PSI Parelsnoer Institute

EUROPE BIOBANK WEEK

Europe Biobank Week
Biosharing for Scientific Discovery
September 4-7, 2018 | Antwerp, Belgium

NFU NETHERLANDS FEDERATION OF UNIVERSITY MEDICAL CENTRES

NFU biobank Parelsnoer: Data security & privacy guarantees

An approach to determine biobank compliancy aspects
for a federative Biobank organization
as the Dutch Parelsnoer Institute,

Erik Flikkenschild, Security Officer and national IT coordinator
Flikkenschild@Parelsnoer.org

Radboudumc · Erasmus MC University Medical Center Rotterdam · umcg · Leiden University Medical Center · Maastricht UMC+ · UMC Utrecht · Amsterdam UMC University Medical Centers

PSI in a nutshell

- PSI founded in 2007 by the Netherlands Federation University Medical Centra (NFU)
- Central IT Infrastructure (CI), ISO 27001 certified, standard procedures for setting up, optimize clinical biobanks (pearls)
- Privacy by design applied (we maintain an IT architecture for communication with the suppliers)
- Issue of clinical data, MRI and samples

Parelsnoer institute (PSI) governance

Parelsnoer Institute

Other Institutes & suppliers

Researchers (PI) Pearls

(8) University medical Centres

Information Security Management

PSI Framework regulations
(kader- en parel reglement)

Data security & privacy guarantees

1. GDPR processor & controller aspects
2. IT architecture: security domains / TTP
3. Informed consent go/no-go
4. Linked data

