



4Y
FN

MWC
GSMA

Digital Health & Wellness Summit:

Data Protection Challenges by Using the European Data Health Space (EHDS)



Marit Hansen

Land Schleswig-Holstein, ULD



Xavier Urios

Catalan Data Protection
Authority



Meritxell Borràs Solé

Catalan Data Protection Authority

28th February | 12:15 - 12:45 | Sky Stage

#4YFN24

#DHWS24

European Data Health Space (EHDS) – Data Protection by Design and by Default

(... some bits & pieces ...)

Dr. h.c. Marit Hansen
State Data Protection Commissioner
of Schleswig-Holstein, Germany
Barcelona, 28 February 2024

Overview

1. What is the EHDS?
2. The notion of risk
3. Data protection by design in data sharing
4. Summary
5. Links

https://health.ec.europa.eu/ehealth-digital-health-and-care/european-health-data-space_en

The EHDS

“The **European Health Data Space** is a health specific ecosystem comprised of rules, common standards and practices, infrastructures and a governance **framework** that aims at

- **empowering individuals** through increased digital access to and control of their electronic personal health data, at national level and EU-wide, and support to their free movement, as well as fostering a genuine single market for electronic health record systems, relevant medical devices and high risk AI systems (primary use of data)
- providing a **consistent, trustworthy and efficient** set-up for the use of health data for **research, innovation**, policy-making and regulatory activities (secondary use of data)”

And what about the GDPR?

Overview

1. What is the EHDS?
2. The notion of risk
3. Data protection by design in data sharing
4. Summary
5. Links

https://health.ec.europa.eu/ehealth-digital-health-and-care/european-health-data-space_en

The EHDS

“The **European Health Data Space** is a health specific ecosystem comprised of rules, common standards and practices, infrastructures and a governance **framework** that aims at

This Regulation shall be without prejudice to other Union legal acts regarding access to, sharing of or secondary use of electronic health data, or requirements related to the processing of data in relation to electronic health data, in particular Regulations (EU) 2016/679, (EU) 2018/1725, [...] [Data Governance Act COM/2020/767 final] and [...] [Data Act COM/2022/68 final].

This Regulation shall be without prejudice to Regulations (EU) 2017/745 and [...] [AI Act COM/2021/206 final], as regards the security of medical devices and AI systems that interact with EHR systems.

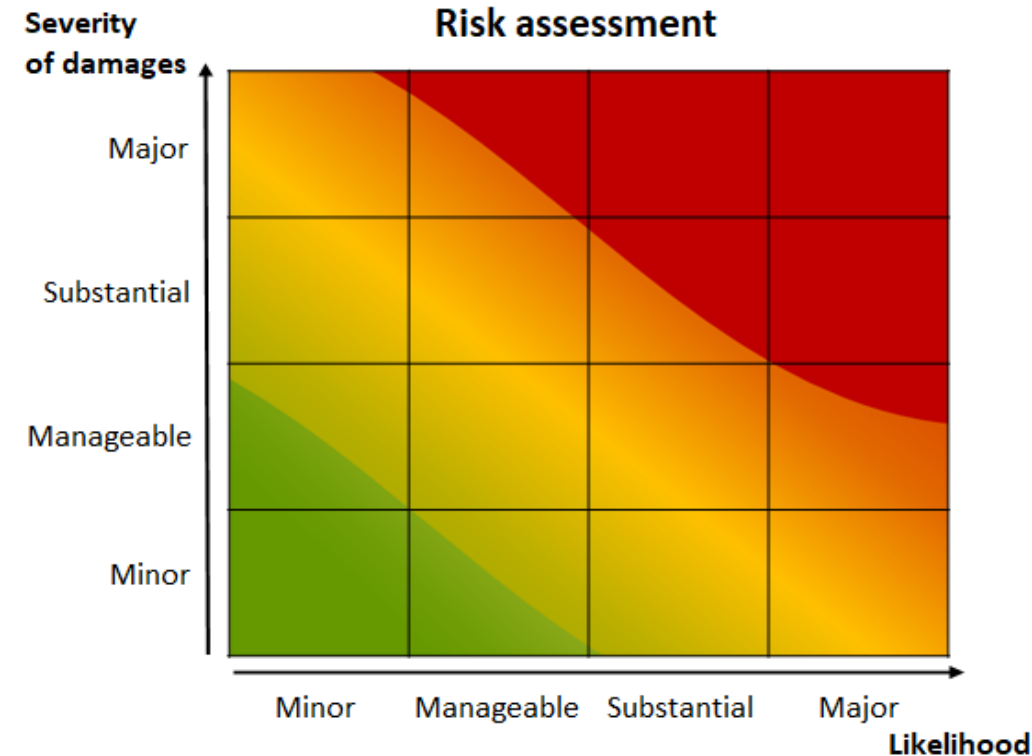
↑ *And what about the GDPR?* ↑

Overview

1. What is the EHDS?
2. The notion of risk
3. Data protection by design in data sharing
4. Summary
5. Links



Trustworthy? The GDPR's notion of risk



Risk for the **rights and freedoms of natural persons** – see Charter of Fundamental Rights

