bakertilly

VitaValley

SET-up ondersteuningsprogramma

Webinar 'Veiligheid & Privacy'

14 november 2019

Opbouw Webinar

1.	Welkom en korte kennismaking	5 min
2.	Privacy Compliance in het ICT geheel	10 min
3.	Status huidige privacy regelgeving	15 min
	- wat is duidelijk en wat nog niet?	
	- wat zijn beschikbare practices / instrumenten?	
4.	Advies aanpak voor dit moment	15 min
5.	Top 4 gestelde vragen	10 min
6.	What's next…	5 min

VitaValley

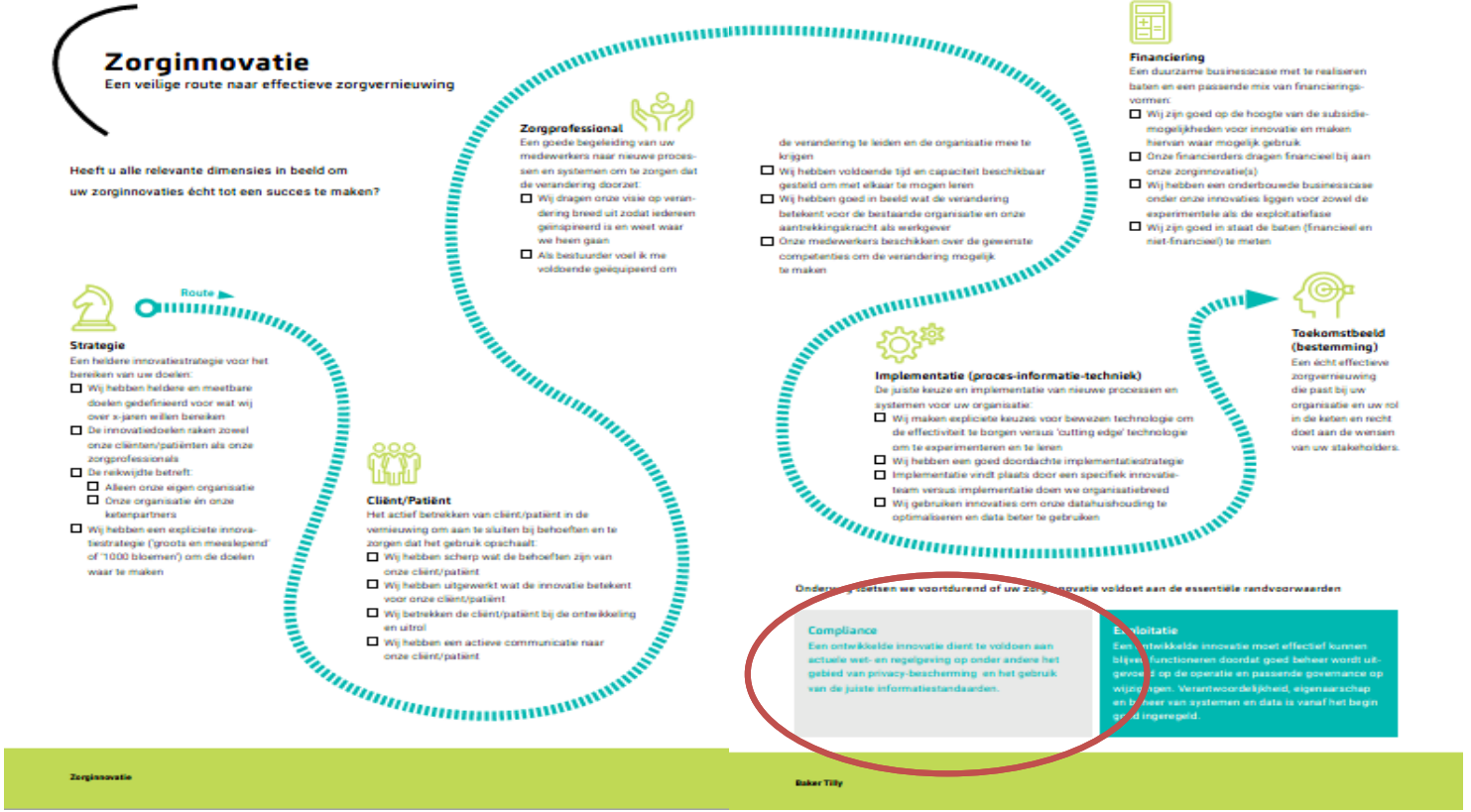
1. Welkom en korte kennismaking

- Expertpool SET-up als flexibele schil in programma
- Baker Tilly disciplines met mix van advies-achtergronden
- Zorginnovatiemodel als basis

  –> wordt i.s.m. VitaValley in SET-up uitgewerkt als rode draad

- Wilco Brouwers: IT auditor / adviseur met zorg als focus
- Achtergrond accountancy en internal audit bij zorgverzekeraar
- Nauw betrokken geweest bij zorginkoop en zorginnovatie

What's next ?



