www.pwc.nl

Digitale toegang tot het eigen medisch dossier: mogelijkheden voor een elektronische sleutel

Definitief

25 november 2011

A-2011-2087/OV/cdb/mp

pwc

Managementsamenvatting

Aanleiding en onderzoeksvragen

01 De Eerste Kamer heeft op 5 april 2011 het wetsvoorstel EPD-wet (Elektronisch Patiëntdossier) afgewezen en daarmee de invoering van een landelijk EPD een halt toegeroepen. Tegelijkertijd is door middel van motie Y gevraagd om standaardisatie van gegevensuitwisseling op regionale schaal en de uitvoering van een onderzoek naar het gebruik van een zorgpas om beter invulling te geven aan de zeggenschap van de zorgconsument over het eigen medisch dossier.

02 Dit rapport bevat de resultaten van het onderzoek dat is uitgevoerd ter verkenning van de mogelijkheden tot realisatie van een elektronische sleutel, waarmee invulling kan worden gegeven aan de rechten van zorgconsumenten ten aanzien van het eigen medisch dossier. Hierbij wordt onder het medisch dossier verstaan het dossier dat de hulpverlener inricht op grond van artikel 7:454 lid 1 BW uit de Wet op de geneeskundige behandelingsovereenkomst (WGBO). Het onderzoek richt zich op de toegang tot dit dossier. De opslag van of ontsluiting van gegevens door de zorgconsument valt buiten het onderzoek.

03 De volgende onderzoeksvragen worden beantwoord:

Nr	Vraag
1	Wat zijn de eisen en wensen van zorgconsumenten ten aanzien van een digitale invulling van de patiëntrechten voor het eigen medisch dossier en daaraan gerelateerd de juridische, functionele en technische eisen aan een elektronische sleutel voor zorgconsumenten?
2	Welke verschijningsvormen van een elektronische sleutel kunnen invulling geven aan de juridische en technische eisen inclusief de door de Eerste en Tweede Kamer geformuleerde wensen en wat zijn de ervaringen hiermee in het buitenland?
3	Welke verschijningsvormen zijn, gegeven de noodzakelijke bestuurlijke, financiële, organisatorische en technische maatregelen voor implementatie, het meest haalbaar?
4	Wat zijn de voor- en nadelen van een elektronische sleutel voor de verschillende belanghebbenden?
5	Welke implementatiedrempels staan de realisatie van een elektronische sleutel in de weg?
6	Hoe kunnen eventuele implementatiedrempels worden weggenomen?

04 Afgesproken is om het onderzoek in hoofdzaak uit te voeren als literatuuronderzoek. Daarnaast hebben wij gesproken met onder meer vertegenwoordigers van de Nederlandse Patiënten Consumenten Federatie (NPCF), de Diabetesvereniging Nederland, Nictiz, Collis en mevrouw mr. M. de Die (expert gezondheidsrecht).

05 De elektronische sleutel is in dit onderzoek als concept geoperationaliseerd door middel van de volgende twee componenten:

- Het ***toegangsmiddel:*** het identificatie- en authenticatiemiddel dat de zorgconsument moet gebruiken om de toegangsmethode te kunnen toepassen.
- De ***toegangsmethode:*** de wijze waarop een zorgconsument een digitale versie van het eigen medisch dossier kan inzien en opslaan, en vervolgens zijn overige patiëntrechten in praktijk kan brengen.

06 Toegangsmiddelen en toegangsmethodes kunnen in verschillende combinaties voorkomen.

Referentiekader

07 Om de onderzoeksvragen te kunnen beantwoorden, hebben wij een referentiekader ontwikkeld met daarin de eisen waaraan de elektronische sleutel moet voldoen:

- De patiëntrechten beschreven in de bestaande wetgeving en de gewenste aanvullingen hierop, geformuleerd door andere belanghebbenden zoals de Eerste en Tweede Kamer en patiëntenverenigingen. Deze eisen en wensen hebben wij benoemd als *juridische eisen*: welke patiëntrechten moeten worden geborgd?
- De *functionele eisen:* wat moet een zorgconsument met een elektronische sleutel kunnen?

- De *technische eisen:* waaraan moeten toegangsmiddelen en -methodes voldoen om patiëntrechten ten aanzien van het eigen medisch dossier te borgen?

08 Op deze manier zijn aspecten als privacy, actualiteit, regierol van de patiënt, gebruiksvriendelijkheid en toekomstgerichtheid vastgelegd in de bovenstaande eisen. Een overzicht is opgenomen in bijlage A bij dit rapport.

Drie toegangsmiddelen getoetst

09 In eerder onderzoek was op basis van vergelijkbare eisen al een selectie gemaakt uit een groter aantal toegangsmiddelen. Daaruit kwamen twee toegangsmiddelen als passend naar voren. Daaraan is op verzoek van de Eerste Kamer een derde toegangsmiddel – de zorgpas – toegevoegd. Dit betekent dat de volgende drie potentiële toegangsmiddelen (identificatie- en authenticatiemiddelen) aan het referentiekader zijn getoetst:

a) De zorgpas: een smartcard, specifiek voor zorgtoepassingen, met daarop een persoonlijk certificaat met een geheime sleutel voor de zorgconsument. De zorgpas zou ook als gegevensdrager gebruikt kunnen worden (met limiteringen aan de opslagcapaciteit).
b) De elektronische Nederlandse Identiteitskaart ofwel eNIK: een toegangsmiddel dat gebruikt kan worden bij een beveiliging op het niveau van DigiD-hoog. De eNIK is niet specifiek voor de zorg bedoeld, maar beoogt een breder toepassingsgebied. De eNIK wordt momenteel ontwikkeld onder verantwoordelijkheid van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties.
c) De DigiD Middenvariant met face-to-faceuitgifte van een activatiecode, aan te vullen met een conversietabel (kort: DigiD Middenvariant). Dit toegangsmiddel past bij DigiD met vertrouwensniveau midden en bevat een combinatie van een gebruikersnaam, wachtwoord en SMS-code. In verband met de GSM-A5/1-kwetsbaarheid[1] van DigiD Midden is het toegangsmiddel aan te vullen met een procedure die inhoudt dat gebruikers een face-to-facecontrole doorlopen en een persoonlijke conversietabel krijgen om de verkregen SMS-code om te zetten.

10 De *zorgpas* voldoet aan alle juridische, functionele en technische eisen. Het nadeel is dat de zorgpas momenteel nog niet beschikbaar is en niet op korte termijn ingevoerd kan worden, onder meer omdat er nog geen infrastructuur voor aanwezig is. Het gebruik van de zorgpas vergt naar alle waarschijnlijkheid een kaartlezer.

11 Voor de *eNIK* geldt hetzelfde: het toegangsmiddel voldoet aan alle eisen maar is nog niet beschikbaar en heeft een lange implementatieperiode, ook vanwege het ontbreken van een infrastructuur. Ook het gebruik van de eNIK vergt naar alle waarschijnlijkheid een kaartlezer.

12 De *DigiD Middenvariant met face-to-faceuitgifte van een activatiecode, aan te vullen met een conversietabel* zal met toevoeging van beperkte functionaliteit eveneens voldoen aan alle eisen. Deze extra functionaliteit moet een oplossing bieden voor het feit dat zorgconsumenten momenteel geen mogelijkheid hebben om berichten te ondertekenen, bijvoorbeeld om derden inzage in het dossier te verlenen. Zorgpas en eNIK kunnen deze mogelijkheid wel bieden, voor de DigiD Middenvariant zou toestemmingsfunctionaliteit op basis van authenticatie in plaats van ondertekening plaats moeten vinden. Een verdere uitleg hiervan is gegeven in de rapportage. Het toegangsmiddel zou op relatief korte termijn beschikbaar kunnen zijn gezien het hergebruik van infrastructuur[2], waardoor de investeringen ook lager zouden kunnen blijven dan in de andere varianten.

Twee toegangsmethoden getoetst

13 In het onderzoek zijn de volgende twee toegangsmethoden aan het referentiekader getoetst:

a) Directe toegang van de zorgconsument tot het digitale medisch dossier. Zorgconsumenten krijgen toegang binnen een gecontroleerde omgeving. Dit kan een beveiligd webportaal zijn waarmee de digitale medische gegevens bij de zorgverlener worden ontsloten, al dan niet via een samenwerkingsverband tussen zorgverleners zoals een schakelpunt. De verantwoordelijkheid voor de gegevens en de toegang ligt in dit geval bij de zorgverlener, de gegevens blijven onder beheer van de zorgverlener.

[1] Risicoanalyse EPD-DigiD - Naar aanleiding van de A5/1 kwetsbaarheid in GSM, 30 juni 2010, referentie: 2010-1400/OV/ev/mp (de SMS-codes bleken relatief eenvoudig gehackt te kunnen worden).
[2] Zowel de DigiD Middenvariant met face-to-faceuitgifte van een activatiecode aangevuld met een conversietabel als de eNIK komen naar alle waarschijnlijkheid alleen beschikbaar voor personen met een BSN.

b) Indirecte toegang via een door een derde partij[3] beheerd portaal. Toegang tot het digitale medisch dossier wordt verleend via een patiëntenportaal als intermediair tussen de zorgverlener en de zorgconsument. Het portaal verzamelt gegevens uit dossiers van individuele hulpverleners. De verantwoordelijkheid voor de gegevens en de toegang ligt bij deze methode bij de derde partij of de zorgconsument.

14 Een aantal methoden hebben wij niet onderzocht, omdat ze niet als toegangsmethoden in de zin van dit onderzoek te beschouwen zijn. Zo zijn de zogeheten digitale medische dagboeken niet meegenomen omdat deze geen toegang geven tot de medische gegevens die bij zorgverleners beschikbaar zijn. Zorgconsumenten kunnen hooguit medische gegevens die zij op papier hebben verkregen overnemen in het dagboek.

De mogelijkheid van opslag op een lokale gegevensdrager voldoet niet aan eisen aan actualiteit van gegevens en raadpleging in noodsituaties

15 De opslag van medische gegevens op een persoonlijke gegevensdrager is verder niet meegenomen in de analyse van de verschillende toegangsmethoden omdat:

- Niet voldaan kan worden aan de eis ten aanzien van de directe actualisatie van medische gegevens. Door het ontbreken van een (continue) verbinding met het zorginformatiesysteem van de zorgverlener kunnen medische gegevens maar in beperkte mate actueel worden gehouden. Actualiteit van gegevens is zeer belangrijk voor zowel de zorgconsument als de zorgverlener. Als gegevens niet actueel zijn kan de zorgconsument niet in voldoende mate actie ondernemen op de gegevens waardoor de mogelijkheid tot 'patient empowerment' wordt beperkt. Daarnaast zal de zorgverlener geen beslissingen kunnen baseren op gegevens die niet actueel zijn. De kans op fouten die voorkomen hadden kunnen worden door een actuele informatievoorziening zou hierbij vergroot worden.
- Niet goed voldaan kan worden aan de eis ten aanzien van de mogelijkheid om medische gegevens in het geval van nood beschikbaar te maken. Aangezien de toegang tot de gegevensdrager moet worden beveiligd tegen onbevoegde raadpleging kunnen de gegevens (bijvoorbeeld door het invoeren van een pincode) in eerste instantie alleen door de zorgconsument zelf worden ingezien. Als de patiënt buiten bewustzijn is kunnen de gegevens daardoor niet lokaal worden ingezien in geval van nood. Ook blijkt uit ervaringen met de Duitse gesundheitskarte dat 70% van de zorgconsumenten zijn pincode niet meer wist bij poging tot raadpleging van de pas gedurende de behandeling met als consequentie dat de gegevens niet beschikbaar zijn.
- Niet eenvoudig kan worden voldaan aan de eis wat betreft het gestandaardiseerd ontsluiten van medische gegevens. De opslag van medische gegevens op gegevensdragers als een USB-stick, mobile devices of een zorgpas biedt stand-alone in de huidige situatie geen ontsluitingswijze voor de medische gegevens die aanwezig zijn bij de zorgverleners omdat er geen koppeling met informatiesystemen van zorgverleners bestaat. Er dienen hiervoor speciale interfaces en software ontwikkeld te worden om het automatisch kopiëren van de medische gegevens in het informatiesysteem bij de zorgverlener naar de gegevensdrager van de zorgconsument mogelijk te maken. Deze functionaliteit moet daarnaast breed worden geïmplementeerd bij zorgverleners.

16 Opslag van medische gegevens op gegevensdragers als een USB-stick of een zorgpas biedt stand-alone evenmin toegang tot het medisch dossier. Omdat de zorgconsument bovendien geen (continue) verbinding heeft met het zorginformatiesysteem van de zorgverlener kunnen de medische gegevens maar in beperkte mate actueel worden gehouden. De actualiteit van gegevens is zeer belangrijk in het ondersteunen van het behandelingsproces. Dit geldt voor zowel de consument (die zelf actie kan ondernemen op inzage in de gegevens) als de zorgverlener (die moet kunnen vertrouwen op de actualiteit om beslissingen in de behandeling te kunnen nemen).

17 De *directe* toegangsmethode voldoet aan alle eisen uit het referentiekader en heeft als voordeel dat de zorgconsument altijd toegang heeft tot de meest recente gegevens en direct verzoeken tot wijzigingen of aanvullingen kan doen. Een nadeel is dat zorgconsumenten voor een totaaloverzicht van de eigen medische gegevens moeten inloggen op soms vele verschillende webportalen van individuele zorgverleners. Dit is alleen op te lossen door verregaande samenwerking tussen hulpverleners, met regels voor een gestandaardiseerde gegevensuitwisseling.

[3] Bijvoorbeeld een commerciële partij, een zorgverzekeraar of een patiëntenvereniging.

18 De *indirecte* toegangsmethode via een door een derde partij beheerd portaal voldoet eveneens aan alle eisen uit het referentiekader. Deze methode heeft als voordeel dat het medisch dossier integraal inzichtelijk is (ook van belang in noodsituaties). Ook deze methode vergt echter samenwerking en standaardisatie. Ten opzichte van de directe toegangsmethode heeft deze derde-partijmethode als nadeel dat private partijen, met uitzondering van zorgverzekeraars, niet net als hulpverleners de mogelijkheid hebben om gegevens op het niveau van een individuele zorgconsument aan elkaar te koppelen gegeven de bescherming van persoonsgegevens. Verder biedt het werken met private partijen de zorgconsument niet de garantie dat werkelijk alle gegevens worden meegenomen en is ook de toestemmingsprocedure omslachtiger. De gegevens binnen het portaal dienen ten slotte dusdanig frequent te worden gesynchroniseerd met de gegevens uit de medisch dossiers dat ze altijd voldoende actueel zijn.

Voor- en nadelen toegangsmiddelen en -methoden getoetst aan verwachte effecten

19 Nu zowel de onderzochte toegangsmiddelen als de onderzochte toegangsmethoden aan de eisen uit het referentiekader voldoen, spelen bij het maken van een keuze vooral aspecten als beschikbaarheid en beleidsafwegingen een rol. Om de keuze verder te ondersteunen, zijn de toegangsmiddelen en -methoden onderzocht op basis van de volgende vier categorieën effecten:

a) Bestuurlijke effecten: Wie is verantwoordelijk voor de implementatie, welke additionele wet- en regelgeving is noodzakelijk en hoe moet toezicht worden gehouden op de naleving hiervan?
b) Financiële effecten: Welke kosten moeten worden gemaakt voor het ontwerp ontwikkeling, bouw, uitgifte en beheer van de betreffende verschijningsvorm?
c) Organisatorische effecten: In hoeverre kan de verschijningsvorm aansluiten bij de bestaande zorgprocessen en de interactie tussen zorgverleners en zorgconsumenten?
d) Technische effecten: Welke apparatuur, programmatuur en gegevens zijn noodzakelijk voor de realisatie van de betreffende verschijningsvorm en hoe wordt de interoperabiliteit tussen verschijningsvormen geborgd?

20 De *zorgpas* vergt naar verwachting grote investeringen door partijen in de zorgsector: kosten voor de pas zelf, de kaartlezers, de nieuw op te zetten centrale identificatie- en authenticatie-infrastructuur, maar ook het proces van ontwerp en uitgifte. Er moet een volledig nieuwe infrastructuur worden ontworpen, terwijl het toepassingsgebied beperkt is tot de zorgsector. Uit een vergelijkbaar systeem in Duitsland blijkt weliswaar dat er ook sprake is van financiële baten (voor zorgverzekeraars) maar de terugverdientijd is zeer lang. Bovendien blijkt het systeem risico's in zich te bergen, zoals het vergeten van de zorgpas door de zorgconsument. Een vanuit overheidswege uitgegeven toegangsmiddel specifiek voor het verlenen van toegang tot het eigen medische dossier sluit onvoldoende aan bij de interactie tussen zorgconsument en zorgverlener. Uit onderzoeken in het buitenland blijkt dat mede daardoor de zorgpas door de zorgconsument maar beperkt wordt gebruikt.

21 Ook de eNIK vergt grote investeringen op dezelfde gebieden als de zorgpas waarbij de kosten voor de infrastructuur worden gedragen door de overheid. De kosten om de eNIK in te bedden in toegangsmethoden voor zorgtoepassingen komen dan voor rekening van de zorgverleners. Het toepassingsgebied voor de eNIK is breder dan die voor de zorgpas. Hierdoor kunnen kostenvoordelen ontstaan waarbij verschillende toepassingen gebruik maken van dezelfde investeringen. Voor het benodigde face-to-face uitgifteproces voor de eNIK kan gebruik worden gemaakt van de uitgifteprocessen die hiertoe al zijn ingericht voor de uitgifte van de nu geldende identiteitsdocumenten bij de gemeenten. Daarnaast is een voordeel dat de besluitvorming voor de invoering van DigiD met authenticatieniveau hoog op basis van de eNIK door BZK al in gang is gezet. Nadeel is dat de ontwikkeling nog een aantal jaren zal vergen en door de vervangingsperiode pas vijf jaar na de invoering van de kaart de complete vervanging gereed zal zijn.

22 De *DigiD Middenvariant met face-to-faceuitgifte van een activatiecode* moet nog worden aangevuld met de conversietabel. Overigens bestaan daarvoor op het moment nog geen concrete plannen. Rekening houdend met de doorontwikkeling van de DigiD-variant die specifiek voor elektronische patiëntdossiers is ontworpen als reactie op de GSM A5/1-kwetsbaarheid zal het toegangsmiddel binnen ongeveer 1,5 jaar beschikbaar kunnen zijn. De kosten liggen naar verwachting lager dan die van de zorgpas en de eNIK, omdat een deel van het toegangsmiddel al is ontwikkeld.

23 Wat de toegangsmethoden betreft: de *directe* toegangsmethode sluit goed aan bij de zorgprocessen en interactie tussen zorgconsument en hulpverlener, zeker als met ingang van 1 januari 2013 de verplichting voor hulpverleners wordt ingevoerd om de zorgconsument langs digitale weg inzage te bieden in zijn dossier. Deze verplichting vergt investeringen (door de zorgverleners) in onder meer beveiliging van gegevens, en afspraken over bijvoorbeeld het markeren van informatie die de zorgconsument zelf heeft aangepast of toegevoegd. Voor de gegevensuitwisseling tussen zorgconsument en zorgverlener zijn technische standaarden nodig. Als zorgverleners samenwerken om tot een integraal dossier te komen, zijn ook voor deze samenwerking technische standaarden nodig.