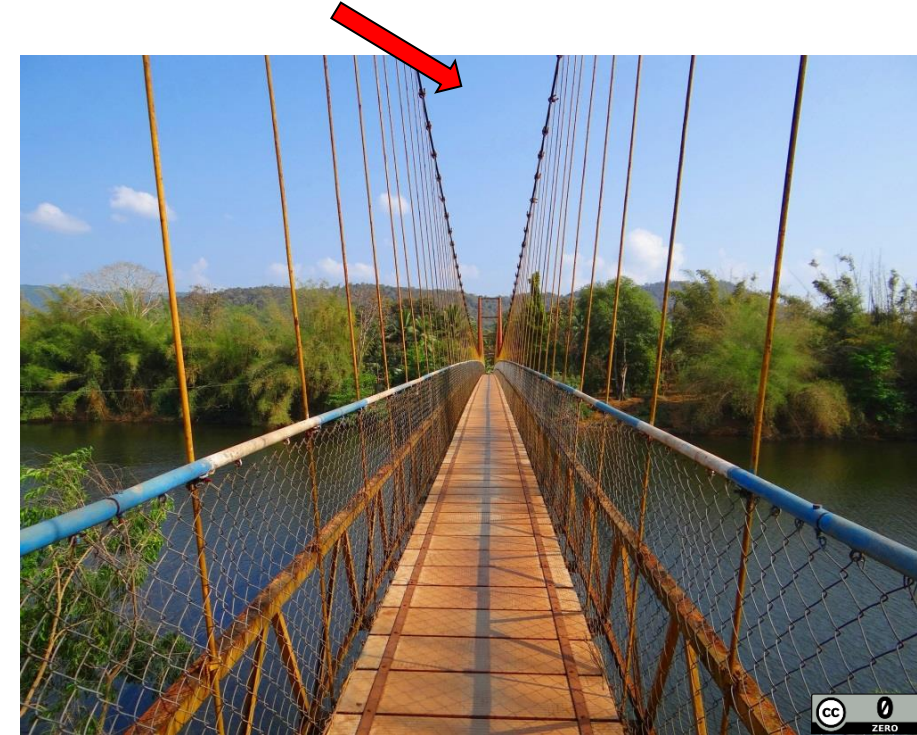
Overview

1. What is the EHDS?
2. The notion of risk
3. Data protection by design in data sharing
4. Summary
5. Links

GDPR demands risk mitigation



High risk – not lawful without **prior risk mitigation** (design, technical and organisational measures)



Trustworthiness through appropriate built-in measures and checkability

Overview

1. What is the EHDS?
2. The notion of risk
3. Data protection by design in data sharing
4. Summary
5. Links

Risks concerning health data

Examples in recital 75 of the GDPR:

- “physical, material or non-material damage”
- Personal data of vulnerable persons

For health data:

- (Not only) security risks
- Wrong diagnosis
- Wrong treatment
- Loss of confidentiality
- Identification
- Economic or social disadvantage
- Discrimination
- Deprivation of rights and freedoms including data subject rights

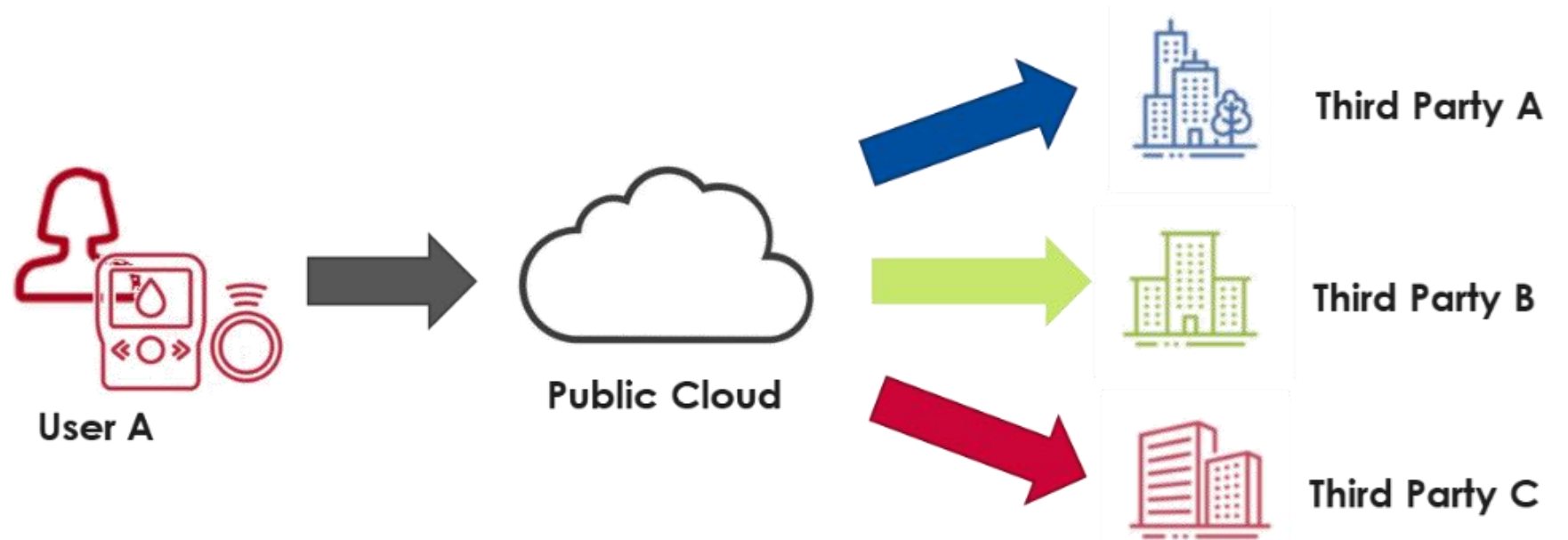
Art. 25 GDPR:
Data protection by design
and by default
i.e. through the **entire lifecycle**

Overview

1. What is the EHDS?
2. The notion of risk
3. Data protection by design in data sharing
4. Summary
5. Links



Data sharing scenarios (same principle for public clouds and data spaces)



