

Privacy and Ethics in Secondary Use of Sensitive Data

CyberSecurityCoalition, June 16 2022
© dr. Griet Verhenneman



Requests for secondary use of health-related data ↑

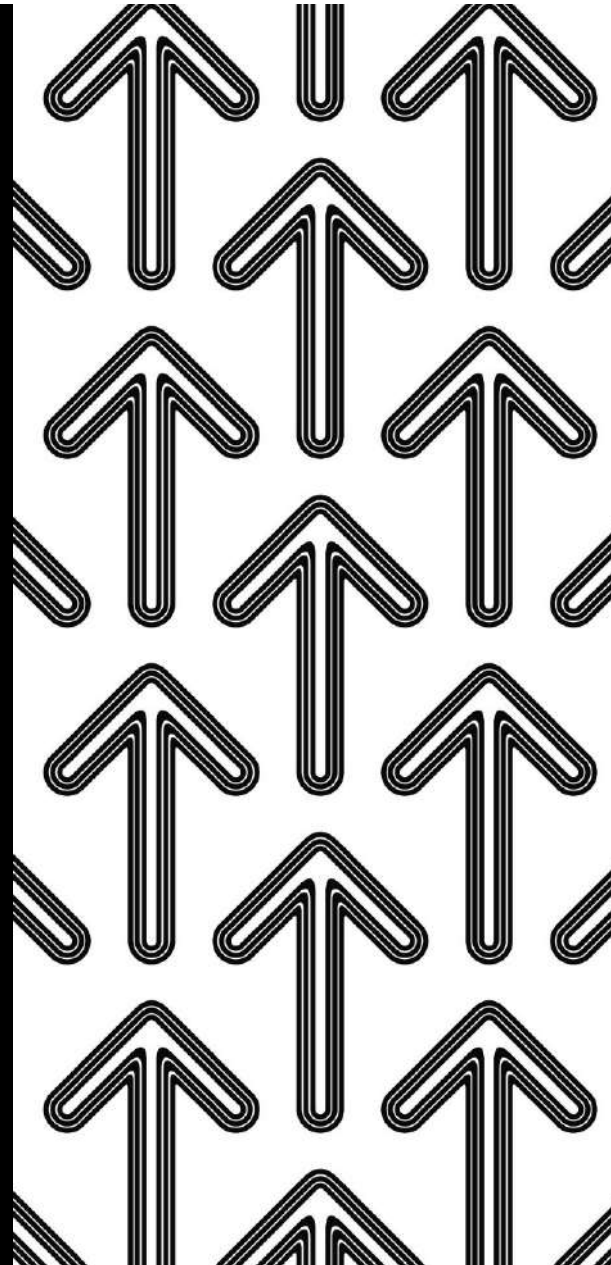
- Legal obligations (incl. MDR / IVDR)
- Data-driven scientific research
- Data-driven projects on efficiency, safety and quality,...

Secondary use is
of all times,
where is the key
change?



Data availability

Data linkability



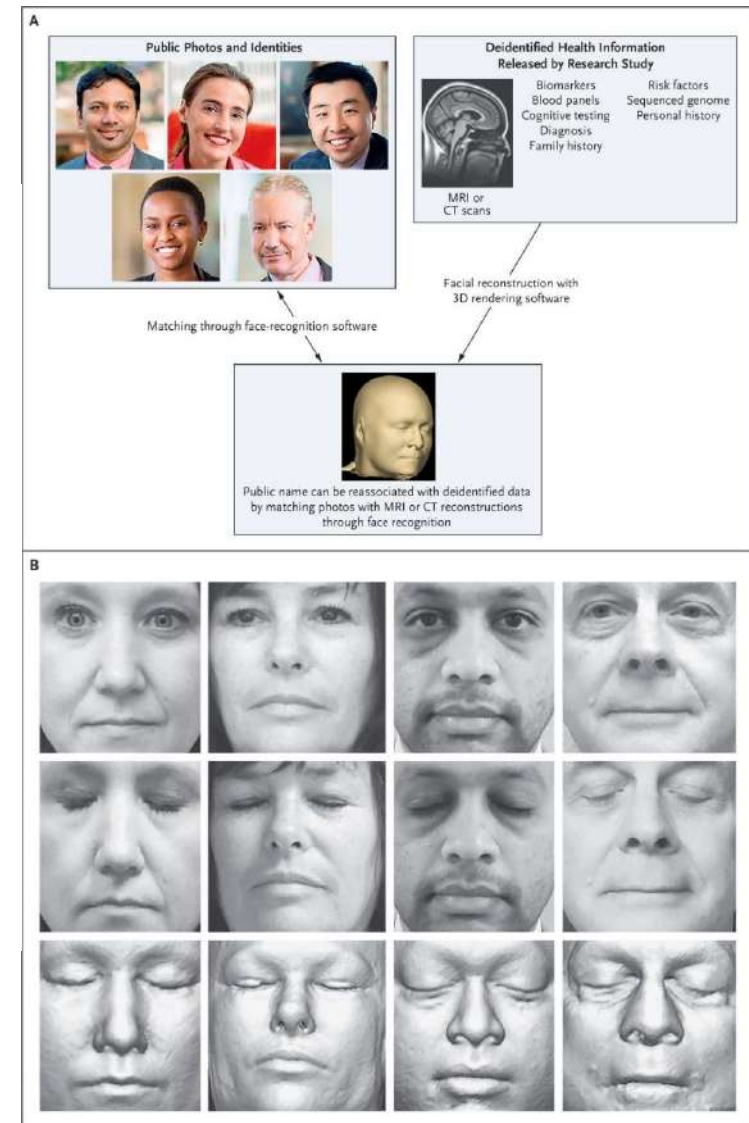
CORRESPONDENCE



Identification of Anonymous MRI Research Participants with Face-Recognition Software