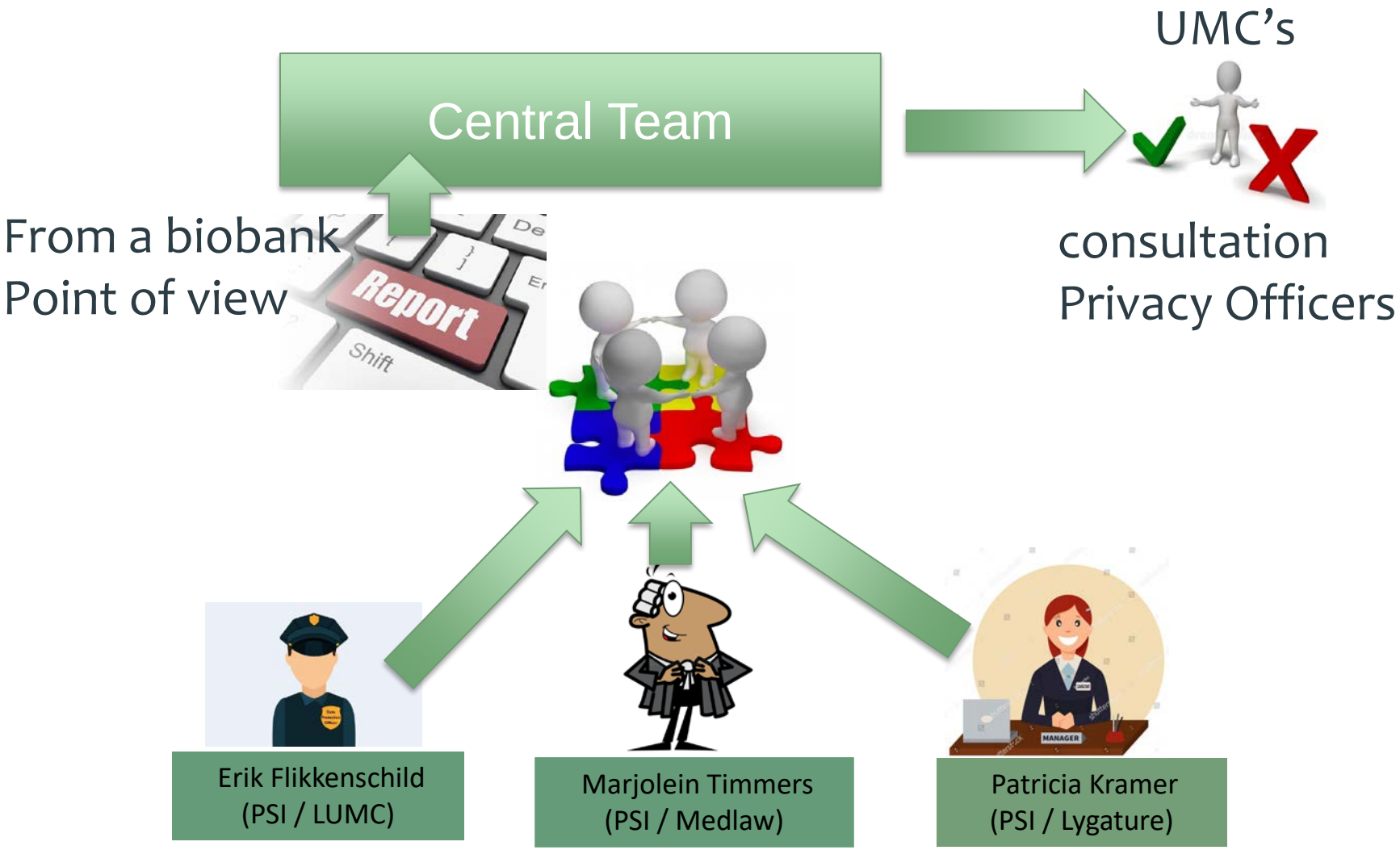
Data security & privacy guarantees

1. GDPR processor & controller aspects
2. IT architecture: security domains / TTP
3. Informed consent go/no-go
4. Linked data

First step PSI approach to GDPR compliance

1. Compile GDPR analyse team
2. Decide on tooling: BBMRI-NL's web application for GDPR Records, DPIA & Compliance
3. Fill in the GDPR questionnaire from a biobank point of view
4. Describe the GDPR biobank start position (biobank point of report)
5. Discuss this with all stakeholders

Methods:
the core GDPR analyse team approach



GDPR Questionnaire

https://bbmri.dataprotectioncompliancetool.com/>

AVG Checklists voor Register, Compliance & DPIA Applicatie inzake verwerkingen van persoonsgegevens voor wetenschappelijk onderzoek in Populatie Biobanken en Cohorten

Parelsnoer

- + 1. Hoe kunt u deze AVG applicatie gebruiken?
- + 2. Worden Persoonsgegevens Verwerkt?
- + 3. Zijn er meerdere verwerkingsverantwoordelijken?
- − 4. Maak het AVG Register
  - ✔ **4.1. Wat is de naam van de Bioba...**
  - ✔ 4.2. Beschrijf de categorieën van bet...
  - ✔ 4.3. Wat zijn de naam en de contact...
  - ✔ 4.4. Is of zijn er gezamelijke verwerk...
  - ↳ Geef de naam en de contactgegeven...
  - ✔ 4.5. Wat zijn, in voorkomend geval,...
  - ✔ 4.6. Geef de naam en de contactgeg...
  - ✔ 4.7. Wat zijn de verwerkingsdoelein...
  - ✔ 4.8. Zijn of zullen de persoonsgegev...
  - ↳ Beschrijf de categorieën van ontvang...
  - ✔ 4.9. Geeft de verwerkingsverantwoo...
  - ↳ Vermeld doorgiften van persoonsgeg...
  - ✔ 4.10. Beschrijf, indien mogelijk, de b...
  - ✔ 4.11. Geef, indien mogelijk, een alge...
- + 5. Toon uw Compliance met de AVG aan
- + 6. Heeft u de deelnemers van uw Biobank of Cohort (betrokkenen) geïnformeerd conform de AVG?
- + 7. Beveiliging, Verwerkers en Datalekken
- + 8. Passende waarborgen voor

4.1. Wat is de naam van de Biobank of het Cohort?

Antwoord:

PSI is een samenwerkingsverband maar geen rechtspersoon. Er is geen sprake van een verwerker. De 8 UMC's zijn de gezamenlijke verantwoordelijken.

answer

body p span span font — Characters: 145/400

Toelichting:

De 8 UMC's zijn gezamenlijke verwerkersverantwoordelijke zoals bepaald in artikel 26 AVG. Parelsnoer valt onder de NFU zie ook: www.parelsnoer.org

