Data Protection Impact Assessment (Gegevensbeschermingseffectbeoordeling)

Houten, 5 november 2019

ZorgTTP
Privacy & vertrouwen

Welkom!
Even voorstellen…

Simone van Wijngaarden

Adviseur, CIPP/e, Stichting ZorgTTP

Dienstverlening Stichting ZorgTTP

- Onomkeerbare pseudonimisatie d.m.v. ons pseudonimisatieplatform
- Omkeerbare pseudonimisatie d.m.v. onze encryptiedienst TRES (Trusted Reversible Encryption Service)
- Data Protection Impact Assessment (DPIA) / gegevensbeschermingseffectbeoordeling (GEB)

ZorgTTP
Privacy & vertrouwen

Welkom!
Even voorstellen…

Feikje Groenhof

Database Coördinator, Academisch Huisarts Ontwikkel Netwerk, afdeling Huisartsgeneeskunde, UMCG

Namens

De huisartsennetwerken van:

- UMCG
- UMCU
- Amsterdam UMC, locatie VUmc
- Amsterdam UMC, locatie AMC
- Maastricht University

ZorgTTP
Privacy & vertrouwen

Waar gaan we het over hebben?

Wetgevend kader met betrekking tot DPIA

- Wat, wanneer, wie, waarom, hoe, vereisten

Uitvoering door ZorgTTP

- Methode/werkwijze
- Toetsingskader
- Eindresultaat

Praktijkcasus: DPIA voor de huisartsennetwerken uit het samenwerkingsverband Intercity

- Intercity
- Infrastructuur
- Bevindingen
- Aanbevelingen
- Vervolgacties

Vragen en afronding

Vragen tijdens de presentatie? Stel ze gerust!

ZorgTTP
Privacy & vertrouwen

Wetgevend kader DPIA

Simone van Wijngaarden
Adviseur, CIPP/e, Stichting ZorgTTP

ZorgTTP
Privacy & vertrouwen

Wat is een DPIA?

- ENG: Data Protection Impact Assessment (DPIA)
- NL: gegevensbeschermingseffectbeoordeling (GEB)
- Anders dan een PIA
- Bescherming van de persoonsgegevens binnen een gegevensverwerking om de privacy van betrokkenen te waarborgen

ZorgTTP
Privacy & vertrouwen

Wanneer voer je een DPIA uit?

Art. 35 AVG:

‘’op het moment dat een verwerking, in het bijzonder een verwerking waarbij nieuwe technologieën worden gebruikt, gelet op de aard, omvang, context en doeleinden daarvan, waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen”

*Bij voorkeur voorafgaand aan een gegevensverwerking / zo vroeg mogelijk in het proces in verband met privacy by **design** en by **default**.*

ZorgTTP
Privacy & vertrouwen

Wanneer is een DPIA vereist?

Een DPIA is met name vereist op het moment dat er (AVG. Art 35 lid 3):

- Een **systematische en uitgebreide beoordeling** is van persoonlijke aspecten van natuurlijke personen, die is gebaseerd op geautomatiseerde verwerking, waaronder profilering en waarop besluiten worden gebaseerd waaraan voor natuurlijke personen rechtsgevolgen zijn verbonden of die de natuurlijke persoon op vergelijkbare wijze wezenlijk treffen;
- **Grootschalige verwerking** van bijzondere categorieën van persoonsgegevens plaatsvindt;
- **Stelselmatige en grootschalige monitoring** plaatsvindt van openbaar toegankelijke ruimten.

Wat valt onder grootschalig?

ZorgTTP
Privacy & vertrouwen

EDPB - Criteria voor een DPIA

- **Beoordelen van mensen op basis van persoonskenmerken**;
- Geautomatiseerde beslissingen;
- Stelselmatige en grootschalige monitoring;
- **Gevoelige gegevens;**
- **Grootschalige gegevensverwerkingen;**
- **Gekoppelde databases**;
- **Gegevens over kwetsbare personen**;
- Gebruik van nieuwe technologieën;
- Blokkering van een recht, dienst of contract.

Voldoet uw gegevensverwerking aan 2 of meer criteria? Dan DPIA.

