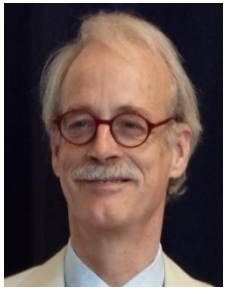
Veiligheid op de digitale snelweg

Beer Franken, Hans van Hemert

7 december 2017

Hans van Hemert



Achtergrond

- Publiek recht
- Beleid en management gezondheidszorg

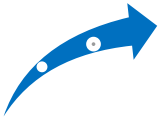
- Sinds 2006 informatiebeveiliging, gegevensbescherming
- Albert Schweitzer ziekenhuis
- Maasstad Ziekenhuis, Coöperatie Zorg op Zuid
- Auditeren informatiebeveiliging in de zorg vanaf 2012
- Voorbereiding AVG vanaf 2015

Vragen

Hans van Hemert
06 4135 6753
hans@vanhemert-zorgrecht.nl

Beer Franken, Piasau
06 5534 7977
beer.franken@piasau.nl

Ontwikkelingen in de zorg



- Explosieve groei digitaal verkeer: zorgnetwerken, patiëntinteractie
- Bezuinigingen, diversiteit verdienmodellen
- Groeiende complexiteit, afhankelijkheid, kwetsbaarheid

- Behoud vertrouwen Patiënt
  Zorgverlener
  Leverancier, derden … maatschappelijk vertrouwen

Naar vertrouwde groei in het digitale verkeer

Enkele verkeersregels

- Gegevensbescherming (AVG / Wbp)
- Medische behandelingsovereenkomst (wgbo)
- Kwaliteit van de zorg (wkkgz)
- Cliëntrechten bij elektronische verwerking van gegevens
- Wet medische hulpmiddelen (wmh)

- Logius-DigiD, UZI-CIBG, NCSC etc

NEN7510 – Informatiebeveiliging in de zorg

Buzz-vraag

Wie heeft NEN7510 Geïmplementeerd

→ Gevraagd uw inschatting voor uw organisatie

4 – Geheel	90% - 100%
3 – Grotendeels	66% - 90%
2 – Gedeeltelijk	33% - 66%
1 – Onbekend of beperkt	< 33%

Implementatie - NEN7510 – Informatiebeveiliging in de zorg?

Prioriteiten en (zelf-)evaluatie

- NVZ-toetsingskader 2010: NVZ - CBP / IGZ
- NEN7512 / NEN7513: NEN - AP
- ICT assessment DigiD: Logius
- Zekere zorg 3 (zwaarwegend)

- Citi audit (commissie intercollegiale toetsing informatiebeveiliging)
- Benchmark - gereedschap NVZ
- Certificering - in ontwikkeling

NEN7510 – Implementatie

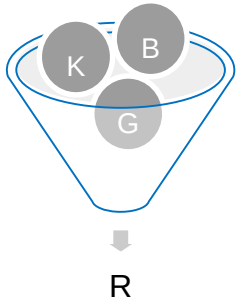
Beveiliging gebaseerd op risico

- Aard en omvang gegevensverzameling: ziekenhuis
  - Bijzondere persoonsgegevens: gezondheid, BSN,
    Maatschappelijk werk, Psychiatrie, infectiezieken, erfelijkheid,etniciteit etc.
  - Honderdduizenden tot meer dan een miljoen patiënten

  - Risico's
    - > Schade gezondheid; stigmatisering, uitsluiting, identiteitsfraude, gewone hinder
    - > Beschadiging gegevens, stagnatie / uitval zorgproces, imago

Groot to zeer groot risico

Integrale risicoanalyse

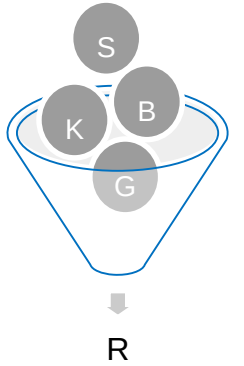


- Mens
- Apparatuur
- Programmatuur
- Gegevens
- Omgeving
- Organisatie
- Diensten

Kansen ?
Bedreigingen ?
Kwetsbaarheden ?
Gevolgen ?
Benodigde maatregelen ?
Effect van maatregelen ?
Restrisico – Accepteren ?

Diverse, verschillende benaderingen

Risicoanalyse in samenwerking



- Mens
- Apparatuur
- Programmatuur
- Gegevens
- Omgeving
- Organisatie
- Diensten

Kansen samen ?
Bedreigingen samen ?
Kwetsbaarheden samen ?
Gevolgen samen ?
Benodigde maatregelen samen ?
Effect van maatregelen samen ?

Restrisico – Accepteren ?

Risicoanalyse → vergelijkbaar met partners

Buzz-vraag

Wie heeft een actuele, integrale risicoanalyse beschikbaar?

→ Gevraagd uw inschatting voor uw organisatie

4 – Zeer recent	2017
3 – Actueel	2014 - 2016
2 – Al wat ouder	2012 - 2013
1 – Nog ouder, onvolledig, onbekend	

Risicobeoordeling ?

Informatiebeveiliging – toepassen

• Zorgverlener	Prestatiedruk
• Projecten:	Realisatiedruk
• Beheer:	Tijdsdruk
• Management	Budgetdruk
• Medewerker	Werkdruk
• Leverancier	Verkoopdruk
• Informatiebeveiliging	Verantwoordingsdruk

Presteren, zonder tijd om te puzzelen

NEN7510 - informatiebeveiliging

4 Norm als geheel ***breed*** geïmplementeerd en ***structureel*** gecontroleerd, ***aangetoond***

3 Norm als geheel geïmplementeerd en op ***kritische*** plaatsen gecontroleerd, ***aangetoond***

2 Norm als geheel gedefinieerd en geïmplementeerd

1 Ad Hoc en niet aantoonbaar bepaald, gecontroleerd

Volwassenheid in informatiebeveiliging

Buzz-vraag

Wie heeft welke volwassenheidsniveau

→ Gevraagd uw inschatting voor uw organisatie en de norm als geheel

1 – Adhoc

2 – Gedefinieerd en geïmplementeerd

3 – Gedefinieerd op ***kritische*** plaatsen ***gecontroleerd, aangetoond***

4 – Gedefinieerd en, ***breed, structureel gecontroleerd***, ***aangetoond***

Uw niveau van volwassenheid ?

Informatiebeveiliging

Als dit uw APK was …

Is uw organisatie
klaar voor de digitale snelweg?

Wordt vervolgd …

Informatiebeveiliging - Tweedelijns

Beer Franken