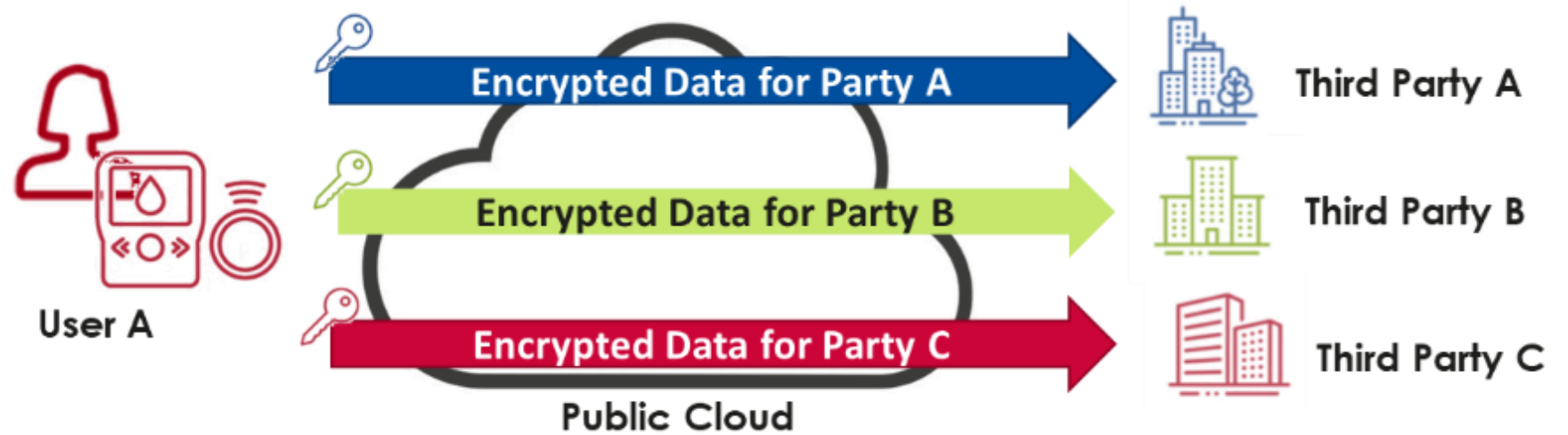
Generic model of user-controlled data sharing (Figure 1)

Overview

1. What is the EHDS?
2. The notion of risk
3. Data protection by design in data sharing
4. Summary
5. Links



Data sharing with encryption: Asymmetric encryption [1.]



Encryption? – Sure thing.
Hmm, but we don't know all recipients beforehand.

User-controlled data sharing through asymmetric encryption (Figure 2)

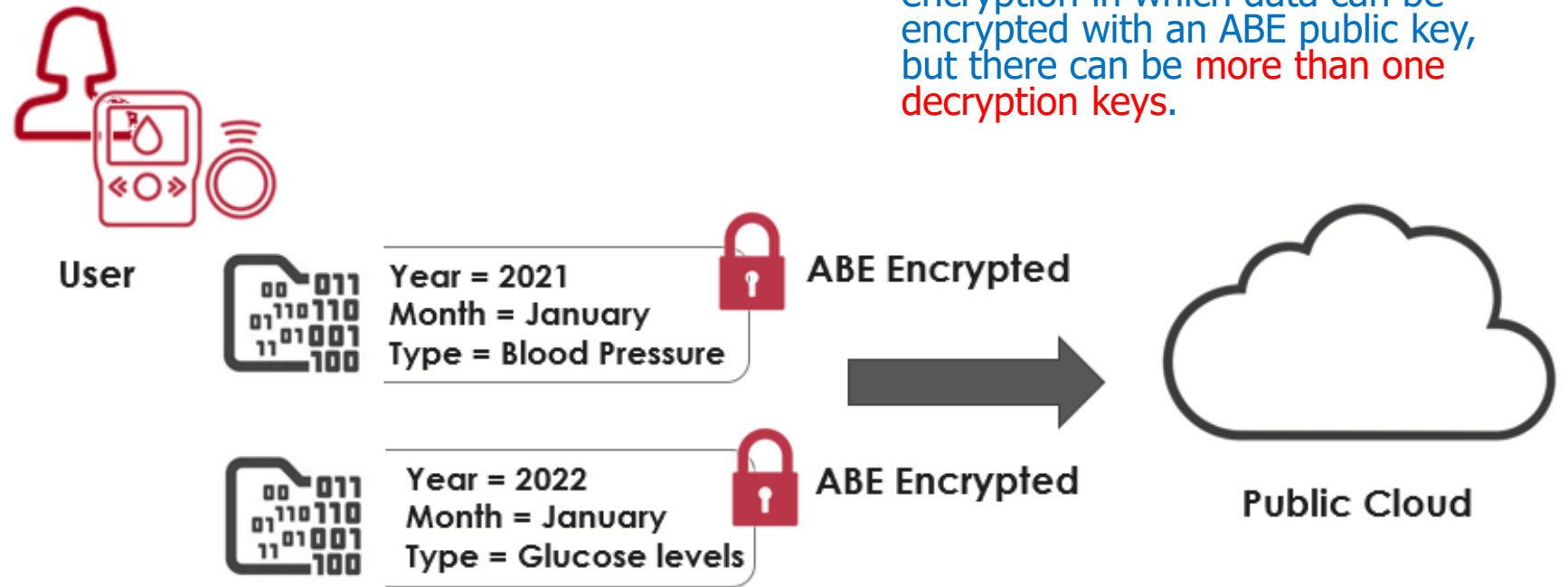
Overview

1. What is the EHDS?
2. The notion of risk
3. Data protection by design in data sharing
4. Summary
5. Links



Data sharing with encryption: Attribute Based Encryption (ABE) [2.]

ABE: special type of asymmetric encryption in which data can be encrypted with an ABE public key, but there can be **more than one decryption keys**.