explanation

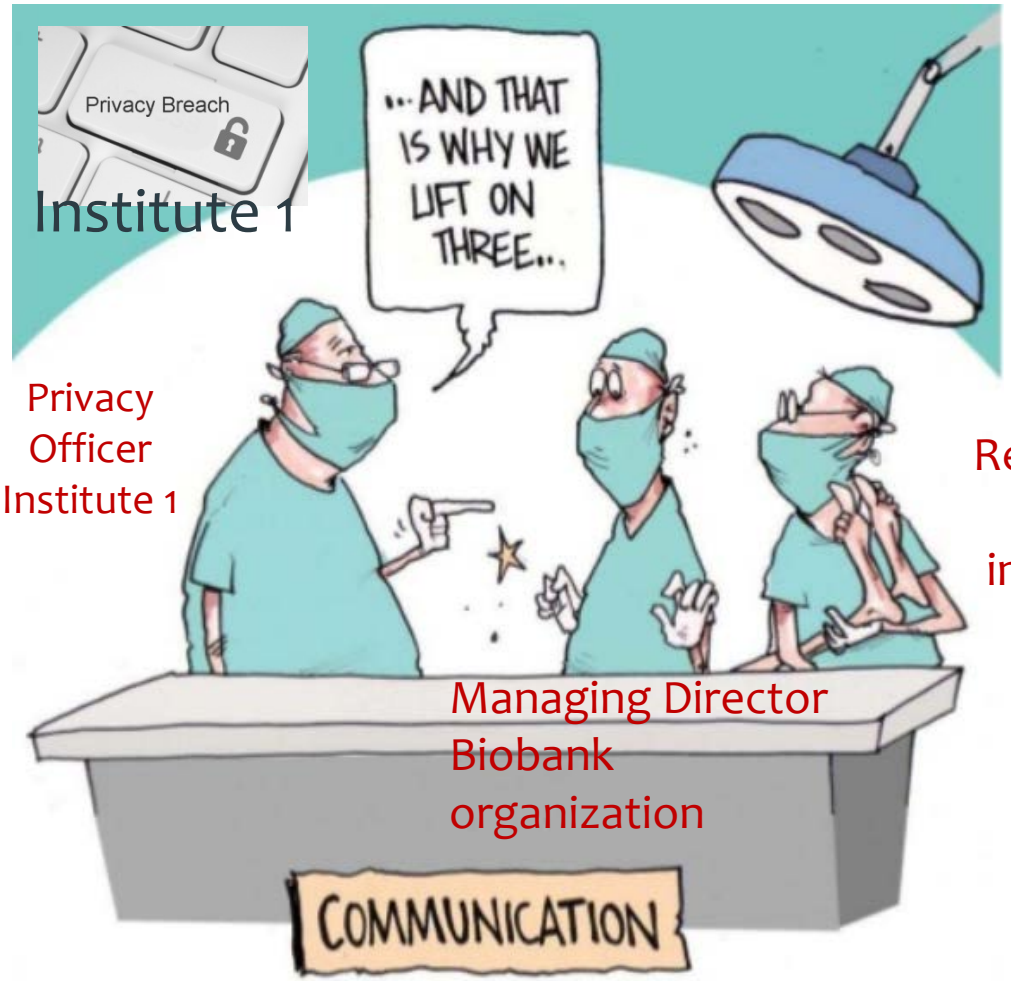
Characters: 146/400

Upload hier het betreffende bestand (Bij meerdere bestanden kan u een zipfile uploaden):

Upload document

First step biobank approach to GDPR compliance

Controller
or
Processor?



Privacy Officer Institute 1

Researcher (PI) institute 2

Managing Director Biobank organization

Biobank GDPR analyses PSI conclusions

1. Role PSI biobank was not evident, discussion about legal entity, therefore role as processor unclear.
2. GDPR article 26 is applicable (joint controllers)
3. With 8 controllers we have to find an efficient procedure to review privacy concerns as indirect traceability
4. Dataleak procedure alignment with all suppliers needed

UMC's

PSI biobank Institute

Suppliers

PSI
Parelsnoer Institute

- **Implementing the GDPR requires a first step (analysis) carried out by a multidisciplinary team that has knowledge and experience within a biobank organization (awareness)**

