GDPR

Peter Raeymaekers (Zorgnet-Icuro)

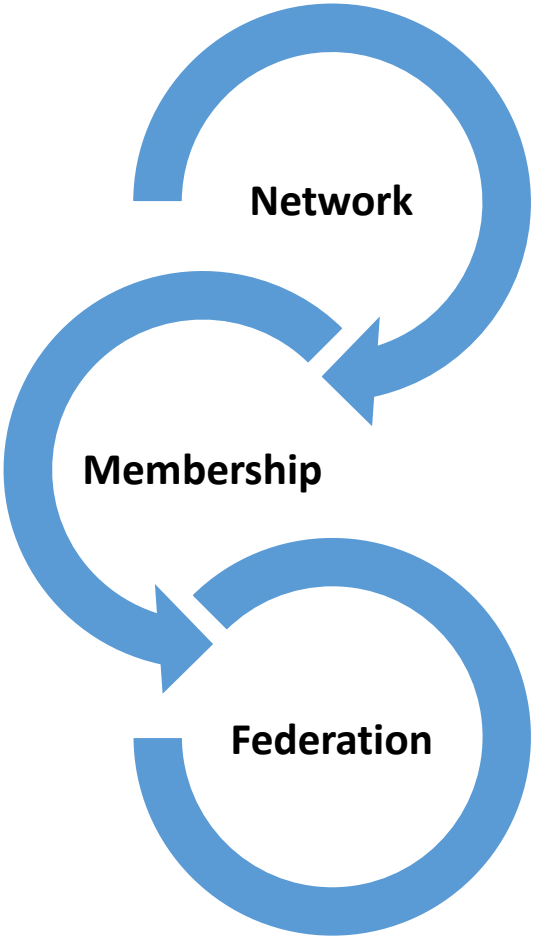
Marrow Donor Program Belgium Symposium
28/11/19

Overview

- Zorgnet-Icuro
- GDPR situation of Belgian hospitals
- Challenges
- GDPR and secondary use of patient data
- Outlook

Zorgnet-Icuro

Zorgnet-Icuro?



- **Membership organisation/federation**
  - General and university hospitals
  - Mental care organisations
  - Elderly care organisations

775 care organisations
129.000 employees

3 sectors in figures: hospitals

AZ

All hospitals for acute care in Flanders:
55 hospitals – **29.322** beds

3 sectors in figures: mental care

GGZ

- **Mental care hospitals**:
  32 organisations – **10.056** beds
- **Other organisations**
  89 organisations, > **4.000** beds:

3 sectors in figures: elderly care

OZ

- **Elderly care homes**:
  303 organisations – 31.866 beds
- **Assisted living facilities**:
  204 organisations – 6.252 units
- **Day care centers**: 120 centers
- **Local service centers**: 27 centers

zorg net ICURO

zorgnet ICURO

GDPR Situation
Belgian hospitals

Information security (CISO)

- Information security advisors
- Legal obligation
- 0,4 FTE
- Formal application procedure
- Reports to general manager
- No part of ICT department
- CISO -> DPO

1st publication: January 2017

Manual for a procedure for data protection in care organisations

Collective collaboration

- Big challenge
- Limited resources
- Expertise sharing experience
- Tool for information security management
- Need for collective GDPR strategy
- Avalanche of input from lawyers/consultants
- Legal meets technology

Code of conduct: definition(Art. 40)

Associations and other bodies representing categories of controllers or processors may prepare codes of conduct, or amend or extend such codes, for the purpose of **specifying the application of this Regulation**, such as with regard to:

Specifying the application of this Regulation

- fair and transparent processing;
- the legitimate interests pursued by controllers in specific contexts;
- the collection of personal data;
- the pseudonymisation of personal data;
- the information provided to the public and to data subjects;
- the exercise of the rights of data subjects;
- the information provided to, and the protection of, children, and the manner in which the consent of the holders of parental responsibility over children is to be obtained;
- the measures and procedures referred to in Articles 24 and 25 and the measures to ensure security of processing referred to in Article 32;
- the notification of personal data breaches to supervisory authorities and the communication of such personal data breaches to data subjects;
- the transfer of personal data to third countries or international organisations; or
- out-of-court proceedings and other dispute resolution procedures for resolving disputes between controllers and data subjects with regard to processing, without prejudice to the rights of data subjects pursuant to Articles 77 and 79.