24 De toegangsmethode via een *door derden beheerd portaal* kan eveneens – afhankelijk van de mogelijkheden van het portaal – goed aansluiten bij de zorgprocessen en interactiebehoefte. De methode vergt investeringen die vergelijkbaar zijn met die voor de directe methode, maar deze investeringen zullen geheel of gedeeltelijk voor rekening komen van de derde partij. Het bijeenbrengen van informatie vergt technische standaarden, en wordt bemoeilijkt door de genoemde barrière voor derde partijen om gegevens van individuele zorgconsumenten aan elkaar te koppelen. Mogelijk zijn voor de toegangsmethode via een door derden beheerd portaal extra standaarden nodig om een voldoende niveau van beveiliging en betrouwbaarheid te borgen. Daar staat tegenover dat derde partijen wellicht meer geneigd zijn om te zoeken naar innovaties en naar dienstverlening die uitgaat van de voordelen voor de zorgconsument.

Drempels voor belanghebbenden aanwezig

25 Welk toegangsmiddel en welke methode ook wordt gekozen, belanghebbende partijen kunnen drempels ervaren bij de implementatie.

26 Voor de zorgconsumenten zal het vooral gaan om het vertrouwen in de veiligheid en bruikbaarheid van het systeem. Hoge eisen aan toegangsmiddel en -methode gecombineerd met goede communicatie daarover en een adequaat toezicht op de naleving kunnen dit vertrouwen stimuleren. Daarnaast zullen zorgconsumenten de meerwaarde van toegang tot het medisch dossier willen ervaren. Uit buitenlandse voorbeelden blijkt dat dit vaak maar beperkt het geval is. Het kan daarom van nut zijn om de gebruiksmogelijkheden voor zorgconsumenten te vergroten door bijvoorbeeld een gebruiksvriendelijke procedure voor wijziging of aanvulling van het dossier te ontwikkelen.

27 Voor zorgverleners kunnen de benodigde investeringen een drempel vormen. Bovendien blijkt de gewenste samenwerking soms op problemen te stuiten. Als daardoor het vereiste niveau van beveiliging of functionaliteit niet wordt bereikt, kan een situatie ontstaan waarin zorgverleners tegenover een toezichthouder komen te staan.

28 Voor private partijen kan het ontbreken van de mogelijkheid om gegevens van individuele zorgconsumenten te koppelen door middel van het Burgerservicenummer een belangrijke drempel zijn. Daarnaast zullen zij altijd uitgaan van een kosten-batenanalyse die voor hen voordelig uitvalt. Mogelijk dat de situatie voor hen na invoering van de verplichting voor de zorgverleners om zorgconsumenten digitaal inzicht in hun dossier te bieden gunstiger wordt, omdat dan vanuit zorgverleners vraag naar het inrichten van een portaal kan ontstaan.

29 Voor de overheid kan het een drempel zijn dat voor een voldoende veilige en betrouwbare elektronische sleutel standaarden ontwikkeld moeten worden op het gebied van gegevens, beveiliging en uitwisseling, al dan niet deels uit te voeren door partijen buiten de overheid. Bovendien zal de overheid worden aangesproken op een adequaat toezicht op naleving van de standaarden.

Verlagen van drempels door groeistrategie mogelijk

30 Wij bevelen aan de drempels te verlagen door een groeistrategie te kiezen, waarin wordt toegewerkt naar implementatie van de eNIK wegens het hoge vertrouwensniveau, en in de tussentijd de DigiD Middenvariant met face-to-faceuitgifte van een activatiecode aangevuld met een conversietabel als aanvaardbaar alternatief wordt ingezet. De investeringen in DigiD behouden een deel van hun waarde als wordt overgegaan op de eNIK, omdat DigiD bruikbaar blijft voor toepassingen buiten de zorg waarvoor een middenniveau voldoende is. Op die wijze wordt de meest kostenefficiënte route gekozen.

31 Daarnaast bevelen wij aan dat de overheid in samenwerking met de andere belanghebbenden standaarden ontwikkelt, zodat de belangen van alle partijen kunnen worden ingebracht. Daarbij behoren voldoende

toezichtmogelijkheden voor het College bescherming persoonsgegevens. Aansluiting van portalen op bestaande gegevensuitwisseling tussen zorgverleners met het doel om te komen tot een integraal dossier kan plaatsvinden onder toezicht van de overheid.

32 Tot slot bevelen wij aan om de activiteiten te koppelen aan toch al lopende regelgevingtrajecten. De toekomstige verplichting voor zorgverleners om ook digitale gegevensuitwisseling tussen zorgverleners en zorgconsumenten mogelijk te maken, kan leiden tot verhoogde vraag naar portalen en dus een aantrekkelijker markt voor de betrokken partijen.

Inhoudsopgave

1. Introductie

1.1. Achtergrond en aanleiding

34 Op 5 april 2011 heeft de Eerste Kamer het wetsvoorstel EPD-wet afgewezen en moties X en Y[4] aangenomen. Door middel van motie X is de minister gevraagd om alle financiële, beleidsmatige en organisatorische steun bij de ontwikkeling van het LSP te staken. Motie Y vraagt aan de regering om standaardisatie van gegevensuitwisseling op regionale schaal en de uitvoering van een onderzoek naar het gebruik van een zorgpas om beter invulling te geven aan de zeggenschap van de zorgconsument over het eigen medisch dossier.

35 Als gevolg van de stemmingen in de Eerste Kamer heeft de minister aan de Tweede Kamer laten weten[5] dat de invulling van motie 68[6] (recht op inzage en aanvulling voor de zorgconsument van medische gegevens uitgewisseld via het LSP) komt te vervallen. Ten aanzien van motie 69[7] (de zorgconsument krijgt bij de uitgifte van medicijnen direct kostenloze inzage in papieren en/of elektronische vorm en recht op aanvulling) en motie 70[8] (aanvulling WGBO zodat zorgconsumenten per 1 januari 2013 recht hebben op inzage in en afschrift van hun gehele elektronische dossier bij de zorgverlener) heeft de minister aangegeven dat gelet op de Motie Y van de Eerste Kamer bezien zal worden hoe elektronische inzage in algemene zin nader wettelijk geregeld kan worden.

36 Tevens heeft de minister richting de Eerste Kamer laten weten[9] geen voorstander te zijn van een zorgpas gezien de ervaringen met de zorgpasproef eind jaren 90 in de regio Eemland. Hieruit kwam naar voren dat de uitgifte van zorgpassen en de integratie daarvan met zorgsystemen moeizaam verliep. Daarnaast sluit een zorgpas in deze vorm niet aan bij het zorgproces en geeft het een te grote uitvoeringslast.

37 In het overleg van 10 mei 2011 tussen de vaste Kamercommissie van de Eerste Kamer en de minister is door de commissieleden aangegeven dat het niet gaat om de zorgpas maar om een persoonlijke elektronische sleutel voor de zorgconsument met toegangs-, autorisatie- en opslagmogelijkheid[10].

38 In het beleidsdebat in de Tweede Kamer op woensdag 24 mei 2011[11] heeft de minister aangegeven een onderzoek te zullen laten uitvoeren naar de wijze waarop aan zorgconsumenten inzicht verschaft kan worden in de medische gegevens in de verschillende systemen van zorgverleners.

1.2. Doelstelling

39 De doelstelling van dit onderzoek is het uitbrengen van een advies over de mogelijkheden tot realisatie van een elektronische sleutel als toegangs-, autorisatie- en opslagmogelijkheid waarmee invulling kan worden gegeven aan de rechten van zorgconsumenten ten aanzien van het eigen medisch dossier.

40 De volgende onderzoeksvragen zijn leidend geweest voor de uitvoering van het onderzoek:

1. Wat zijn de eisen en wensen van zorgconsumenten ten aanzien van een digitale invulling van de patiëntrechten voor het eigen medisch dossier en daaraan gerelateerd de juridische, functionele en technische eisen aan een elektronische sleutel voor zorgconsumenten?
2. Welke verschijningsvormen van een elektronische sleutel kunnen invulling geven aan de juridische en technische eisen inclusief de door de Eerste en Tweede Kamer geformuleerde wensen en wat zijn de ervaringen hiermee in het buitenland?

---

[4] Moties EK 31.466, X en Y van het Kamerlid Tan c.s, voorgesteld 5 april 2011.
[5] Verzoek om stand van zaken brief Elektronisch Consumenten Dossier met kenmerk 2011Z05361/2011D13564, 11 april 2011, kenmerk: MEVA-U-3057580.
[6] Motie TK VAO, nr. 68 van het lid Omtzigt.
[7] Motie TK VAO, nr. 69 van het lid Kuiken.
[8] Motie TK VAO, nr. 70 van het lid Omtzigt.
[9] Reactie moties 29 maart 2011 en 5 april 2011 in een brief richting de Eerste Kamer, 11 april 2011, kenmerk: MEVA/ICT-3060636.
[10] Verslag van het mondeling overleg, EK 31.466, AB.
[11] Zie verslag op http://www.tweedekamer.nl/kamerstukken/verslagen/plenaire_vergadering_24_mei_2011.jsp#0

3. Welke verschijningsvormen, zijn gegeven de noodzakelijke bestuurlijke, financiële, organisatorische en technische maatregelen voor implementatie, het meest haalbaar?
4. Wat zijn de voor- en nadelen van een elektronische sleutel voor de verschillende belanghebbenden?
5. Welke implementatiedrempels staan de realisatie van een elektronische sleutel in de weg?
6. Hoe kunnen eventuele implementatiedrempels worden weggenomen?

1.3. Reikwijdte

41 Het onderzoek richt zich generiek op de wijze waarop de door middel van een elektronische sleutel op digitale wijze invulling gegeven kan worden aan de patiëntrechten ten aanzien van het eigen medisch dossier zoals deze zijn beschreven in de Wet op de geneeskundige behandelovereenkomst (WGBO) en de Wet bescherming persoonsgegevens (Wbp).

42 Ten aanzien van de ontsluiting van de digitale versie van het eigen medisch dossier van de zorgconsument valt alleen het medisch dossier zoals dit in het kader van de geneeskundige behandeling door de zorgverlener wordt bijgehouden binnen de reikwijdte van het onderzoek.

43 Ontsluiting van medische gegevens vanuit de zorgconsument richting de zorgverlener (het kan dan zowel gaan om gegevens die via de zorgconsument worden uitgewisseld tussen zorgverleners als gegevens die door de zorgconsument zelf aan het dossier worden toegevoegd) valt buiten de reikwijdte van de opdracht evenals de wijze waarop zorgconsumenten gegevens vastleggen ten behoeve van zelfzorg.

44 Dit onderzoek heeft als doel de mogelijkheden in kaart te brengen om door middel van een elektronische sleutel op digitale wijze invulling te geven aan de patiëntrechten die in de huidige wet- en regelgeving ten aanzien van het medisch dossier in het kader van de geneeskundige behandeling zijn opgenomen. De elektronische sleutel is in dit onderzoek als concept geoperationaliseerd door middel van de volgende twee componenten:

- Het ***toegangsmiddel*** is het identificatie- en authenticatiemiddel wat wordt gebruikt om gebruik te kunnen maken van de toegangsmethode.
- De ***toegangsmethode*** is de wijze waarop een zorgconsument een digitale versie van het eigen medisch dossier kan inzien en opslaan, en vervolgens de overige patiëntrechten hierop kan uitvoeren.

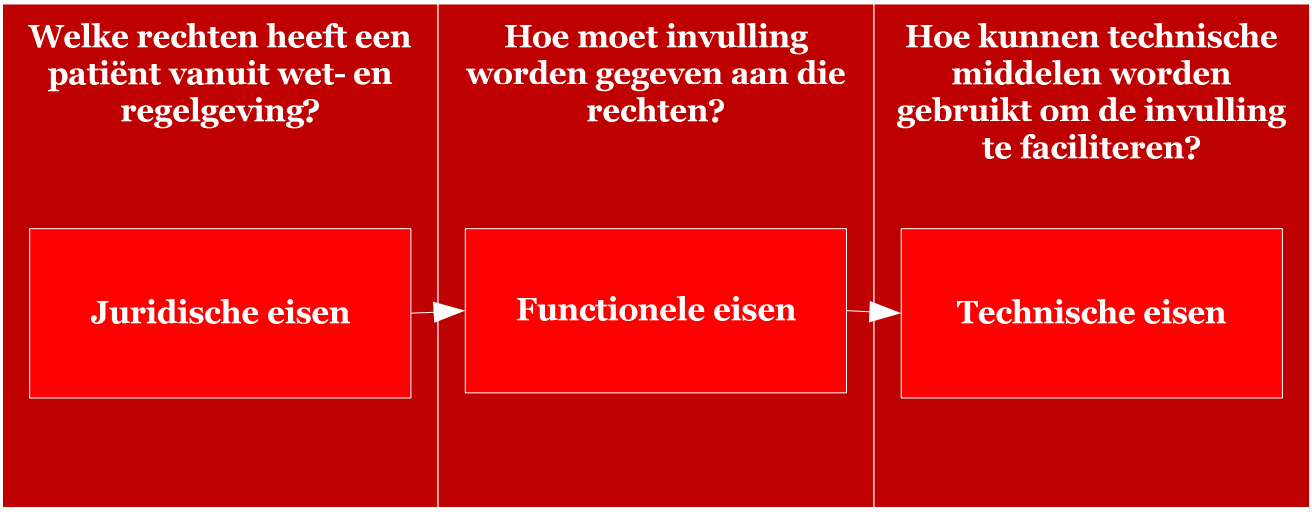
45 Overige aspecten ten aanzien van de geautomatiseerde gegevensverwerking door een zorgverlener en de uitwisseling van digitale medische gegevens tussen zorgverleners onderling vallen buiten de reikwijdte van het onderzoek.

2. Toegangsmethode en -middel zijn getoetst aan een referentiekader

2.1. Het referentiekader is gebaseerd op juridische eisen

46 Om te bepalen wat de eisen en wensen zijn voor het uitoefenen van patiëntrechten met betrekking tot toegang tot de eigen digitale medische gegevens hebben wij een referentiekader ontwikkeld voor de analyse van de verschillende verschijningsvormen van een elektronische sleutel bestaande uit een combinatie van een toegangsmiddel en een toegangsmethode.

47 Het referentiekader bestaat uit technische eisen voor enerzijds het toegangmiddel en anderzijds de toegangsmethode. Deze technische eisen zijn tot stand gekomen via de in de onderstaande figuur weergegeven stappen.



48 Wij zijn uitgegaan van patiëntrechten zoals die zijn beschreven in de bestaande wetgeving en gewenste aanvullingen hierop zoals deze zijn geformuleerd door andere belanghebbenden zoals de Eerste en Tweede Kamer en patiëntenverenigingen. Deze eisen en wensen hebben wij benoemd als *juridische eisen*.

49 Vervolgens zijn als tussenstap de juridische eisen (welke patiëntrechten moeten worden geborgd?) vertaald naar *functionele eisen* (wat moet een zorgconsument met een elektronische sleutel kunnen?). Uit deze eisen moet vervolgens bepaald worden hoe invulling gegeven kan worden aan de patiëntrechten. Dit hebben wij beschreven in de vertaling van de juridische eisen naar de *functionele eisen*.

50 Daarna zijn de functionele eisen verwerkt tot *technische eisen* (waaraan moet een toegangsmiddel en een toegangsmethode voldoen om patiëntrechten ten aanzien van het eigen medisch dossier te borgen?). De toegangsmethoden en -middelen die wij hebben meegenomen in dit onderzoek zijn gedurende de uitgevoerde analyse tegen het referentiekader met technische eisen gehouden.

51 In het resterende deel van dit hoofdstuk wordt het uitgevoerde stappenplan om te komen tot het referentiekader voor de elektronische sleutel verder onderbouwd. Hierbij zijn de juridische, functionele en technische eisen slechts samengevat weergegeven. Een volledig overzicht en een meer uitgebreide beschrijving van deze eisen is te vinden in bijlage A.

2.1.1. *Patiëntrechten voor het digitale medisch dossier zijn geborgd in wet- en regelgeving*

52 Er zijn diverse wetten waarin het medisch dossier, de digitale invulling daarvan en de rechten van de zorgconsument worden beschreven. Dit zijn niet alleen wetten die specifiek zijn ontworpen voor het digitale dossier of zelfs specifiek voor medische gegevens[12].

De eisen voor het medisch dossier zijn kaderstellend

53 Voor de realisatie van een methode om de genoemde patiëntrechten uit te kunnen oefenen dient zowel een toegangsmethode als een toegangsmiddel te worden ingericht.

54 In dit onderzoek wordt met het eigen digitale medisch dossier het medisch dossier verstaan wat door de zorgverlener wordt bijgehouden in het kader van de geneeskundige behandeling zoals gedefinieerd in artikel 454 lid 1 van de WGBO:

> *"De hulpverlener richt een dossier in met betrekking tot de behandeling van de patiënt. Hij houdt in het dossier aantekening van de gegevens omtrent de gezondheid van de zorgconsument en de te diens aanzien uitgevoerde verrichtingen en neemt andere stukken, bevattende zodanige gegevens, daarin op, een en ander voor zover dit voor een goede hulpverlening aan hem noodzakelijk is."*

55 In de onderstaande tabel zijn alleen die wettelijke eisen ten aanzien van de verwerking van het medisch dossier opgenomen die als kaderstellend worden beschouwd. Een meer gedetailleerde beschrijving is opgenomen onder dezelfde referentie in bijlage A.

Ref.	Samenvatting
J.1	Voorkómen van onbevoegd gebruik: goede identificatie van de zorgconsument, zodat zekerheid bestaat over zijn identiteit.
J.2	Voldoende borging van de vertrouwelijkheid van de gegevens.
J.3	De mogelijkheid voor de zorgverlener om gegevens af te schermen en anderen toegang te verlenen.

56 Eis J.1 is van belang omdat zo kan worden geborgd dat alleen die medische gegevens worden ontsloten aan een zorgconsument die daadwerkelijk op hem of haar betrekking hebben.

57 Eis J.2 betreft in wezen de beveiligingseis van het medisch dossier. Hiermee wordt onder meer geborgd dat alleen daartoe gerechtigde (zoals omschreven in de WGBO) personen toegang krijgen tot het medisch dossier.

58 Eis J.3 heeft als doel om de zorgconsument te beschermen tegen nadelige effecten van inzage in het eigen dossier. Wel kan in dat geval inzage worden verstrekt aan andere betrokkenen (denk aan belangenbehartigers zoals familieleden en mantelzorgers).

De rechten van zorgconsumenten ten aanzien van het medisch dossier zijn vastgelegd in wetgeving

59 De rechten die zorgconsumenten kunnen uitoefenen ten aanzien van het medisch dossier zijn vastgelegd in de Wet op de geneeskundige behandelovereenkomst (WGBO) en de Wet bescherming persoonsgegevens (Wbp). Deze patiëntrechten zijn in de onderstaande tabel samengevat. Een meer gedetailleerde beschrijving is opgenomen onder dezelfde referentie in bijlage A.