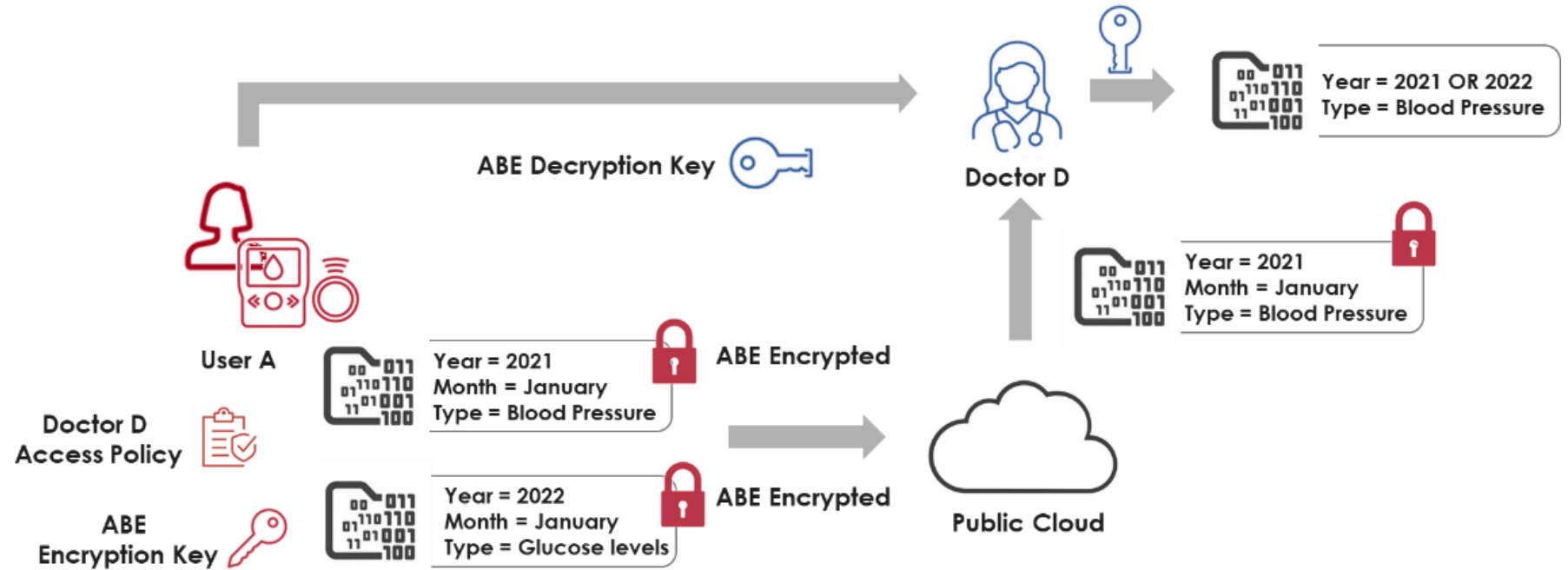
Storing encrypted objects to the cloud (Figure 3)

Overview

1. What is the EHDS?
2. The notion of risk
3. Data protection by design in data sharing
4. Summary
5. Links



Data sharing with encryption: Attribute Based Encryption (ABE) [2.]



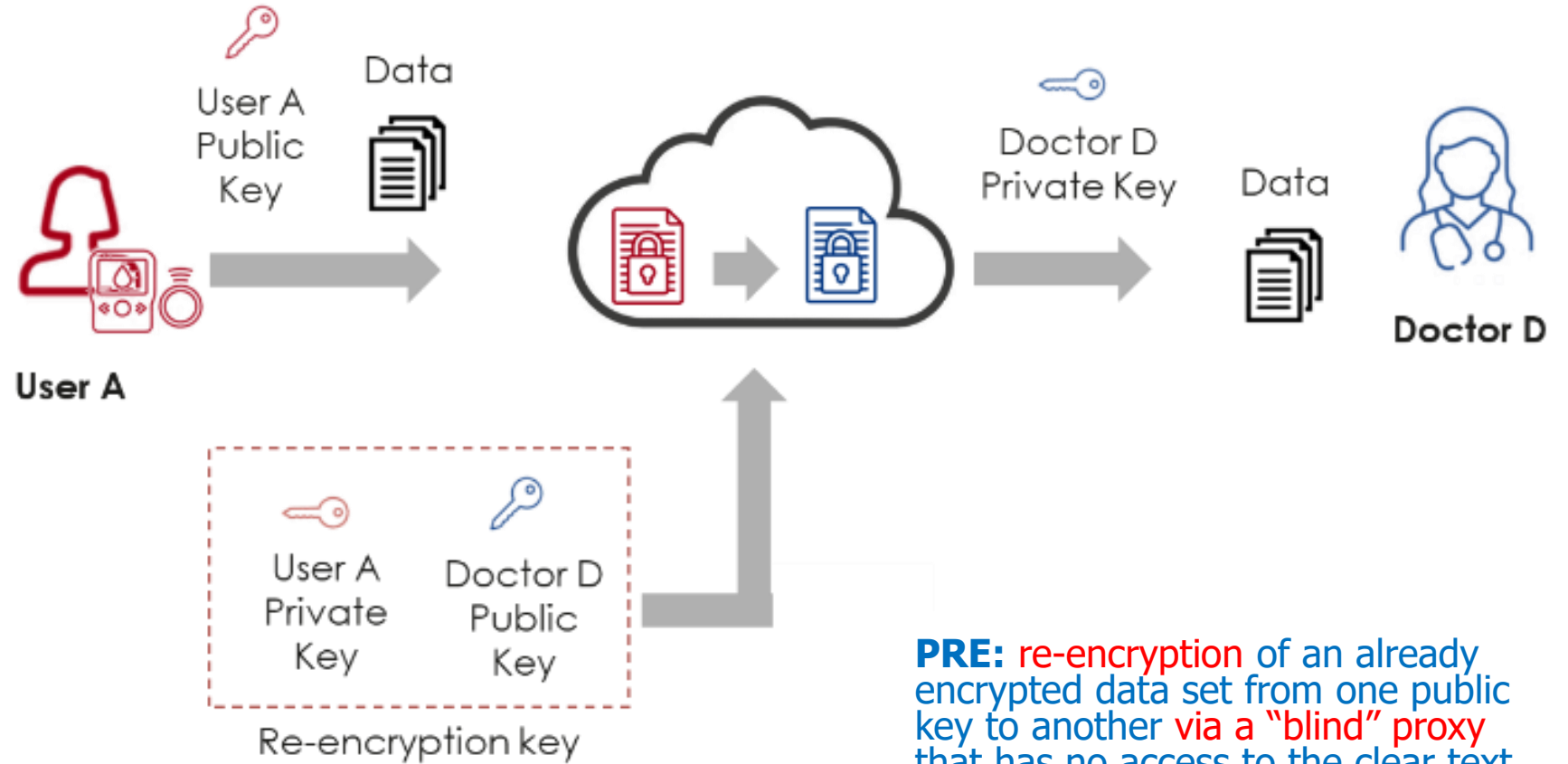
Sharing the ABE decryption key and encrypted data (Figure 4)

