
bakertilly
SET
Stimuleringsregeling
E-health Thuis
VitaValley
SET-up Webinar
Privacy compliance
12 mei 2020

Opbouw Webinar

1.	Welkom en korte kennismaking	5 min
2.	Basis voor privacy-compliance	15 min
3.	Advies aanpak: hoe te starten	15 min
4.	Concrete toepassing beeldschermzorg	15 min
	veel slides maar ook naslag ☺	

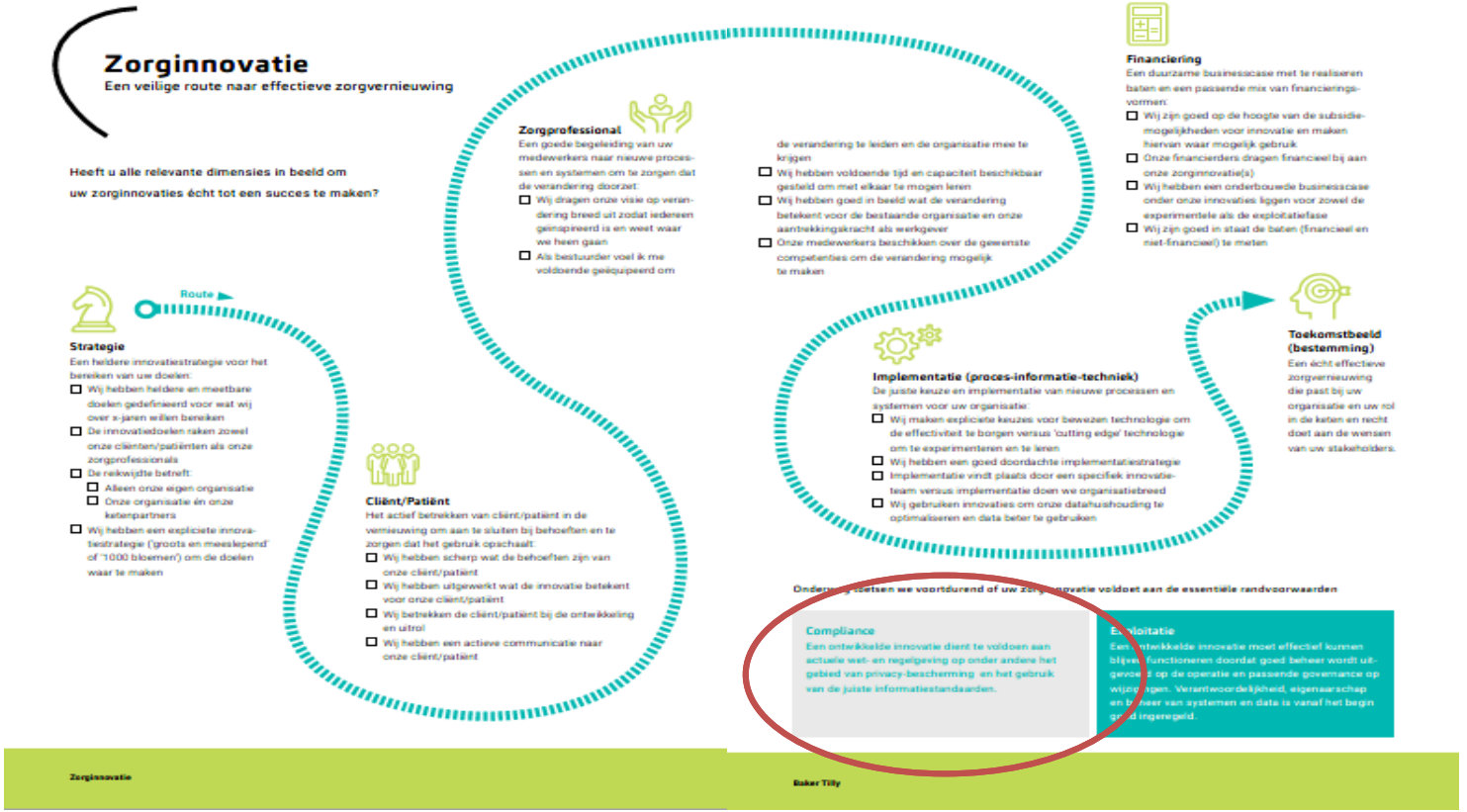
Vragen in de chat !

1. Welkom en korte kennismaking

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

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

Compliance in het grote geheel !