Ref.	Samenvatting
J.4	Inzage in het dossier op een zo kort mogelijke termijn.
J.5	Doorlevering van gegevens aan derden alleen met toestemming van de zorgconsument, tenzij een wettelijke verplichting tot doorlevering bestaat of het een doorlevering aan een hulpverlener betreft die op dat moment een behandelrelatie heeft met de zorgconsument.
J.6	De zorgconsument dient informatie te krijgen over de verwerking van zijn persoonsgegevens.
J.7	De zorgconsument moet kunnen verzoeken om zijn gegevens aan te vullen, te wijzigen, te verwijderen of af te schermen.

[12] Welke eis op welke wet is gebaseerd kan gevonden worden in Bijlage A.

60 Deze patiëntrechten worden momenteel veelal nog op fysieke wijze ingevuld door de zorgverlener. Een zorgconsument kan bijvoorbeeld via de website of een fysiek aanvraagformulier een aanvraag voor inzage en/of afschrift doen bij de betreffende zorgverlener. Zorgverleners zijn vanuit de Wbp verplicht om dergelijke afschriften binnen vier weken na ontvangst van de aanvraag te verstrekken. Dergelijke afschriften worden vaak als een kopie op papier in fysieke vorm verstrekt. Een dergelijke procedure moet door de zorgconsument worden doorgelopen voor alle zorgverleners waarmee hij of zij een behandelovereenkomst is aangegaan om zijn of haar complete medisch dossier in te kunnen zien.

2.1.2. *Patiëntrechten worden mogelijk verder aangevuld met nieuwe wetgeving en wensen van zorgconsumenten*

Aanvullende eisen zijn gesteld door de Kamers

61 Gedurende de behandeling van de EPD-wet in de Eerste en Tweede Kamer en de Kamerdebatten over dit onderwerp zijn verschillende eisen en wensen geformuleerd (motie Y in de Eerste Kamer en moties 69 en 70 in de Tweede Kamer) ten aanzien van patiëntrechten voor het eigen digitale medisch dossier. In de onderstaande tabel is een samenvatting opgenomen van deze eisen en wensen. Een gedetailleerdere beschrijving is opgenomen onder dezelfde referentie in bijlage A.

Ref.	Samenvatting
J.8	De zorgconsument moet inzage krijgen in de uitwisseling van gegevens.
J.9	De zorgconsument moet op digitale wijze inzage krijgen in het eigen medisch dossier dat in het kader van de geneeskundige behandeling door zorgverleners wordt bijgehouden.
J.10	De zorgconsument moet kunnen beschikken over een lijst met voorgeschreven medicatie en moet deze kunnen aanvullen met zelfmedicatie.

Zorgconsumenten hebben aanvullende wensen ten aanzien van de invulling van hun rechten

62 Er zijn verschillende mogelijkheden om te kunnen voldoen aan de eisen en wensen van zorgconsumenten. Om te kunnen bepalen op welke wijze hieraan kan worden voldaan dient eerst vastgesteld te worden wat deze eisen zijn, om vervolgens hiertegen te kunnen toetsen.

63 Zorgconsumenten hebben eisen en wensen met betrekking tot een toegangsmiddel en -methode om op digitale wijze invulling aan patiëntrechten te kunnen geven. Deze eisen zijn deels ingevuld door de op dit gebied bestaande wetgeving. Aanvullend bestaan er wensen die de invulling van rechten voor de zorgconsument eenvoudiger of helderder maken. In vereenvoudigde vorm zijn de eisen en wensen in de onderstaande tabel opgenomen.

Ref.	Samenvatting
J.11	De toegang tot de digitale medische gegevens is gebruiksvriendelijk, algemeen beschikbaar en bezorgt de zorgconsument zo min mogelijk administratieve lasten.
J.12	Digitale medische gegevens dienen altijd actueel te zijn, zowel voor de zorgconsument als voor de zorgverlener.

64 Deze eisen zijn met een toelichting opgenomen in bijlage A.

2.2. *De elektronische sleutel is getoetst aan de technische eisen*

65 De juridische eisen zijn vertaald naar de volgende functionele eisen:

Ref.	Samenvatting
F.1	De zorgconsument kan gebruikmakend van de elektronische sleutel op veilige en betrouwbare wijze zijn actuele digitale patiëntgegevens elektronisch opvragen, raadplegen en aanvullen.
F.2	De zorgconsument heeft gebruikmakend van de elektronische sleutel controle over wie toegang heeft tot zijn digitale medische gegevens.

Ref.	Samenvatting
F.3	De zorgconsument kan, gebruikmakend van de elektronische sleutel, toestemming geven om gegevens aan derden beschikbaar te stellen.
F.4	De zorgconsument kan, gebruikmakend van de elektronische sleutel, inzage te krijgen in de verwerking van zijn gegevens.
F.5	Er wordt gebruikt gemaakt van algemeen geaccepteerde beveiligingsmethoden, rekening houdend met het risiconiveau van de gegevens.
F.6	De elektronische sleutel heeft de mogelijkheid om beperkt medische gegevens op te slaan voor gebruik in noodgevallen.
F.7	De elektronische sleutel kan gebruikt worden om het recht op verbetering, aanvulling, verwijdering of afscherming uit te oefenen.
F.8	Er is sprake van eenheid van taal tussen de elektronische sleutel en de informatiesystemen van zorgaanbieders waar het aan wordt gekoppeld.
F.9	Het recht op inzage in de digitale medische gegevens moet overgedragen en afgeschermd kunnen worden.
F.10	De elektronische sleutel kan de zorgconsument op sterke wijze identificeren.

66 Deze functionele eisen zijn verder uitgewerkt in technische eisen voor zowel het toegangsmiddel als de toegangsmethode die het referentiekader voor de analyse van de verschillende verschijningsvormen voor een elektronische sleutel vormen.

67 Voor het formuleren van de technische eisen voor het toegangsmiddel hebben wij gebruik gemaakt van onze eerdere onderzoeken[13,15]. In deze eerdere onderzoeken is alleen gekeken naar de technische oplossing voor het toegangsmiddel bij een gegeven toegangsmethode. Wij hebben de resultaten van deze onderzoeken nogmaals kritisch beschouwd. Ook hebben wij gewijzigde inzichten in de toegangsmiddelen meegenomen bij het formuleren van de technische eisen voor de toegangsmiddelen. Hiermee is gekomen tot de volgende set aan technische eisen voor het toegangsmiddel:

Ref.	Samenvatting	Relevant voor
T.1	Het toegangsmiddel zelf is niet kopieerbaar.	Toegangsmiddel
T.2	Het toegangsmiddel is 1-op-1 gekoppeld aan een gebruikersaccount en is uniek identificeerbaar.	Toegangsmiddel
T.3	Het authenticatieniveau van het toegangsmiddel is tenminste sterk conform NEN 7512.	Toegangsmiddel
T.4	Het toegangsmiddel is toekomstvast.	Toegangsmiddel
T.5	Het toegangsmiddel is beschikbaar voor (vrijwel) de gehele bevolking.	Toegangsmiddel
T.6	De echtheid van het toegangsmiddel kan worden gecontroleerd.	Toegangsmiddel
T.7	Het bezit van een al bestaand toegangsmiddel kan worden geverifieerd.	Toegangsmiddel
T.8	Het bezit van een toegangsmiddel en de verificatie van de zorgconsument worden geregistreerd.	Toegangsmiddel
T.9	Natuurlijke controlemomenten hebben de voorkeur.	Toegangsmiddel
T.10	Voorregistratie is wenselijk.	Toegangsmiddel
T.11	Gebruik of activering van het toegangsmiddel kan worden teruggekoppeld.	Toegangsmiddel
T.12	Alleen identificatoren met registratieniveau 3 conform NEN 7512 worden toegepast.	Toegangsmiddel

68 Daarnaast is vanuit de functionele eisen een aantal nieuwe (lees niet voortgekomen uit de eerder uitgevoerde onderzoeken) technische eisen ontstaan voor het toegangsmiddel en de toegangsmethode:

Ref.	Samenvatting	Relevant voor
T.13	Het toegangsmiddel kan gebruikt worden om toestemming voor inzage te geven.	Toegangsmiddel
T.14	De toegangsmethode beschikt over de mogelijkheid om medische gegevens in het geval van nood beschikbaar te maken.	Toegangsmethode
T.15	Het is mogelijk de digitale medische gegevens vrijwel direct te actualiseren, onafhankelijk van waar deze zich bevinden.	Toegangsmethode

[13] Beveiligingeisen ten aanzien van identificatie en authenticatie voor toegang zorgconsument tot het Elektronisch Patiëntendossier (EPD), 2 december 2008, 2008-3027/OV/rvdk/mp.

Ref.	Samenvatting	Relevant voor
T.16	De oplossing maakt gebruik van een gestandaardiseerde wijze van communiceren (en opslag).	Toegangsmethode
T.17	De oplossing kan gebruikt worden om het BSN van de zorgconsument te verifiëren.	Toegangsmethode

69 De bovenstaande tabellen met technische eisen vormen het referentiekader dat wij hebben gebruikt voor de analyse van zowel de mogelijke toegangsmiddelen als toegangsmethoden.

2.3. Conclusies

70 De wettelijke eisen ten opzichte van het medisch dossier, de digitale invulling daarvan en de rechten van de zorgconsument worden beschreven in de juridische eisen. De overige eisen en wensen van zorgconsumenten ten aanzien van een digitale invulling van de patiëntenrechten voor het eigen medisch dossier zijn vertaald naar eisen J.11 en J.12. De juridische eisen zijn vertaald naar functionele eisen. Deze functionele eisen zijn verder uitgewerkt in technische eisen voor zowel het toegangsmiddel als de toegangsmethode. Deze eisen zijn gebruikt om de verschillende mogelijkheden voor een elektronische sleutel te toetsen.

3. Analyse van geschiktheid toegangsmiddel en -methode

71 Voor het uitoefenen van de patiëntrechten van een zorgconsument zijn wij ervan uitgegaan dat een tweetal onderdelen relevant is. In de eerste plaats moet gekozen worden op welke wijze de zorgconsument toegang krijgt, daarnaast is relevant hoe de zorgconsument hiervan gebruik kan maken. Aan deze onderdelen worden verschillende eisen gesteld en er kunnen verschillende combinaties tussen deze vormen worden ingericht.

3.1. Drie toegangsmiddelen geselecteerd op basis van eerdere onderzoeken en bespreking Eerste Kamer

72 Om als zorgconsument op een voldoende veilige en betrouwbare wijze toegang te krijgen tot de eigen medische gegevens, is het noodzakelijk dat de toegang wordt beveiligd met een toegangsmiddel. In eerdere onderzoeken[14],[15] is uiteengezet wat de meest geschikte toegangsmiddelen zouden zijn om zorgconsumenten toegang te verlenen tot de medische gegevens die, in het kader van de behandeling, tussen zorgverleners via het landelijk EPD worden uitgewisseld.

73 Hiertoe werd een patiëntenportaal bovenop het LSP voorzien, waarmee zorgconsumenten gebruik zouden kunnen maken van de volgende functionaliteiten:

1. **Totaal bezwaar**: de zorgconsument kan totaal bezwaar maken tegen opname in het landelijk EPD. Dit houdt in dat er geen indexopbouw en gegevensuitwisseling plaatsvindt.
2. **Uitsluiten op naam en beroepsgroep**: de zorgconsument kan besluiten bepaalde beroepsgroepen of specifieke zorgverleners geen toegang te verlenen tot zijn/haar EPD.
3. **Inzage in verwijsindex**: de zorgconsument kan via de verwijsindex inzien welke medische gegevens bij welke zorgaanbieders aanwezig zijn.
4. **Inzage in logginggegevens**: de zorgconsument heeft hiermee inzage in de zorgaanbieders / zorgverleners die toegang hebben gehad tot de medische gegevens.
5. **Inzage in medische gegevens**: zorgconsumenten krijgen hiermee inzage in (het EPD-deel van) de eigen medische gegevens.

74 Uit het eerste onderzoek[16], uit december 2008, kwamen een aangepaste versie van DigiD Midden (aangevuld met een face-to-face uitgifteproces voor de activatiecode en later EPD-DigiD genoemd) en RTDA (een manier waarop door middel van speciale kaartlezers reisdocumenten konden worden gebruikt als toegangsmiddel) als meest geschikte alternatieven naar voren. Op basis van dit rapport is er door VWS voor gekozen om in samenwerking met het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) de DigiD Middenvariant met face-to-faceuitgifte van een activatiecode als toegangsmiddel voor zorgconsumenten tot het landelijk EPD te ontwikkelen.

75 Eind 2009 heeft GOVCERT een factsheet[17] gepubliceerd waarin wordt gewezen op de gepubliceerde kwetsbaarheid in de A5/1 encryptie die wordt toegepast voor het GSM spraak- en data (SMS) verkeer in Nederland. Naar aanleiding hiervan is in een tweede onderzoek[15] uit juni 2010 geconcludeerd dat, van de beschikbare mitigerende maatregelen, de DigiD Middenvariant indien deze naast het face-to-faceuitgifteproces aangevuld zou worden met een persoonlijke conversietabel de geïdentificeerde risico's konden worden teruggebracht.

[14] Beveiligingeisen ten aanzien van identificatie en authenticatie voor toegang zorgconsument tot het Elektronisch Patiëntendossier (EPD), 2 december 2008, 2008-3027/OV/rvdk/mp.
[15] Risicoanalyse EPD-DigiD - Naar aanleiding van de A5/1 kwetsbaarheid in GSM, 30 juni 2010, referentie: 2010-1400/OV/ev/mp.
[16] Beveiligingeisen ten aanzien van identificatie en authenticatie voor toegang zorgconsument tot het Elektronisch Patiëntendossier (EPD), 2 december 2008, 2008-3027/OV/rvdk/mp.
[17] Zie www.govcert.nl

76 In beide onderzoeken is de elektronische Nederlandse Identiteitskaart (eNIK) geanalyseerd als een veelbelovend alternatief toegangsmiddel voor het landelijk EPD voor zorgconsumenten. In beide gevallen is echter ook geconcludeerd dat op het tijdstip waarop de onderzoeken werden uitgevoerd er geen zicht was op de daadwerkelijke implementatie van de eNIK binnen afzienbare tijd. Op dit moment (september 2011) wordt de implementatie van eNIK opnieuw overwogen door het ministerie van BZK.

77 Op basis van de eerder uitgevoerde onderzoeken en de vraag vanuit de Eerste Kamer om opnieuw de zorgpas als alternatief toegangsmiddel te beschouwen, zijn, hoewel er meer alternatieve middelen beschikbaar zijn, in overleg met VWS de volgende toegangsmiddelen meegenomen in dit onderzoek:

a) **Zorgpas**: De zorgpas is een smartcard (specifiek voor zorgtoepassingen) met daarop een persoonlijk certificaat met een geheime sleutel voor de zorgconsument. De zorgpas kan ook als gegevensdrager gebruikt worden, hier gaan wij verder op in bij het kiezen van de toegangsmethode.
b) **eNIK**: De elektronische Nederlandse Identiteitskaart ofwel eNIK is een middel dat als invulling van het bij DigiD-hoog benodigde middel gebruikt zou kunnen worden om de gebruiker te authenticeren. Deze kaart en het bijbehorende DigiD-niveau zijn op dit moment nog niet beschikbaar.
c) **De DigiD Middenvariant met face-to-faceuitgifte van een activatiecode aangevuld met een conversietabel**: door gebruik te maken van een aanvulling op DigiD met vertrouwensniveau midden (combinatie van een gebruikersnaam, wachtwoord en SMS-code) die inhoudt dat gebruikers een face-to-facecontrole doorlopen en een persoonlijke conversietabel krijgen om de verkregen SMS-code om te zetten (in verband met de GSM-A5/1-kwetsbaarheid[18]).

78 In de onderstaande analyse is alleen een beschrijving opgenomen van de eisen in het referentiekader waaraan het betreffende toegangsmiddel niet voldoet. Wij wijzen er in algemene zin op dat wij dit onderzoek hebben uitgevoerd op basis van de huidige inzichten. Het is mogelijk dat in de toekomst nieuwe technische mogelijkheden ontstaan of nieuwe dreigingen zichtbaar worden waardoor de genoemde toegangsmiddelen niet meer aan de gestelde eisen voldoen.

79 Geen van deze toegangsmiddelen is daadwerkelijk geïmplementeerd. Bij de analyse van de implementatieaspecten van deze toegangsmiddelen zullen wij aangeven welke van deze mogelijkheden haalbaar zijn.

3.2. Drie toegangsmiddelen geanalyseerd voor de toegang tot digitale medisch dossiers

3.2.1. Zorgpas voldoet aan alle eisen uit het referentiekader maar is niet beschikbaar

80 Met een zorgpas kan invulling worden gegeven aan een toegangsmiddel in de vorm van een smartcard met een chip. Een zorgpas kan op diverse manieren worden gebruikt. Zo kan de zorgpas worden ingericht als een toegangsmiddel met daarop een persoonlijk certificaat met een geheime sleutel voor de zorgconsument. Met behulp van dit persoonlijke certificaat kunnen zorgconsumenten berichten ondertekenen waardoor de ontvangende partij (zoals een zorgverlener) kan verifiëren dat dit bericht daadwerkelijk van de betreffende zorgconsument af komt. Dergelijke functionaliteit kan worden gebruikt voor het verlenen van toestemming en voor het indienen van verzoeken tot aanpassing of aanvulling van het eigen digitale medisch dossier. Voor het gebruik van de zorgpas is naar alle waarschijnlijkheid een kaartlezer nodig.

81 Als voorbeeld hiervoor zou de bestaande UZI-pas (die op dit moment alleen door zorgverleners kan worden gebruikt) kunnen worden genomen. In het verleden is een aantal keer geprobeerd een dergelijk initiatief op te zetten (waarvan de meest bekende poging de zorgpasproef in de regio Eemland eind jaren negentig van de vorige eeuw betreft), maar dit heeft niet geleid tot een succesvolle implementatie zoals door de Minister van VWS is uiteengezet[19].

[18] Risicoanalyse EPD-DigiD - Naar aanleiding van de A5/1 kwetsbaarheid in GSM, 30 juni 2010, referentie: 2010-1400/OV/ev/mp
[19] Brief van de minister van VWS aan de Tweede Kamer betreft Voortgangsrapportage landelijke infrastructuur voor gegevensuitwisseling in de zorg vierde kwartaal 2010, kenmerk MEVA/ICT,3044841, 13 januari 2011.

82 Een zorgpas kan theoretisch aan alle eisen aan een toegangsmiddel uit het referentiekader voldoen maar is momenteel niet beschikbaar.

3.2.2. eNIK voldoet aan alle eisen uit het referentiekader maar is nog niet beschikbaar

83 De elektronische Nederlandse Identiteitskaart (eNIK) is een voorgenomen uitbreiding[20] van de 'normale' identiteitskaart. Kenmerkend voor de eNIK is dat de kaart (zoals in de beschrijving van de zorgpas) een persoonlijk certificaat met een geheime sleutel bevat voor de kaarthouder. Hiermee kunnen kaarthouders berichten ondertekenen waarmee ontvangende partijen kunnen verifiëren dat deze berichten daadwerkelijk van de betreffende kaarthouder afkomstig is.

