Sneldiagnose

Landelijk Doorverwijzen

Alpe d'HuZes

Verwijsoplossingen op juridische hoofdlijnen

Om tot een selectie relevante implicaties van wet- en regelgeving op de ICT architecturen te komen, is eerst een inventarisatie en overzicht gemaakt

1. Inventarisatie relevante wet- en regelgeving

- Contact met experts over relevante wetten en normen
- Van de onderlinge samenhang tussen wetten en normen is een weergave gemaakt, deze wordt later in deze presentatie besproken

2. Overzicht impact bepalingen per architectuur

- Overzicht van 72 bepalingen met technische of organisatorische invloed op de invulling van ICT architecturen

3. Selectie relevante bepalingen

- De bepalingen met de grootste impact zijn vervolgens in deze presentatie belicht
- Ook de verschillen in implicatie per ICT architectuur worden besproken
- Als laatste wordt een grove inschatting gemaakt van de Privacy Impact Assessment voor de verschillende architecturen

De wet- en regelgeving bestaat onder andere uit direct verplichte wetten en indirect verplichte normen

Wetten

- Wet bescherming persoonsgegevens (Wbp)
- Wet geneeskundige behandelsovereenskomst
- Wet gebruik burgerservicenummer in de zorg
- Wetsvoorstel 'wet gebruik burgerservicenummer in de zorg' van minister Schippers

Normen

- Gedragscode elektronische gegevensuitwisseling (EGIZ)
- NEN 7510
- NEN 7512
- NEN 7513 (in ontwikkeling)
- NEN 7521
- Richtlijnen over patiëntendossiers
- Richtlijn overdracht medicatiegegevens in de keten

- Privacy Impact Assesment

- Europese norm voor organisaties die persoonsgegevens willen verwerken

- Bevat een vragenlijst met zeven categoriën; deze is bedoeld om de belangrijkste risico's op het gebied van privacy in een vroeg stadium in kaart te brengen

De normen volgen in grote mate uit de wetgeving; in onderstaande slide een overzicht van de onderlinge verhoudingen

Wet bescherming persoonsgegevens (Wbp)
-Voorschriften over verwerking van persoonsgegevens van burgers
-Van toepassing op alle vormen van verwerking

Overlappen deels

Wet geneeskundige behandelings-overeenkomst
-Stelt de wederzijdse rechten en plichten van patiënten en zorgverleners
-Bedoeld om positie van de patiënt te versterken

Wet gebruik burgerservicenummer in de zorg
Schrijft voor hoe zorgverleners een persoon eenduidig moeten identificeren en de kwaliteit van gegevensuitwisseling te verbeteren

Wetten

Normen

NEN 7510
-Norm voor organisatie en borging informatiebeveiliging in de zorg
- Algemene norm, indien voldaan -> WBP ook voldaan

Gedragscode elektronische gegevensuitwisseling (EGIZ)
-Praktische normen voor gebruik van ICT in de zorg
-Interpretatie van Wbp en WGBO

Richtlijnen over patiëntendossiers
-Specifieke richtlijnen nav de dossierplicht zoals beschreven in WGBO
-Beschrijft drie richtlijnen voor verschillende beroepsgroepen

NEN 7512
- Aanvulling op 7510
- Risico-classificatie en uitwerking eisen betreffende identificatie en authenticatie

NEN 7513
-Aanvulling op 7510
- Van toepassing op transport-beveiliging
- Eisen toegangs-registratie zorgverleners bij inzage in EPD's

NEN 7521
-Aanvulling op 7510
- Beschrijft gedetailleerde toestemming en afstemming door patiënt

Richtlijn overdracht medicatiegegevens in de keten
-Doel is het voorkomen van fouten bij overdracht van medicatiegegevens tussen zorgprofessionals in de zorgketen en het vergroten van patiëntveiligheid
-Richtlijn is van toepassing op iedere situatie waarin medicatie wordt voorgeschreven/gestopt/gewijzigd