VitaValley

2. Privacycompliance in het geheel van ICT

ICT in kader van de SET projecten staat in het teken van :

- ❖ herinrichting, koppeling, uitbesteding en regie over ICT
- ❖ ‘oude’ omgeving bevat al risicoanalyses en maatregelen
- ❖ in nieuwe omgevingen moet dit geactualiseerd worden
- ❖ en er moet worden nagedacht over nieuwe data / metingen

Privacycompliance kan in een proportionele balans met innovatie werken en hoeft innovatie zeker niet tegen te werken!

2. Privacycompliance in het geheel van ICT

Privacy-risico: **kans** van optreden van een bedreiging maal de **impact** die de bedreiging heeft

Privacy-compliance: deze risico's vooraf bedenken, inschatten, juiste maatregelen treffen en dit ook duidelijk communiceren, monitoren of ze werken en dit ook aantoonbaar maken.

De concrete oplossing is er vaak nog niet: het is meer een continu proces van zoeken van mogelijkheden gedurende de innovatie dan het vooraf inbedden van een checklist.

3. Status huidige privacyregulering

ICT ontwikkelingen in zorg momenteel op stimulering ontsluiting en koppeling, waarbij de regulering rondom ICT technieken nog achterblijft!

- AVG, NEN 7510, ISO xxx als globale kaders
- Toezicht AP en IGJ blijft ook globaal
  “Toetsingskader IGJ “Inzet van eHealth door zorgaanbieders”
- MedMij en VIPP gaan al concreter op functionaliteit. Verder steunen zij op NEN 7510
- Landelijke voorzieningen zijn nog onderhanden.

3. Status huidige privacyregulering

Kern van de regulering bij bijzondere gegevens gezondheid

❖ mogen worden verwerkt als dit (wettelijk) is vereist in uw taak óf

❖ als het valt onder één van de grondslagen

- toestemming verkregen ← SET
- overeenkomst met betrokkene
- vitale belangen
- gerechtvaardigd belang ← SET

Doelbinding: leveren en meten van ketenzorg ? ← SET

3. Status huidige privacyregulering

Vergelijk sociaal domein: in 2018 zelfde uitdaging.

Programma Sociaal Domein gestart met werksessies en AP afstemming:

- Balans tussen privacy en goede dienstverlening, geen tegenstelling
- Gegevens delen mag, maar met goede reden en niet meer dan nodig
- Goede praktische werkinstructie voor zorgprofessionals
- Start bij intake met zorgconsument: casusoverleg met ketenpartners, noodzakelijkheid, welke middelen en informatie nodig

https://www.programmasociaaldomein.nl/trajecten/uitwisseling-persoonsgegevens-en-privacy-upp/

3. Status huidige privacyregulering

Doelbinding/gerechtvaardigd belang

- ‘welbepaald, uitdrukkelijk omschreven en gerechtvaardigd’ doel
- niet méér persoonsgegevens verzamelt en gebruikt dan nodig voor een specifiek doel en niet langer bewaard dan nodig voor het doel.
- voor de SET initiatieven
  - in de basis het verlenen van zorg
  - voor een specifieke doelgroep
  - de nieuwe toepassing had hierin al een plaats
  - en daar komt een uitwisseling met andere partijen en/of verzameling van nieuwe data bij **hier nieuwe doelbinding bepalen**

VitaValley

4. Advies aanpak

Wat gebeurt er in de SET initiatieven

- verschillende silo's met eigen doelbinding worden verbonden en gecombineerd en er ontstaan:
  - koppelingen tussen bestaande silo's
  - nieuwe silo's met combinaties van reeds bestaande data
  - nieuwe silo's met nieuwe data

Voor de doelen:

- verbeteren van zorg / doelmatigheid van de zorg
- evaluatie van kwaliteit / effectiviteit van de zorg
- eventueel wetenschappelijk onderzoek?