84 De uitgifte van de eNIK dient via een veilig uitgifteproces met face-to-facecontrole te verlopen. Het gebruik van de eNIK vereist naar alle waarschijnlijkheid (net als de zorgpas) een kaartlezer. Het is op dit moment nog niet duidelijk welke vorm de eNIK precies zal krijgen. Beperkingen zijn in elk geval dat waarschijnlijk niet elke zorgconsument over een eNIK zal beschikken (uitzonderingen zijn bijvoorbeeld burgers zonder de Nederlandse nationaliteit).

3.2.3. DigiD Middenvariant voldoet na aanpassing aan het referentiekader

85 De DigiD Middenvariant met face-to-faceuitgifte van een activatiecode aangevuld met een conversietabel (voor het deels mitigeren van het risico geïntroduceerd door de geconstateerde GSM-hack) voldoet na aanpassing aan alle eisen aan een toegangsmiddel uit het referentiekader.

86 Het is voor zorgconsumenten met de DigiD Middenvariant niet zonder additionele functionaliteit mogelijk om berichten te ondertekenen. Wel zou een toestemmingsverklaring kunnen worden verstuurd via een inlogprocedure gebruikmakend van de DigiD Middenvariant (op een soortgelijke wijze wordt door burgers nu gebruik gemaakt van DigiD Laag om de belastingaangifte elektronisch te versturen aan de belastingdienst) voor het inzien van medische gegevens uit het eigen medisch dossier door derden (lees zorgverleners waarmee een nieuwe behandelrelatie wordt aangegaan en andere bij de zorg betrokken personen zoals mantelzorgers).

87 De DigiD Middenvariant zal hoogstwaarschijnlijk, net als het huidige DigiD met vertrouwensniveau midden, alleen beschikbaar zijn voor mensen met een BSN die zijn ingeschreven op een Nederlands adres (geregistreerd in de Gemeentelijke Basisadministratie van een Nederlandse gemeente). Een uitzondering hierop zouden wellicht Nederlanders woonachtig in het buitenland die via de Sociale Verzekeringsbank AOW ontvangen kunnen zijn. Dit is in lijn met het huidige DigiD vertrouwensniveau midden.

3.3. Toegangsmethoden op basis van ontsluitingswijze geselecteerd

88 Er zijn verschillende wijzen waarop een zorgconsument toegang kan krijgen tot zijn gegevens. Enkele voorbeelden van de huidige mogelijkheden voor zorgconsumenten om een eigen digitaal dossier in te richten zijn:

- Digitale medische dagboeken zijn websites waarin zorgconsumenten na inloggen met een eigen account zelfstandig medische gegevens invoeren en bijhouden. Dergelijke systemen zijn vaak niet gekoppeld aan informatiesystemen bij zorgverleners waarin het medisch dossier in het kader van de geneeskundige behandeling wordt bijgehouden.
- Medische webportalen hebben vaak soortgelijke functionaliteit als de digitale medische dagboeken maar bieden daarnaast functionaliteit om gegevens te downloaden uit informatiesystemen van zorgverleners. De initiërende partij voor dergelijke portalen verschilt. Bestaande portalen worden geïnitieerd door zorgverleners, patiëntenverenigingen en private partijen.

[20] Zie bijvoorbeeld 2010Z04840, Antwoord op vragen van het lid Gerkens (SP) van de staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties over de veiligheid van DigiD (ingezonden 17 maart 2010).

- Persoonlijke gegevensdragers zoals USB-sticks, mobile devices (zoals smartphones en tablets) of een zorgpas waarop programmatuur aanwezig is om een eigen digitaal medisch dossier bij te houden. In het geval van een USB-stick is de functionaliteit beperkt tot die van een digitaal medisch dagboek. In het geval van mobile devices wordt vaak gebruik gemaakt van zogenaamde apps, eenvoudige maar gebruiksvriendelijke programma's die al dan niet tegen betaling kunnen worden gekocht op een Marketplace voor het betreffende technische platform. Dergelijke apps kunnen tevens het functionaliteitniveau van webportalen behalen. Een voorbeeld van een dergelijke gegevensdrager is een USB-stick met daarop speciale software voor het handmatig bijhouden van het eigen medisch dossier door de zorgconsument. Ook de door de Eerste Kamer geopperde mogelijkheid van opslag van (nood)gegevens op een zorgpas is een voorbeeld.

89 Digitale medische dagboeken zijn niet meegenomen als toegangsmethode omdat deze alleen de mogelijkheid bieden een eigen dossier in te richten, maar geen ontsluitingwijze bieden voor de digitale medische gegevens die bij zorgverleners beschikbaar zijn. In de huidige situatie kunnen zorgconsumenten wel van deze systemen gebruik maken om medische gegevens verkregen op papier over te nemen in het eigen medische dagboek.

90 Omdat de hierboven genoemde voorbeelden in vele facetten van elkaar verschillen is gezocht naar voor dit onderzoek relevante aspecten op basis waarvan typen toegangsmethoden konden worden geïdentificeerd. Na analyse bleek de meest onderscheidende factor voor de toegangsmethoden de ontsluitingswijze te zijn.

3.3.1. Opslag op een lokale gegevensdrager voldoet niet aan eisen aan actualiteit van gegevens en raadpleging in noodsituaties

91 Een belangrijk nadeel van lokale opslag bij de zorgconsument is dat door het ontbreken van een (continue) verbinding met het zorginformatiesysteem van de zorgverlener medische gegevens maar in beperkte mate actueel kunnen worden gehouden. Hiermee kan niet worden voldaan aan de eis ten aanzien van de directe actualisatie van medische gegevens. Actualiteit van gegevens is zeer belangrijk voor zowel de zorgconsument als de zorgverlener. Als gegevens niet actueel zijn kan de zorgconsument niet in voldoende mate actie ondernemen op de gegevens waardoor de mogelijkheid tot 'patient empowerment' wordt beperkt. Daarnaast zal de zorgverlener geen beslissingen kunnen baseren op gegevens die niet actueel zijn. De kans op fouten die voorkomen hadden kunnen worden door een actuele informatievoorziening zou hierbij vergroot worden.

92 Daarnaast kan met de lokale opslag van gegevens op een gegevensdrager niet goed worden voldaan aan de eis ten aanzien van de mogelijkheid om medische gegevens in het geval van nood beschikbaar te maken. Aangezien de toegang tot de gegevensdrager moet worden beveiligd tegen onbevoegde raadpleging kunnen de gegevens (bijvoorbeeld door het invoeren van een pincode) in eerste instantie alleen door de zorgconsument zelf worden ingezien. Als de patiënt buiten bewustzijn is kunnen de gegevens daardoor niet lokaal worden ingezien in geval van nood. Ook blijkt uit ervaringen met de Duitse gesundheitskarte dat 70% van de zorgconsumenten zijn pincode niet meer wist bij poging tot raadpleging van de pas gedurende de behandeling met als consequentie dat de gegevens niet ter beschikking konden worden gesteld aan de zorgverlener.

93 Tot slot kan niet eenvoudig worden voldaan aan de eis betreffende het gestandaardiseerd ontsluiten van medische gegevens. Opslag van medische gegevens op gegevensdragers als een USB-stick, mobile devices of een zorgpas biedt stand-alone in de huidige situatie geen ontsluitingswijze voor de medische gegevens die aanwezig zijn bij de zorgverleners omdat er geen koppeling met informatiesystemen van zorgverleners bestaat. Er dienen hiervoor speciale interfaces en software ontwikkeld te worden om het automatisch kopiëren van de medische gegevens in het informatiesysteem bij de zorgverlener naar de gegevensdrager van de zorgconsument mogelijk te maken. Deze functionaliteit moet daarnaast breed worden geïmplementeerd bij zorgverleners.

94 Om deze redenen biedt ook de opslag op een lokale gegevensdrager geen adequate oplossing voor toegang tot het eigen medische dossier en is deze niet meegenomen als toegangsmiddel.

3.3.2. *Twee toegangsmethoden kunnen wel aan de voorwaarden voldoen*

95 Op basis van de bestaande voorbeelden van webportalen en de wijze waarop hiermee medische gegevens kunnen worden ontsloten vanuit digitale medisch dossiers bij zorgverleners naar zorgconsumenten maken wij onderscheid tussen de volgende toegangsmethoden:

a) **Directe toegang tot de gegevens:** zorgconsumenten krijgen direct toegang tot het digitale medisch dossier binnen een gecontroleerde omgeving. Dit kan een beveiligd webportaal zijn waarmee de digitale medische gegevens bij de zorgverlener worden ontsloten, al dan niet via een samenwerkingsverband tussen zorgverleners zoals een schakelpunt. De verantwoordelijkheid voor de gegevens en de toegang ligt in dit geval bij de zorgverlener, de gegevens blijven onder beheer van de zorgverlener.

b) **Indirecte toegang tot de gegevens (via een door een derde partij beheerd portaal):** toegang tot het digitale medisch dossier wordt verleend via een patiëntenportaal als intermediair tussen de zorgverlener en de zorgconsument. Zorgconsumenten hebben daardoor geen directe toegang tot het digitale medisch dossier aanwezig bij de zorgverlener. Het portaal kan worden beheerd door een derde (dus niet zijnde een zorgverlener) partij. De verantwoordelijkheid voor de gegevens en de toegang ligt bij deze methode bij de derde partij of de zorgconsument. Bij indirecte toegang via een door een derde partij beheerd portaal worden de medische gegevens na toestemming van de zorgconsument overgeheveld naar een eigen persoonlijk dossier.

96 In onze analyse is alleen een beschrijving opgenomen van de eisen in het referentiekader waaraan de betreffende toegangsmethode niet voldoet.

3.4. *Twee toegangsmethoden geanalyseerd voor de inrichting van digitale medisch dossiers*

3.4.1. *Directe toegang voldoet aan alle eisen uit het referentiekader maar behoeft vergaande samenwerking tussen zorgverleners*

97 Het is mogelijk om de zorgconsument directe toegang te verlenen tot zijn gegevens binnen een gecontroleerde omgeving.

98 Een voorbeeld hiervan is het ontsluiten van medische gegevens uit het digitale medisch dossier bij de zorgverlener (het medisch dossier zoals beschreven in de WGBO) via een webportaal die als aanvullende functionaliteit door de leverancier van het betreffende informatiesysteem van de zorgverlener (zoals een ziekenhuisinformatiesysteem) aangeboden wordt. Ook het geven van toegang tot de eigen medische gegevens via een webportaal bovenop een gegevensuitwisselingsnetwerk voor zorgverleners zoals het LSP is een voorbeeld van deze toegangsmethode. Er zijn diverse varianten mogelijk waarbij zorgverleners bijvoorbeeld (regionale) samenwerkingsverbanden aangaan. Het is daarbij denkbaar dat specifieke groepen zorgverleners (zoals ziekenhuizen) hierbij het initiatief nemen.

99 Een voordeel van deze methode is dat de zorgconsument altijd toegang heeft tot de meest recente gegevens en direct verzoeken tot wijzigingen of aanvullingen kan doen.

100 Een nadeel is dat zorgconsumenten voor een overzicht van de eigen medische gegevens in voorkomende gevallen moeten inloggen op een veelheid aan webportalen van individuele zorgverleners. Een diabeteszorgconsument zal bijvoorbeeld minimaal toegang willen tot de webportalen van zijn of haar huisarts, apotheek en specialist in het ziekenhuis. Dit kan worden geadresseerd wanneer zorgverleners samenwerken om ontsluiting van medische gegevens via een gegevensuitwisselingsnetwerk naar zorgconsumenten mogelijk te maken. Hiertoe dienen gegevens te worden uitgewisseld op basis van het BSN. Voor de controle op de correctheid van de registratie van digitale medische gegevens op basis van het BSN zijn (via de Wgbn-z) reeds centrale voorzieningen beschikbaar (SBV-Z). Het opzetten van een gegevensuitwisselingsnetwerk is ook een voorwaarde om het mogelijk te maken medische gegevens in het geval van nood beschikbaar te maken.

101 Indien de directe toegang als toegangsmethode wordt ingericht op basis van een samenwerkingsverband tussen verschillende zorginstellingen (bijvoorbeeld met behulp van een schakelpunt waarbij wel directe toegang tot de

gegevens blijft bestaan) dienen duidelijke regels en richtlijnen te bestaan over de gestandaardiseerde gegevensuitwisseling tussen de zorgconsument en de verschillende deelnemende zorgverleners.

3.4.2. *Indirecte toegang via een door een derde partij beheerd portaal vereist standaarden voor koppelen en uitwisselen van gegevens*

102 Zorgconsumenten kunnen ook toegang krijgen tot hun medische gegevens via een ontkoppeld (indirect) patiëntenportaal. Hierbij is er geen directe aansluiting op de digitale medisch dossiers bij de zorgverleners, maar worden (specifieke) medische gegevens uit de informatiesystemen bij de zorgverleners opgehaald en opgeslagen bij het patiëntenportaal.

103 Voorbeelden zijn de patiëntenportalen die door commerciële partijen worden opgezet met als doel om functionaliteit tegen abonnementsgelden ter beschikking te stellen aan zorgconsumenten. Andere voorbeelden zijn patiëntenportalen die voor een specifieke groep zorgconsumenten met een bepaalde chronische ziekte door patiëntenverenigingen ter beschikking worden gesteld.

104 Een dergelijk patiëntenportaal functioneert losstaand van de informatiesystemen van de zorgverleners en kan daarom tevens worden gebruikt om de medische gegevens vanuit verschillende zorginformatiesystemen op te halen en weer te geven. Een zorgconsument heeft daarmee het voordeel dat zijn of haar eigen medisch dossier op één plek inzichtelijk is en er een mogelijkheid is om medische gegevens in het geval van nood in te zien. Dit vergt echter vergaande standaardisatie (bij voorkeur op basis van open standaarden) van de berichtenstructuren en uitwisselingssystemen.

105 Een nadeel van deze toegangsmethode voor private partijen is dat deze niet zijn opgenomen in de Wgbn-z en daarmee medische gegevens uit de verschillende informatiesystemen bij zorgverleners niet zonder meer op basis van het BSN kunnen terugherleiden naar één zorgconsument. Private partijen kunnen daarbij ook geen gebruik maken van de faciliteiten voor de controle van persoons- en BSN-gegevens die zijn ingericht voor de zorg (SBV-Z).

106 Bovendien hangt de mate waarin de verschillende digitale medisch dossiers vanuit zorgverleners bij elkaar kunnen worden gebracht sterk af van de initiërende partij. Zo zouden patiëntenportalen aangeboden door een leverancier van een bepaald type informatiesysteem (bijvoorbeeld ziekenhuisinformatiesystemen) alleen een geïntegreerd portaal voor haar klanten binnen een bepaalde deelsector (zoals de ziekenhuizen) kunnen aanbieden. Ditzelfde geldt ook voor patiëntportalen aangeboden door patiëntenverenigingen. Zorgconsumenten met meerdere chronische ziekten zijn dan genoodzaakt om bij meerdere patiëntportalen in te loggen voor een integraal overzicht van het eigen medisch dossier.

107 Het patiëntenportaal kan door een willekeurige partij worden geïmplementeerd en beheerd. De zorgconsument dient dan echter wel toestemming te geven voor de verwerking van deze gegevens (waaronder het beheer en eventuele overige verwerkingen) aangezien het een ander verwerkingsdoel dan de geneeskundige behandeling betreft. Een nadeel van deze toegangsmethode is daarom dat deze toestemming per zorgverlener die gegevens ter beschikking stelt aan het patiëntenportaal moet worden gegeven.

108 De synchronisatie van de centrale gegevens met dit portaal dient dusdanig frequent plaats te vinden dat de gegevens binnen het portaal altijd voldoende actueel te zijn om te kunnen ondersteunen in het zorgproces.

3.5. Conclusies

109 Wij beschouwen de elektronische sleutel als een oplossing die bestaat uit een toegangsmiddel en een toegangsmethode. De verschijningsvormen van een toegangsmiddel die invulling kunnen geven aan de juridische en technische eisen inclusief de door de Eerste en Tweede Kamer geformuleerde wensen zijn de zorgpas, eNIK en DigiD Middenvariant met face-to-face-uitgifteprocedure van een activatiecode en conversietabel. De geselecteerde verschijningsvormen van een toegangsmethode zijn directe toegang tot de gegevens en indirecte toegang via een door een derde partij beheerd portaal. Uit de analyse van de geselecteerde toegangsmethoden kan geconcludeerd worden dat alle mogelijkheden kunnen voldoen aan de eisen gesteld in het referentiekader.

110 Of de toegangsmiddelen en toegangsmethoden daadwerkelijk geïmplementeerd kunnen worden heeft te maken met beschikbaarheid, compatibiliteit tussen een toegangsmiddel en toegangsmethode en beleidsafwegingen. Deze implementatieaspecten bepalen de haalbaarheid en geschiktheid van de oplossing. Deze aspecten behandelen wij in hoofdstuk 4.

4. De oplossingsrichtingen hebben voor- en nadelen

111 De in het vorige hoofdstuk behandelde verschijningsvormen hebben diverse voor- en nadelen voor de betrokken partijen. Wij hebben de meest haalbare vormen op basis van de invulling van de eisen en wensen van zorgconsumenten geanalyseerd welke effecten opgedeeld in de volgende categorieën kunnen optreden bij implementatie:

a) **Bestuurlijke effecten**: Wie is verantwoordelijk voor de implementatie, welke additionele wet- en regelgeving is noodzakelijk en hoe moet toezicht worden gehouden op de naleving hiervan?
b) **Financiële effecten**: Welke kosten moeten worden gemaakt voor het ontwerp ontwikkeling, bouw, uitgifte en beheer van de betreffende verschijningsvorm?
c) **Organisatorische effecten:** In hoeverre kan de verschijningsvorm aansluiten bij de bestaande zorgprocessen en de interactie tussen zorgverleners en zorgconsumenten?
d) **Technische effecten**: Welke apparatuur, programmatuur en gegevens zijn noodzakelijk voor de realisatie van de betreffende verschijningsvorm en hoe wordt de interoperabiliteit tussen verschijningsvormen geborgd?

112 Wij hebben deze effecten afzonderlijk bepaald voor de in het voorgaande hoofdstuk haalbare toegangsmiddelen en toegangsmethoden.

4.1. Implementatie-effecten toegangmiddelen verschillen op het gebied van kosten en implementatietermijnen

4.1.1. De kosten van een zorgpas zijn zeer hoog en toepassingsgebied beperkt tot de zorgsector

113 Een zorgpas, in de vorm van een smartcard, kan gebruikt worden met beide toegangsmethoden. Onderstaande aspecten geven een beeld van de effecten die alleen voor de smartcard zelf van belang zijn.