VitaValley

2. Privacy compliance binnen innovatie

ICT in kader van de SET-projecten :

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

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

2. Kern van privacy compliant zijn

1. Je moet de **grondslag** bepalen:
   - (wettelijk) vereist in uw taak of één van de grondslagen:
     - toestemming verkregen ← SET
     - overeenkomst met betrokkene
     - vitale belangen
     - gerechtvaardigd belang ← SET
2. Vervolgens duidelijk je **doel** formuleren
   Doelbinding: op basis van grondslag verwerk je voor doel
3. En op basis daarvan **risico's** inschatten en passende **maatregelen** treffen

VitaValley

2. Concreet

- Grondslag wettelijk: WLZ, WGBO voor dossier, BSN in zorg
- Grondslag overeenkomst: behandelovereenkomst biedt basis voor gegevensverwerking
- Gerechtvaardigd doel en belang van de zorgverlener :
  - noodzakelijk voor de belangen van verwerkingsverantwoordelijke, tenzij de privacybelangen van de betrokkene zwaarder wegen
  - in hoeverre had de betrokkene mogen verwachten dat voor de doelen deze gegevens nodig zijn.
- Extra toestemming vragen en vastleggen voor nieuwe verwerking

2. Concreet doelen

Doelen voor de verwerking:

- verlenen van zorg
- verminderen fysiek contact om verspreiding COVID-19 te voorkomen
- verbeteren kwaliteit van leven
- ondersteuning van mantelzorgers
- communicatie met cliënten ter voorkoming van sociaal isolement
- verbeteren van zorg / doelmatigheid van de zorg
- evaluatie van kwaliteit / effectiviteit van de zorg
- eventueel wetenschappelijk onderzoek

2. Wat is doelbinding?

Doelbinding zien te bereiken, dan heb je een 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 heeft hierin wellicht al een plaats
  - óf betreft nieuwe toepassing met andere partijen en/of data

  hier nieuwe doelbinding bepalen

2. Privacy compliance is risico-denken

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.

2. Welke kaders en referenties?

- AVG, WGBO, branchecodes als globale kaders
- Toezicht AP en IGJ blijft ook globaal
  Toetsingskader IGJ 'Inzet van eHealth door zorgaanbieders'
- Toezicht op concrete functionaliteit, zoals portalen of koppelingen:
  - ZelfzorgOndersteund
  - MedMij en VIPP

  Allemaal steunen zij op NEN 7510 en de aanpak zoals hier uitgewerkt.

3. Advies aanpak

Basis in de organisatie

- Privacy-statement met gerechtvaardigd belang en doel
- Register met verwerkingen van de organisatie, gekoppeld aan doel
- Inzichtelijk welke data wordt gebruikt
- Een privacy impact assessment te hebben gedaan (voor elke verwerking)

Voor innovatiecluster komt daar bij :

- 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

3. Advies aanpak Data inventarisatie

1. **Welke activiteiten en doelen** **PROCES SCHEMA**
   Werk stappen in het zorgproces uit en bepaal per stap de doelbinding. Wees zo concreet mogelijk. Het doel: ‘ik probeer mensen goede zorg te verlenen’ is te algemeen.
   - doel: ondersteunen bij dagelijkse activiteiten
   - stappen het inlichten van de mantelzorger, het begeleiden bij dagelijkse boodschappen

2. **Wat zijn de noodzakelijke gegevens per doel** **DATA**
   Bepaal vervolgens welke gegevens nodig zijn per stap en waarom die gegevens nodig zijn.
   - dataminimalisatie: niet meer data dan nodig
   Stel vast bij welke bron je de gegevens zelf hebt of 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?
   Zijn er eventueel al mogelijke toekomstige wensen omtrent het verzamelen van informatie?

3. Advies aanpak: Privacy impact assessment

Een DPIA = Data Protection Impact Assessment of Gegevensbeschermingseffectbeoordeling

is verplicht als je nieuwe processen / technieken introduceert.

Doel is **instrumenteler** dan bij de data inventarisatie:

hoogte risico's voor privacy voor betrokkenen om de zwaarte van maatregelen te bepalen

Het is een risicoanalyse instrument en geen naleving instrument/checklist!

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.

3. 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/processchema)**

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

- een beoordeling van de benoemde risico's voor de rechten en vrijheden van betrokkenen (**de PIA)**; 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 **(de PIA)**.