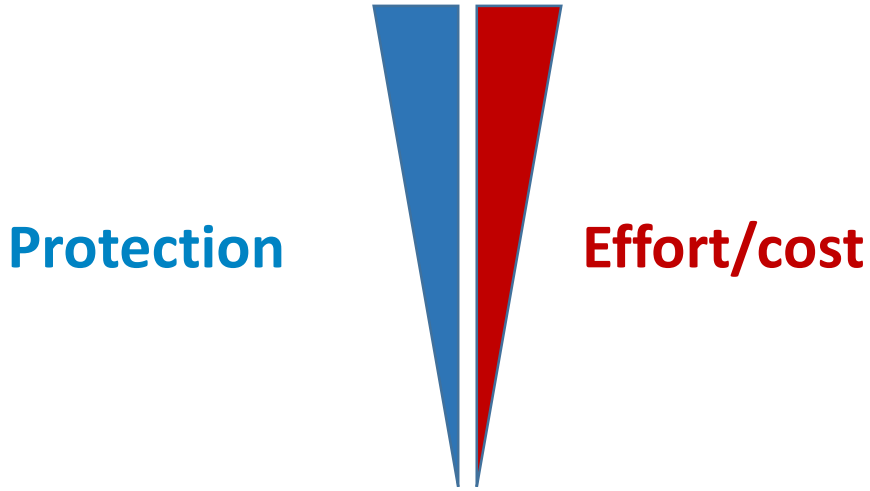
zorg net ICURO

Rationale code of conduct

- Efficiency
  - Maximum of reuse
- Uniformity
  - Less undershoot (underperformance)
  - Less overshoot (overperformance)
- Legal
  - Depends on formal character
  - Begin of proof of compliance ("can be used to show that …")
  - Factor for financial penalty

Code of conduct: possible implementation/enforcement

Certified body
for compliancy audits



Reference document

Reference document

zorg net
ICURO

Tools for compliancy

- Processing agreement (public)
- Informed consent
- Task description DPO
- Record of processing activities
- Privacy policy
- Privacy rules patients
- Privacy Impact Assessment
- Procedures data access en data extraction
- Data breach procedure
- Data breach record

Challenges

LOLLOJ - FOTOLIA

Dutch audit finds Microsoft Office leaks confidential data

The diagnostics Microsoft Office collects from users should be a source of concern for any government CISO, according to a DPIA audit

By **Cliff Saran**, Managing Editor

Published: 20 Nov 2018 15:15

A report commissioned by the Dutch government has recommended disabling any settings in Microsoft Office 2016 that sends data to Microsoft servers.

Latest News

Not there yet …

- Awareness on all levels
- Processing agreements
- Non-hospitals
- Objective measures and benchmarking
- Internal process management
- Data Protection Authority
- Big data and research

Secondary use of data

GDPR essentials

- May 25th 2018
- (Sensitive) Personal data (broadly interpreted)
- Controllers and processors
- Processing is lawful, fair and transparent
- Healthcare is legitimate purpose
- Accountability
- Preventive measures (privacy by design, by default, …)
- Rights of data subjects

zorg net
ICURO

Research on health data

- Essential difference between
  - Primary research (collecting data for research)
  - Secondary research (re-using clinical data)

- Difference between
  - Processing data for clinical studies
  - Processing data of clinical trial-data for other scientific purposes
  - Retrospective studies

GDPR

- Very important for both types of research
- With several exemptions in favor of scientific research