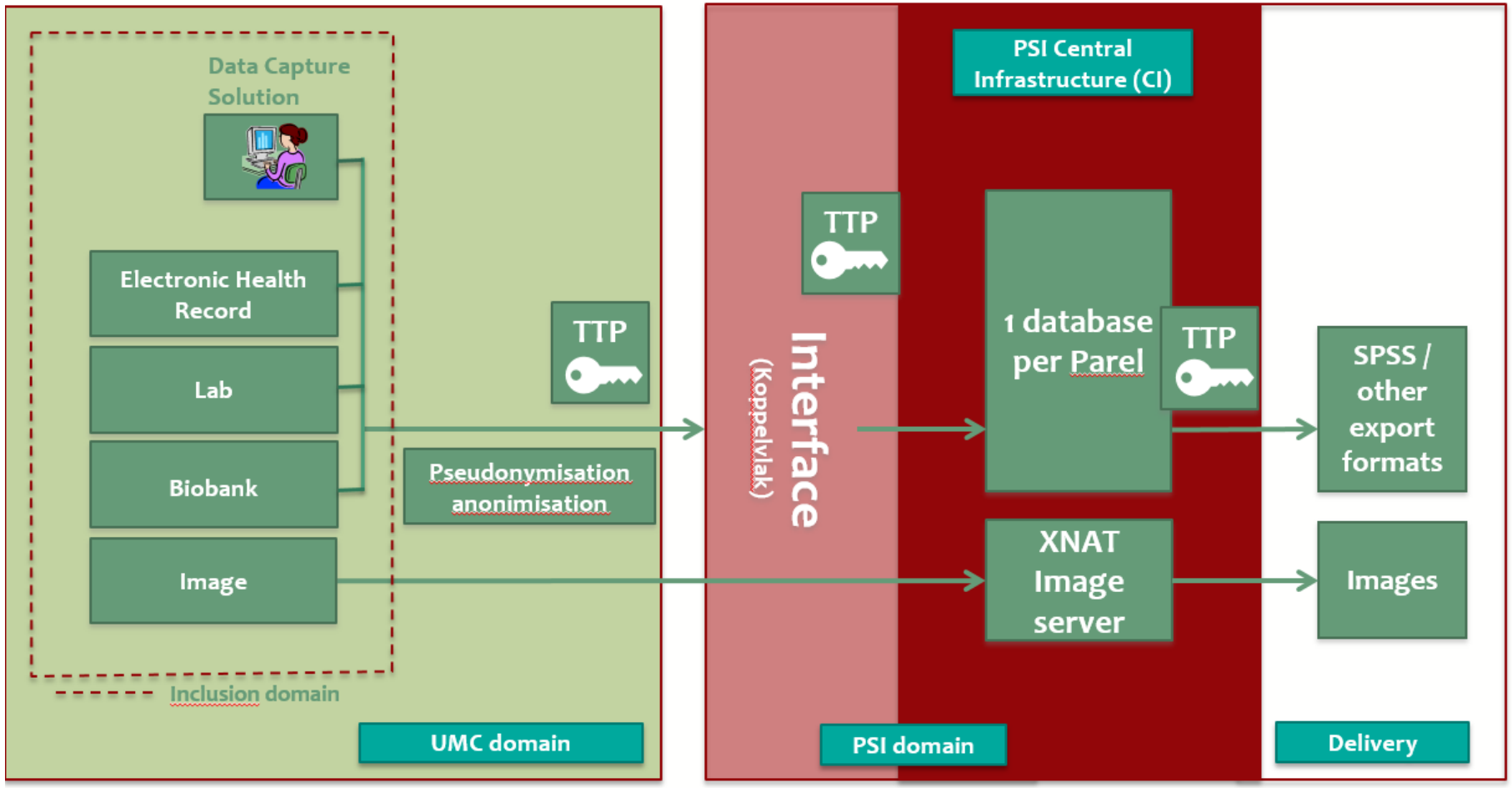
- **The BBMRI tooling was very helpful**

- **Second step: GDPR implementation is not feasible without a proper pronunciation of the processor and controller roles in the context of a federated biobank**

Data security & privacy guarantees

1. GDPR processor & controller aspects
2. IT architecture: security domains / TTP
3. Informed consent go/no-go
4. Linked data

Introduction:
starting point: IT infrastructure domains



AVG alignment (on-going discussion)

- **De activiteiten van de Parel vinden plaats in overeenstemming met de vigerende wettelijke bepalingen, gedragscodes, reglementen en procedures,**
  - waaronder de Wet op de geneeskundige behandelingsovereenkomst (WGBO), de Algemene Verordening Gegevensbescherming (AVG), de uitvoeringswet AVG (UAVG), de gedragscode 'Verantwoord omgaan met lichaamsmateriaal ten behoeve van wetenschappelijk onderzoek' uit 2011, het kaderreglement (KR) van het Parelsnoer Instituut (PSI), reglementen geldend binnen de UMC's, dit reglement en de van toepassing zijnde standard operating procedures (SOP's).

- **Daarbij dient gesteld te worden dat het Parelsnoer Instituut (PSI) aangaande de Algemene Verordening Gegevensbescherming (AVG) geen verwerker of verwerkingsverantwoordelijke is, derhalve heeft PSI formeel geen Functionaris Gegevensbescherming (FG).**
  - De UMC's zijn als aanleverende partij van gecodeerde (gepseudominiseerde) gegevens verantwoordelijk voor het borgen van de privacy binnen het samenwerkingsverband van een Parel. De UMC's hebben ieder in hun rol als verwerkingsverantwoordelijke een FG aangesteld en moeten binnen het PSI samenwerkingsverband waarborgen en monitoren dat aan de AVG wordt voldaan.