114 **Bestuurlijk**: Aangezien een zorgpas in de beschreven opzet alleen gebruikt wordt ten behoeve van de zorg ligt het voor de hand de implementatieverantwoordelijkheid bij de gebruiker (binnen de zorgsector) neer te leggen. Dit kan bij de zorgverlener aangezien deze de processen hiermee kan optimaliseren, maar ook bij de zorgverzekeraars aangezien uit de Duitse eGK blijkt dat deze met name de financiële baten hebben van de invoering van een dergelijke kaart (zie ook onder 'financieel')[21]. Het beheer van de kaart kan door een willekeurige instantie worden uitgevoerd. Omdat met de zorgpas persoonsgegevens worden verwerkt zal hierop de Wbp van toepassing zijn het College bescherming persoonsgegevens (CBP) hierop toezicht houden.

115 **Financieel:** Een nieuw in te voeren zorgpas brengt zeer hoge kosten met zich mee. Hierbij kan gedacht worden aan initiële investeringen in de technische (voor de kaart, kaartlezers voor zorgconsumenten en een nieuwe centrale identificatie- en authenticatie-infrastructuur) en organisatorische (voor de uitgifte) infrastructuur en het ontwerp van een uitgifteproces. Daarnaast zijn er hoge beheer- en onderhoudskosten voor de technische infrastructuur en het uitvoeren van het uitgifteproces[22].

116 **Organisatorisch**: De zorgpas kan als smartcard worden gebruikt om zorgspecifieke functionaliteiten in te richten ten behoeve van het zorgproces. Hierbij kan gedacht worden aan identificatie van zorgconsumenten

[21] Evaluationsbericht im Rahmen der Testregionen übergreifenden Evaluation der 10.000er Tests bei der Einführung der elektronischen Gesundheitskarte, juni 2009.
[22] Uit informatie verkregen van VWS blijkt dat ramingen uit het verleden uitgaan van geschatte structurele overheidskosten van EUR 18 miljoen per maand. De kosten voor de Duitse eGK worden geschat op EUR 13,5 miljard over tien jaar, wat neerkomt op EUR 112,5 miljoen per maand. De invoering van de eGK resulteert naar verwachting pas na tien jaar tot een positief nettoresultaat en komen met name ten bate van de zorgverzekeraars.

tijdens het verblijf in het ziekenhuis (in plaats van de ponsplaatjes en/of de polsbandjes), het doen van betalingen van eigen risico en het bepalen van de verzekeringsstatus van een zorgconsument. Verdere beïnvloeding van het zorgproces is sterk afhankelijk van de gekozen toegangsmethode en diens functionaliteit. Uit de eerste testen met de eGK blijkt dat diverse problemen met de bruikbaarheid bestaan[23], waaronder het vergeten van de pas of de bijbehorende PIN vanwege het beperkte gebruik ervan. Ook uit de voorbeelden van een centraal door de overheid uitgegeven toegangsmiddel voor een landelijk patiëntenportaal in het Verenigd Koninkrijk (Summary Care Records zijn in te zien via een zogenaamde HealthSpace account) en Frankrijk (Carte Vitale 2)[24] blijkt dat grote investeringen noodzakelijk zijn terwijl het gebruik door zorgconsumenten zeer laag is. Ervaringen uit het Verenigd Koninkrijk laten zien dat het gebruik door zorgconsumenten van een vanuit overheidswege uitgegeven toegangsmiddel specifiek voor het verlenen van toegang tot een landelijk patiëntenportaal zeer beperkt is[25]. De voornaamste reden hiervoor is dat de geboden functionaliteit slechts zeer beperkt aansluit bij de interacties tussen zorgconsumenten en zorgverleners tijdens het zorgproces. Voorbeelden van Nederlandse patiëntenportalen geïnitieerd vanuit zorgverleners lijken meer bezocht te worden. Dergelijke portalen bieden zorgconsumenten dan wel functionaliteiten voor het maken van persoonlijke notities, mogelijkheden voor het online maken van afspraken en het inzien van röntgenbeelden, labwaarden en ontslagbrieven tijdens de behandeling.

117 **Technisch:** Voor de invoering van een smartcard is een volledige infrastructuur nodig die is ingericht op de kaart. Hieronder vallen tenminste de kaarten (inclusief een gecontroleerd uitgifteproces en sleutelbeheerprocedures), paslezers voor zorgconsumenten en een centrale identificatie- en authenticatie-infrastructuur voor toegangsverlening.

118 De zorgpas is een toegangsmiddel dat kan voldoen aan alle gestelde eisen maar zou tegen zeer hoge kosten ingevoerd moeten worden waarbij het toepassingsgebied beperkt blijft tot de zorgsector.

4.1.2. De eNIK is met structurele overheidsinvesteringen breed inzetbaar maar pas op langere termijn beschikbaar

119 De eNIK is een van overheidswege ingevoerde smartcard met een zodanige functionaliteit dat ook toegang tot medische gegevens mogelijk gemaakt kan worden. Veel implementatieaspecten komen hierdoor overeen met de specifiek voor dit doel ingestelde smartcard zoals de zorgpas. Het belangrijkste verschil is dat de eNIK meer mogelijkheden biedt voor het gebruik als toegangsmiddel voor andere (overheids)diensten waardoor synergievoordelen behaald kunnen worden ten aanzien van de implementatiekosten en te realiseren baten.

120 **Bestuurlijk**: De verantwoordelijkheid voor identiteitsgerelateerde onderwerpen binnen de overheid ligt bij het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK). Op dit moment wordt er door BZK gewerkt aan de besluitvorming over de wenselijkheid en de haalbaarheid van de invoering van DigiD met het authenticatieniveau hoog op basis van de eNIK als toegangsmiddel[26] [27]. Naar verwachting zal de ontwikkeling van de eNIK en de daarvoor benodigde DigiD-infrastructuur nog enkele jaren vergen. Daarnaast zal het na de eerste uitgifte van de eNIK nog de geldigheidsduur van de huidige Nederlandse Identiteitskaart (5 jaar) duren

[23] Evaluationsbericht im Rahmen der Testregionen übergreifenden Evaluation der 10.000er Tests bei der Einführung der elektronischen Gesundheitskarte, juni 2009.
[24] http://www.sesam-vitale.fr/divers/vitale2/index.asp
[25]Adoption, non-adoption, and abandonment of a personal electronic health record: case study of HealthSpace, Greenhalgh et. al., 2010, BMJ, http://www.bmj.com/highwire/filestream/398293/field_highwire_article_pdf/0.pdf. Uit dit onderzoek blijkt dat tussen de start van Healthspace in 2007 tot oktober 2010 172.950 burgers op de website hebben ingelogd om een basisaccount aan te maken. In hoeverre de accounts ook werden aangemaakt en gebruikt is niet bekend op basis van de beschikbare gegevens. Ten aanzien van de zogenaamde advanced accounts is bekend dat tot oktober 2010 voor 2.442.215 burgers in het Verenigd Koninkrijk een 'summary care record' beschikbaar was en daartoe een brief hebben ontvangen om deze via een advanced account in te kunnen zien op Healthspace. Hiervan hebben 11.952 (0,49% van aangeschrevenen) burgers de eerste stap gezet door het aanvraagformulier van de website te downloaden, 3.933 (0,16% van de aangeschrevenen) het formulier daadwerkelijk ingediend en 2.913 (0,13% van de aangeschrevenen) de healthspace account daadwerkelijk gebruikt.
[26] Aanbiedingsbrief van minister van BZK aan de Tweede Kamer met antwoorden op kamervragen Nepperus ten aanzien van inbreuk op DigiD, 23 augustus 2011.
[27] Brief aangaande de stand van zaken moties Diginotar en ICT-problemen bij de overheid van de minister van BZK aan de Tweede Kamer.

voor deze via de reguliere vervangingstermijn[28] en tegen vergoeding[29] beschikbaar is voor alle personen met de Nederlandse identiteit. De verantwoordelijkheid voor de implementatie van eNIK als toegangsmiddel voor zorgtoepassingen ligt afhankelijk van de gekozen toegangsmethode bij de zorgverleners (in geval van directe toegang) of private partijen (in geval van een door derde partijen beheerd patiëntenportaal).

121 **Financieel:** Het ligt (gezien de gelijksoortige inrichting) voor de hand dat de kosten voor de eNIK vergelijkbaar zijn met de invoering van een zorgpas zoals hierboven genoemd. BZK heeft aangegeven het kostenaspect nadrukkelijk mee te nemen in de voorbereidingen voor de besluitvorming omtrent het inrichten van DigiD met authenticatieniveau hoog op basis van de eNIK[28]. Deze kosten zullen voor het centrale deel worden gedragen door de overheid (implementatie eNIK en aanpassingen DigiD-infrastructuur), productie en uitgifteprocessen, beheer van de DigiD-infrastructuur) en voor de implementatie en het beheer van de toepassingsgebieden door de gebruikende instanties (in het geval van zorgspecifieke toepassingen, afhankelijk van de gekozen toegangsmethode, de zorgverleners of private partijen). De kaart kan echter voor verschillende doeleinden worden gebruikt en kan dienen als identiteitsmanagementoplossing voor verschillende elektronische (overheids)diensten. Ook kan de kaart gezien worden als invulling van de 'standaard'-identiteitskaart die gebruikt wordt om fysieke identificatie uit te voeren. Hierdoor kunnen kostenvoordelen ontstaan waarbij verschillende toepassingen gebruik maken van dezelfde investeringen. Voor het benodigde face-to-faceuitgifteproces voor de eNIK kan gebruik worden gemaakt van de uitgifteprocessen die hiertoe al zijn ingericht voor de uitgifte van de nu geldende identiteitsdocumenten bij de gemeenten.

122 **Organisatorisch:** Net als de zorgpas is een eNIK als smartcard goed in te passen in de bestaande zorgprocessen. Dit omdat een losstaande authenticatiedienst (mits DigiD met vertrouwensniveau hoog wordt vormgegeven gebruikmakend van de eNIK) flexibel inzetbaar is bij de verschillende toegangsmethoden.

123 **Technisch:** De eNIK-infrastructuur moet nog ingericht worden. De DigiD-infrastructuur is echter al aanwezig en hoeft niet opnieuw opgezet te worden. Met de eNIK kan daardoor een efficiëntievoordeel worden behaald. Een voorwaarde voor organisaties om gebruik te maken van DigiD als identificatie- en authenticatiemiddel (los van het vertrouwensniveau) is dat zij gebruik mogen maken van het Burgerservicenummer (BSN). Zonder aanpassingen, kunnen daarom alleen in de Wbsn-z aangewezen zorgverleners, zorgverzekeraars en indicatie-instellingen Wbsn-z die het BSN mogen verwerken, gebruik maken van DigiD met vertrouwensniveau hoog op basis van de eNIK. Uit het onderzoek wat is uitgevoerd door Nictiz naar de verschillende bestaande patiëntenportalen in Nederland blijkt dan ook dat vele private partijen eigen toegangsmiddelen hebben geïmplementeerd[30]. Bij het inrichten van een toegangsmethode door een private partij zou ofwel deze partij wettelijk moeten mogen beschikken over het BSN, ofwel een technische aanvulling op DigiD moeten worden gedaan die het mogelijk maakt de identiteit van een zorgconsument te bevestigen zonder terugkoppeling van het BSN.

124 De eNIK biedt (indien het als middel wordt gebruikt voor de invulling van DigiD met vertrouwensniveau hoog) tegen structurele overheidsinvesteringen een voldoende veilig, breed beschikbaar en flexibel toegangsmiddel voor het geven van toegang tot het eigen digitale medisch dossier aan zorgconsumenten. De eNIK is echter nog niet beschikbaar en zal bij het nemen van het besluit tot invoering pas op de lange termijn beschikbaar zijn.

4.1.3. De DigiD Middenvariant als toegangsmiddel voor zorgtoepassingen op kortere termijn

125 De DigiD Middenvariant is de aanvulling van DigiD met vertrouwensniveau midden (combinatie van een gebruikersnaam, wachtwoord en een SMS-code) met een face-to-faceuitgifteproces van een activatiecode. De

[28] Vroegtijdige vervanging is momenteel alleen mogelijk met een geldige reden zoals diefstal, verlies, beschadiging en langer verblijf in het buitenland. Zie de paspoortwet en onderliggende regelingen zoals geldend op 18 november 2011.
[29] Uit een uitspraak van de Hoge Raad d.d. 9 september 2011 (LJN: BQ4105, Hoge Raad, 10/04967) blijkt dat geen leges meer voor het de uitgifte van de (niet-elektronische) Nederlandse identiteitskaart gevraagd mogen worden. Hiermee is een uitspraak van het Hof 's Hertogenbosch d.d. 7 oktober 2010 (LJN: BN9659, gerechtshof 's-Hertogenbosch, 09/00474) bevestigd. De regering heeft op 21 september 2011 een wetsvoorstel ingediend bij de Tweede Kamer waarin een wettelijke grondslag wordt gecreëerd voor de heffing van leges voor de Nederlandse identiteitskaart. Deze wet is inmiddels zowel in de Tweede Kamer als Eerste Kamer aangenomen waardoor deze met terugwerkende kracht in werking is getreden met ingang van 22 september 2011. Sinds 22 september 2011 worden aan burgers weer leges gevraagd voor de Nederlandse identiteitskaart. Waarschijnlijk zullen dergelijke leges tevens worden geheven voor de eNIK als vervanger van de NIK.
[30] Online inzage in mijn medische gegevens, Patiëntportalen in Nederland, Nictiz, RP 110013, 16 mei 2011.

blootstelling van de DigiD Middenvariant aan de GSM-A5/1-kwetsbaarheid dient beperkt te worden door het uitgeven van een persoonlijke conversietabel waarmee de verkregen SMS-code door een burger kan worden vertaald naar een unieke in te geven toegangscode [31]. Net als de eNIK biedt DigiD Middenvariant brede toepassingsmogelijkheden als toegangsmiddel voor (overheids)diensten waaronder zorgspecifieke toepassingen.

126 **Bestuurlijk**: De DigiD Middenvariant zonder conversietabel was in de eerste plaats gericht op (tijdelijk) gebruik voor toegang voor zorgconsumenten tot het landelijk EPD. De ontwikkeling hiervan zou gezien de aanpassing van DigiD onder het ministerie van BZK vallen. In de zomer van 2010 heeft de minister van VWS besloten om de doorontwikkeling van het zogeheten 'toegang patiënt', waarbij de DigiD Middenvariant zonder conversietabel als toegangsmiddel gebruikt zou worden, te staken[32]. Voornaamste redenen hiervoor waren het verwachte laag frequent gebruik van de toepassing door burgers en de risico's die de geconstateerde GSM-hack met zich meebrachten. Omdat hiermee momenteel alleen DigiD met vertrouwensniveau midden beschikbaar is, is er geen DigiD vertrouwensniveau voor handen waarmee online dienstverlening ten aanzien van de verwerking van medische gegevens kan worden aangeboden. Dit kan door BZK worden opgelost door alsnog de DigiD Middenvariant met face-to-faceuitgifte van een activatiecode, aangevuld met een conversietabel te implementeren en aan te bieden. Er zijn momenteel geen concrete plannen bekend over het implementeren van de DigiD Middenvariant. Uit voorgaand onderzoek[33] komt naar voren dat de noodzakelijke aanpassingen voor het toevoegen van een conversietabel aan de DigiD Middenvariant zonder conversietabel ongeveer één jaar doorlooptijd zouden vergen, de ontwikkeling van het huidige DigiD Midden naar de versie met face-to-faceuitgifte van een activatiecode zal naar verwachting ook nog een half jaar innemen. Indien hiermee tevens een nieuwe invulling wordt gegeven aan DigiD met vertrouwensniveau midden, heeft dit als voordelen dat het vertrouwensniveau geschikt is voor zorgtoepassingen en dat het naar aanleiding van de GSM-hack gesignaleerde risico wordt teruggebracht. De verantwoordelijkheid voor de implementatie van DigiD Middenvariant als toegangsmiddel voor zorgtoepassingen ligt afhankelijk van de gekozen toegangsmethode bij de zorgverleners (in geval van directe toegang) of derde partijen (in geval van een door anderen dan zorgverleners beheerd patiëntenportaal). Het is voor de DigiD Middenvariant (net als bij het huidige DigiD Midden) wel noodzakelijk dat zorgconsumenten een mobiele telefoon hebben.

127 **Financieel:** Het is niet volledig duidelijk wat het invoeren van de DigiD Middenvariant aan kosten met zich mee zou brengen. Net als bij de eNIK geldt dat er vanuit de overheid structurele investeringen noodzakelijk zijn in de (technische en organisatorische) aanpassingen van de DigiD-infrastructuur en de productie en uitgifte van het toegangsmiddel (lees de face-to-face uitgifte van de activatiecode en de conversietabel). Met name het inrichten van noodzakelijke face-to-faceuitgifteprocessen en het ontwikkelen en uitgeven van persoonlijke conversietabellen kunnen aanzienlijke inspanningen en daarmee gemoeide investeringen vergen. De uitgave van de DigiD Middenvariant zal niet via de bestaande postroute (voor DigiD Midden) kunnen lopen.[33] Vanwege het generieke karakter van het toegangsmiddel zal het uitgifteproces van de passen centraal geregeld moeten worden. De kosten van aanpassing van de DigiD-infrastructuur en de implementatie- en productiekosten voor het toegangsmiddel zullen echter naar verwachting lager zijn dan bij het creëren van een geheel nieuw DigiD vertrouwensniveau hoog op basis van de eNIK. De kosten voor de implementatie en het beheer van zorgtoepassingen die gebruik maken van de DigiD Middenvariant zullen komen te liggen bij de gebruikende instanties (in het geval van zorgspecifieke toepassingen, afhankelijk van de gekozen toegangsmethode, de zorgverleners of private partijen).

128 **Organisatorisch:** De wijze waarop de DigiD Middenvariant als toegangsmiddel is in te passen in de zorgprocessen en de mate waarin deze het zorgproces zouden beïnvloeden zijn vergelijkbaar met het gebruik van de eNIK als toegangsmiddel. Ook hier geldt wederom dat de beïnvloeding van het zorgproces met name zal afhangen van de functionaliteiten die de te kiezen toegangsmethode biedt.

129 **Technisch:** Voor de DigiD Middenvariant moet worden bijgehouden welke conversietabellen bij welke zorgconsument horen. Hiertoe dient nieuwe functionaliteit te worden ingepast in de al beschikbare

[31] Risicoanalyse EPD-DigiD - Naar aanleiding van de A5/1 kwetsbaarheid in GSM, 30 juni 2010, referentie: 2010-1400/OV/ev/mp.
[32] Brief van de minister van VWS aan de Tweede Kamer betreft Voortgangsrapportage landelijke infrastructuur voor gegevensuitwisseling in de zorg vierde kwartaal 2010, kenmerk MEVA/ICT,3044841, 13 januari 2011.
[33] Risicoanalyse EPD-DigiD - Naar aanleiding van de A5/1 kwetsbaarheid in GSM, 30 juni 2010, referentie: 2010-1400/OV/ev/mp.

infrastructuur voor DigiD met vertrouwensniveau midden. Voor de DigiD Middenvariant geldt dezelfde beperking in het BSN-gebruik voor private partijen als voor de eNIK. Zoals beschreven bij de eNIK dienen partijen die gebruik wensen te maken van DigiD als toegangsmiddel het BSN te mogen verwerken. De huidige implementatiestatus van de DigiD Middenvariant is onbekend.