Geen DPIA vereist? Dan wel verantwoorden waarom niet, onder de verantwoordingsplicht van de AVG.

ZorgTTP
Privacy & vertrouwen

Geen DPIA?

Mogelijkheid tot oplegging van boete door bevoegde toezichthoudende autoriteit.

- **Geen DPIA** uitgevoerd terwijl dat voor de verwerking wel verplicht is?
- Gegevensbeschermingseffectbeoordeling **niet correct** uitgevoerd?
- De bevoegde toezichthoudende autoriteit **niet geraadpleegd** terwijl dat wel vereist is?

Boete

Administratieve boete van maximaal 10 miljoen euro of in het geval van een onderneming maximaal 2% van de totale wereldwijde omzet van het voorgaande boekjaar, waarbij het hoogste bedrag van toepassing is.

ZorgTTP
Privacy & vertrouwen

Toegevoegde waarde van een DPIA

DPIA niet verplicht, dan alsnog voordelen:

- Privacy risico's voor betrokkenen in beeld en mogelijkheid tot verbeteringen
- Specifiek vraagstuk binnen gegevensverwerking beantwoord krijgen;
- Mogelijkheid om geïnformeerd, betere afwegingen te maken, helpt bij besluitvorming;
- Dient ter verantwoording en uitleg;
- Haalbaarheid project, gedragen gegevensverwerking;
- Vertrouwen en betrouwbaarheid;
- Bewustzijn creëren;
- Verschaft inzicht in de gegevensverwerking;
- Beperking van negatieve schade (imago, boetes).

ZorgTTP
Privacy & vertrouwen

Wie voert een DPIA uit?

- Verwerkingsverantwoordelijke verantwoordelijk dát een DPIA wordt uitgevoerd;
- Als een FG is aangewezen, moet u de FG om advies vragen;
- Daarnaast advies van betrokkenen, of hun vertegenwoordigers om mening vragen;
- Uitbesteding mag;
- Onafhankelijke toets van uitgevoerde DPIA.

ZorgTTP
Privacy & vertrouwen

Iteratief proces DPIA

Advies

- Elke 2 a 3 jaar herhaling van de DPIA

In ieder geval

- Altijd monitoren of verandering in de verwerking plaatsvindt
- Bij een grootschalige wijziging in de gegevensverwerking, in positieve of negatieve zin, een DPIA uitvoeren

ZorgTTP
Privacy & vertrouwen

Vereisten DPIA

Methode staat vrij, wel enkele vereisten (AVG Art. 35 lid 7):

- Een **systematische beschrijving** van de beoogde verwerkingen en de verwerkingsdoeleinden, waaronder, in voorkomend geval, de gerechtvaardigde belangen die door de verwerkingsverantwoordelijke worden behartigd;
- Een beoordeling van de **noodzaak en evenredigheid** van de verwerkingen met betrekking tot de doeleinden;
- Een **beoordeling** van de in lid 1 bedoelde **risico's** voor de rechten en vrijheden van betrokkenen;
- De **beoogde maatregelen** om de risico's aan te pakken, waaronder waarborgen, veiligheidsmaatregelen en mechanismen om de bescherming van persoonsgegevens te garanderen en om aan te tonen dat aan deze verordening is voldaan, met inachtneming van de rechten en gerechtvaardigde belangen van de betrokkenen en andere personen in kwestie.

WP29: het advies van de FG's wordt gevraagd en de belanghebbenden of hun vertegenwoordigers worden indien nodig betrokken.

ZorgTTP
Privacy & vertrouwen

Uitvoering DPIA door ZorgTTP

Simone van Wijngaarden
Adviseur, Stichting ZorgTTP

ZorgTTP
Privacy & vertrouwen

Uitvoering door ZorgTTP

Norea model als uitgangspunt

Multidisciplinair team bij ZorgTTP

- Juridisch
  - CIPP/e
- Organisatorisch
- Technisch

Multidisciplinaire informatieverzameling door middel van documentatie en interviews

- Juridisch
  - Samenwerkingsovereenkomsten, verwerkersovereenkomsten
- Organisatorisch
  - Afspraken, procedures, informatievoorziening aan betrokkenen, documentatie, certificering
- Techniek
  - Bewaartermijnen, toegang, versleuteling

ZorgTTP
Privacy & vertrouwen

Eindresultaat DPIA via ZorgTTP

Rapportage

- Beschrijving van de gegevensverwerking;
- Kwalitatieve risicoanalyse;
- Adviezen voor verbetering;
- Aanbevelingen voor een volgende DPIA.