4. Advies aanpak

Wat moet er al zijn binnen de eigen organisatie?

- Privacy-statement te hebben met gerechtvaardigd belang en doel
- Opgenomen in het register met verwerkingen voor de organisatie
- Inzichtelijk te hebben welke data wordt gebruikt
- Een privacy impact assessment te hebben gedaan

Voor innovatiecluster adviseer ik nu gezamenlijk voor de toepassing:

- Een nieuwe data inventarisatie uit te voeren
- Een privacy impact assessment op de nieuwe situatie
- Eventueel een eigen privacy statement van deze toepassing uit te werken

4. Advies aanpak Data inventarisatie

1. **Taak en werkzaamheden**
   Bepaal in het kader van welke (wettelijke) taak jouw organisatie de werkzaamheden met gegevens verricht. Vanuit welke taak betrek je de partners bij een zorgtraject? Begin altijd bij de inhoud van je werk. Duidelijk moet zijn waar je bepaalde gegevens voor nodig hebt.
   - verlenen van zorg
   - meten en verbeteren van zorg / evalueren

2. **Welke activiteiten en doelen**
   Bepaal het doel waarvoor je de gegevens nodig hebt. Wees zo concreet mogelijk. Het doel: ‘ik probeer mensen goede zorg te verlenen’ is te algemeen. Koppelen van het doel aan een stap in het zorgproces maakt het al een stuk concreter:
   - verlenen van zorg: het inlichten van de mantelzorger, het bijsturen van medicatie, het begeleiden bij dagelijkse boodschappen etc.

4. Advies aanpak Data inventarisatie

3. **Wat zijn de noodzakelijke gegevens per doel?**
   Bepaal vervolgens welke gegevens nodig zijn voor het doel en stel vast bij welke bron je de gegevens kan opvragen. Dit kan zijn de zorgconsument zelf, mantelzorg, ketenpartner, verzekeraar.
   - Welke taak en rol heeft die organisatie en waarom stel je die vraag aan hen?
   - Voor welke inhoudelijke afweging sta je en welke informatie heb je dan precies nodig?
   - Zijn er eventueel al mogelijke toekomstige wensen omtrent het verzamelen van informatie?

4. **Juridische onderbouwing**
   Na het doorlopen van de eerste drie stappen, volgt (pas) het privacy-technische deel. Welke grondslag van de AVG is van toepassing voor mijn werk? Dit kan aansluiten bij de grondslag van de zorgorganisatie, het uitvoeren van zorg.

   Benoem die gegevens waarover je twijfelt of je die mag delen. Indien mogelijk, verzin een minder ingrijpend alternatief.

4. Advies aanpak: Privacy impact assessment

Een PIA of ook wel een ‘gegevensbeschermingseffectbeoordeling’ is verplicht als je nieuwe processen / technieken introduceert.

Doel is al **instrumenteler** dan bij de data inventarisatie:
om vanuit risico’s voor privacy voor betrokkenen de juiste zwaarte van maatregelen te bepalen

Het is een risicoanalyse instrument en geen naleving instrument.

Reeds in het proces van implementatie – en dan het liefst helemaal aan het begin –
onderzoeken wat de impact op en risico’s voor de privacy van betrokken patiënten zal zijn.

Er is overlap met de data inventarisatie, zie volgende pagina.

4. Advies aanpak: Privacy impact assessment

- een systematische beschrijving van de beoogde verwerkingen en de verwerkingsdoeleinden, waaronder, in voorkomend geval, de gerechtvaardigde belangen die door de verwerkingsverantwoordelijke worden behartigd (**de data inventarisatie)**

- een beoordeling van de noodzaak en de evenredigheid van de verwerkingen met betrekking tot de doeleinden (**de data inventarisatie)**

- een beoordeling van de benoemde risico's voor de rechten en vrijheden van betrokkenen; en

- 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.

