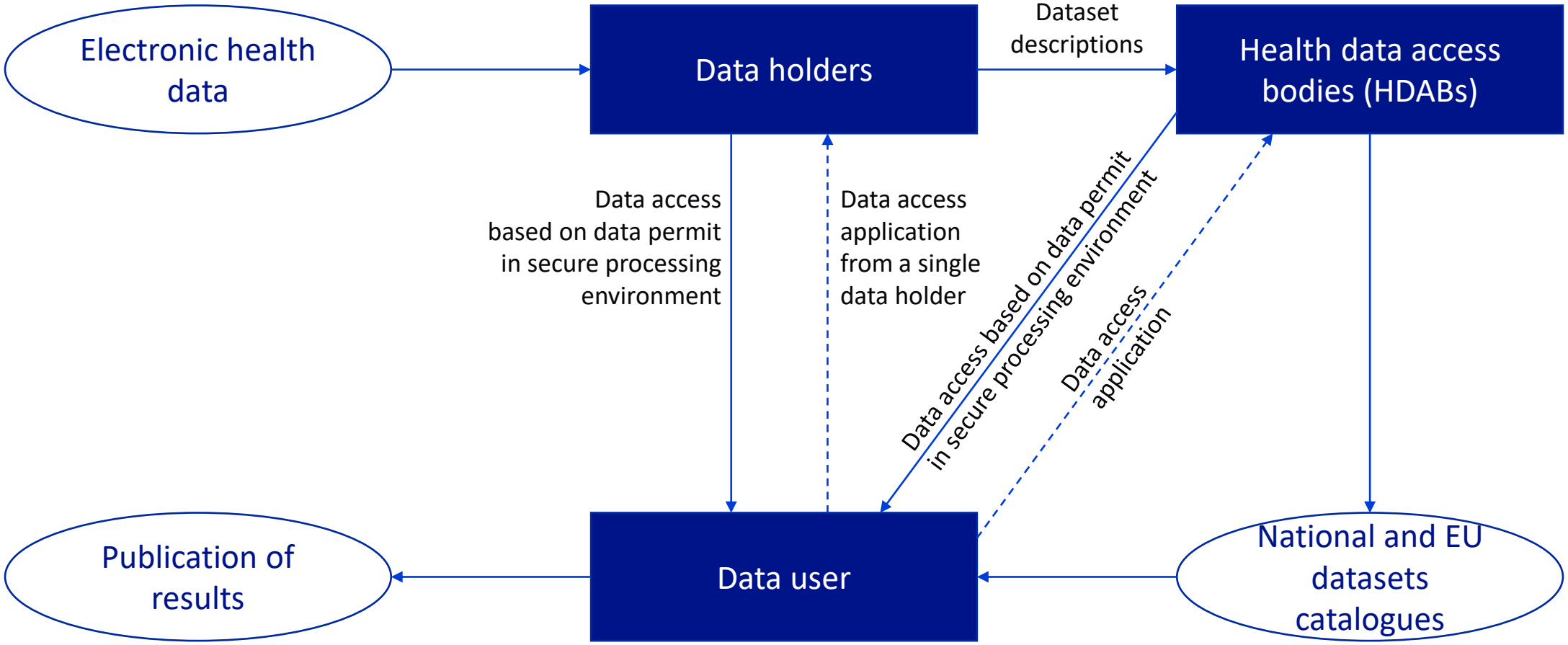
Talking points

DIGITALEUROPE

- Data governance in EHDS2: an overview
- Data minimisation and allocation of data protection responsibilities in EHDS2
- Outlook: Finnish model for secondary use of health data
- Secure processing environments in EHDS2

Data governance in EHDS2

DIGITALEUROPE



Data minimisation and data protection responsibilities in EHDS2

DIGITALEUROPE

General rule:

Art. 44(2) The health data access bodies shall provide the **electronic health data in an anonymised format**, where the purpose of processing by the data user can be achieved with such data, taking into account the information provided by the data user.

- Who should perform anonymisation: HDABs? Pseudonymisation bodies? Data holders (if they have the necessary means)?
- Anonymisation standard should be relative (from data holders') or absolute (from third parties' perspective)?
- Recital 26 GDPR: reidentification must be 'reasonably unlikely' (Malgieri & Comandé: 'data sensitiveness by computational distance' test?)
- A29WP Opinion 05/2014: original (identifiable) data at event-level must be deleted for a data set to be anonymised?

Specific rule:

Art. 44(3) Where the purpose of the data user's processing cannot be achieved with anonymised data, taking into account the information provided by the data user, the health data access bodies shall provide access to **electronic health data in pseudonymised format**. The information necessary to reverse the pseudonymisation shall be available only to the health data access body. […]

- *'Personal* electronic health data' in pseudonymised format (but such data has distinct characteristics)
- Data user should demonstrate that its purpose cannot be achieved with anonymised data?
- Who should hold the encryption key: HDABs? Pseudonymisation bodies? Data holders?

Outlook: Finnish model for secondary use of health data

DIGITALEUROPE

Finnish regulatory framework for secondary use of electronic health data:

- controller ('data holder') is required to perform pre-processing (data cleaning) to provide **ready-made datasets**, but the HDAB performs the pseudonymisation, and performs anonymisation only if the data permit requires this ↔ under Art. 44(2) EHDS, the general rule is to provide electronic health data in an anonymised format

- health data repositories and data lakes were established primarily from **high-quality data registries** held by public providers of healthcare services ↔ Art. 33 of the EHDS would require the making available of broader electronic health data categories for secondary use, and the EHDS would apply to a wider range of data holders than in the Finnish system

- Finland has 9 secure processing environments (SPEs) and detailed rules on information security and auditing of SPEs

- cultural difference: **trust** in authorities is the highest in the EU

- Finnish experience: importance of HDABs facilitating **communication** between data holders and data users

Secure processing environments in EHDS2

DIGITALEUROPE

1. Data access via health data access bodies:

Art. 50(1) The **health data access bodies shall provide access to electronic health data only through a secure processing environment**, with technical and organisational measures and security and interoperability requirements.

- But the intention is that the HDABs do not actually have to operate the SPEs, it is sufficient to oversee them (like in Finland).

Art. 50(2) The health data access bodies shall ensure that electronic health data can be **uploaded** by data holders and can be accessed by the data user in a secure processing environment. The data users shall only be able to **download** non-personal electronic health data from the secure processing environment.

- Upload in any format? Or should the data permit define the format?
- 'Download' is not the only way to make a copy.
- 'Non-personal electronic health data': how to delimit (e.g. for aggregated data)? does HDAB oversee this requirement?

Secure processing environments in EHDS2

DIGITALEUROPE

2. Data access via single data holders:

Art. 49(1) Where an applicant requests access to electronic health data only from a single data holder in a single Member State [.], that applicant may file a data access application [.] **directly to the data holder**.

- 'Single data holder'?

Art. 49(2) [.] The **data holder shall then provide access to the electronic health data in a secure processing environment** in compliance with Article 50 [.].

- Would the data holder bear all related duties of a HDAB?
- Is it realistic to expect that all single data holders will meet the technical, information security and interoperability requirements and have dedicated personnel and resources for operating secure processing environments?
- 'Electronic health data' would cover non-personal electronic health data [in line with Art. 2(2)(b)]?
- But *cf.* Art. 41(6): "Data holders of non-personal electronic health data shall ensure access to data through trusted open databases to ensure unrestricted access for all users and data storage and preservation."

#AStrongerDigitalEurope | @DIGITALEUROPE | linkedin.com/digitaleurope

Thank you for your attention

DIGITALEUROPE