GDPR Principles – Data can only be processed

- Lawfully, fairly and in a transparent manner (***lawful basis***)
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (***purpose limitation***)
- Accurate and, where necessary, kept up to date (***accuracy***)

GDPR Principles – Data can only be processed (ctd)

- Kept in a form which permits identification of data subject no longer than is necessary (***storage limitation***)
- In a manner that ensures appropriate security (**integrity and confidentiality)**
- In a way that demonstrates compliance (***accountability***)

SIX Possible Lawful bases

- Consent of the data subject
- Performance of a contract
- Legal obligation
- Protecting vital interest of the data subject
- Task carried out in the public interest
- *'processing is necessary for the purposes of the legimate interests pursued by the controller, except when such interest are overridden by the interests of fundamental rights and freedoms of the data subject'*

Discussion about consent

- Is consent necessary?
- Is consent the (best) lawful basis for research?
  - Free?
  - Informed?
  - What if consent is withdrawn?

Confusion between types of consent

- Consent as legal basis for
  - treatment
  - or clinical trial
- Consent as legal basis for processing
  - Data necessary for diagnosis or treatment
  - Data collected during clinicial trial
  - Re-processing data for research

Primary research

- Lawful basis is generally the consent of the data subject
- Consent of the data subject means any “freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by statement or by clear affirmative action, signifies agreement to the processing of personal data relating to him or her” (art. 4 GDPR)

Broad consent ?

- *'It is often not possible to fully identify the purpose of personal data processing for scientific research purposes at the time of data collection. Therefore, data subjects should be allowed to give their consent to certain areas of scientific research when in keeping with recognised ethical standards for scientific research. Data subjects should have to opportunity to give their consent only to certain areas of research'* (recital 33)

Broad consent ?

- How broad ?
  - ‘research ?’
  - ‘areas of research’ ?
  - How restricted?

- Discussion about trustworthy use
  - Individual control ?
  - Collective control?