Presentatie van de **bevindingen**

Evaluatie inclusief uiteenzetting van de **vervolgstappen**

ZorgTTP
Privacy & vertrouwen

Gegevensverwerking Intercity
DPIA gezamenlijke database-infrastructuur

Feikje Groenhof
Database Coördinator, Academisch Huisarts Ontwikkel Netwerk (AHON)
afdeling Huisartsgeneeskunde en Ouderengeneeskunde, UMCG

Namens de samenwerkende huisartsennetwerken van het
UMCU, UMCG, AmsterdamUMC – locaties VUmc en AMC en MU

ZorgTTP
Privacy & vertrouwen

Gegevensverwerking Intercity

- Waar staat het voor?
- Ontstaan van de samenwerking
- Stand van zaken
- Database-infrastructuur
- Uitvoeren DPIA
- Resultaten/bevinding DPIA
- Aanbevelingen n.a.v. DPIA
- Vervolgacties n.a.v. DPIA
- Ervaringen met deze DPIA

ZorgTTP
Privacy & vertrouwen

Intercity – waar staat het voor?

ZorgTTP
Privacy & vertrouwen

Intercity – waar staat het dan wel voor?

Samenwerking tussen **huisartsgeneeskundige registratienetwerken (huisartsennetwerken)** vanuit vijf afdelingen Huisartsgeneeskunde:

- UMCU
- UMCG
- AmsterdamUMC – locatie VUmc
- AmsterdamUMC – locatie AMC
- Maastricht University

Maar ook samenwerking met:

- Calculus/Proigia → doorleveren van data
- ZorgTTP → pseudonimisatie van data

ZorgTTP
Privacy & vertrouwen

Intercity – ontstaan van de samenwerking (1)

2015

Huisartsennetwerken UMCU, **VUmc** en **UMCG** → start gezamenlijke verkenning nieuwe **database-infrastructuur** om **huisartsgeneeskundige registratiedata** te kunnen

- **extraheren/aanleveren** vanuit het HIS (Huisartsen Informatie Systeem)
- **opslaan/beheren** in de eigen database
- **uitgeven** t.b.v. onderzoek en feedback/benchmark

Netwerken hadden o.a. de volgende **wensen/eisen**:

- ontwikkelen **stabiel patiëntnummer** t.b.v. longitudinaliteit
- koppelen met externe bronnen d.m.v. **pseudoniemen** (via Trusted Third Party).
- **terugrapportage** aan huisarts op patiëntniveau
- niet doorleveren van HIS-data van **databaseweigeraars**
- en … **minimale inspanning** voor de deelnemende **huisartsen**!

Na inventarisatie **samenwerking** gezocht met

- **Calculus/Proigia** → extraheren/aanleveren van data
- **ZorgTTP** → pseudonimiseren van data

ZorgTTP
Privacy & vertrouwen

Intercity – ontstaan van de samenwerking (2)

2016

Start **pilot** t.b.v. het **inrichten** van de **database-infrastructuur** met o.a.

- opzetten beveiligde verbinding
- realiseren wensen/eisen van de netwerken
- ontwikkelen software t.b.v. opbouw longitudinale database
- externe validatie bestanden (per HIS)
- scheppen kaders samenwerking → intern (UMC's) en extern (Calculus/Proigia en ZorgTTP)

2017

Februari → **eerste aanlevering** van data vanuit een pilotpraktijk

September → **database-infrastructuur operationeel** voor netwerken van het **UMCU**, **VUmc** en **UMCG**

2018

Januari → netwerken van het **AMC** en **MU** sluiten aan bij de samenwerking

ZorgTTP
Privacy & vertrouwen

Intercity – stand van zaken

- Na 3 jaar gezamenlijk ontwikkelen is de **database-infrastructuur** vanaf **januari 2018** operationeel voor **vijf huisartsennetwerken** en wordt er nauw samengewerkt met **Calculus/Proigia** en **ZorgTTP**