TO THE EDITOR: Public sharing of research data is being widely promoted. Medical image files contain “metadata” such as the name of the participant, the date of the scan, and the identification number. Such data are typically removed (deidentified) before data sharing, but images of the face in magnetic resonance imaging (MRI)

MRI scans, we recruited 84 volunteers between the ages of 34 and 89 years, stratified according to sex and decade of age, and photographed each participant’s face from five slightly varying angles. Each participant had undergone MRI of the head (three-dimensional fluid-attenuated inversion recovery [FLAIR] sequence, conducted



i I IA t “ F
A ASPRAREgcRReghI

SHE REALLY LIKED THAT SHIRT —

Masked arsonist might've gotten away with it if she hadn't left Etsy review

Woman who burned two police cars IDed by tattoo and Etsy review of her T-shirt.

JON BRODKIN - 6/18/2020, 6:48 PM



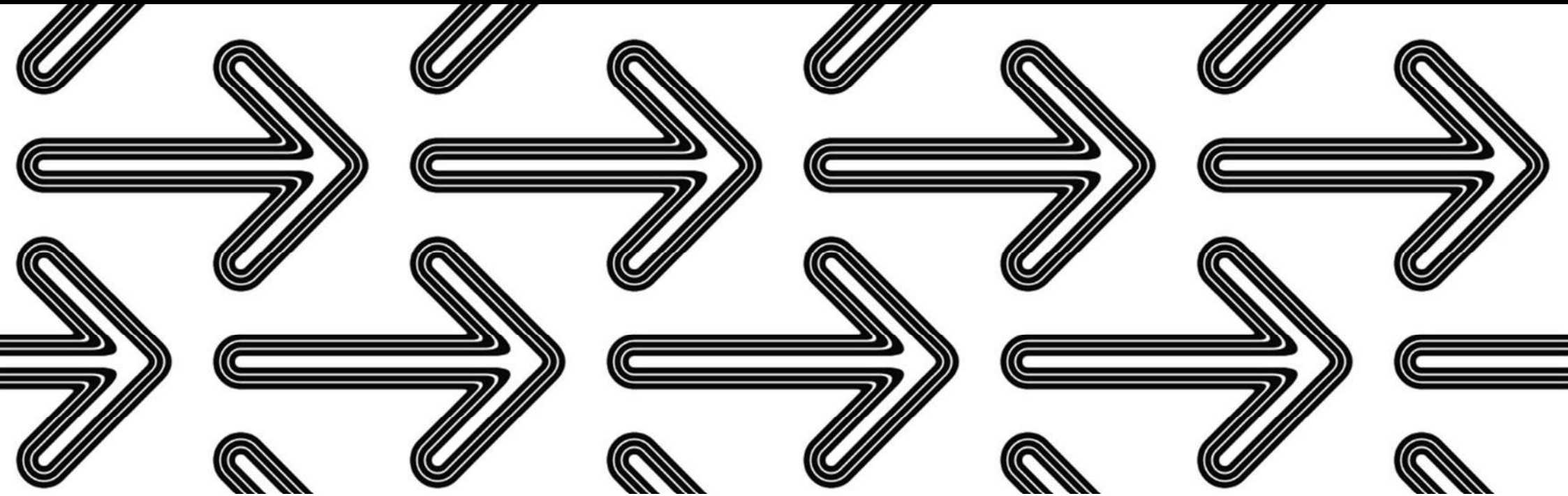
[Enlarge](#) / Instagram photo of a masked woman, identified by the FBI as Lore-Elisabeth Blumenthal, on May 30, 2020 in Philadelphia.

Moreover:

Open Science
Explainability
Patient
empowerment



source data
have to be kept



“It is critical to understand that when a data controller does not delete the original (identifiable) data at event-level, and the data controller hands over part of this dataset (for example after removal or masking of identifiable data), the resulting dataset is still personal data”

Article 29 Working Party, 2014

“Let wel op: gegevens zijn enkel (voldoende) anoniem, als zij ook in combinatie met andere gegevens (ook van andere partijen) niet meer tot heridentificatie kunnen leiden (bvb. IP adressen zijn altijd persoonsgegevens, want met de hulp van een telecomoperator kan men iemand re-identificeren).”