Overview

1. What is the EHDS?
2. The notion of risk
3. Data protection by design in data sharing
4. Summary
5. Links



Data sharing with encryption: Proxy Re-Encryption (PRE) [3.]



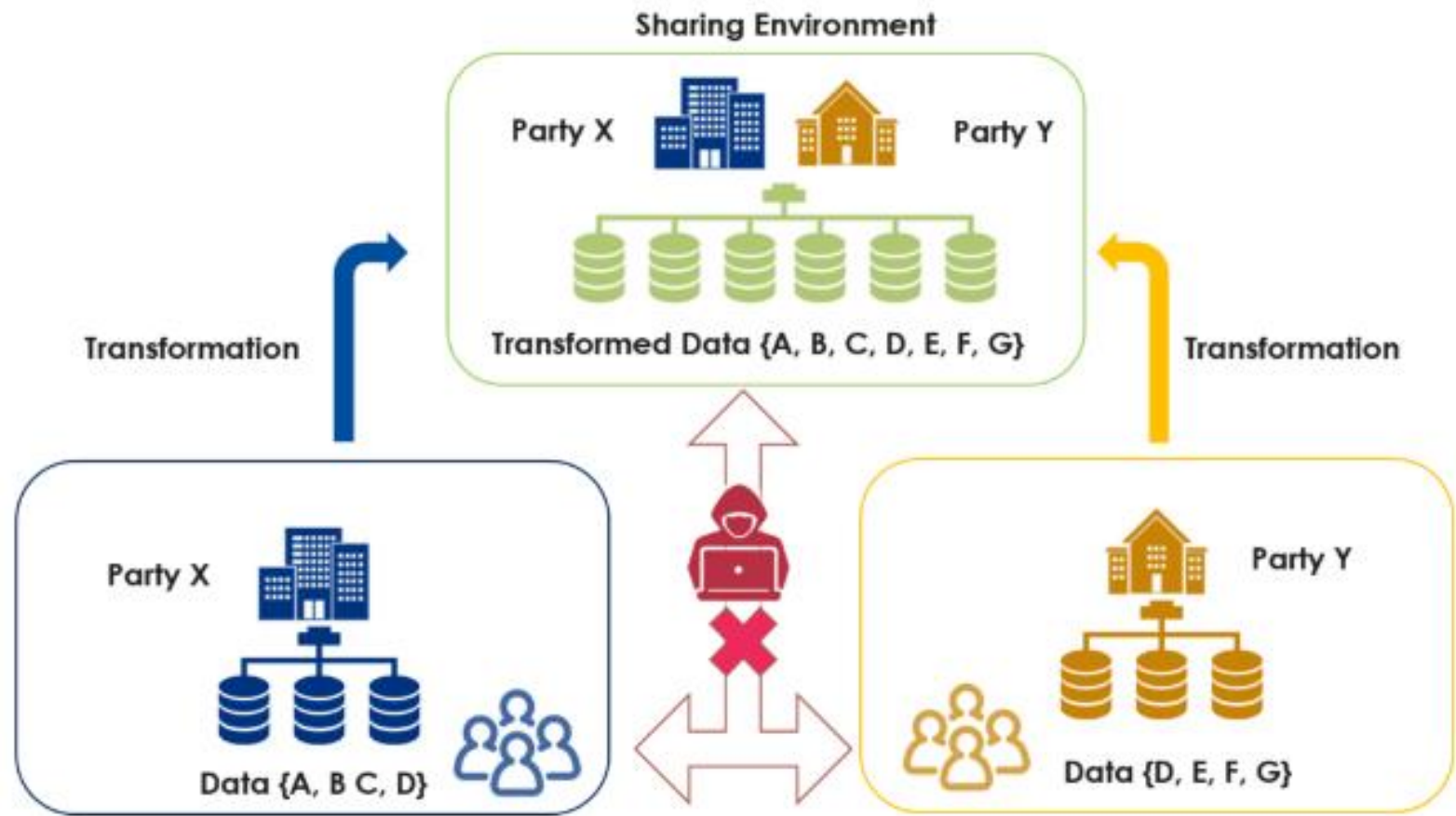
PRE: re-encryption of an already encrypted data set from one public key to another via a "blind" proxy that has no access to the clear text.