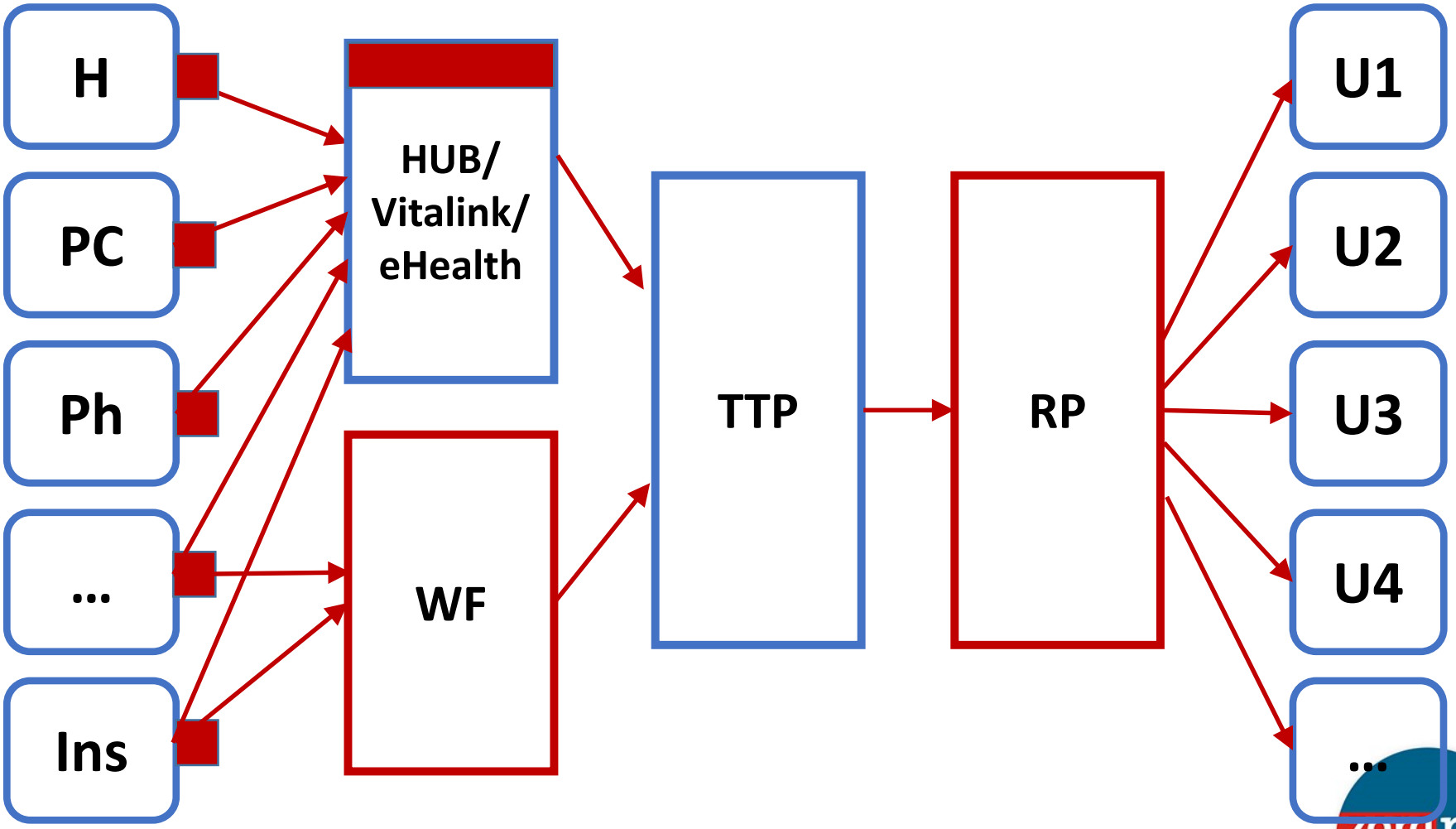
Secondary research

- Lawfull basis is not consent, but general interest !
- Re-using clinical data seems to be an infringement of the principle of purpose limitation
- Important exemption in GDPR: *"further processing for scientific purposes shall not be considered to be incompatible with the initial purpose"* (art. 5 b)

ART. 89.1 GDPR

- “Processing for scientific research purposes shall be subject to ***appropriate safeguards*** in accordance with this regulation, for the rights and freedoms of the data subject. Those safeguards shall ensure that technical and organisational measures are in place in particular in order to respect the principle.***Those measures may include pseudonymisation*** of data minimisation. provided that those purposes can be fulfilled in that manner. Where those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner”