- Netwerken zijn verschillend in grootte en groeien nog steeds; momenteel:

• UMCU	Julius Huisartsen Netwerk (JHN)	± 75 huisartsenpraktijken
• UMCG	Academisch Huisarts Ontwikkel Netwerk (AHON)	± 35 huisartsenpraktijken
• AUMC – VUmc	Academisch Netwerk Huisartsgeneeskunde (ANH)	± 60 huisartsenpraktijken
• AUMC – AMC	Academisch Huisartsennetwerk AMC (AHA)	± 50 huisartsenpraktijken
• MU	Research Network Family Medicine (RNFM)	± 30 huisartsenpraktijken

CALCULUS VIP HET KAN WEL

proigia improving health care through information

Zorg TTP Privacy & Vertrouwen

UMC Utrecht

umcg

Amsterdam UMC Universitair Medische Centra

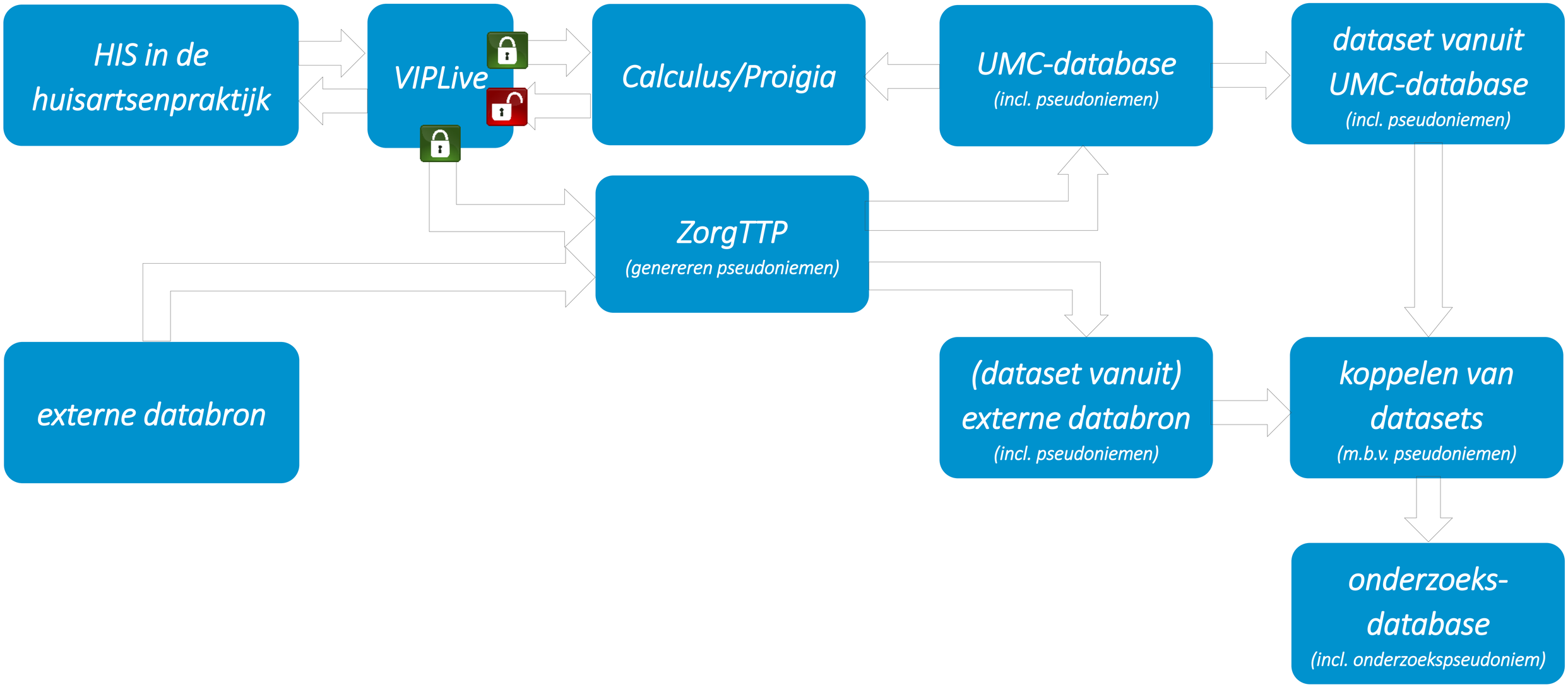
Maastricht University

VUmc Samen kiezen voor beter

amc

ZorgTTP Privacy & vertrouwen

Intercity – database-infrastructuur



ZorgTTP
Privacy & vertrouwen

Intercity – uitvoeren DPIA (1)

Reden om een DPIA uit te voeren op de gegevensverwerking van Intercity