130 De DigiD Middenvariant kan naar verwachting op kortere termijn (lees ongeveer 1,5 jaar) zorgen voor een toegangsmiddel waarmee zorgtoepassingen kunnen worden geraadpleegd.[33] Een dergelijk middel is momenteel binnen de DigiD-infrastructuur niet voor handen totdat DigiD vertrouwensniveau hoog op basis van de eNIK is geïmplementeerd. De DigiD Middenvariant kan daarnaast worden hergebruikt als nieuwe implementatievorm voor DigiD vertrouwensniveau midden.

4.2. Beide toegangsmethoden lijken implementeerbaar

4.2.1. Directe toegang sluit goed aan op zorgprocessen maar vergt samenwerking en standaardisatie tussen zorgverleners

131 Bij het verlenen van directe toegang tot gegevens worden de digitale medische gegevens aanwezig bij de zorgverleners direct ontsloten via webportalen bovenop de informatiesystemen van individuele zorgverleners of via uitwisselingsnetwerken voor zorgverleners zoals een schakelpunt.

132 **Bestuurlijk**: Met de aanname van motie 70 in de Tweede Kamer is de basis gelegd voor de verplichting voor zorgverleners om vanaf 1 januari 2013 zorgconsumenten op digitale wijze inzage te geven in het eigen medisch dossier. Directe toegang tot gegevens is alleen mogelijk als voldoende maatregelen zijn genomen om de vertrouwelijkheid, maar vooral ook de juistheid van gegevens te waarborgen. Voor een veilige en betrouwbare invulling van deze toegangsmethode dienen zorgverleners als verantwoordelijke partijen (ook indien delen van de dienstverlening worden uitbesteed aan derden of bewerkers) de huidige wet- en regelgeving hieromtrent te volgen. Via de beveiligingseis in artikel 13 van de Wbp dient de toegangsmethode te worden beveiligd tegen onrechtmatige inzage en verlies van persoonsgegevens. Daarnaast dienen zorgverleners via de Wgbn-z de informatieverwerking voor deze toegangsmethode te beveiligen op basis van de NEN 7510 norm voor informatiebeveiliging in de zorg. Overigens kan voor de nadere technische invulling van beveiligingsmaatregelen voor deze toegangsmethode gebruik worden gemaakt van de NEN 7512 (beveiliging van de uitwisseling van medische gegevens) en NEN 7513 (logging van toegang tot en uitwisseling van medische gegevens) normen worden toegepast. Het CBP en de IGZ zullen als reguliere toezichthouders voor de verwerking van medische gegevens in de zorgsector toezicht houden op de naleving van deze standaarden en eisen door zorgverleners. Ook de gegevensuitwisseling tussen zorgverleners en zorgconsumenten behoeft standaardisatie. De naleving hiervan kan worden getoetst door daartoe geaccrediteerde instellingen.

133 **Financieel:** De ontwikkeling, naleving en toetsing van beveiligings- en uitwisselingsstandaarden evenals de aansluitkosten voor zorginstellingen zullen investeringen van zorgverleners en private partijen vergen. Investeringen vanuit de overheid in dergelijke infrastructuren zijn niet waarschijnlijk gelet op de ontwikkelingen rondom het LSP.

134 **Organisatorisch:** Met directe toegang zal een zorgconsument altijd dezelfde (vastgelegde) informatie hebben als de zorgverlener. Dit kan als voordeel hebben dat zorgconsumenten zelf veel beter op de hoogte zijn van het verloop van het proces. Op het moment dat zorgconsumenten echter een verzoek willen doen voor het toevoegen of wijzigen van informatie in het dossier zal deze informatie op een heldere wijze geannoteerd moeten. Zo is ook voor zorgverleners duidelijk dat deze informatie niet van andere zorgverleners maar van de zorgconsument zelf afkomstig is. Hiervoor zullen mogelijk ook individuele systemen van zorgverleners aangepast moeten worden. Daarnaast zal bij de implementatie van de directe toegang tot de eigen medische gegevens voor zorgconsumenten door zorgverleners moeten worden bepaald welke gegevens kunnen worden ontsloten in het kader van de bescherming van de zorgconsument tegen eventuele nadelige effecten van inzage (zoals bedoeld in BW7:456 lid 3).

135 **Technisch:** Voor een gestandaardiseerde gegevensuitwisseling tussen zorgverleners en zorgconsumenten zijn technische standaarden vereist. Deze kunnen een vergelijkbaar detailniveau hebben als de eisen die in het Programma van Eisen Goed Beheerd Zorgsysteem werden gesteld aan de gegevensuitwisseling tussen zorgverleners via het landelijk schakelpunt. Het is overigens vanuit de optiek van de zorgverlener onwenselijk

om webportalen direct informatie te laten ophalen uit de productieomgeving van het bij de zorgverlener aanwezig informatiesysteem. Dit zou immers bij incidenten kunnen leiden tot een verstoring van de gegevensverwerking en dus de zorgverlening.

136 Directe toegang tot het digitale medisch dossier van zorgverleners voor zorgconsumenten kan goede aansluiting vinden bij de zorgprocessen mits hiertoe voldoende functionaliteiten beschikbaar worden gesteld. Om deze functionaliteiten daadwerkelijk tot nut te laten zijn voor zorgconsumenten dienen zorgverleners samen te werken voor het samenbrengen van medisch dossiers bij de ontsluiting via een webportaal. Hiertoe dienen minimaal gezamenlijke standaarden voor privacy, beveiliging en gegevensuitwisseling overeengekomen te worden. Vervolgens kunnen op basis hiervan uitwisselingsnetwerken worden ingericht.

4.2.2. Portaal beheerd door een derde partij zorgt voor nieuwe functionaliteiten maar vereist ander toezicht

137 Bij het verlenen van toegang via een portaal beheerd door een derde partij zal deze partij de medische gegevens moeten ophalen uit de informatiesystemen van de verschillende zorgverleners en deze vervolgens via een eigen ingericht portaal moeten ontsluiten aan zorgconsumenten.

138 **Bestuurlijk**: Deze vorm van toegang kan aan de markt worden overgelaten. Hierbij dienen wel eisen en standaarden opgesteld te worden als uitwerking van de wettelijke eisen. Door (bestaande of aangepaste) standaarden te hanteren voor de toegang tot de infrastructuur en het beheren van de gegevens kan gewaarborgd worden dat de beherende partij zorgvuldig omgaat met de medische gegevens. Om toegang te krijgen tot de gegevens zal deze partij uitdrukkelijke toestemming van de zorgconsument moeten kunnen aantonen. Daarnaast zullen specifieke eisen aan de standaardisering van de beveiliging en de uitwisseling van medische gegevens moeten worden gesteld zodat derden eenzelfde betrouwbaarheidsniveau inrichten als waartoe zorgverleners via de huidige wet- en regelgeving verplicht zijn.

139 **Financieel**: De kosten voor de invoering van deze toegangmethode zullen uit dezelfde elementen bestaan als die voor de toegangsmethode directe toegang. Deze kosten zullen naar waarschijnlijkheid wel anders worden gedragen. De partijen zouden hierbij verschillende verdienmodellen kunnen opperen, zoals het vragen van een bijdrage door de zorgconsument, verzekering of zorgverlener. In het geval van patiëntportalen die worden ingericht door patiëntenverenigingen zou gedacht kunnen worden aan het afdekken van de ontwikkelkosten via abonnementsgelden van leden of via partners die deze kosten voor door hen gewenste functionaliteiten dragen.

140 **Organisatorisch**: Het door een derde partij beheren van portalen kan – zolang de actualiteit van gegevens voldoende is – even goed aansluiten bij zorgprocessen als een directe toegang. Daarnaast zullen derde partijen meer gericht zijn op het bieden van nieuwe functionaliteiten en zorgapplicaties aan zorgconsumenten. Het is bijvoorbeeld mogelijk om vanuit een verzekeraar een standaardportaal aan te bieden dat aansluit bij de dienstverlening van deze partij, of vanuit een patiëntenvereniging een portaal aan te bieden dat specifieke diensten verleent voor de patiëntengroep. Hierbij is het wel van belang is om voor het beschermen van de rechten van de zorgconsument regels of richtlijnen op te stellen op het gebied van bijvoorbeeld beveiliging en informering zoals bedoeld in de Wbp. Het aanleveren van informatie door de zorgconsument wordt met deze toegangsmethode vereenvoudigd, en zal ook niet leiden tot de noodzaak tot annotatie van data of 'vervuiling' van medisch dossiers. Daarnaast zal ook zorgvuldig de afweging moeten worden gemaakt in welke mate een partij die niet direct bij de behandeling betrokken is mag beschikken over medische gegevens van een zorgconsument. Zoals ook blijkt uit de reactie van het CBP op vragen van Nictiz over het te hanteren doorstartmodel[34] voor het Landelijke Schakelpunt is het niet mogelijk om (zonder expliciete toestemming van de zorgconsument) partijen die niet direct betrokken zijn bij de behandeling van een zorgconsument gegevens hiervan te laten verwerken. Een voorbeeld van een bestaand patiëntenportaal is dat van de Diabetesvereniging Nederland, waarbij het aantal gebruikers zeer hoog is. Een ander voorbeeld is Google Health, dit initiatief is echter beëindigd omdat het gebruik niet hoog genoeg was[35].

141 **Technisch**: Wanneer medische gegevens uit verschillende bronsystemen van zorgverleners moeten worden samengebracht in een door een derde beheerd patiëntenportaal is gegevensstandaardisatie net als bij de

[34] Brief 'Zienswijze CBP over doorstartmodel voor landelijke uitwisseling medische gegevens', 9 augustus 2011.
[35] http://googleblog.blogspot.com/2011/06/update-on-google-health-and-google.html

toegangsmethode directe toegang essentieel. Het is echter te verwachten dat private partijen met eigen verdienmodellen voor de aan de zorgconsument te leveren dienstverlening op een andere manier het belang van geboden functionaliteit tegen aspecten als standaardisering, beveiliging en privacy afwegen. De noodzaak voor normen en standaarden hiervoor lijkt daarmee groter te zijn als voor de toegangsmethode direct toegang. Bovendien komt standaardisering door onderlinge concurrentie tussen private partijen moeizamer tot stand. Een technische drempel voor derde partijen is het feit dat volgens de Wbsn-z private partijen geen gebruik mogen maken van het BSN. Private partijen zullen dan ook over het algemeen (nog) geen gebruik mogen maken van de DigiD-infrastructuur, met behulp van de eNIK of de DigiD Middenvariant als toegangsmiddel.

142 Patiëntenportalen die worden aangeboden en beheerd door private partijen hebben als voordeel dat meer gericht wordt gezocht naar functionaliteit die zorgconsumenten wensen. Private partijen moeten immers een verdienmodel creëren dat is geënt op de voordelen die zorgconsumenten hebben bij gebruik van de aangeboden zorgtoepassingen. Een nadeel hierbij kan zijn dat derde partijen om juist die reden het belang van goede functionaliteit anders afwegen tegen aspecten als standaardisering, beveiliging en privacy dan zorgverleners.

4.3. Conclusie

143 Alle geanalyseerde toegangsmiddelen zijn implementeerbaar, gegeven de noodzakelijke bestuurlijke, financiële, organisatorische en technische maatregelen voor implementatie. De effecten ten gevolge van implementatie van de verschillende toegangsmiddelen verschillen echter op het gebied van kosten en implementatietermijnen. De kosten van een zorgpas zijn zeer hoog en het toepassingsgebied is in de voorgestelde opzet beperkt tot de zorgsector. Daarnaast blijkt uit ervaringen in het buitenland dat het gebruik van een dergelijke pas zeer laag ligt. De eNIK is dankzij structurele overheidsinvesteringen breed inzetbaar maar moet nog ontwikkeld worden en is dus pas op langere termijn beschikbaar (enkele jaren voor de ontwikkeling en maximaal vijf jaar voor de uitgifte). De DigiD Middenvariant met face-to-face-uitgifteproces en conversietabel is als toegangsmiddel voor zorgtoepassingen op kortere termijn beschikbaar (lees ongeveer anderhalf jaar). DigiD Middenvariant is dus op korte termijn het meest haalbaar, maar eNIK is kwalitatief beter en kan op de lange termijn als een haalbaar alternatief worden gezien.

144 Uit de analyse blijkt ook dat beide toegangsmethodes implementeerbaar lijken, gegeven de noodzakelijke bestuurlijke, financiële, organisatorische en technische maatregelen voor implementatie. Directe toegang sluit goed aan op de zorgprocessen, maar vergt samenwerking tussen zorgverleners voor het samenbrengen van medisch dossiers bij de ontsluiting via een webportaal. Hiertoe dienen minimaal gezamenlijke standaarden voor privacy, beveiliging en gegevensuitwisseling overeengekomen te worden. Patiëntenportalen die worden aangeboden en beheerd door derde partijen zorgen voor nieuwe functionaliteiten maar vereisen toezicht op aspecten als standaardisering, beveiliging en privacy. De haalbaarheid van de geselecteerde toegangsmethodes is afhankelijk van de voor- en nadelen van de implementatieaspecten.

5. Drempels voor de realisatie van een elektronische sleutel

5.1. Betrokken partijen ervaren drempels

145 De volgende betrokken partijen ervaren verschillende voor- en nadelen bij de implementatie van een elektronische sleutel bestaande uit een combinatie van de verschillende mogelijkheden voor een toegangsmiddel en -methode:

a) Zorgconsumenten.
b) Zorgverleners.
c) Private partijen.
d) Overheid.

146 Uit onze analyse van de implementatieaspecten voor de geselecteerde toegangsmiddelen en -methoden blijkt dat voor alle betrokken partijen de ervaren nadelen in meer of mindere mate leiden tot drempels voor de implementatie van oplossingen voor een elektronische sleutel.

5.2. Gebruik door zorgconsumenten afhankelijk van vertrouwen en geboden functionaliteit

147 Voor zorgconsumenten speelt voor het toegangsmiddel met name vertrouwen een rol. Daardoor zal een gebrek aan vertrouwen in de beveiliging van het middel een grote drempel kunnen betekenen. Het is daarom noodzakelijk dat over de wijze waarop het middel is ingericht en de beveiliging daarvan is geregeld, transparant naar de zorgconsument wordt gecommuniceerd. Om deze transparantie te vergroten en het vertrouwen van de zorgconsument zo hoog mogelijk te houden is een sterke toezichthouder nodig die de mogelijkheid heeft om stevige maatregelen te treffen en zichtbaar op te treden in het publieke domein.

148 Ditzelfde geldt voor de toegangsmethode. Zorgconsumenten moeten erop kunnen vertrouwen dat zorgverleners de wettelijk verplichte maatregelen ten aanzien van informatiebeveiliging en privacy nemen om hun eigen medische gegevens bij de toegangsmethode direct toegang te beschermen. Transparantie en communicatie hierover wordt nog belangrijker indien de direct toegang wordt geregeld via een webportaal op basis van een uitwisselingsnetwerk van zorgverleners. Daartoe dienen zorgverleners eigen normen en standaarden te ontwikkelen, door te voeren en te laten toetsen om aan de wettelijke eisen te voldoen.

149 Het is ook noodzakelijk dat zorgconsumenten vertrouwen hebben in de toegevoegde waarde van de inzage om dit succesvol te kunnen maken. Wanneer dit onvoldoende aanwezig is zal een oplossing beperkt gebruikt worden waardoor eventuele verbeteringen in de efficiëntie en effectiviteit van zorgverlening niet vergroot worden. Verschillende voorbeelden in het buitenland laten zien dat de toegevoegde waarde niet altijd gerealiseerd kan worden. Zo is het gebruik in het Verenigd Koninkrijk zeer laag[36], blijkt dat het gebruik van de Duitse eGK ook tegenvalt[37] en heeft Google het initiatief Google Health beëindigd vanwege het beperkte gebruik[38]. Nieuwe functionaliteiten zoals het indienen van een verzoek tot aanpassing of aanvulling van het eigen medisch dossier bij de zorgverleners kunnen het gebruik van een elektronische sleutel door zorgconsumenten stimuleren.

[36] Brief van de minister van VWS aan de Tweede Kamer betreft Voortgangsrapportage landelijke infrastructuur voor gegevensuitwisseling in de zorg vierde kwartaal 2010, kenmerk MEVA/ICT,3044841, 13 januari 2011.
[37] Evaluationsbericht im Rahmen der Testregionen übergreifenden Evaluation der 10.000er Tests bei der Einführung der elektronischen Gesundheitskarte, juni 2009.
[38] http://googleblog.blogspot.com/2011/06/update-on-google-health-and-google.html

5.3. Zorgverleners moeten huidige informatiesystemen aanpassen en beveiligen

150 Voor zorgverleners is het gekozen toegangsmiddel van beperkte invloed. Wel kunnen zorgverleners baat hebben bij de wijze waarop de zorgconsument toegang krijgt tot de gegevens en de wijze waarop de zorgconsument gegevens kan aanvullen. Met name met de toegangsmethode directe toegang kunnen verzoeken vanuit zorgconsumenten tot het aanpassen en aanvullen van het eigen medisch dossier zorgverleners ondersteunen bij de uitvoering van de zorgprocessen.

151 Voor zorgverleners is het wel van belang dat rekening wordt gehouden met de benodigde aanpassingen in systemen en de noodzakelijke maatregelen voor de informatiebeveiliging van de gegevensverwerking.

152 De invoering van de NEN 7510 norm bij de ziekenhuizen in de laatste drie jaar laten echter zien dat zorgverleners nog niet altijd uit zichzelf genegen zijn de benodigde normen en standaarden zelfstandig op te zetten en te implementeren. Bij indirecte toegang via een door een derde partij beheerd portaal geldt dit uiteraard ook, met de toevoeging dat er ook aan de opslag en verwerking van de persoonsgegevens strenge eisen gesteld dienen te worden.

5.4. Private partijen hebben niet dezelfde faciliteiten als zorgverleners

153 Volgens de Wbsn-z is het BSN vanwege privacy overwegingen alleen voor bij wet aangewezen zorgverleners, zorgverzekeraars en indicatie-instellingen beschikbaar. Private partijen zijn niet bij wet aangewezen tot het gebruik van het BSN, dit is een technische drempel voor private partijen om gebruik te mogen maken van de DigiD-infrastructuur, met behulp van de eNIK of de DigiD Middenvariant als toegangsmiddel. Dit vormt tevens een drempel bij het opzetten van patiëntenportalen waarbij de medische gegevens vanuit verschillende zorgverleners bij elkaar worden gebracht door een private partij (na uitdrukkelijke toestemming van de zorgconsument per toe te voegen dossier). Private partijen kunnen immers ook geen gebruik maken van het BSN om medische gegevens vanuit meerdere zorgverleners via het BSN te relateren aan één zorgconsument. Daarnaast kunnen persoons- en BSN-gegevens door private partijen niet worden gecontroleerd en geverifieerd via de centrale voorzieningen die hiertoe voor zorgverleners beschikbaar zijn (SBV-Z).