- **De uitwerking van het veiligheidsbeleid betreffende privacy bescherming van de deelnemers wordt gedaan langs de vier onderdelen van PSI:**
  - de centrale infrastructuur (CI) met (TRES) codering t.b.v. pseudonimisatie en / of anonimisatie,
  - de Trusted Third Party (TTP) functionaliteit,
  - de aangesloten instelling en de onderzoeker.
  - Daarnaast zijn er uitwerkingen die overkoepelend zijn binnen PSI zoals het aanstellen van een functionaris voor de dagelijkse verantwoordelijkheid voor Informatiebeveiliging (Security Officer) en het uitrollen van een datalekprocedure. In alle gevallen/aspecten waarin het Parelreglement niet voorziet, geldt het PSI Kaderreglement . In geval van strijd tussen de bepalingen van het PSI KR met het Parelreglement, gelden de bepalingen van het PSI KR. In geval van strijdigheid tussen de bepalingen van dit Parelreglement en de bepalingen in reglementen geldend binnen de UMC's, prevaleert het reglement van het betreffende UMC.

Data security & privacy guarantees

1. GDPR processor & controller aspects
2. IT architecture: security domains / TTP
3. **Informed consent go/no-go**
4. Linked data

IC en Open Science

Hoe gaat PSI om met Open Data/Science en op welke wijze wordt data geïdentificeerd?

Beleid in PSI is altijd geweest dat verzamelingen beschikbaar zijn voor alle onderzoekers met een goed onderzoeksplan. Bij voorkeur in samenwerkingsverband met de Parel. Alles vastgelegd in PSI kaderreglement. Alle verzamelingen zijn raadpleegbaar via catalogus van BBMRI-NL. Strikte driedubbele pseudonimisatie met tussenkomst van ZorgTTP is onderdeel van de PSI standaard

Informed Consent

- Biobank per definition broad consent
- No delivery (upload to PSI) without Informed consent

Data security & privacy guarantees

1. GDPR processor & controller aspects
2. IT architecture: security domains / TTP
3. Informed consent go/no-go
4. Linked data

SIG Veilige koppelingen (LCRDM / Data4LIfesciences)

health RI

14-09-2018 | 3

Secure record linking

What Why How

What

Researchers can link personal data without privacy breaches
(METC approved research study)

Why

Record linkage is a highly efficient approach to enrich existing biobanks or databanks containing clinical, socio-economic or other phenotypic data. It increases the value and usability of these biobanks and databanks to medical and scientific research in general. source Rainbow project, slides Ronald Stolk former chairman SIG-VK

How

Collaboration of national experts groups
Data4lifesciences, BBMRI-NL / PSI, LCRDM (Surfsara, VSNU)
Coordination
SIG VDK (veilige koppelingen)

Personal data linkage in health and biobanking research: combining scientific robustness with privacy and security requirements

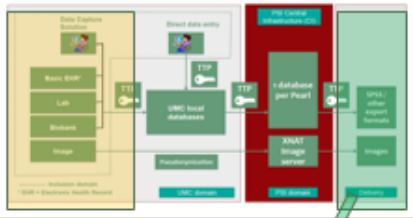
E.L.A. Flikkenschild[1,2], J. Mannien[1,2], M.Boeckhout[3], R.A.Verheij[4], K. Hek[4], F.Rutters[1,5], J.J.Uitterdijk[6] , H.Bastiaens[7],

[1]Parelsnoer Institute, The Netherlands, [2]Leiden University Medical Centre, [3]BBMRI-NL, [4]Netherlands Institute for Health Services Research, [5]VU University Medical Center, [6]University Medical Centre Groningen, [7]University of Antwerp, Belgium.

Parelsnoer Institute, PSI the Netherlands

- www.parelsnoer.org
- Collaborative biobanking project
- 8 University Medical Centers in the Netherlands
- 18 disease- specific cohorts
- Aim: national linking data guidelines, use-case descriptions and practical solutions
- National special interest group ("SIG secure data linkage") is working on a model

Parelsnoer ICT infrastructure



Privacy by design

- Findable, Accessible, Interoperable en Re-usable (FAIR) datasets
- to develop national data linking guidelines in order to comply to the EU-GDPR (May 2018).
- SIG secure data linkage is working on a model
- Easy understandable use –cases based on best practices

Linking datasets, choose a method:

- deterministic method (unique identifier, / exact comparison or
- probabilistic (compare several filed values and assign).
- A secure ICT architecture / TTP security zones design
- Organizational procedures
- Technical data link procedure

Use case 1: Pearl Diabetes T2D in EU TRANSFoRm project

The overall purpose of the T2D clinical use was to drive the development of ICT tools aimed at supporting large scale genotype-phenotype epidemiological studies across Europe.

The main tool is the TRANSFoRm Query Workbench (QWB), a web based user interface to query patient data across data sources and countries.

As a use-case (EU) project TRANSFoRm has built an application involving Pseudonimisation, by a Trusted Third Party (TTP), matching data from general practice registries (Nivel primary care database) and bio-banking data for people with type 2 diabetes of the Dutch Parelsnoer Institute.