3. 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. Hoe verzamelen?
5. Hoe gebruiken?
6. Hoe bewaren en vernietigen?
7. Hoe beveiligen?

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

Let op: versie 2015 wordt momenteel geactualiseerd

3. Advies aanpak: welke maatregelen?

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. Opslag en beveiliging bij de bron en minimale datacommunicatie 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)

3. 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

3. Advies aanpak Afronding

Met de data inventarisatie en PIA heb je **taak, doel en noodzaak van het verzamelen en delen van gegevens** in beeld.

Je kan dit uitwerken naar de beschrijving van de gekozen beveiligingsmaatregelen, zodat je als organisatie altijd kan **aantonen** dat je heb nagedacht over de risico's.

Bij twijfel over compliance is het raadzaam:

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

3. Advies aanpak

Handige instrumenten:

- DPIA van NOREA	risicoanalyse instrument
- PCF van NOREA	inrichting/naleving
- NEN 7510 e.d.	Inrichting/naleving
- IGJ Toetskader eHealth	naleving

4. Beeldschermzorg

- Alleen **beeldbellen / communicatie** met generieke chat/videobel oplossingen:
  - gratis v.s. betaald — verdienmodel? Advertenties, doorgeven informatie — **snel inzetbaar**
  - vertrouwelijk of niet — versleuteling — **weinig inrichting**
  - metadata — wat wordt vastgehouden van wie met wie belt?
  - gebruikersgemak

- Specifieke **beeldschermzorg** oplossingen (Fasttrack):
  - zakelijke toepassing afgestemd op zorgproces (link EPD/PGO)
  - uitgebreidere beveiligingsinstellingen — **inrichting**
  - verwerkersovereenkomst

  Kijk op https://vitavalley.nl/fasttrack-beeldschermzorg/ voor overzicht oplossingen.

4. Generieke oplossingen beeldbellen

Algemeen advies

Gebruik deze categorie applicaties **niet om vertrouwelijke zorginhoudelijke informatie** te bespreken of te delen. Er is op dit moment geen eenvoudige oplossing voorhanden die voldoet aan de hoogste beveiligingseisen voor het bespreken en delen van vertrouwelijke informatie.

Zet deze toepassingen alleen in voor niet kritieke communicatie en als het niet anders kan. Meldt bij de patiënt dat de communicatie niet veilig is. Zorg ook voor instemming van de patiënt.

Maak daarnaast binnen uw organisatie een instructie / afspraken over het gebruik, met name over toestaan van bijvoorbeeld het delen van documenten/foto via de videoapplicatie.

4. Beeldschermzorg aandachtspunten

1. Verdiep je in leverancier en product
    - Lees het privacy beleid van de leverancier door. Wees u ervan bewust welke informatie de leverancier verzamelt en voor welke doeleinden deze worden gebruikt. Let extra goed op de voorwaarden bij leveranciers van buiten de EU.
    - Beoordeel de mogelijke (technische) beveiligingsmaatregelen (zie volgende slide), neem kennis van hiervoor beschikbare rapportages (Actiz)
    - Ga na of leverancier een certificering of andere assurance heeft
2. Metadata over gebruikers
    - Niet-noodzakelijke persoonlijke data in het profiel van de applicatie, zoals naam werkgever, LinkedIn ID, etc. Alleen het e-mailadres, een naam die wordt getoond
    - Wat slaat de applicatie op over de gesprekken? Datum en tijdstip, deelnemers, log?
    - Opnames van gesprekken/meetings mogelijk? Bespreken met aanwezigen en vraag om toestemming. Deel geen inhoud/foto van een sessie op social media.

4. Beeldschermzorg aandachtspunten

3. Encryptie
    - Onderzoek welke communicatie precies versleuteld is en tot welke informatie de beheerders van de leverancier toegang hebben. Bij end-to-end-encryptie zouden alleen de deelnemers van een vergadering toegang tot de inhoud moeten hebben.
    - Controleer ook de instellingen. Niet altijd staat encryptie standaard ingeschakeld.
    - Ga ook na wat gebeurt met de encryptie wanneer een deelnemer aan een online vergadering inbelt per eigen telefoon / consumenten applicatie. Dit kan resulteren in de uitschakeling van de versleutelde verbinding die staat ingesteld.
    - De mogelijkheid om een wachtwoord te genereren voor toegang tot de vergadering. Als de mogelijkheid er is, gebruik het dan altijd.