154 Voor private partijen, dat wil zeggen alle partijen die geen zorgverlener zijn, is een zelfstandige positieve business case noodzakelijk, ongeacht het toegangsmiddel of de toegangsmethode. Private partijen hebben per definitie het meeste baat bij een zo vrij mogelijke invulling van de patiëntrechten, maar vanwege privacyoverwegingen zijn zorgconsumenten hier niet altijd bij gebaat. Indien geen voldoende rendabel verdienmodel kan worden gecreëerd door private partijen zullen de voor de zorgconsument benodigde functionaliteiten en diensten voor de digitale invulling van de patiëntrechten niet worden gerealiseerd. Hoewel enkele initiatieven van koplopers op het gebied van patiëntenportalen laten zien dat het mogelijk is om diensten voor zorgconsumenten te realiseren (en er dus een beoogde businesscase bestaat) lijkt met name het verschil in de plaats waar de kosten en de baten worden gerealiseerd een drempel te vormen. Indien het verlenen van toegang tot een digitale versie van het medisch dossier door zorgverleners aan zorgconsumenten per 1 januari 2013 een verplichting wordt (zoals omschreven in de door de Tweede Kamer aangenomen motie 70) zou een stimulans kunnen betekenen voor het opzetten van portalen omdat dan tenminste de inzage- en afschriftfunctionaliteit wettelijk verplicht wordt gesteld.

5.5. Standaardisatie- en toezicht moeten worden ingevoerd

155 De overheid kan een belangrijke rol vervullen bij de correcte invulling van een toegangsmiddel voor zorgapplicaties waarmee medische gegevens worden uitgewisseld tussen zorgverleners en zorgconsumenten. Dit kan via de implementatie van een nationaal toegangsmiddel en via toezicht op de goede inrichting van toegang tot verwerkingen van medische gegevens door private partijen (zoals in het geval van door private partijen beheerde patiëntenportalen).

156 Voor private partijen is het gebruik van de DigiD-infrastructuur zoals toegelicht een drempel, aangezien het BSN niet mag worden verwerkt. Zoals uit de inventarisatie van Nictiz van al bestaande patiëntenportalen in Nederland[39] blijkt, bestaan er momenteel initiatieven in de markt waarvoor het toegangsmiddel niet aan het noodzakelijke beveiligingsniveau voldoet. Toezicht op een goede en veilige implementatie van alternatieven door private partijen is niet eenvoudig in te richten zonder heldere standaard voor het minimaal te hanteren vertrouwensniveau voor het te gebruiken toegangsmiddel.

157 Ten aanzien van de toegangsmethode is in het geval van directe toegang het huidige stelsel van geldende eisen en toezicht ten aanzien van de verwerking van medische gegevens van toepassing. Welke beveiligingsniveaus moeten worden gehanteerd bij de inrichting van webportalen zijn momenteel niet expliciet niet beschreven in de geldende wet- en regelgeving.

158 Ten aanzien van de toegangsmethode waarbij een patiëntenportaal door een derde partij wordt beheerd, is een belangrijke drempel het toelaten van partijen om op een veilige wijze uitvoering te geven aan de toegangsmethode directe toegang. Bij het kiezen van een scenario waarbij marktpartijen delen van de uitvoering van de oplossing uitvoeren kunnen innovatieve oplossingen ontstaan. Dit is een voordeel vanwege de mogelijke positieve effecten op de efficiëntie van zorgverlening. Dit kan echter ook leiden tot het opzoeken van grenzen van wetgeving. Daarom dient duidelijkheid te bestaan ten aanzien van de geldende eisen voor zorgverleners en marktpartijen. De overheid zal een verantwoordelijkheid houden om erop toe te zien dat zorgconsumenten voldoende beschermd worden tegen onzorgvuldige omgang met hun gegevens. Het ligt daarom voor de hand dat gegevens-, uitwisselings- en beveiligingsstandaarden dienen te worden opgesteld, ingevoerd en getoetst.

159 Het opstellen van de standaard hoeft niet noodzakelijk een taak van de overheid te zijn, het handhaven van naleving wel. Aangewezen toezichthouders daarvoor zijn het CBP (immers voor alle toegangsmiddelen en -methoden geldt dat het verwerkingen van persoonsgegevens en/of medische persoonsgegevens betreft) en de IGZ (in het geval van implementatie door zorgverleners).

5.6. Conclusie

160 Zorgconsumenten, zorgverleners, private partijen en de overheid kunnen verschillende voor- en nadelen ervaren bij de implementatie van een elektronische sleutel bestaande uit een combinatie van de verschillende mogelijkheden voor een toegangsmiddel en -methode. Uit onze analyse van de implementatieaspecten voor de geselecteerde toegangsmiddelen en -methoden (hoofdstuk 4) blijkt dat voor alle betrokken partijen de ervaren nadelen in meer of mindere mate leiden tot drempels voor de implementatie van oplossingen voor een elektronische sleutel.

161 De volgende implementatiedrempels staan de realisatie van een middel voor elektronische toegang tot de eigen medische gegevensmogelijk in de weg:

a) Het gebruik van een elektronische sleutel door zorgconsumenten is afhankelijk van het vertrouwen in de sleutel en de geboden functionaliteit.
b) Zorgverleners zullen hun huidige informatiesystemen moeten aanpassen en beveiligen om zorgconsumenten toegang te geven tot medische gegevens.
c) Private partijen hebben niet dezelfde faciliteiten als zorgverleners. Private partijen zijn niet bij wet aangewezen tot het gebruik van het BSN, dit is een drempel voor private partijen om gebruik te mogen maken van de DigiD-infrastructuur, met behulp van de eNIK of de DigiD Middenvariant als toegangsmiddel.
d) Standaardisatie en toezicht moeten worden ingevoerd. Bij het kiezen van een scenario waarbij marktpartijen delen van de uitvoering van de oplossing uitvoeren kunnen innovatieve oplossingen ontstaan. Dit is een voordeel vanwege de mogelijke positieve effecten op de efficiëntie van zorgverlening. Dit kan echter ook leiden tot het opzoeken van grenzen van wetgeving. Daarom dienen de toezichthouders sterk in het publieke domein optreden indien noodzakelijk. Het ligt daarom voor de hand dat gegevens-, uitwisselings- en beveiligingsstandaarden dienen te worden opgesteld, ingevoerd en getoetst.

[39] Online inzage in mijn medische gegevens, Patiëntportalen in Nederland, Nictiz, RP 110013, 16 mei 2011

6. Verlagen van drempels via groeipad en regulering

6.1. Kies voor een groeistrategie voor het toegangsmiddel

162 De afwezigheid van een breed beschikbaar toegangsmiddel voor het verlenen van toegang tot het eigen digitale medisch dossier aan zorgconsumenten kan worden opgelost door de implementatie van de eNIK en/of de DigiD Middenvariant met face-to-faceuitgifte van een activatiecode aangevuld met een conversietabel te implementeren binnen de DigiD-infrastructuur. De implementatie van een zorgpas biedt, gezien de zeer hoge implementatiekosten en de ervaringen uit het verleden ten aanzien van de zeer beperkte toegevoegde waarde in het zorgproces, geen afdoende oplossing.

163 Daarbij is de eNIK op de lange termijn technisch gezien het meest geschikte middel. De implementatie daarvan vergt echter nog enkele jaren implementatietijd waarna in een overgangsfase via reguliere vervanging het nog 5 jaar duurt alvorens iedere Nederlander over dit toegangsmiddel kan beschikken.

164 Gezien het feit dat er de komende jaren geen eNIK voorhanden zal zijn en de afwezigheid van een centraal beschikbaar gesteld toegangsmiddel dat kan voldoen aan het referentiekader een drempel vormt, bevelen wij aan een 'groeipadstrategie' te overwegen. Het is mogelijk een'groeipadstrategie' te hanteren waarbij op de kortere termijn (denk aan ongeveer 1,5 jaar) de DigiD Middenvariant als hoogst beschikbare vertrouwensniveau voor DigiD wordt gehanteerd ten behoeve van toepassingen in de zorgsector. Daarbij wordt dan tegelijkertijd een groeipad gedefinieerd om op de langere termijn invulling te geven aan DigiD met vertrouwensniveau hoog op basis van de eNIK als middel. Zo kan worden aangesloten bij de eis om gegevens te beveiliging 'rekening houdend met de stand van de techniek en de kosten van tenuitvoerlegging' (art. 13 Wbp). Ook wordt hiermee de implementatie van een toegangsmiddel en -methode onafhankelijk van de introductie van de eNIK, en kan de DigiD Middenvariant dienen als alternatief tot de methode niet meer veilig genoeg wordt geacht.

165 Het hanteren van een dergelijke strategie kan kostenvoordelen opleveren wanneer door middel van de DigiD Middenvariant een nieuwe invulling wordt gegeven aan DigiD met vertrouwensniveau midden. De DigiD Middenvariant kan immers ook na het beschikbaar komen van de eNIK worden gebruikt voor andere (overheids)diensten.

166 Voor private initiatieven waarbij geen gebruik kan worden gemaakt van de DigiD-infrastructuur, kan de overheid ervoor kiezen het veld een standaard voor het in te richten vertrouwensniveau voor het toegangsmiddel in overleg met de betrokken partijen op te laten stellen, waarbij geldt dat een invulling van de wet als minimumeis tenminste zo veilig dient te zijn als DigiD of eNIK. Het toezicht op de naleving van deze standaard kan dan bij het CBP als toezichthouder voor de verwerking van persoonsgegevens worden belegd. Een wijze om dit te realiseren is het formuleren van generieke eisen aan het te gebruiken toegangsmiddel voor het geven van toegang tot de eigen digitale medische gegevens aan zorgconsumenten. Deze zouden dan kunnen worden geborgd in de voorgenomen specifieke functionele, technische en organisatorische eisen aan elektronische gegevensverwerking in de zorg via een Algemene Maatregel van Bestuur op basis van artikel 26 Wbp[40].

6.2. Reguleer en houd toezicht op de toegangsmethode

167 Na het afwijzen van de EPD-wet ligt de invulling van gestandaardiseerde digitale gegevensuitwisseling tussen zorgverleners onderling en tussen zorgverleners en zorgconsumenten primair bij partijen in de zorgsector. Dit betekent dat de zorgsector zelf (eventueel in samenwerking met derde partijen) de gegevensuitwisseling tussen zorgverleners verder vorm moet gaan geven.

[40] Juridische analyse elektronische gegevensuitwisseling in de zorg, brief van minister van VWS aan de Tweede Kamer, d.d. 27 juni 2011.

168 In de nabije toekomst zal motie 70 (zoals aangenomen in de Tweede Kamer) ten uitvoer worden gebracht, dientengevolge zullen zorgverleners verplicht worden om ook digitale gegevensuitwisseling tussen zorgverleners en zorgconsumenten mogelijk te gaan maken. Hierbij zou het aansluiten van portalen op bestaande uitwisselingsnetwerken voor zorgverleners plaats kunnen vinden. De omgang met gegevens binnen de portalen en de toegang door zorgconsumenten zou ook onder strikt toezicht moeten staan van de toezichthouders IGZ (voor zover het de kwaliteit van geleverde zorg betreft) en het CBP (voor wat betreft de verwerking van gevoelige persoonsgegevens onder de Wbp en Wgbo). Door middel van de aangenomen motie Y[41] in de Eerste Kamer is al aangegeven dat een bepaalde mate van beveiliging door de overheid door middel van een wettelijke regeling zal moeten worden ingericht. Ook dit lijkt het beste te realiseren via aanvullende eisen via een AMvB op basis van artikel 26 Wbp. Dergelijke eisen vormen tevens een noodzakelijke basis voor goed toezicht.

6.3. Conclusie

169 De implementatiedrempels beschreven in hoofdstuk 5 kunnen worden weggenomen als wordt gekozen voor de volgende adviezen:

a) *Kies voor een groeistrategie voor het toegangsmiddel.* Gezien het feit dat er de komende jaren geen eNIK voorhanden zal zijn en de afwezigheid van een centraal beschikbaar gesteld toegangsmiddel dat kan voldoen aan het referentiekader een drempel vormt, bevelen wij aan een 'groeipadstrategie' te overwegen. Het is mogelijk een'groeipadstrategie' te hanteren waarbij op de kortere termijn de DigiD Middenvariant als hoogst beschikbare vertrouwensniveau voor DigiD wordt gehanteerd ten behoeve van toepassingen in de zorgsector. Daarbij wordt dan tegelijkertijd een groeipad gedefinieerd om op de langere termijn invulling te geven aan DigiD met vertrouwensniveau hoog op basis van de eNIK als middel.
Voor private initiatieven waarbij geen gebruik gemaakt kan worden van de DigiD-infrastructuur kan de overheid ervoor kiezen het veld een standaard voor het minimaal in te richten vertrouwensniveau voor het toegangsmiddel in overleg met de betrokken partijen op te laten stellen. Het toezicht op de naleving van deze standaard kan dan bij het CBP als toezichthouder voor de verwerking van persoonsgegevens worden belegd.

b) *Reguleer en houd toezicht op de toegangsmethode.* In de nabije toekomst zal motie 70 ten uitvoer worden gebracht, zorgverleners zullen verplicht worden om ook digitale gegevensuitwisseling tussen zorgverleners en zorgconsumenten mogelijk te gaan maken. Dit kan op verschillende manieren worden gerealiseerd. De omgang met gegevens en de toegang door zorgconsumenten moet onder strikt toezicht komen te staan. De IGZ kan samen met het CBP deze taak op zich nemen.

170 Deze adviezen zouden beide kunnen worden geborgd via een Algemene Maatregel van Bestuur op basis van artikel 26 Wbp. In deze AMvB kunnen de specifieke functionele, technische en organisatorische eisen (waaronder een minimumniveau van beveiliging) aan elektronische gegevensverwerking in de zorg worden beschreven. De invulling van deze eisen zal door de markt op zich worden genomen.

[41] Motie Y van het Kamerlid Tan c.s, voorgesteld 5 april 2011

A. Eisen aan de elektronische sleutel

A.1. Juridische eisen

171 De juridische eisen geven weer welke rechten een zorgconsument heeft. Deze rechten kunnen voortkomen uit de wetgeving die op dit gebied bestaat, maar ook uit (voorgenomen) besluiten en moties.

J.1	Type eis:	Bron:
	Juridisch / regelgeving	4 Wbsn-z 12 Wabb NEN7512
Samenvatting:	Voorkómen van onbevoegd gebruik: goede identificatie van de zorgconsument, zodat zekerheid bestaat over zijn identiteit.	
Beschrijving:	*Een zorgaanbieder gebruikt het burgerservicenummer van een cliënt met het doel te waarborgen dat de in het kader van de verlening van zorg te verwerken persoonsgegevens op die cliënt betrekking hebben.*	

J.2	Type eis:	Bron:
	Juridisch / regelgeving	88 Wet BIG 13 Wbp AV23
Samenvatting:	Voldoende borging van de vertrouwelijkheid van de gegevens.	
Beschrijving:	*Een ieder is verplicht geheimhouding in acht te nemen ten opzichte van al datgene wat hem bij het uitoefenen van zijn beroep op het gebied van de individuele gezondheidszorg als geheim is toevertrouwd, of wat daarbij als geheim te zijner kennis is gekomen of wat daarbij te zijner kennis is gekomen en waarvan hij het vertrouwelijke karakter moest begrijpen.* *De verantwoordelijke legt passende technische en organisatorische maatregelen ten uitvoer om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Deze maatregelen garanderen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau gelet op de risico's die de verwerking en de aard van te beschermen gegevens met zich meebrengen. De maatregelen zijn er mede op gericht onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen.*	

J.3	Type eis:	Bron:
	Juridisch / regelgeving	7:448 BW (WGBO)
Samenvatting:	De mogelijkheid voor de zorgverlener om gegevens af te schermen en anderen toegang te verlenen.	
Beschrijving:	*3. De hulpverlener mag de zorgconsument bedoelde inlichtingen slechts onthouden voor zover het verstrekken ervan kennelijk ernstig nadeel voor de zorgconsument zou opleveren. Indien het belang van de zorgconsument dit vereist, dient de hulpverlener de desbetreffende inlichtingen aan een ander dan de zorgconsument te verstrekken. De inlichtingen worden de zorgconsument alsnog gegeven, zodra bedoeld nadeel niet meer te duchten is. De hulpverlener maakt geen gebruik van zijn in de eerste volzin bedoelde bevoegdheid dan nadat hij daarover een andere hulpverlener heeft geraadpleegd.*	

J.4	Type eis:	Bron:
	Juridisch / regelgeving	7:456 BW (WGBO)
Samenvatting:	Inzage en het dossier op een zo kort mogelijke termijn.	
Beschrijving:	*De hulpverlener verstrekt aan de zorgconsument desgevraagd zo spoedig mogelijk inzage in en afschrift van de bescheiden, bedoeld in artikel 454. De verstrekking blijft achterwege voor zover dit noodzakelijk is in het belang van de bescherming van de persoonlijke levenssfeer van een ander. De hulpverlener mag voor de verstrekking van het afschrift een redelijke vergoeding in rekening brengen.*	

J.5	Type eis:	Bron:
	Juridisch / regelgeving	7:457 BW (WGBO)
Samenvatting:	Doorlevering van gegevens aan derden alleen met toestemming van de zorgconsument, tenzij een wettelijke verplichting tot doorlevering bestaat of het een doorlevering aan een hulpverlener betreft die op dat moment een behandelrelatie heeft met de zorgconsument.	
Beschrijving:	*1. Onverminderd het in artikel 448 lid 3, tweede volzin, bepaalde draagt de hulpverlener zorg, dat aan anderen dan de zorgconsument geen inlichtingen over de zorgconsument dan wel inzage in of afschrift van de bescheiden, bedoeld in artikel 454, worden verstrekt dan met toestemming van de patiënt. Indien verstrekking plaatsvindt, geschiedt deze slechts voor zover daardoor de persoonlijke levenssfeer van een ander niet wordt geschaad. De verstrekking kan geschieden zonder inachtneming van de beperkingen, bedoeld in de voorgaande volzinnen, indien het bij of krachtens de wet bepaalde daartoe verplicht.* *2. Onder anderen dan de zorgconsument zijn niet begrepen degenen die rechtstreeks betrokken zijn bij de uitvoering van de behandelingsovereenkomst en degene die optreedt als vervanger van de hulpverlener, voor zover de verstrekking noodzakelijk is voor de door hen in dat kader te verrichten werkzaamheden.* *3. Daaronder zijn evenmin begrepen degenen wier toestemming ter zake van de uitvoering van de behandelingsovereenkomst op grond van de artikelen 450 en 465 is vereist. Indien de hulpverlener door inlichtingen over de zorgconsument dan wel inzage in of afschrift van de bescheiden te verstrekken niet geacht kan worden de zorg van een goed hulpverlener in acht te nemen, laat hij zulks achterwege.*	