The used combination of proven strong encryption technology and uniform deterministic identifiers allows for more secure linkage, resulting in robust datasets anonymized for the purposes of research.

ICT architecture Security zones (TRANSFoRm)

A standardised graphic method for describing dataprivacy frameworks in primary care research usinga flexible zone model, Wolfgang Kuchinke et all

How many personal data linkage scenarios are there?

The challenge is to link personal health data sources from different institutes (safely with a high scientific deterministic quality) and not to invent the wheel any time!

Use case 2: Pearl IBD / pathology (PALGA)

BBMRI WP4: Registry linkage

- More use of data and materials of biobank cohorts / registries

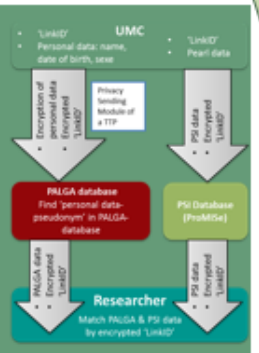
Methods:

- Link biobank / cohorts / registries
- One Request Portal for all biobanks/cohorts/registries (soon available)
- Pilot link: Inflammatory bowel disease patients
- PSI: phenotypic data & biomaterials
- PALGA (nationwide registry): pathology test results ; research question: Does the progression or regression of cervical (pre)neoplastic lesions in IBD women differ from the general Dutch population?
- Matching: probabilistic by date of birth, name & sex
- Pseudonimisation by a TTP
- Lessons learned: expected end of 2017

Future linking?

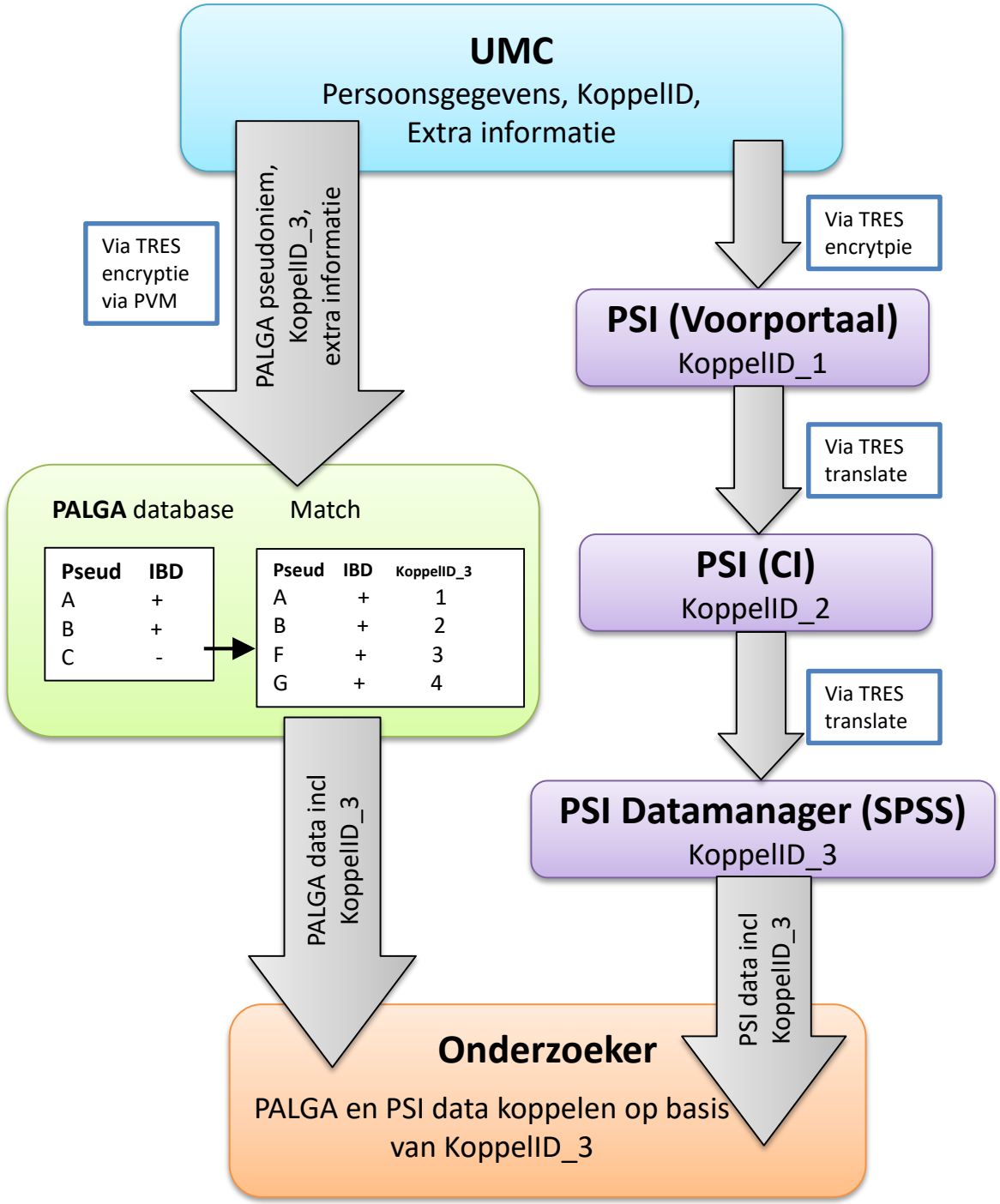
Statistics Netherlands (CBS); Netherlands Cancer Registry (NCR); PHARMO database network (e.g. in- and out-patient pharmacies, clinical laboratories, hospitals, the cancer registry)