Nictiz: Wet- en regelgeving in de zorg, 2013

SOULVE

Uit het onderzoek volgen de volgende hoofdbevindingen

- De wet- en regelgeving is omvangrijk, bestaat uit meerdere afzonderlijke documenten en is weinig inzichtelijk
- Wetgeving is niet heel specifiek; de duidelijkere richtlijnen zijn niet formeel juridisch afdwingbaar. De richtlijnen zijn echter wel de professionele standaard; in wgbo wordt beschreven dat er gehandeld moet worden als goed zorgverlener. Op het moment voldoen veel instellingen niet aan de wet- en regelgeving
- Als het wetsvoorstel van minister Schippers aangenomen wordt, zullen de NEN richtlijnen in grotere mate wettelijk bindend worden

- De toepassing van de wet- en regelgeving is ingewikkeld; kleine verschillen tussen ICT architecturen (bijvoorbeeld Microsoft Healthvault & medischegegevens.nl) kunnen grote verschillen in compliance met de regels tot gevolg hebben. De inrichting van een oplossing bepaalt hoe de regels gelden
- Geen enkele oplossingsrichting voldoet volledig aan de wettelijke vereisten. IHE-XDS komt het dichtst in de buurt. Het ontbreekt echter aan grootschalige uniformiteit van bepaalde IHE-profielen ('Basic Patiënt Privacy Concent' (IHE-BPPC) en 'Cross-Enterprise User Assertion' (IHE-XUA)).

- Als aan de technische voorwaarden is voldaan, ligt er nog een grote verantwoordelijkheid bij de invoerende instantie. Er zijn meerdere organisatorische vereisten bij wet geregeld (v.b.: periodieke controle van logging-gegevens)
- PGD omzeilt veel van deze organisatorische verantwoordelijkheden, omdat de patiënt het dossier beheert (staat tegenover dat een PGD het brondossier nog niet lijkt te kunnen vervangen)

De wet- en regelgeving is bekeken in de context van vier generieke ICT architecturen; er wordt per architectuur uitgegaan van bepaalde algemene karakteristieken

Direct

- Hierbij worden berichten direct tussen zorgverleners verzonden.
- Stappenplan directe verzending: A moet weten wie B is → A initieert de communicatie → A stuurt → B ontvangt → B is afhankelijk van A
- Voorbeeld is Secure-eMail

Indirect

- Gegevens worden in een tijdelijke opslag geplaatst. De ontvangende zorgverlener ontvangt een notificatie en kan de gegevens aan de hand hiervan uit de opslag halen. Alleen de ontvangende zorgverlener kan de opgeslagen gegevens inzien. Opslag wordt door een derde partij beheerd
- Stappenplan indirecte verwijzing: A moet weten wie B is → A initieert de communicatie → A stelt B op de hoogte → A stuurt, B haalt op → B is afhankelijk van A
- Voorbeeld is Evocs

Registry - repository

- Organisatie A geeft in een central registry aan te beschikken over bepaalde patiëntgegevens en geeft tevens aan waar die zijn te vinden. B kan de gegevens a.d.h.v. de registry vinden en ophalen
- Stappenplan registry/repository: A hoeft niet te weten wie B is → A publiceert bericht (vult index) → A plaatst patiëntgegevens in repository (lokaal of centraal) → Patiëntgegevens blijven langdurig in repository → B vraagt waar info beschikbaar is via index → B haalt patiëntgegevens op uit repository
- Voorbeelden zijn (IHE-)XDS en LSP

Persoonlijk gezondheidsdossier

- De patiëntgegevens staan in een centraal dossier, waar de patient toegang toe heeft. De patient beheert de gegevens en kan dus beslissen wie welke gegevens in kan zien. De gegevens staan in een cloud, de faciliteit wordt beheerd door een derde partij.
- A stelt patiëntgegevens ter beschikking aan de patiënt → Patiënt slaat gegevens op in eigen PGD → Patiëntgegevens blijven in PGD → Patiënt geeft B toegang tot PGD
- Voorbeelden zijn Microsoft Healthvault en medischegegevens.nl.

Welke artikelen hebben over alle ICT architecturen het meeste invloed?