Gegevensbeschermingsautoriteit, 2020

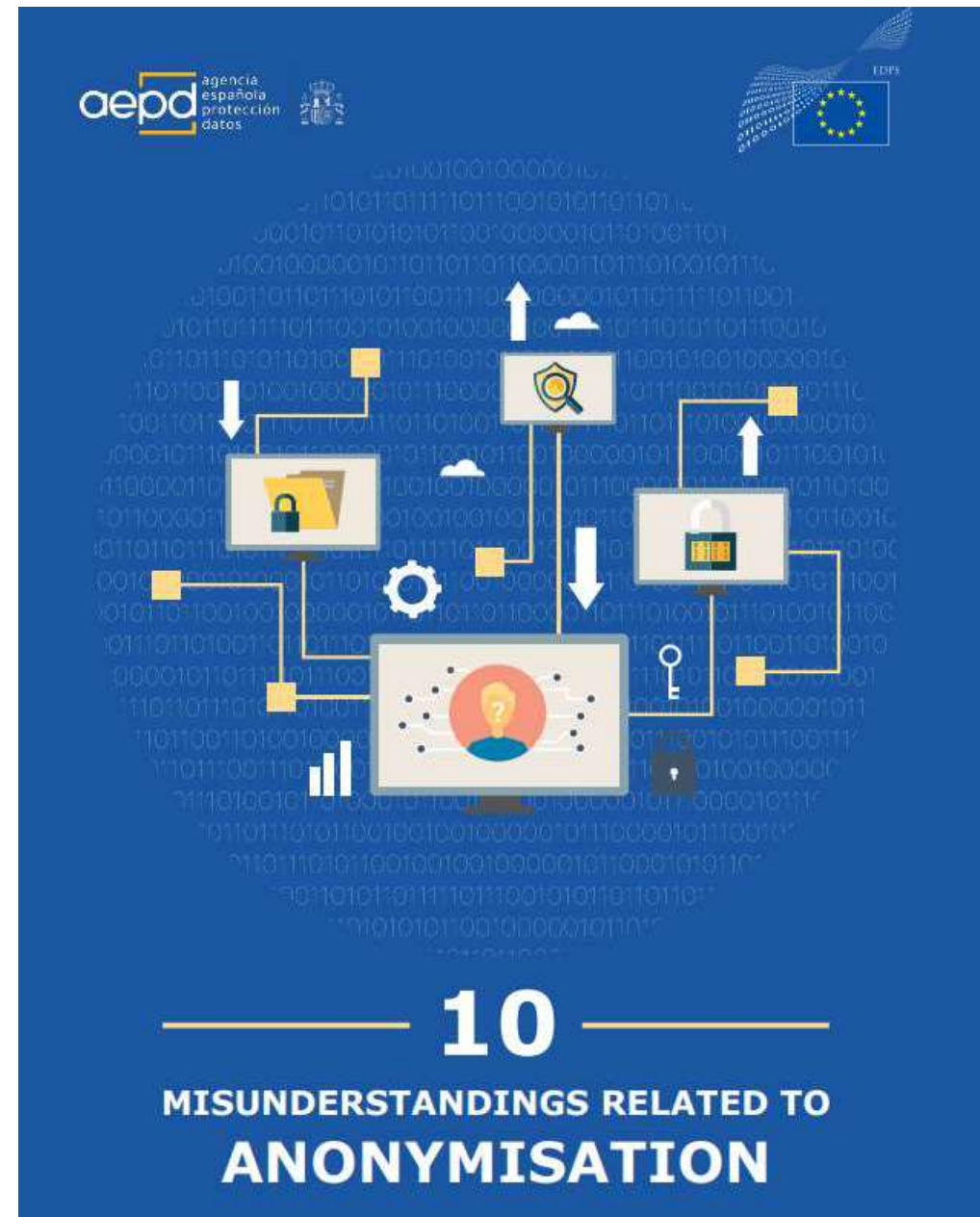
US Health Insurance Portability and Accountability Act (HIPAA) identifiers:

1. Name
2. Address (all geographic subdivisions smaller than state, including street address, city county, and zip code)
3. All elements (except years) of dates related to an individual (including birthdate, admission date, discharge date, date of death, and exact age if over 89)
4. Telephone numbers
5. Fax number
6. Email address
7. Serial number or unique identifier of (medical) device
8. Social Security Number (INSZ, RRN)
9. Medical record number (EAD, EMD)
10. Health plan beneficiary number
11. Account number
12. Certificate or license number
13. Any vehicle or other device serial number
14. Web URL
15. Internet Protocol (IP) Address
16. Finger or voice print
17. Photographic image - Photographic images are not limited to images of the face
18. Any other characteristic that could uniquely identify the individual



European Data Protection Supervisor, April 2021, available at:

https://edps.europa.eu/system/files/2021-04/21-04-27_aepd-edps_anonymisation_en_5.pdf



Privacy and ethics in secondary use of sensitive data. 3 key questions to a DPO:

1. As a DPO, do you (have to) always pass negative judgements to requests for secondary use?
2. Can personal (health-related) data be used for secondary purposes without the data subject's consent? The patient is the owner of the data, right?
3. When you receive a request for secondary use, what rules of thumb do you consider to assess the legal and ethical compliance?



Q1: As a DPO, do you have to always pass negative judgements to requests for secondary use?

Statement



Statement on the processing of personal data in the context of the COVID-19 outbreak.

Adopted on 19 March 2020

- Data protection rules (such as the GDPR) do not hinder measures taken in the fight against the coronavirus pandemic
- Even so, the EDPB would like to underline that, even in these exceptional times, the data controller and processor must ensure the protection of the personal data of the data subjects.
- The proportionality principle also applies. The least intrusive solutions should always be preferred, taking into account the specific purpose to be achieved.