4. Advies aanpak: Privacy impact assessment

De onderdelen van een PIA :

1. Het type project en de maatschappelijke context / stakeholders
2. De gegevens die u wilt gebruiken
3. De partijen betrokken bij de uitvoering (ketenpartners en dienstverleners)
4. Verzamelen
5. Gebruik
6. Bewaren en vernietigen
7. Beveiligen

https://www.norea.nl/download/?id=522

Let op: versie 2015 wordt momenteel geactualiseerd

4. Advies aanpak: Privacy impact assessment

Wat zijn – hoe dan ook – de belangrijkste maatregelen die in deze fase van het SET project de meeste aandacht vragen :

1. Inzicht en helderheid over data en limitering hiervan
2. Doelen voor verzamelen en verwerken nader specificeren en hierover communiceren

Architectuur

3. Gefragmenteerde opslag en minimale datacommunicatie altijd beter dan centrale database
4. Encryptie en logische toegangsbeveiliging op elk lokaal niveau en voor datacommunicatie

Governance

5. Transparantie in wat het cluster doet: opstellen beleid, gedragscode en laten begeleiden/toetsen / certificeren van de verwerking.
6. Rechten van betrokkenen: geef vanaf het begin voldoende zeggenschap over de gegevens aan de zorgconsument (idealiter via portaal)

4. Advies aanpak: Privacy impact assessment

Illustratie

#	Vraag	Extra informatie	Ja	Nee
1.9	Zijn er veel maatschappelijke belanghebbenden?	Houd bij de beantwoording rekening met: 1. Medewerkers, afnemers, leveranciers, belangengroeperingen, burgers, klanten toezichthouders. 2. Welke beroepsgroepen betrokken zijn bij de verwerking.	U loopt een verhoogd risico. De wijze waarop maatschappelijke belanghebbenden reageren varieert waardoor het project kan vertragen. U wordt geadviseerd een plan te maken waarin u aangeeft op welke manier de verschillende belanghebbenden bij het project worden betrokken of over het project worden geïnformeerd.	Ga verder.
2.3	Kunnen de gegevens gebruikt worden om het gedrag, de aanwezigheid of prestaties van mensen in kaart te brengen en/of te beoordelen (ook al is dit niet het doel)?	Denk hierbij bijvoorbeeld ook aan geolocatie, personeelsvolgsystemen, beslisondersteuning bij het als dan niet aanbieden van producten of diensten.	U loopt een verhoogd risico. Het risico bestaat dat de betrokkenen of de algemene opinie dit als een potentiële bedreiging voor hun privacy zien. Ook als de gegevens niet voor dit doel worden gebruikt bestaat het risico dat dit (in de toekomst) wel gebeurt. Voor de invoering van een personeelsvolg-systeem is instemming van de OR nodig.	Ga verder.

VitaValley

4. Advies aanpak Afronding

Met de data inventarisatie en PIA heb je **taak, doel en noodzaak van het verzamelen en delen van gegevens** in beeld en dan pas volgt de vraag: mogen we de gegevens delen en onder welke voorwaarden ?

- die vraag kun je vervolgens aan een jurist voorleggen
- of als cluster / SET voorleggen aan Autoriteit Persoonsgegevens

Regelmatig blijkt gaandeweg dat het mogelijk is om mensen de juiste zorg te bieden, zonder dat hun privacy in het geding is. Of dat het privacyvraagstuk beperkt is.

4. Advies aanpak

Handige instrumenten:

- PIA van NOREA	risicoanalyse instrument
- PCF van NOREA	inrichting/naleving
- NEN 7510 e.d.	Inrichting/naleving
- IGJ Toetskader eHealth	naleving
- Programma Sociaal Domein	best practise gezamenlijke aanpak

5. Top detail vragen

❖ wanneer ben je als dienstverlener een sub-verwerker (hosting, applicatiebeheer)

Je bent als IT dienstverlener eigenlijk altijd ‘bewerker’: je ‘verwerkt’ ten behoeve van de verantwoordelijke zonder onder het gezag van de verantwoordelijke te zijn onderworpen.
Verwerken = verzamelen, ordenen, bewaren, afschermen van data.

❖ omgaan met leveranciers die nog niet voldoen, welke koppelingen zijn zo risicovol dat dit niet kan?

Je moet enigszins vaststellen dat passende technische en organisatorische maatregelen getroffen zijn en dit in een verwerkersovereenkomst vastleggen.