Proxy Re-Encryption process (Figure 5)

For Data Spaces: prevention of identification for all unauthorised stakeholders

Overview

1. What is the EHDS?
2. The notion of risk
3. Data protection by design in data sharing
4. Summary
5. Links



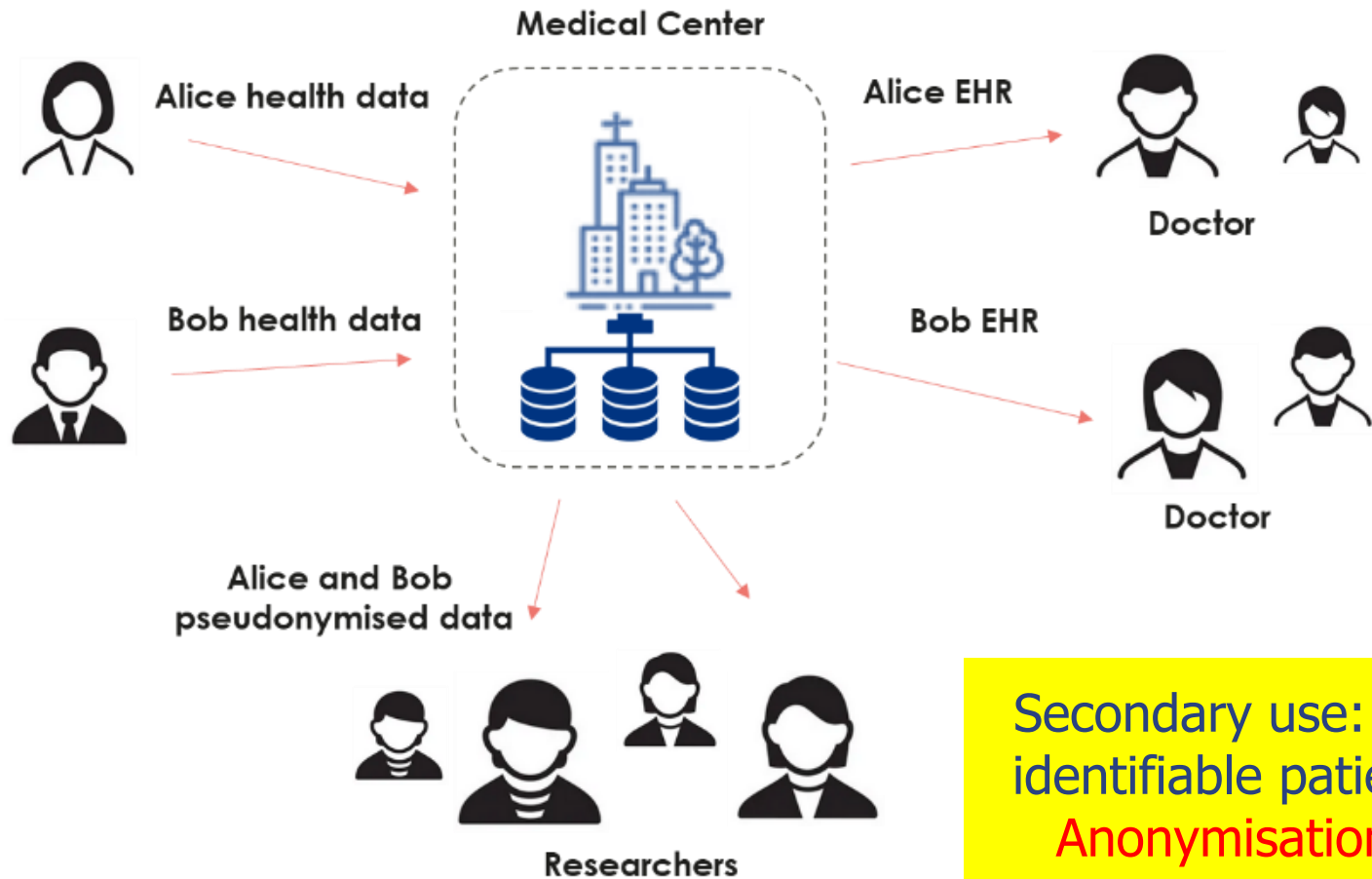
(Input +) Output Privacy Problem (Figure 3)

Overview

1. What is the EHDS?
2. The notion of risk
3. Data protection by design in data sharing
4. Summary
5. Links



Data sharing with pseudonymisation [4.]



Secondary use: without identifiable patient data
Anonymisation? No, rather pseudonymisation!