[Comment](#) | [Published: 27 March 2020](#)

On the responsible use of digital data to tackle the COVID-19 pandemic

Marcello Ienca  & Effy Vayena

Nature Medicine **26**, 463–464(2020) | [Cite this article](#)

27k Accesses | **110** Citations | **204** Altmetric | [Metrics](#)

Large-scale collection of data could help curb the COVID-19 pandemic, but it should not neglect privacy and public trust. Best practices should be identified to maintain responsible data-collection and data-processing standards at a global scale.

As big data will be critical for managing the COVID-19 pandemic in today's digital world, the conditions for responsible data collection and processing at a global scale must be clear. We argue that the use of digitally available data and algorithms for prediction and surveillance—e.g., identifying people who have traveled to areas where the disease has spread or tracing and isolating the contacts of infected people—is of paramount importance in the fight against the COVID-19 pandemic. It is equally important, however, to use these data and algorithms in a responsible manner, in compliance with data-protection regulations and with due respect for privacy and confidentiality. Failing to do so will undermine public trust, which will make people less likely to follow public-health advice or recommendations and more likely to have poorer health outcomes¹⁰.

A DPO's job:

create awareness on GDPR and inspire your organisation to aim for GDPR*-compliance

Legally:

- Inform and advice controller or processor and its employees
- Compliance assessment, on policy level and in day-to-day operations
- Advice on data protection impact assessments and monitor its performance
- Cooperate with and act as contact person for Data Protection Authority

(see art 39 GDPR)

wagging the finger ↔ participate in creation of a solution 

*And in future also compliance with Data Act, Data Governance Act, Act on AI, European (Health) Data Spaces Act(s)?

Preserving privacy through organisational measures – example transparency

Right to transparency via consumer interface (e.g. patient app to access medical record)

Why focus on transparency?

- Basic condition to every form of patient empowerment
- Basic right for every data subject
 - Right to information does not depend on legal basis for data processing → information is always required, informed consent is just one of the legal bases
 - In principle information at individual level and purpose-specific → general information included in privacy policy is insufficient; restrictive interpretation of exceptions to this principle

Does it solve all GDPR-issues? No!

Advantages:

- Safety and confidentiality of the data ↑
- Risk for illicit data usage ↓
- Cut Data *Transfer* Agreements
- Satisfy issues around cloud-based solutions better
 - Central platform contains aggregated data (= anonymous) only -> cloud ✓
 - Decentral platforms contain pseudonymised data only -> condition to adoption of additional measures cloud ✓

But:

Data are processed for a (secondary) purpose.

Data are collected, analysed, stored... = data processing operations

The “requestor” does have GDPR responsibility

- The party that decides about the purpose = controller or joint-controller
- Where the data are processed is irrelevant in this conclusion
- Who has access to the data is irrelevant in this conclusion

Data Processing / Joint-controller agreement required

Compliance with applicable data subjects' rights required



Q2: Can personal (health-related) data be used for secondary purposes without the data subject's consent?

The patient is the owner of the data, right?

Ownership vs custodianship

No patients, no data *but* no doctor, lab technician, nurse,... no added knowledge or inferred interpretations.

Legally data “ownership” would imply the right to solely decide about who can have, hold, destroy,... the data.

European / Belgian legal framework no data ownership, but framework formulates rights and obligations

- GDPR
- Sector specific legislation (in healthcare for example Proposal for Regulation on EHDS, national laws on patients' rights; in law enforcement for example national laws on data retention)

European / Belgian legal frameworks can foresee obligation to collect, store, manage,... data → custodianship

Conclusion:

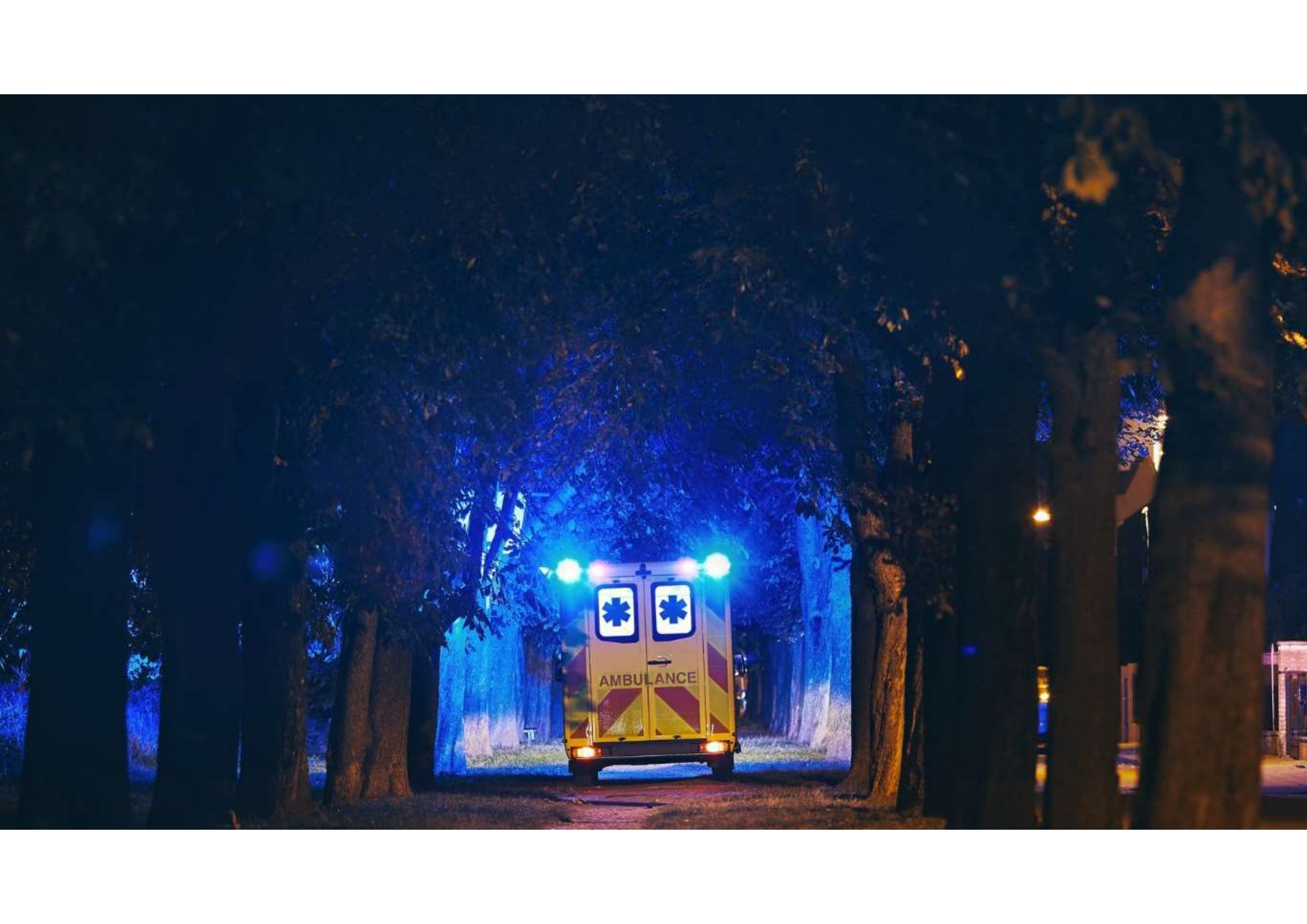
“patient owner of the data”

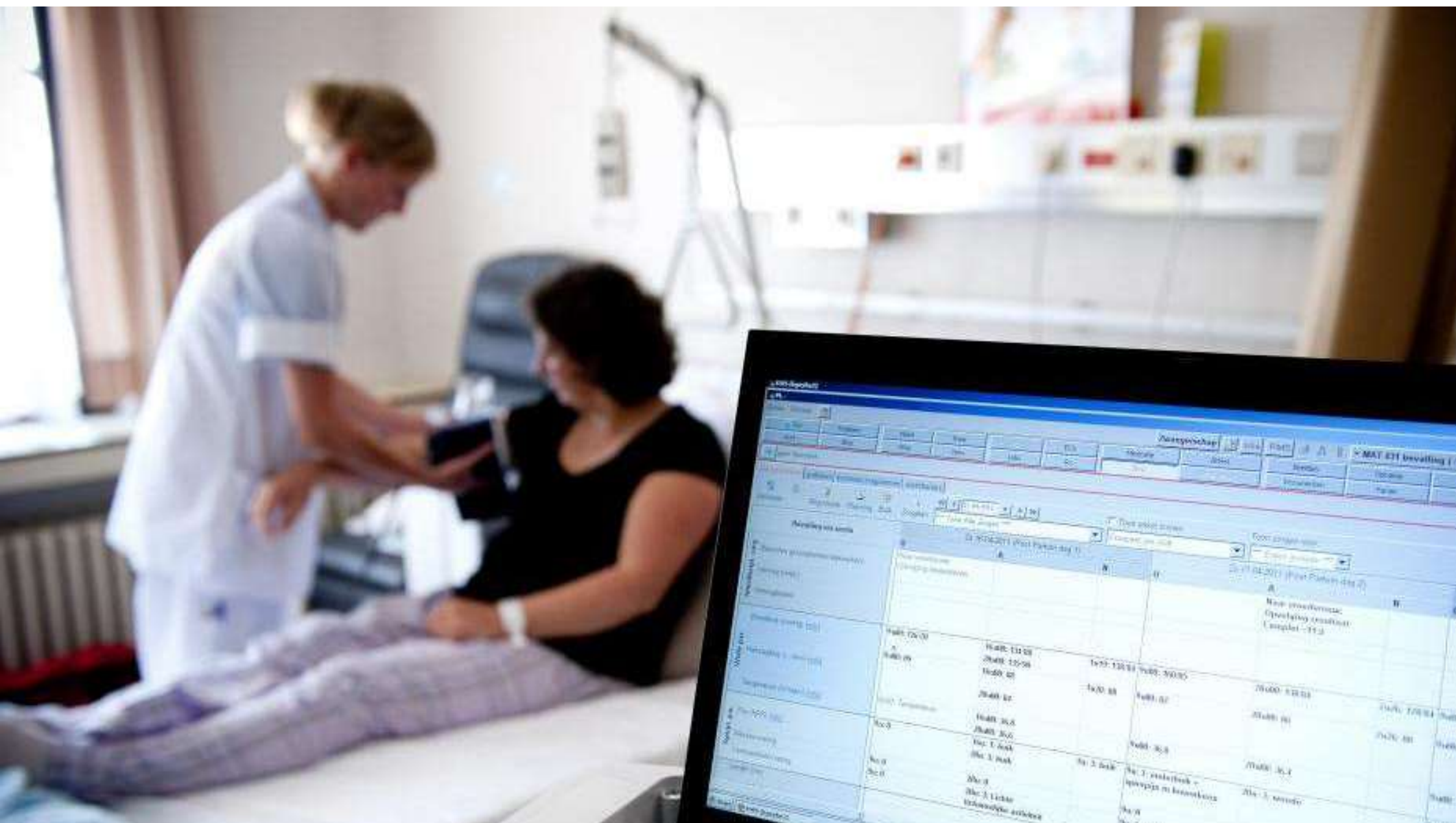
= from legal point of view a witticism rather than fact

= problem?