- minimum niveau beveiliging: servers patches, anti virus beveiliging, admin rechten
- data versleuteld opslaan en verbindingen beveiligd (Https)
- datalekken afspraak maken

o.a. pagina 46 en 47 van het privacy control framework van NOREA biedt checklist

5. Top detail vragen

- logische toegangsbeveiliging en eID

  Brief van 4 oktober 2018 van de AP aan VWS over het gewenste betrouwbaarheidsniveau in de zorg
  “bij patiëntauthenticatie in het kader van de uitwisseling van gegevens over gezondheid in beginsel dient te worden uitgegaan van een “hoog betrouwbaarheidsniveau”. In de terminologie van de eIDAS-verordening : minimaal niveau “substantieel”. Als het gaat om medisch beroepsgeheim, is betrouwbaarheidsniveau “hoog” vereist.”
  De AP erkent dat het middel “substantieel “ en “hoog” op dit moment nog niet op redelijke schaal beschikbaar is en vereist daarom voor dit moment het hoogst mogelijke betrouwbare middel, te weten 2-factor (naam, wachtwoord en sms of app).

  ‘dient authenticatie plaats te vinden met tenminste tweefactorauthenticatie (zoals DigiD in combinatie met sms). Randvoorwaarde daarbij is dat er zo nodig aanvullende maatregelen worden getroffen om openstaande risico’s, die niet worden weggenomen met tweefactorauthenticatie, te mitigeren.

5. Top detail vragen

- Vragen over normen op het gebied van informatiebeveiliging (met name NEN familie):

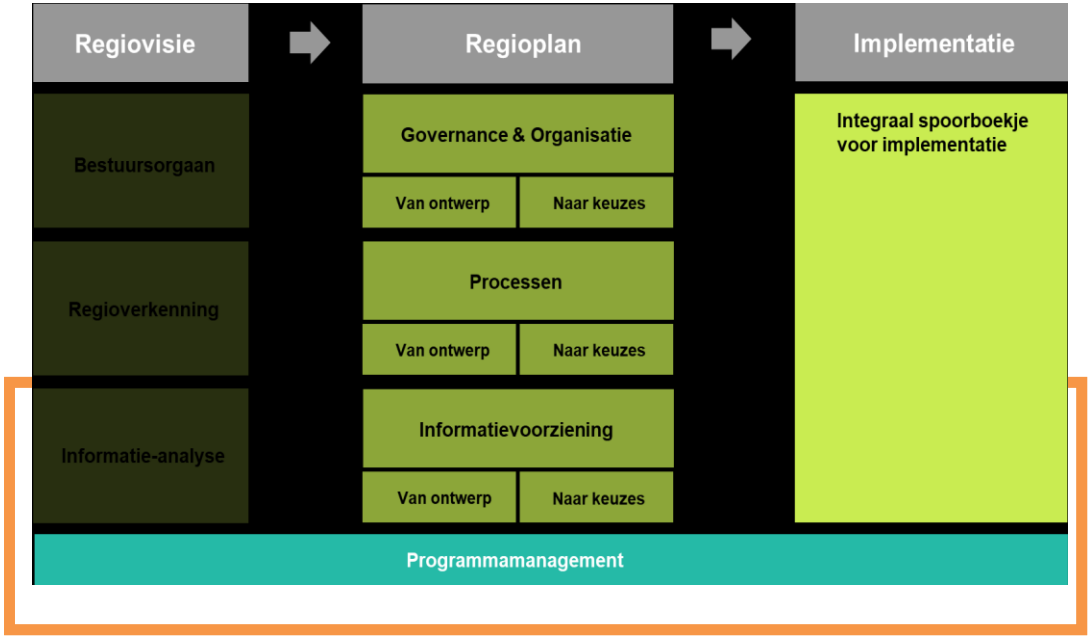
  De AP ziet die normen als een beveiligingsstandaard die binnen de sector algemeen wordt geaccepteerd en die organisaties binnen de zorgsector moeten toepassen.

  NEN 7513 logging: maak zeker groepen aan en sluit bepaalde logregels uit.

  Functioneel specificeren welke acties gelogd moeten worden.

6. What's next?

We gaan graag met jullie in overleg over onderwerpen en vorm van ondersteuning !



VitaValley

VitaValley

Dank voor uw aandacht.

Pim Ketelaar – Programmadirecteur
pketelaar@vitavalley.nl

Pasquelle van Ruiten – Programmamanager
pvanruiten@vitavalley.nl

Sanne Kok – Programma ondersteuning
skok@vitavalley.nl

Dorien Faber – Programma- & Eventassistent
dfaber@vitavalley.nl