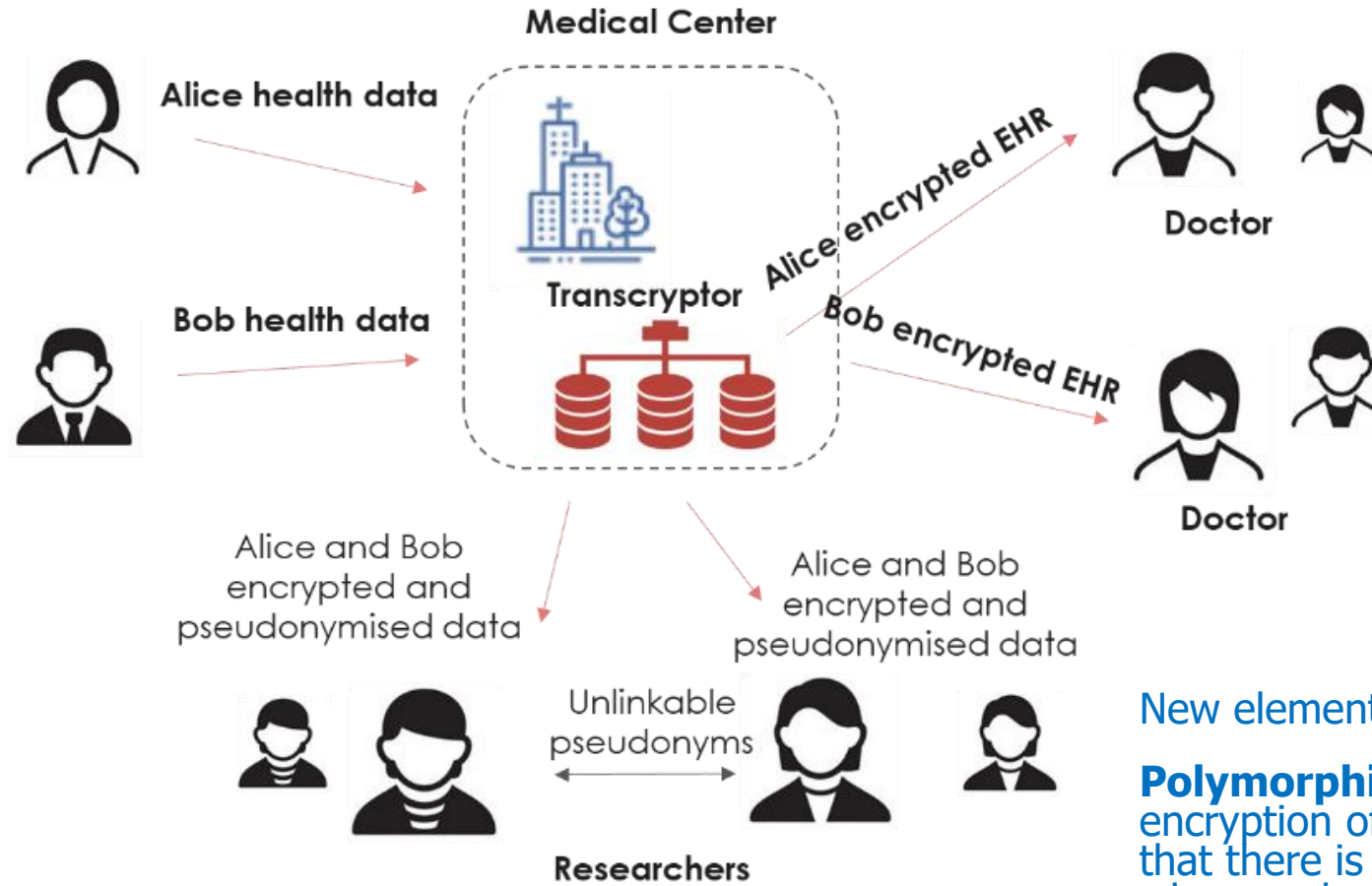
Large scale data gathering example (Figure 6)

Overview

1. What is the EHDS?
2. The notion of risk
3. Data protection by design in data sharing
4. Summary
5. Links



Data sharing with Polymorphic Encryption and Pseudonymisation (PEP) [5.]



New element: **Transcriptor**.

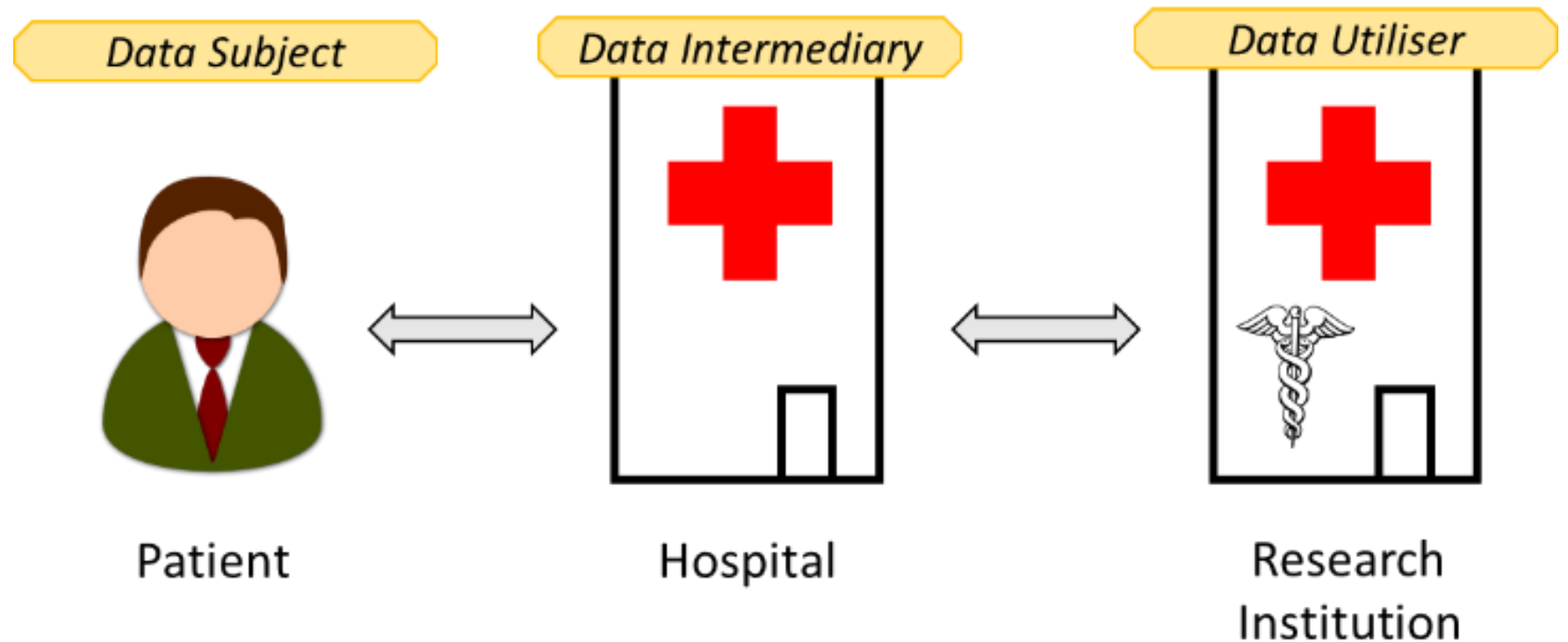
Polymorphic encryption: enables encryption of data in such a way that there is no need to fix a priori who can decrypt the data.