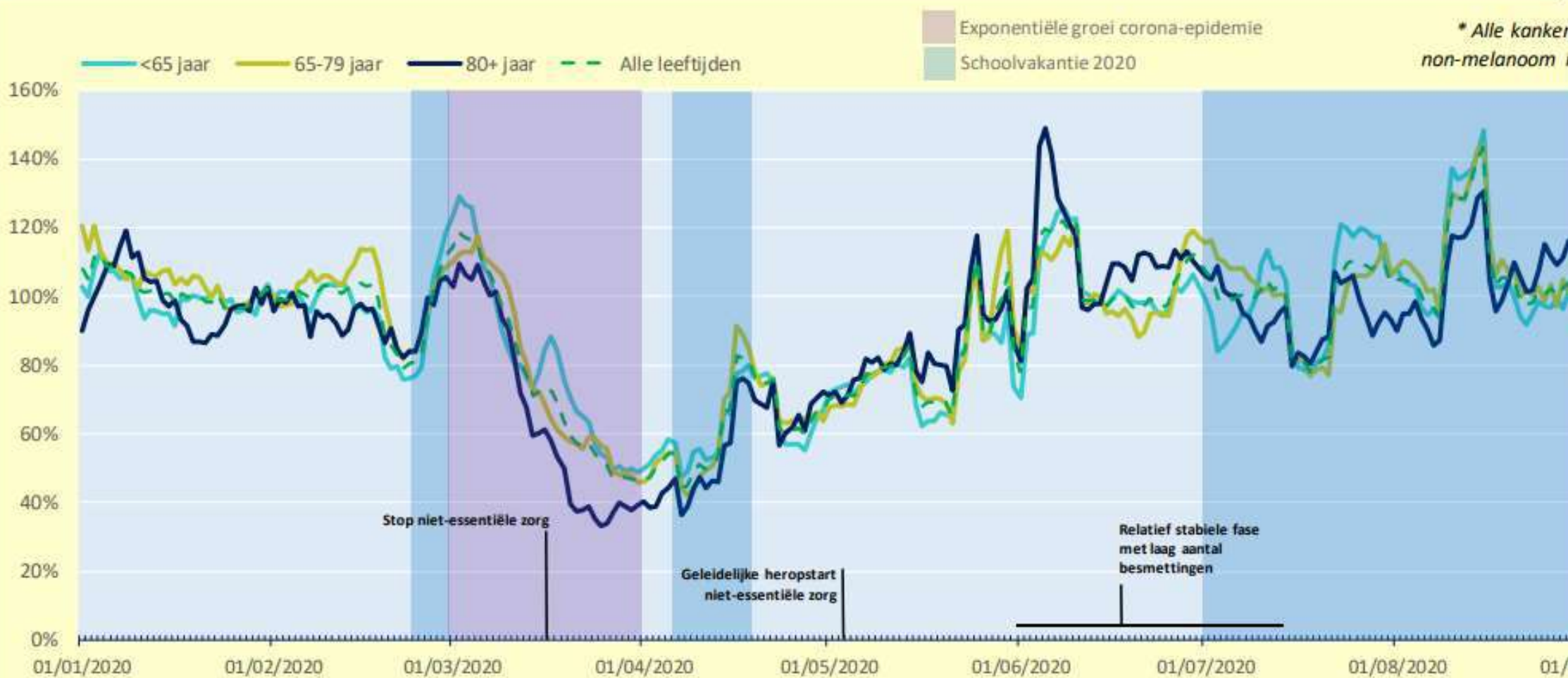
Not necessarily, on condition that we are aware that there are flesh-and-blood people behind these data. In healthcare, vulnerable patients.