- goede **beveiliging** van **gegevens** van de betrokkenen
- **transparantie** van **afspraken** rondom de **beveiliging**
- **waarborgen privacy** van betrokkenen

AVG – Artikel 35 lid 1 → **wanneer** moet er een **DPIA** worden uitgevoerd

'… op het moment dat een verwerking, in het bijzonder een verwerking waarbij nieuwe technologieën worden gebruikt, gelet op de aard, omvang, context en doeleinden daarvan, waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen …'

AVG – Artikel 35 lid 7 → **hoe** moet een **DPIA** moet worden uitgevoerd

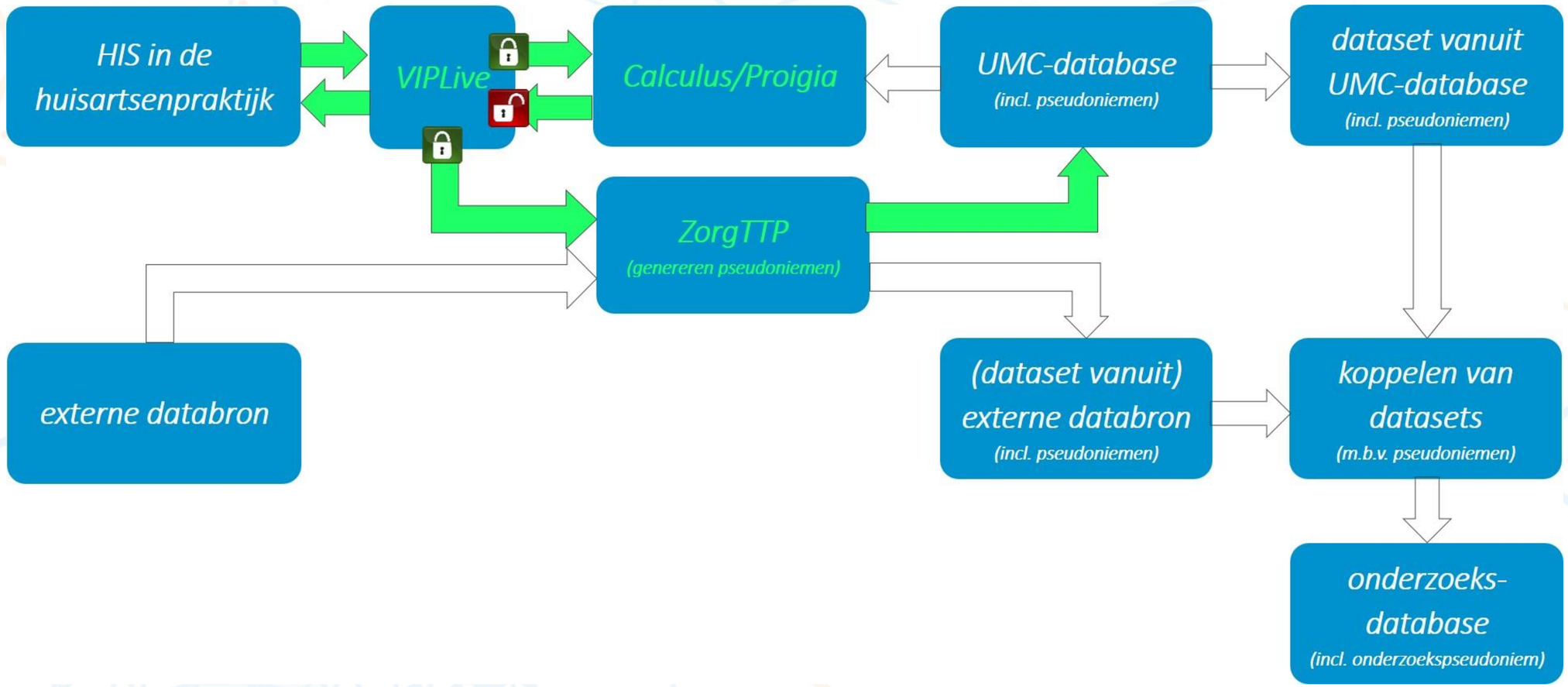
- geven systematische beschrijving van **gegevensverwerking** en **verwerkingsdoelen**
- beoordelen **noodzaak en evenredigheid** gegevensverwerking m.b.t. verwerkingsdoelen
- in kaart brengen **privacy risico's** voor **betrokkenen**
- geven van **aanbevelingen** om de **privacy risico's** aan te pakken