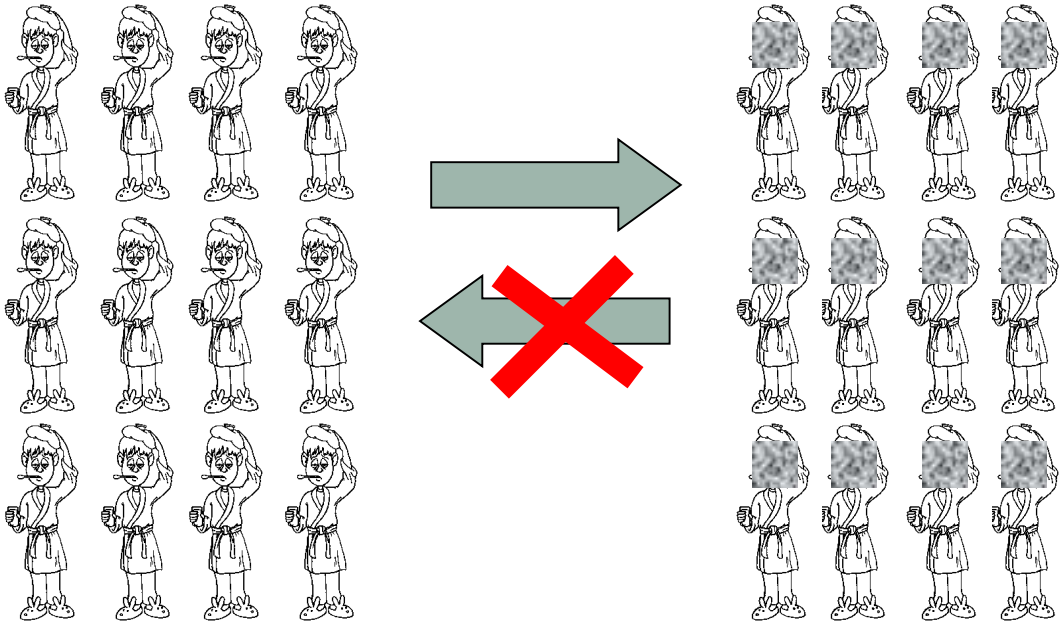
Example



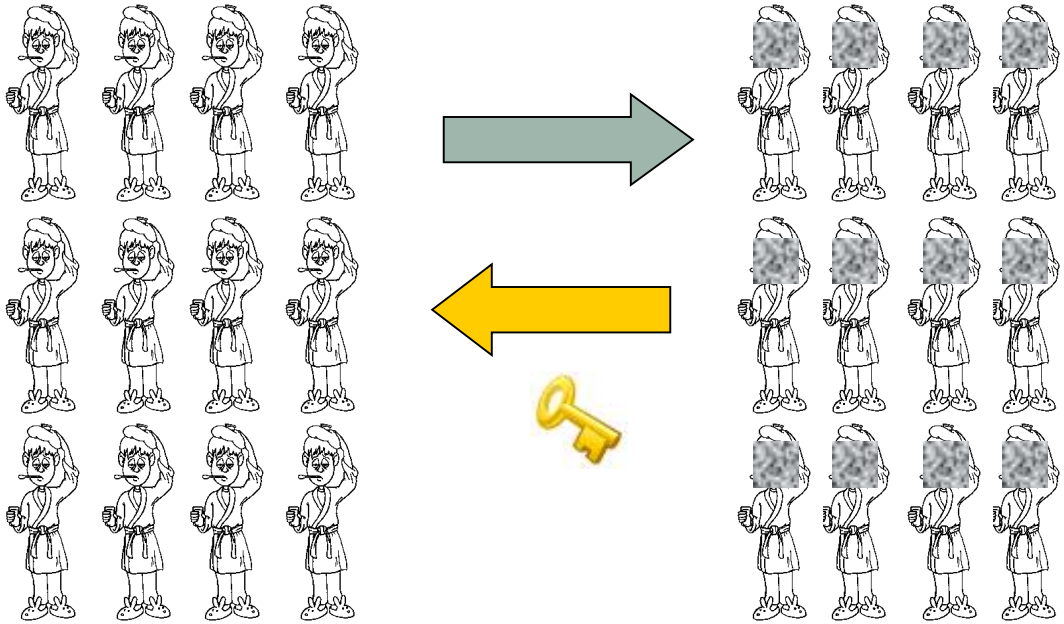
Appropriate safeguards

- ‘Technical and organisational measures’
- Measures may include pseudonymisation
- The ongoing confusion between ‘anonymisation’ and ‘pseudonymisation’

anonymisation



pseudonymisation



zorg net ICURO

Is anonymity still possible ?

- When human material (tissue, blood, bone) is stored (in bio bank) the DNA itself is an identifier
- Complete anonymity is an illusion
- Strong ‘PET’s’ can protect the privacy and make re-identification very difficult, but not impossible

Outlook

Outlook

- Training and awareness creation
- Empowerment of DPO
- Implement tools for follow-up
- Increase collaboration
- Stabilize regulatory instruments
- Legal and ethical framework for secondary use of clinical data

zorg net ICURO

Peter Raeymaekers

Peter.raeymaekers@zorgneticuro.be

+32478405221