Wet/norm	*Artikel*	Implicatie
Wbp	*13 – logging*	Logging van gegevens en de periodieke controle hierop is belangrijk voor compliance met het Wbp
Wbp	*21 – autorisatie*	Autorisatie op basis van functie en werkcontext op het moment gedoogd, maar in de toekomst waarschijnlijk niet voldoende: autorisatie dient te gebeuren nadat rechtstreekse betrokkenheid is vastgesteld
Wbp	*13 (College Bescherming Persoonsgegevens: 2013)*	Cbp benadrukt het belang van goede structuur om alleen werknemers met behandelrelatie toegang te geven: voor zowel administratief personeel, systeembeheerders en niet-betrokken specialisten dient een systeem opgesteld te worden
WGBO	*457 – toestemming*	Push oplossingen impliciete (veronderstelde) toestemming voldoende Pull expliciete toestemming nodig. In WGBO is dit nog niet zo specifiek beschreven, onderscheid push/pull volgt uit EGIZ
WGBO	*457 – behandelrelatie*	Alleen delen van informatie met andere zorgaanbieders in de behandelrelatie, de aanwezigheid van een behandelrelatie is niet altijd duidelijk
Wijzigings-voorstel 'clientenrechten bij 'Wbsn-z	*Nog in behandeling*	Mogelijke wetswijziging die het in de toekomst verplicht stelt om patiënten digitale inzage te geven in hun dossier
NEN 7510	*Vertrouwelijkheid*	De verantwoordelijke zorgaanbieder moet vertrouwelijkheid kunnen garanderen, onder andere door een beveiligde verbinding tussen verwijzende partijen. Organisatorische en up-to-date technologische maatregelen moeten genomen worden. Dit is momenteel nog een richtlijn en is daarom niet afdwingbaar

Bepaalde artikelen verschillen qua implicatie het meest over de verschillende architecturen; deze zijn hieronder weergegeven

Artikel	Bepaling	Direct	Indirect	Registry/repository	PGD
-	*De mogelijke Wsbn-z wetswijziging die verplicht tot digitale inzage van patiëntgegevens*	Biedt geen mogelijkheid tot inzage	Biedt geen snelle mogelijkheid tot inzage	Nog onduidelijk hoe eenvoudig het in deze architectuur te implementeren zou zijn	Inzage zou direct mogelijk zijn
WGBO 457	*Toestemming patiënt vereist*	Impliciete (veronderstelde) toestemming voldoende	Impliciete (veronderstelde) toestemming voldoende	Expliciete toestemming vereist	Impliciete (veronderstelde) toestemming voldoende
NEN 7513 & wetsvoorstel Schippers	*Logging*	Biedt mogelijkheid door de externe server	Biedt mogelijkheid door de externe server	IHE-XDS heeft uitgebreide standaarden om logging mogelijk te maken (ATNA)	Biedt mogelijkheid door de externe server
3.2/3.5 EGiZ	*Verantwoordelijkheid over de bewerker ligt bij zorgaanbieder, deze extra partij zorgt voor extra risico op schending van wetgeving*	Bewerker nodig	Bewerker nodig	Alleen bewerker in geval van centrale registry	Bewerker nodig
8.1 EGiZ	*Notificatie bij iedere toegang*	Erg moeilijk om in te stellen	Niet eenvoudig in te stellen	Technisch gezien mogelijk	Technisch gezien mogelijk
13 Wbp (College Bescherming Persoons-gegevens: 2013)	*Toegang administratieve- en systeemmedewerkers*	▪ Geen administratieve medewerkers betrokken ▪ Geen externe bewerker	▪ Vaak administratieve medewerkers ▪ Externe bewerker zou in theorie toegang hebben tot gegevens	▪ Systeem voor autorisatie bepaalt administratieve toegang ▪ In geval van centrale registry een externe bewerker met theoretische toegang	▪ Geen administratief medewerker toegang ▪ Externe bewerker zou in theorie toegang hebben tot gegevens

De Privacy Impact Assessment (PIA) komt voor de verschillende ICT architecturen voor het grootste deel overeen; in onderstaande figuur zijn zowel de overeenkomsten als de verschillen beschreven