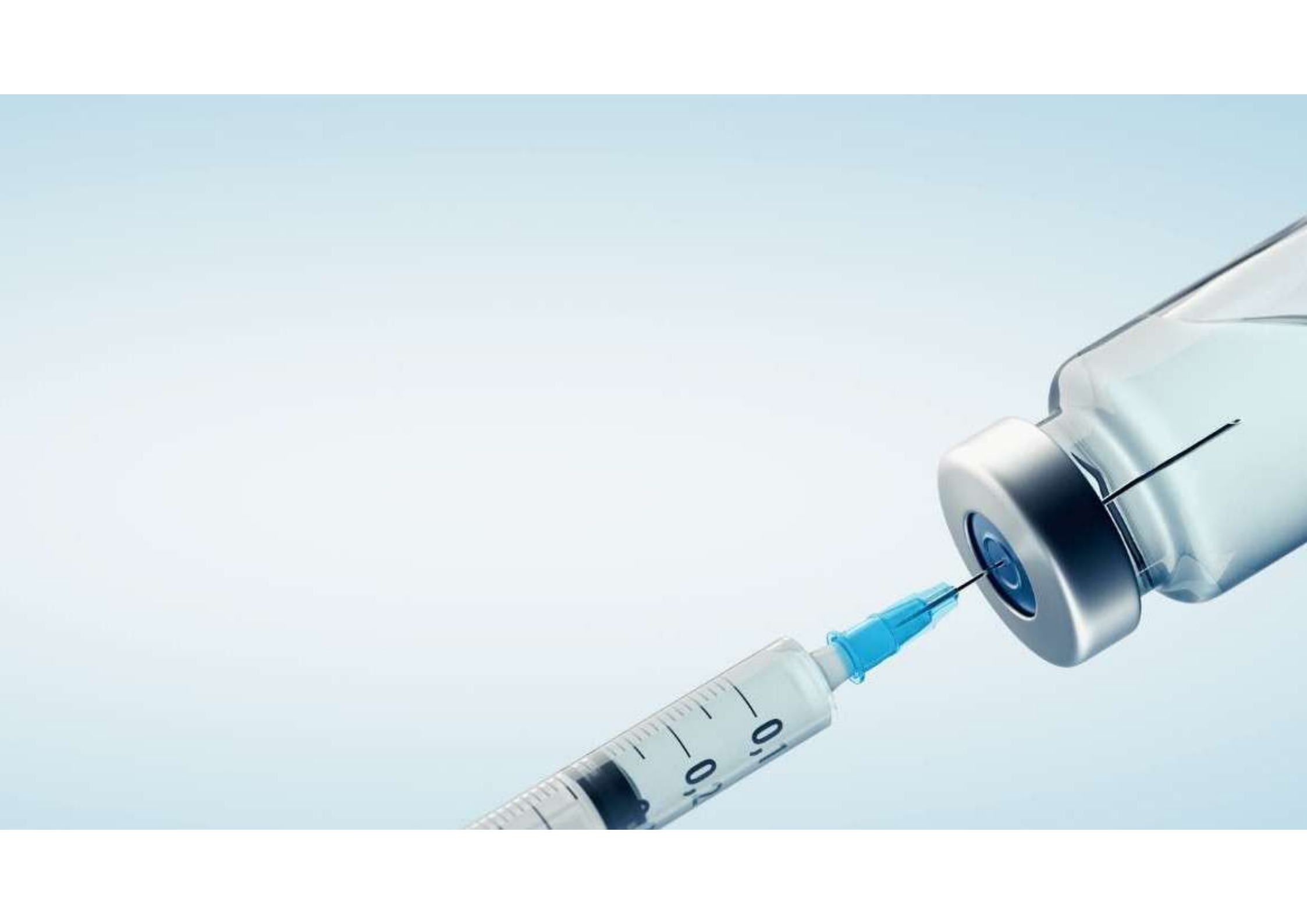




Vergelijking van het aantal nieuwe diagnoses van kanker* in januari-september 2020 t.o.v. januari-september 2019 in België (%)



De resultaten van het aantal kankerdiagnoses op dagniveau werden berekend op basis van een 7-daags voortschrijdend gemiddelde.



Informed consent as legal basis for the processing of personal data

Essence of the concept of “consent”?

It is an instrument to:

- Express your wish
- Provide you with control

⇒ Freely given, informed decision on a specific request for the processing of personal data.

Art 4. (11) GDPR:

“Consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject’s wishes [...].”

⇒ NOT merely signing a form or ticking a box!

Conditions to valid consent

Prof. dr. E. Vayena: “Informed consent as a mechanism is harmful when not meaningful.”

EDPB and Art 29 WP: “If incorrectly used, the data subject’s control becomes illusory and consent constitutes an inappropriate basis for processing”.

⇒ If we would monitor the conditions to validity closer, many requests for consent would fail

⇒ If we would broaden the conditions to validity, its protective nature would be excavated

Informed consent as legal basis for the processing of personal data

Empowerment of the individual requires a true choice.

- Valuable alternative in case data subject does not want to consent?
- Can the data subject understand the scope and implications of the consent? Including further use?
- Once consent, always consent?



Q2: Can personal (health-related) data be used for secondary purposes without the data subject's consent?

The patient is the owner of the data, right?

Article 6 GDPR

list of legal bases

= 1 required if personal data

- Consent
- Contract with data subject
- Compliance with legal obligation on data controller
- Vital interests
- Task in public interest (law required)
- Legitimate interests of data controller

Article 9 GDPR

general prohibition to the processing of special category data + exemptions

= 1 exemption required if special category personal data

- Explicit consent
- Rights and obligations in employment (law required)
- Vital interests
- Foundation, non-profit can keep information on their members
- Manifestly made public by the data subject
- Substantial public interest (law required)
- Healthcare
- Public interest in area of public health (law required)
- Archiving, research, statistics

Article 6 GDPR
list of legal bases

Replaced by compatibility test ?