Aanpak DPIA – **model van NOREA** als toetsingskader

- beschrijven van de **gegevensverwerking** aan de hand van **zeven risicogebieden**
- input voor **risicobeoordeling** toegelicht a.d.h.v. **acht privacy principes**

Intercity – uitvoeren DPIA (2)

- Deze **DPIA** is uitgevoerd op het **gezamenlijke deel** van de **database-infrastructuur**
- Alle **samenwerkende partijen** zijn betrokken: huisartsennetwerken, Calculus/Proigia en ZorgTTP



ZorgTTP
Privacy & vertrouwen

Intercity – resultaten/bevindingen DPIA

ZorgTTP
Privacy & vertrouwen

Intercity – aanbevelingen n.a.v. DPIA

Belangrijkste aandachtspunten/aanbevelingen n.a.v. deze DPIA:

- verhelderen **verwerkingsdoelen** en **rollen** binnen de gegevensverwerking → verschillen tussen netwerken
- documenteren **uitzonderingsgrondslag** voor **wetenschappelijk onderzoek**
- streven naar **dataminimalisatie**
- waar nodig **vernieuwen overeenkomsten** tussen samenwerkende partijen → als gevolg van de invoering van de AVG
- waar nodig **updaten informatievoorziening** richting de betrokkenen → posters, flyers, info website

Intercity – vervolgacties n.a.v. DPIA

Vervolgacties n.a.v. de aanbevelingen vanuit de DPIA zijn inmiddels in gang gezet

- **dataminimalisatie** (op het niveau van velden, periode en pseudoniemen) → staat op de planning om te worden uitgevoerd door Calculus/Proigia en ZorgTTP; zal worden meegenomen in release nieuwe software ZorgTTP
- **documenteren grondslag** voor deze **gegevensverwerking** → wordt aan gewerkt
- **vernieuwen overeenkomsten** → wordt aan gewerkt
- **publieksversie** van de deze **DPIA** → wordt aan gewerkt
- uitvoeren **DPIA's** op het **eigen deel van de database-infrastructuur** → is al uitgevoerd of in de planning

➢ Wanneer aanbevelingen zijn uitgevoerd zal de DPIA nogmaals worden uitgevoerd op deze specifieke onderdelen.

Intercity – ervaringen met deze DPIA

Een DPIA kost tijd … maar ervaringen met de uitvoering van deze DPIA zijn meer dan positief:

- Grondig
- Gestructureerd
- Specialistisch werk is de netwerken uit handen genomen
- Geeft goed inzicht in waar we mee bezig zijn, wat goed gaat en wat beter kan
- Prettige samenwerking met alle partijen!

Vragen?

Dank!

Feikje Groenhof

Database Coördinator, Academisch Huisarts Ontwikkel Netwerk (AHON)

Afdeling Huisartsgeneeskunde en Ouderengeneeskunde, UMCG

f.groenhof@umcg.nl

06-25647145

Simone van Wijngaarden

Adviseur, CIPP/e, Stichting ZorgTTP

Simone.van.wijngaarden@zorgttp.nl

06-13631500

ZorgTTP
Privacy & vertrouwen