Onderdelen PIA	Risico's die gelden voor alle architecturen	Risico's die afwijken
Het type project	- het gebruik maken van (relatief) nieuwe technieken in nieuwe contexten, - de grote hoeveelheid wet- en regelgeving waar de zorgverlener aan moet voldoen en - de grote hoeveelheid maatschappelijke belanghebbenden	- PGD heeft als aanvullende punt dat de patiënt als verantwoordelijke van het dossier gezien zou kunnen worden: de patiënt kan nooit aan regelgeving voldoen, wat de bewerker onevenredig veel macht over het proces geeft
Gegevens die gebruikt worden	- het feit dat de persoonsgegevens altijd gekoppeld moeten zijn aan een persoon (anonimisatie lastig) - het feit dat er gewerkt wordt met bijzondere persoonsgegevens gekoppeld aan een BSN - omdat de gegevens van kwetsbare groepen worden verwerkt	/
Partijen die betrokken zijn bij uitvoering project	- meerdere partijen die inzicht hebben in gegevens (ook organisatorisch punt) - de plaats van opslag van gegevens als die onder niet-Europese wetgeving valt	/
Verzamelen van gegevens	- het bestaan van een behandelrelatie kan in sommige gevallen onduidelijk zijn - als ICT architectuur eenmaal is geaccepteerd, is opt-out dan nog wel mogelijk?	/
Gebruik van gegevens	- onvoldoende kwaliteit (controle van gegevens) - het feit dat er vanuit meerdere bronnen wordt gewerkt, - behandelrelaties en gegevensoverdracht met externe partijen - mogelijkheden voor patiënten om hun gegevens in te zien/ te wijzigen.	- de wettelijke verplichting van de arts dat hij weet op basis waar de diagnose op gebaseerd. IHE-XDS verhoogt risico op twee problemen: iets uit xds halen verwijdert bewijslast en een overload aan informatie en daardoor relevant stuk informatie missen (en daaruitvolgende aanklachten)
Bewaren en vernietigen van gegevens	- beperkte mogelijkheden om gegevens te kunnen vernietigen -> in geval van vernietiging overal verwijderd? - de compleetheid van de vernietiging na de bewaartermijn	- PGD: is dit ook brondossier? Zo ja, kunnen gegevens dan volledig worden vernietigd?

SOULVE

Bijlagen

Bijlage A: Overzicht inschattingen experts op het gebied van security

De uitgangspunten waaraan een infrastructuur moet voldoen zijn in kaart gebracht, in een matrix zijn de infrastructuur opties gescoord tegen de uitgangspunten

ICT architectuur -> Specifieke aanbieder ->	**Direct** Secure-email	**Registry/ repository** LSP	**Registry/ repository** XDS	**Indirect** Postbus (niet IHE)	**PGD** -
Kan eisen wet- en regelgeving implementeren en bewaken [2]					
Ondersteunt richtlijn EGiZ					
Ondersteunt NEN 7512					
Ondersteunt alle typen zorggegevens					
Leverancier onafhankelijk	[3]				
Schaalbaar			[4]		
Gebaseerd op (inter)nationale standaarden					
Bewezen oplossingen en technologie					
Gedeelde informatie blijft binnen verantwoordelijkheidsgrenzen ziekenhuis		[5]	[5]	[5]	

[1]: Zie de bijlagen voor de volledige lijst met uitgangspunten.
[2]: Voor de score op dit uitgangspunt is er van uit gegaan dat de afspraken tussen de communicatiepartners bepalen of wordt voldaan aan wet- en regelgeving. De score geeft aan of met de infrastructuur deze afspraken ook bewaakt resp. afgedwongen kunnen worden.
[3]: Afhankelijk van encryptykey-server van de leverancier.
[4]: Koppeling registry's en repository's nog geen schaalbare oplossing
[5]: Eisen aan third party die de (tijdelijke) decentrale opslag host

- Voldoet volledige aan de uitgangspunten
- Kan aan de uitgangspunten voldoen, vraagt om procedure maatregelen
- Voldoet niet aan de uitgangspunten

SOULVE

Soulve Innovations
a Goeman Borgesiuslaan 77
t 3515 ET Utrecht
e 030-7531486
Bob.joormann@soulve.nu

Bob Joormann