Using PEP in large scale data gathering (Figure 7)

Data sharing with intermediaries enforcing conditions [6.]

Overview

1. What is the EHDS?
2. The notion of risk
3. Data protection by design in data sharing
4. Summary
5. Links



Data sharing scenario with data intermediaries (Figure 14)

Overview

1. What is the EHDS?
2. The notion of risk
3. Data protection by design in data sharing
4. Summary
5. Links



Machine-Readable User's Data Processing Preferences / Conditions [6a.]



User A Data Processing Preferences

I want my data to be processed only by Utiliser X, Y & Z

I want my data to be processed only within the EU

I want my data to be processed only for 2 years

I want my data to be processed only for medical research purposes

Should it be more than "consent" or "opt-out"?

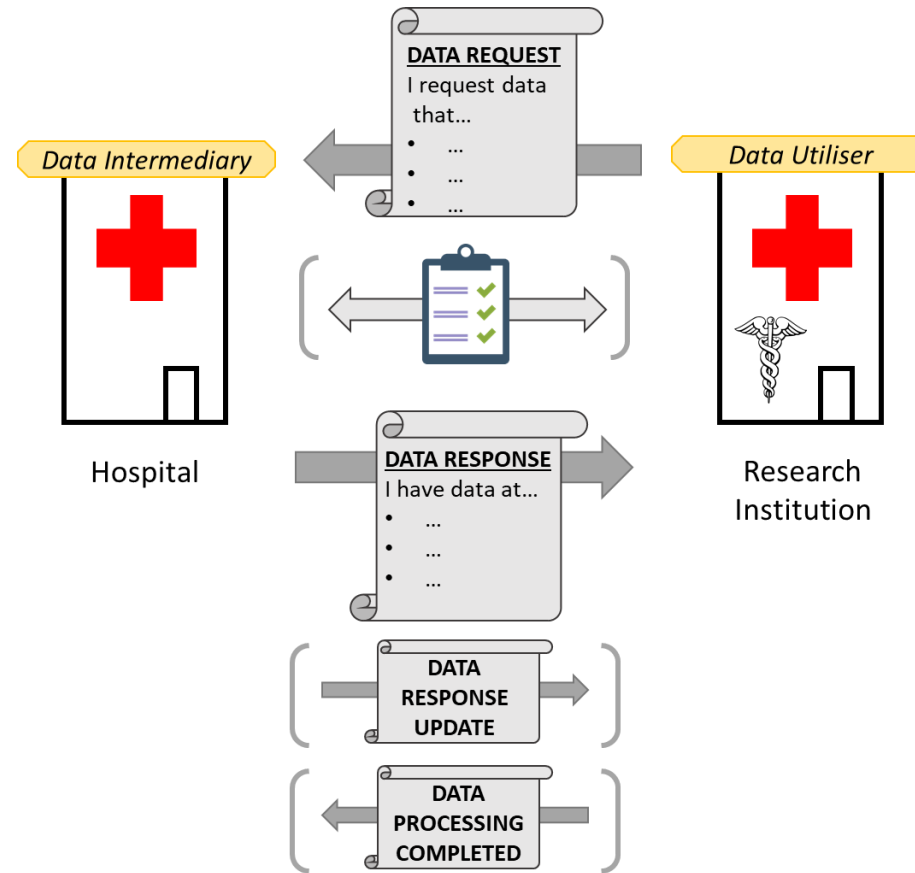
Data Processing Preferences Example (Figure 15)

Overview

1. What is the EHDS?
2. The notion of risk
3. Data protection by design in data sharing
4. Summary
5. Links



Data sharing protocols for interacting with data intermediaries [6b.]



Goals:

- **accountability** (Art. 5 (2), Art. 24 GDPR)
- enabling data subjects to **exercise their rights**

Interaction between Data Intermediary and Data Utiliser (Figure 16)

Overview

1. What is the EHDS?
2. The notion of risk
3. Data protection by design in data sharing
4. Summary
5. Links

Summary & outlook

- Processing of **health data** = **high risk**
- GDPR demands
 - Above all: **risk mitigation**
 - Art. 25: Data protection by design and by default
 - Encryption & pseudonymisation
 - Data subject rights
 - Data protection management
- Note: **anonymisation** in the health context is often **not possible**. Or **not helpful**.
- EHDS = **infrastructure** – we need **proper** standards & defaults, not one centralised huge database without user control

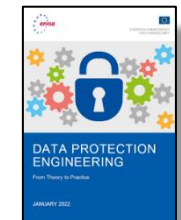


Overview

1. What is the EHDS?
2. The notion of risk
3. Data protection by design in data sharing
4. Summary
5. Links

Links

- DSK: The Standard Data Protection Model Version 3.0a (English version), 2022, https://www.datenschutzm.de/static/DS/Dateien/Datenschutzmodell/SDM_V3_en.pdf
- EDPB: EDPB-EDPS Joint Opinion 03/2022 on the Proposal for a Regulation on the European Health Data Space, 2022, https://edpb.europa.eu/our-work-tools/our-documents/edpb-edps-joint-opinion/edpb-edps-joint-opinion-032022-proposal_en
- ENISA: Data Protection Engineering, January 2022, <https://www.enisa.europa.eu/publications/data-protection-engineering>
- ENISA: Deploying Pseudonymisation Techniques, March 2022, <https://www.enisa.europa.eu/publications/deploying-pseudonymisation-techniques>
- ENISA: Engineering Personal Data Sharing, January 2023, <https://www.enisa.europa.eu/publications/engineering-personal-data-sharing>
- ENISA: Engineering Personal Data Protection in EU Data Spaces, January 2024, <https://www.enisa.europa.eu/publications/engineering-personal-data-protection-in-eu-data-spaces>



Thank you

apdcat

Autoritat Catalana de Protecció de Dades

#4YFN24