Ultimate goal: join forces to facilitate medical research and innovation ultimately leading to better diagnosis, treatment or even prevention of (complex) diseases



(National) Special Interest Group: SIG secure data linkage:

Towards a National Data linkage model (templates)

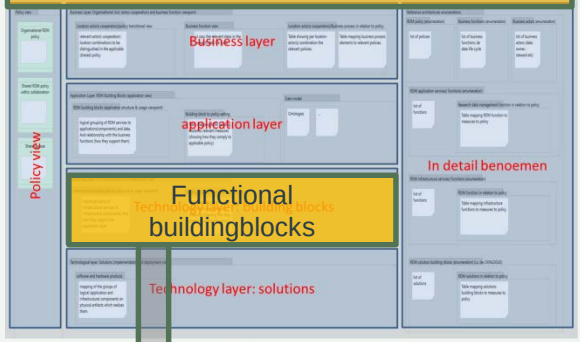


Stappen:
1. UMC stelt voor iedere case een uniek en random KoppelID op en verwerkt dit via het voorportaal als TTP item → KoppelID_1.
2. UMC levert bestand aan PALGA met de PVM software van ZorgTTP, waarbij via TRES translate de KoppelID wordt geconverteerd naar KoppelID_3.
3. PALGA ontvangt een bestand van het UMC met daarin PALGA-pseudoniemen, KoppelID_3 en extra informatie (diagnosedatum IBD en eventueel T-nummer).
4. PALGA koppelt het bestand van het UMC met PALGA-pseudoniemen aan de reeds bij PALGA beschikbare pseudoniemen.
5. PALGA verstuurt een bestand met gegevens van gematchte cases inclusief KoppelID_3.
7. PSI doet een uitgifte van PSI data + KoppelID_3 en verstuurt dit bestand naar de onderzoeker.
8. Onderzoeker koppelt PSI en PALGA data o.b.v. KoppelID_3

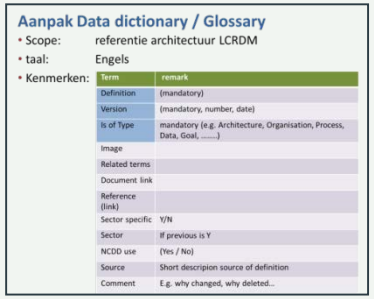
Ongoing work: LCRDM GDPR ready toolkit

https://www.surf.nl/en/lcrdm

Architecture Framework



Glossary

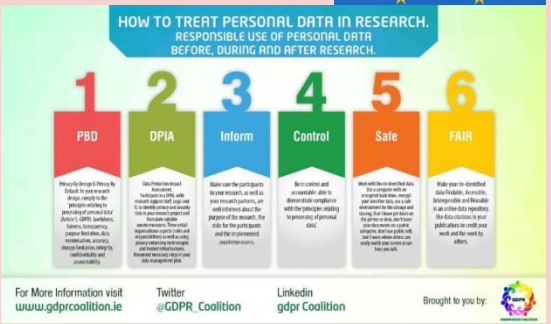


Aanpak Data dictionary / Glossary

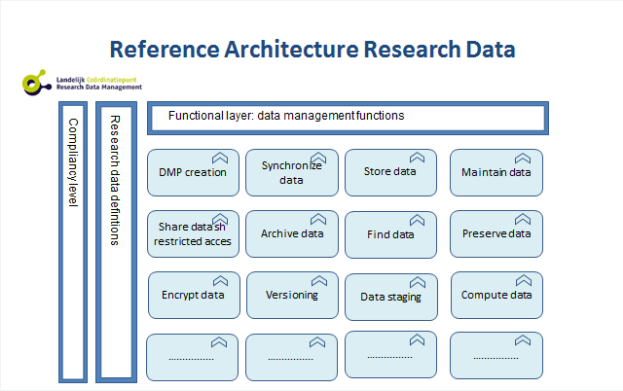
- Scope: referentie architectuur LCRDM
- taal: Engels
- Kenmerken:

Term	remark
Definition	(mandatory)
Version	(mandatory, number, date)
Is of Type	mandatory (e.g. Architecture, Organisation, Process, Data, Goal, ...)
Image	
Related terms	
Document link	
Reference (link)	
Sector specific	Y/N
Sector	If previous is Y
NCDD use	(Yes / No)
Source	Short descripion source of definition
Comment	E.g. why changed, why deleted...