4. De risico’s van de werkplek

Let op wat in beeld en geluid bereik is tijdens gesprek. Haal vertrouwelijke documenten en informatie op bijvoorbeeld whiteboards uit het zicht.

4. Beeldschermzorg aandachtspunten

5. Gebruikersinstructie

- Wijzen van patiënt op risico's / laten bevestigen
- Delen van informatie/documenten
- Werkplek en wat is zichtbaar/hoorbaar bij beeldbellen
- Bij chat: advies na elk gesprek de chathistorie te wissen
- Bij meerdere personen: de organisator dient deelnemers te controleren en identificeren. Tevens de deelnemers wijzen op de te bespreken informatie en wat er van de deelnemers wordt verwacht op het gebied van vertrouwelijkheid.
- Het beperken van de mogelijkheden om een scherm te delen tot de host van de vergadering of tot een persoon die door de host wordt aangewezen. Hiermee wordt voorkomen dat een deelnemer per ongeluk zijn scherm deelt.

4. Beeldschermzorg aandachtspunten

6. Verwerkersovereenkomst

- elke tool vraagt de nodige inrichting om daadwerkelijk veilig en compliant te zijn.
- in de verwerkersovereenkomst - als onderdeel van het contract – maak je afspraken
  - welke instellingen zijn voor verwerker (de leverancier van de tool)
  - welke encryptie techniek gebruikt (blijft) worden
  - wat de verwerker doet met de data die je gebruikt.

Gebruik eventueel het model van Actiz:

https://www.actiz.nl/ouderenzorg/privacy-en-avg-/verwerkersovereenkomst-met-inleiding-en-toelichting-handreiking-en-flow-chart

4. Achtergrondinformatie

Tip: Actiz rapport beeldbel applicaties eind maart 2020 (generieke oplossingen):
https://www.actiz.nl/informatisering/zorgtechnologie/hulpmiddelen-beeldbellen

• Microsoft Teams	+
• Zoom	-
• Microsoft Skype	- (business variant wel beter)
• Google Hangouts	gratis versie niet (commercieel), zakelijk (hangouts meet) wel
• Signal	+
• Whereby	-
• Microsoft Kaizala	-

Conclusies: 1) zakelijke variant beter, 2) pas op met constructie zorgverlener zakelijke variant en cliënt consumenten variant en 3) sluit niet aan op zorgproces

4. Achtergrond Whatsapp en Facetime

Beiden niet veilig genoeg bevonden voor zorg-inhoudelijke informatie:

- Whatsapp videobellen is wel eind-tot-eind versleuteld.
- Whatsapp heeft geen toegang tot de inhoud van de gesprekken, maar verzamelt wel data over het gebruik, zoals met wie je belt, wanneer en hoe lang.
- Er gaat nog steeds informatie naar Facebook over apparaatgegevens, gebruik van diensten etc.
- Facetime vergelijkbare argumentatie maar dan van Apple

Zoals eerder aangegeven:
Zorg dat je voor dergelijke tools een risico analyse hebt gedaan en opgeslagen en dat je patiënt om toestemming vraagt en deze ook vastlegt. Verder gebruikersinstructie.

4. Praktische tips voor mail en chat

Veel hulpverleners willen en zullen ook uitgebreider gebruik willen maken van e-mail en chat in deze tijden.

Voor veilige e-mail en chat heeft NEN een technische afspraak ontwikkeld: NTA 7516 (kosteloos te downloaden). Certificatie voor leveranciers gaat binnenkort van start.

In de tussentijd zijn bij Informatieberaad hulpmiddelen voor implementatie te vinden:
https://www.informatieberaadzorg.nl/over-het-informatieberaad/publicaties/publicaties/2019/12/16/index

Denk aan groepsmailboxen, encryptie van bijlagen, intrekken van berichten, archiveren en opschonen etc.

Bijlage SET 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

Bijlage SET 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.

Bijlage SET 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.

bakertilly

SET Stimuleringsregeling E-health Thuis

VitaValley

Dank voor uw aandacht

Pim Ketelaar – Programmadirecteur
pketelaar@vitavalley.nl

Pasquelle van Ruiten – Programmamanager
pvanruiten@vitavalley.nl

Sanne Kok – Programmamanager
skok@vitavalley.nl

Dorien Faber – Programma- & Event assistent
dfaber@vitavalley.nl