Consider:

- Link between purposes
- Context and relationship controller – data subject
 - Nature of personal data
 - Possible consequences
- Appropriate safeguards such as encryption and pseudonymisation

Article 9 GDPR

general prohibition to the processing of special category data + exemptions

= 1 exemption required if special category personal data

- Explicit consent
- Rights and obligations in employment (law required)
- Vital interests
- Foundation, non-profit can keep information on their members
- Manifestly made public by the data subject
- Substantial public interest (law required)
- Healthcare
- Public interest in area of public health (law required)
- Archiving, research, statistics

Secondary use



Your medical record



✓ care



Retrospective study for new treatment

✓ Scientific research

Art 9, 2.
(j)



National registry for patients in cancer care program

✓ Public interest in area of public health

Art 9, 2.
(i)



Post market validation study medical device diabetes

MDR or Act on AI?



Q3: When you receive a request for secondary use, what rules of thumb do you consider to assess the legal and ethical compliance?

The 6 rules of thumb for secondary use

Registration

- Starting point for compliance
- Request and response

Privacy and comptibility

- No harm for individual data subject or society
- Relevance
- Scientific underpinning
- ↓
- Case-by-case appreciation

Transparency

- General type and goal(s) of the organisation
- Individual Personalised overview of secondary use

Art 6 & 9 GDPR

- Legal basis or compatibility test
- Exemption for special category data
- Consent?
- Mind validity!
- Must be true choice

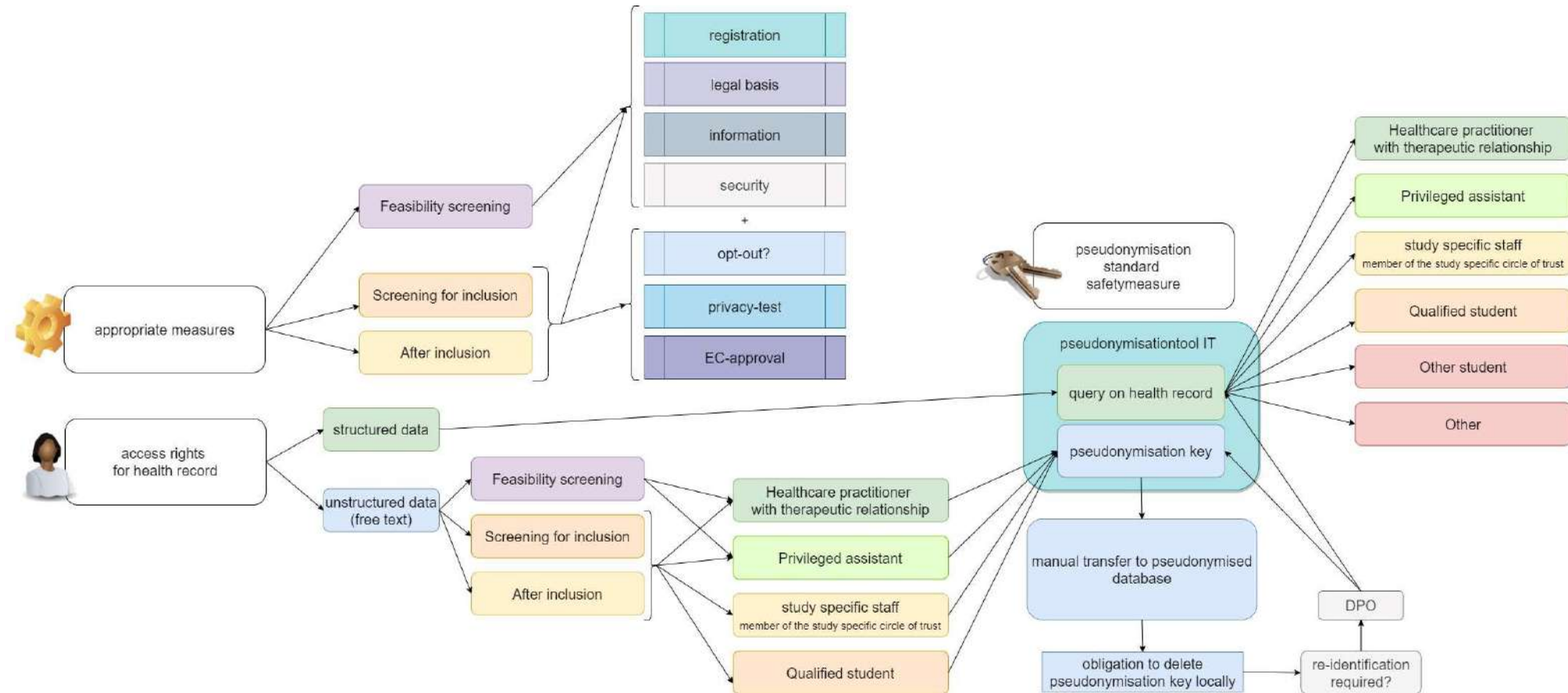
Opt-out (right to object)

- Check legal basis
- Balance individual and general interest

Security

- Technical and organisational
- ↓
- Access control
- logging
- Pseudonymisation
- ...

Rules of thumb for the secondary use of RWD*, including RCD*, in research



* Interpretations of the concepts Real World Data and Routinely Collected Data differ depending on the exact definition that is used. What matters is that de data were collected in the "real world" for a purpose other than research or for the purpose of research but independent of a specific research question.

dr. Griet Verhenneman

DPO UZ Leuven

Lecturer European Privacy and Data Protection Law – KU Leuven

Affiliated Researcher CiTiP – KU Leuven

✉ griet.verhenneman@kuleuven.be or griet.verhenneman@uzleuven.be

✉ Campus Gasthuisberg, Herestraat 49, 3000 Leuven