GDPR



Service catalogue

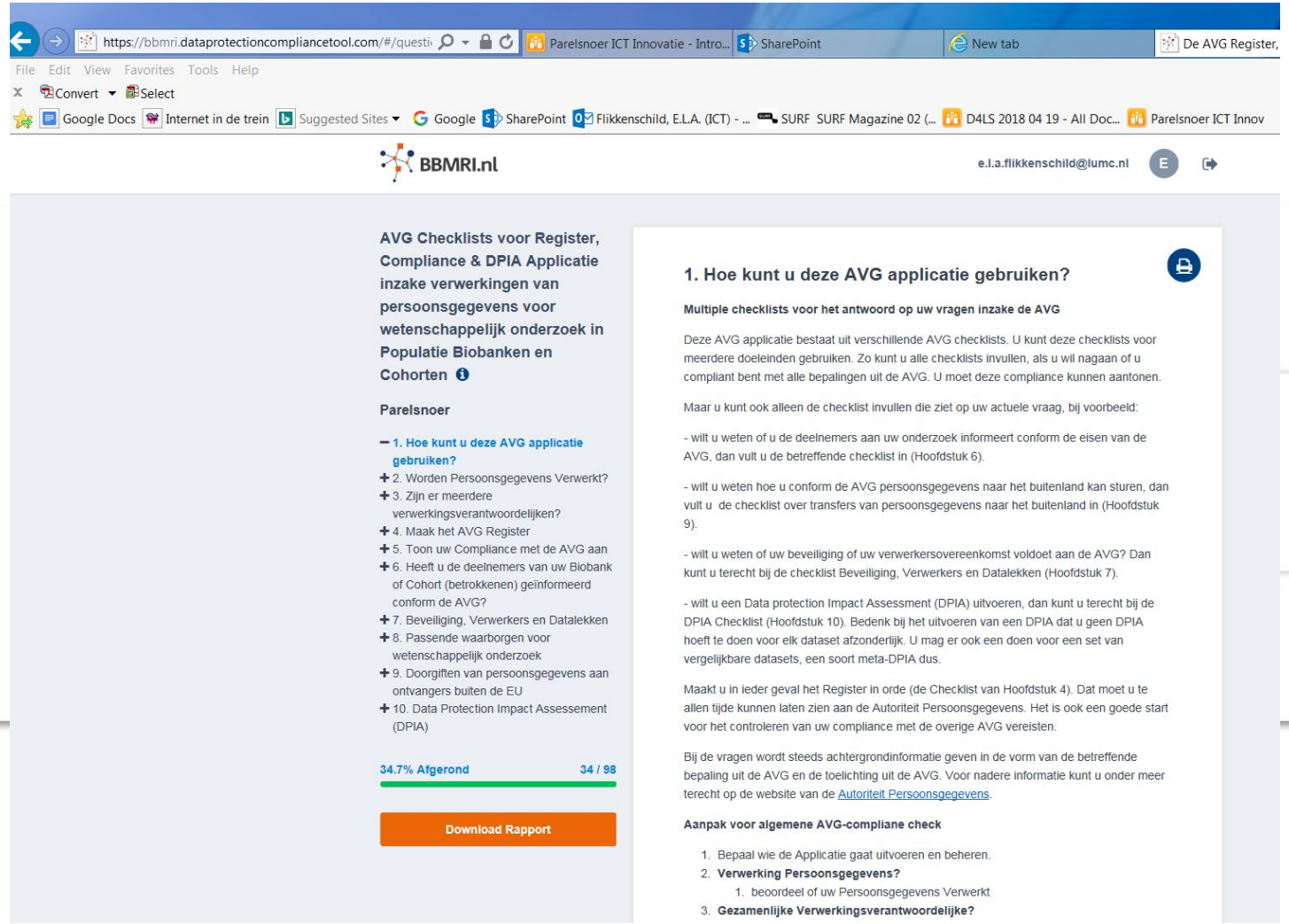


Vendor solutions

PSI
Parelsnoer Institute

Flikkenschild@Parelsnoer.org

Methods: GDPR (AVG) Questionnaire



https://bbmri.dataprotectioncompliancetool.com/#!/login