J.6	Type eis:	Bron:
	Juridisch / regelgeving	35 Wbp
Samenvatting:	De zorgconsument dient informatie te krijgen over de verwerking van zijn persoonsgegevens.	
Beschrijving:	*1.De betrokkene heeft het recht zich vrijelijk en met redelijke tussenpozen tot de verantwoordelijke te wenden met het verzoek hem mede te delen of hem betreffende persoonsgegevens worden verwerkt. De verantwoordelijke deelt de betrokkene schriftelijk binnen vier weken mee of hem betreffende persoonsgegevens worden verwerkt.* *2.Indien zodanige gegevens worden verwerkt, bevat de mededeling een volledig overzicht daarvan in begrijpelijke vorm, een omschrijving van het doel of de doeleinden van de verwerking, de categorieën van gegevens waarop de verwerking betrekking heeft en de ontvangers of categorieën van ontvangers, alsmede de beschikbare informatie over de herkomst van de gegevens.* *3.Voordat een verantwoordelijke een mededeling doet als bedoeld in het eerste lid, waartegen een derde naar verwachting bedenkingen zal hebben, stelt hij die derde in de gelegenheid zijn zienswijze naar voren te brengen indien de mededeling gegevens bevat die hem betreffen, tenzij dit onmogelijk blijkt of een onevenredige inspanning kost.* *4.Desgevraagd doet de verantwoordelijke mededelingen omtrent de logica die ten grondslag ligt aan de geautomatiseerde verwerking van hem betreffende gegevens.*	

J.7	Type eis:	Bron:
	Juridisch / regelgeving	36 Wbp 7:454 BW (WGBO)
Samenvatting:	De zorgconsument moet kunnen verzoeken om zijn gegevens aan te vullen, te wijzigen, te verwijderen of af te schermen.	
Beschrijving:	*1. Degene aan wie overeenkomstig artikel 35 kennis is gegeven van hem betreffende persoonsgegevens, kan de verantwoordelijke verzoeken deze te verbeteren, aan te vullen, te verwijderen, of af te schermen indien deze feitelijk onjuist zijn, voor het doel of de doeleinden van de verwerking onvolledig of niet ter zake dienend zijn dan wel anderszins in strijd met een wettelijk voorschrift worden verwerkt. Het verzoek bevat de aan te brengen wijzigingen.* *2. De verantwoordelijke bericht de verzoeker binnen vier weken na ontvangst van het verzoek schriftelijk of dan wel in hoeverre hij daaraan voldoet. Een weigering is met redenen omkleed.* *3. De verantwoordelijke draagt zorg dat een beslissing tot verbetering, aanvulling, verwijdering of afscherming zo spoedig mogelijk wordt uitgevoerd.* *4. Indien de persoonsgegevens zijn vastgelegd op een gegevensdrager waarin geen wijzigingen kunnen worden aangebracht, dan treft hij de voorzieningen die nodig zijn om de gebruiker van de gegevens te informeren over de onmogelijkheid van verbetering, aanvulling, verwijdering of afscherming ondanks het feit dat er grond is voor aanpassing van de gegevens op grond van dit artikel.* *5. Het bepaalde in het eerste tot en met vierde lid is niet van toepassing op bij de wet ingestelde openbare registers, indien in die wet een bijzondere procedure voor de verbetering, aanvulling, verwijdering of afscherming van gegevens is opgenomen.*	

J.8	Type eis:	Bron:
	Juridisch / regelgeving	Motie Y
Samenvatting:	De zorgconsument moet inzage krijgen in de uitwisseling van gegevens.	
Beschrijving:	*[…]inzage door de patiënt, het verstrekken van afschrift aan de zorgconsument en transport van gegevens op verzoek van de patiënt, teneinde veilig digitaal transport van gegevens (zowel pull als push) mogelijk te maken tussen zorgverleners binnen een regio, […]*	

J.9	Type eis:	Bron:
	Juridisch / regelgeving	Motie 70
Samenvatting:	De zorgconsument moet op digitale wijze inzage krijgen in het eigen medisch dossier wat in het kader van de geneeskundige behandeling door zorgverleners wordt bijgehouden.	
Beschrijving:	*[…]vast te leggen in de WGBO dat consumenten per 1 januari 2013 recht hebben op inzage in en afschrift van, op elektronische wijze, hun gehele elektronische dossier bij de zorgverlener, en de zorgverlener te verplichten, dit recht op elektronische inzage en afschrift te faciliteren, […]*	

J.10	Type eis:	Bron:
	Juridisch / regelgeving	Motie 69
Samenvatting:	De zorgconsument moet kunnen beschikken over een lijst met voorgeschreven medicatie en moet deze kunnen aanvullen met zelfmedicatie.	
Beschrijving:	*[…] verzoekt de regering vast te leggen dat een zorgconsument bij de uitgifte van medicijnen op dat moment direct recht heeft op kostenloze inzage in papieren en/of elektronische vorm van de aan hem voorgeschreven medicijnen, evenals het recht op aanvulling van deze lijst met zelfmedicatie die gebruikt wordt,[…]*	

J.11	Type eis:	Bron:
	Juridisch / regelgeving	Visiedocument NPCF
Samenvatting:	De toegang tot de digitale medische gegevens is gebruiksvriendelijk, algemeen beschikbaar en bezorgt de zorgconsument zo min mogelijk administratieve lasten.	
Beschrijving:	Om de zorgconsument zo min mogelijk administratief te belasten dient rekening gehouden te worden bij de keuze voor en inrichting van een toegangsmiddel en –methode met het proces van uitgifte en het gebruik hiervan. Hierbij is het ook belangrijk dat de zorgconsument het mogelijk wordt gemaakt om op één centrale plek toegang te krijgen tot de gegevens van meerdere zorgaanbieders.	

J.12	Type eis:	Bron:
	Juridisch / regelgeving	Zorgpas Eemland
Samenvatting:	Digitale medische gegevens dienen altijd actueel te zijn, zowel voor de zorgconsument als voor de zorgverlener.	
Beschrijving:	Om de zorgconsument inzicht te kunnen geven in zijn behandeling en de zorgconsument goed geïnformeerd te houden, moeten de beschikbare gegevens zo actueel mogelijk zijn en tijdens de behandeling beschikbaar gemaakt worden.	

A.2. Functionele eisen

172 De functionele eisen volgen uit de rechten die de zorgconsument heeft op het gebied van (toegang tot) zijn digitale medische gegevens. In deze eisen wordt aangegeven hoe invulling gegeven kan worden aan de hiervoor beschreven patiëntrechten.

F.1	Type eis:	Bron:
	Functioneel	J.4, J.9, J.10, J.11, J.12, NPCF
Samenvatting:	De zorgconsument kan gebruikmakend van de elektronische sleutel op veilige en betrouwbare wijze zijn actuele digitale patiëntgegevens elektronisch opvragen, raadplegen en aanvullen.	
Beschrijving:	Een belangrijk doel voor zorgconsumenten is het verlenen van toegang tot de eigen medische gegevens die worden gebruikt binnen de verschillende zorginstellingen. In Nederland hebben zorgconsumenten het recht om inzage te krijgen in de eigen gegevens. Met het introduceren van elektronische zorgconsumenten dossiers is het mogelijk om zorgconsumenten digitaal inzage in het eigen medisch dossier te geven. De actualiteit van de medische gegevens waartoe de zorgconsument toegang verkrijgt dient te zijn geborgd. Ook moet de zorgconsument de mogelijkheid worden geboden om medische gegevens aan te vullen met eigen gegevens (metingen, zelfmedicatie, etc.) waarbij te onderscheiden is dat de zorgconsument deze heeft aangevuld.	

F.2	Type eis:	Bron:
	Functioneel	J.5
Samenvatting:	De zorgconsument heeft gebruikmakend van de elektronische sleutel controle over wie toegang heeft tot zijn digitale medische gegevens.	
Beschrijving:	De zorgconsument moet controle hebben over wie toegang heeft tot zijn medische gegevens. Wettelijke voorzieningen om standaard toegang te verlenen in het geval van een aanwezige behandelrelatie (en controle achteraf op het daadwerkelijk aanwezig zijn van een dergelijke relatie) blijven uiteraard van toepassing. Voor aanvullende toegang dient de zorgconsument te kunnen bepalen wie toegang krijgt.	

F.3	Type eis:	Bron:
	Functioneel	J.5, NPCF
Samenvatting:	De zorgconsument kan gebruikmakend van de elektronische sleutel toestemming geven om gegevens aan derden beschikbaar te stellen.	
Beschrijving:	De elektronische sleutel dient de mogelijkheid te bieden om toestemming te geven voor het transport van gegevens naar derden.	

F.4	Type eis:	Bron:
	Functioneel	J.6, J.8, NPCF
Samenvatting:	De zorgconsument kan gebruikmakend van de elektronische sleutel inzage te krijgen in de verwerking van zijn gegevens.	
Beschrijving:	De zorgconsument heeft het recht inzage in de verwerking van zijn gegevens te krijgen. Door middel van het toegangsmiddel kan de zorgconsument aantonen dat hij de persoon is op wie de gegevens betrekking hebben.	

F.5	Type eis:	Bron:
	Functioneel	J.2
Samenvatting:	Er wordt gebruikt gemaakt van algemeen geaccepteerde beveiligingsmethoden, rekening houdend met het risiconiveau van de gegevens.	
Beschrijving:	Er dient vertrouwelijk omgegaan te worden met de medische gegevens, hierbij rekening houdend met het verhoogde risiconiveau dat hiervoor geldt. Het is noodzakelijk dat er een bepaalde mate van zekerheid is waarbinnen gesteld kan worden dat de gegevens beschermd zijn. Hiervoor dienen algemeen geaccepteerde methoden te worden gebruikt.	

F.6	Type eis:	Bron:
	Functioneel	Brief minister Schippers (T01279), Zorgpas Eemland
Samenvatting:	De elektronische sleutel heeft de mogelijkheid om beperkt medische gegevens op te slaan voor gebruik in noodgevallen.	
Beschrijving:	In noodgevallen kan het nut hebben om bepaalde gegevens direct toegankelijk te hebben voor hulpverleners. De elektronische sleutel zou hiervoor een logische keuze kunnen zijn. Het is van belang om de bepaling *welke* gegevens te laten doen door de gebruikers van de gegevens: de hulpverleners zelf. Alleen deze kunnen bepalen welke gegevens in noodgevallen nut zouden kunnen hebben. De eisen op het gebied van controle van de zorgconsument over toegang tot deze gegevens zijn overigens ook van toepassing op deze specifieke gegevens.	

F.7	Type eis:	Bron:
	Functioneel	J.7
Samenvatting:	De elektronische sleutel kan gebruikt worden om het recht op verbetering, aanvulling, verwijdering of afscherming uit te oefenen.	
Beschrijving:	Zorgconsumenten hebben in het kader van art. 36 Wbp het recht gegevens te verbeteren, aan te vullen, te verwijderen of af te laten schermen. De elektronische sleutel moet geschikt zijn om het uitoefenen van dit recht mogelijk te maken of te faciliteren door middel van identificatie van de zorgconsument.	

F.8	Type eis:	Bron:
	Functioneel	Patiëntportalen
Samenvatting:	Er is sprake van eenheid van taal tussen de elektronische sleutel en de informatiesystemen van zorgaanbieders waar het aan wordt gekoppeld.	
Beschrijving:	Om gegevens uit te wisselen tussen systemen is het belangrijk dat de inhoud uitwisselbaar is. Uit ervaringen met eerdere patiëntportalen blijkt dat het noodzakelijk is voor een effectief gebruik van de gegevens dat deze op eenduidige wijze omgaan met de inhoud.	

F.9	Type eis:	Bron:
	Functioneel	J.3, J.7
Samenvatting:	Het recht op inzage in de digitale medische gegevens moet overgedragen en afgeschermd kunnen worden.	
Beschrijving:	Om derden inzage te kunnen geven in gegevens en deze (gedeeltelijk) af te kunnen schermen dient het mogelijk te zijn het recht op inzage over te kunnen dragen en af te kunnen schermen.	

F.10	Type eis:	Bron:
	Functioneel	J.1
Samenvatting:	De elektronische sleutel kan de zorgconsument op sterke wijze identificeren.	
Beschrijving:	Het is wettelijk verplicht het BSN van de zorgconsument te controleren. Om de koppeling tussen de oplossing, BSN en zorgconsument te kunnen maken moet het mogelijk zijn om na te gaan of het BSN van de zorgconsument het juiste is. Hiervoor is het overigens technisch niet strikt noodzakelijk om het BSN op het middel op te slaan.	

A.3. Technische eisen

173 De hieronder beschreven technische eisen geven aan op welke wijze de invulling van de functionele eisen gefaciliteerd kan worden. Deze eisen kunnen hierdoor zowel betrekking hebben op het gebruik als het uitgifteproces van het toegangsmiddel. Daarnaast zijn eisen geformuleerd voor de inrichting van de toegangsmethode.

174 Als bronnen zijn aangegeven de hierboven genoemde functionele eisen, de standaard NEN 7512: Vertrouwensbasis voor gegevensuitwisseling en onze eerdere rapportages 'Beveiligingeisen ten aanzien van identificatie en authenticatie voor toegang zorgconsument tot het Elektronisch Patiëntendossier (EPD)' (2008-3027/OV/rvdk/mp) en 'Risicoanalyse de DigiD Middenvariant - Naar aanleiding van de A5/1 kwetsbaarheid in GSM', (2010-1400/OV/ev/mp).

T.1	Type eis:	Relevant voor onderdeel:	Bron:
	Technisch	Toegangsmiddel	F.1, 2008-3027
Samenvatting:	Het toegangsmiddel zelf is niet kopieerbaar.		
Beschrijving:	Een middel mag technisch niet (eenvoudig) te kopiëren zijn, zodat als de persoon het middel in bezit heeft met een grote mate van zekerheid kan worden vastgesteld dat het middel alleen in het bezit van de betreffende gebruiker is. Indien gebruik wordt gemaakt van een opslagmogelijkheid op het middel voor noodgevallen geldt deze eis niet voor die gegevens.		

T.2	Type eis:	Relevant voor onderdeel:	Bron:
	Technisch	Toegangsmiddel	F.1, F.3, F.4, 2008-3027
Samenvatting:	Het toegangsmiddel is 1-op-1 gekoppeld aan een gebruikersaccount en is uniek identificeerbaar.		
Beschrijving:	Met één digitale sleutel kan alleen toegang verkregen worden tot één specifiek gebruikersaccount. Dit betekent dat toegang tot meerdere accounts met één digitale sleutel en toegang tot één account met meerdere digitale sleutels voorkomen dient te worden. Aangezien het toegangsmiddel 1-op-1 aan een gebruikersaccount gekoppeld dient te zijn en het middel herkenbaar dient te zijn moet elk middel uniek te identificeren zijn, bijvoorbeeld door dit te koppelen aan het BSN of door bij het uitgifteproces hier gebruik van te maken.		

T.3	Type eis:	Relevant voor onderdeel:	Bron:
	Technisch	Toegangsmiddel	F.1, F.5, NEN 7512, 2008-3027
Samenvatting:	Het authenticatieniveau van het toegangsmiddel is tenminste sterk conform NEN7512.		
Beschrijving:	Authenticatieniveaus worden in NEN 7512 onderverdeeld in Zwak, Matig en Sterk. Voorbeelden van sterke authenticatieniveaus zijn: • Het gebruik van biometrie in combinatie met een ander authenticatiemiddel. De huidige stand der techniek (en eventueel aanvullend gestelde eisen buiten authenticatie) is echter zodanig dat deze combinatie in de thuissituatie van een zorgconsument niet realistisch is. • Een fysiek authenticatiemiddel (bijvoorbeeld “tokens” die telkens een eenmalig wachtwoord genereren, bankpassen, SIM-kaarten in een mobiele telefoon en dragers van een digitaal certificaat). Bij toepassing van een fysiek authenticatiemiddel wordt de sterkte bepaald door het geheel van de processen waarin het wordt gebruikt. Alleen wanneer het toegangsmiddel wordt gebruikt in combinatie met een wachtwoord of een PIN-code en ook bij het initialiseren van het toegangsmiddel en de uitreiking aan de houder wordt gewaarborgd dat het eenduidig aan de houder wordt gebonden, kan men spreken van een Sterk authenticatieniveau. Is aan deze voorwaarden niet voldaan, dan is het authenticatieniveau hooguit Matig.		

T.4	Type eis:	Relevant voor onderdeel:	Bron:
	Technisch	Toegangsmiddel	F.5, 2008-3027
Samenvatting:	Het toegangsmiddel is toekomstvast.		
Beschrijving:	Om te voorkomen dat het middel vervangen moet worden in het geval wijzigingen in de omgeving optreden dient bepaald te worden hoe toekomstvast het middel is. Hierbij kan bijvoorbeeld gedacht worden aan ontwikkelingen op beveiligingsgebied. Ook is het mogelijk dat bij gebruik van een bestaand authenticatiemiddel bij vervanging van het bestaande gebruik ook het gebruik van het toegangsmiddel voor de medische gegevens wordt beïnvloed.		

T.5	Type eis:	Relevant voor onderdeel:	Bron:
	Technisch	Toegangsmiddel	F.10, 2008-3027
Samenvatting:	Het toegangsmiddel is beschikbaar voor (vrijwel) de gehele bevolking.		
Beschrijving:	Om de adoptiegraad van het toegangsmiddel en het gebruik van de geboden functionaliteit door de zorgconsument zo hoog mogelijk te maken dienen zoveel mogelijk Nederlanders het middel vanaf introductie te kunnen gebruiken zonder grote uitgaven.		

T.6	Type eis:	Relevant voor onderdeel:	Bron:
	Technisch	Uitgiftemethode middel	F.1, 2008-3027
Samenvatting:	De echtheid van het toegangsmiddel kan worden gecontroleerd.		
Beschrijving:	De controle-instantie moet kunnen nagaan of een digitale sleutel vervalst of gestolen is om gebruik van het middel niet meer toe te staan / het middel in te kunnen trekken.		

T.7	Type eis:	Relevant voor onderdeel:	Bron:
	Technisch	Uitgiftemethode middel	F.1, 2008-3027
Samenvatting:	Het bezit van een al bestaand toegangsmiddel kan worden geverifieerd.		
Beschrijving:	Indien gebruik gemaakt wordt van een bestaand toegangsmiddel dat al in het bezit is van de zorgconsument dient de controle-instantie te verifiëren of het middel daadwerkelijk in bezit is van de zorgconsument.		

T.8	Type eis:	Relevant voor onderdeel:	Bron:
	Technisch	Uitgiftemethode middel	F.1, 2008-3027
Samenvatting:	Het bezit van een toegangsmiddel en de verificatie van de zorgconsument worden geregistreerd.		
Beschrijving:	Door middel van een door de controle-instantie te voeren registratie dient te achterhalen te zijn dat de identiteit van een gebruiker door middel van een face-to-face is geverifieerd en welke digitale sleutel vervolgens aan deze persoon is verstrekt. Op deze wijze is altijd traceerbaar welke gebruikers over welke digitale sleutels beschikken. Zodoende wordt ook het aanvragen van meerdere digitale sleutels voor één persoon/BSN voorkomen.		

T.9	Type eis:	Relevant voor onderdeel:	Bron:
	Technisch	Uitgiftemethode middel	F.10, 2008-3027
Samenvatting:	Natuurlijke controlemomenten hebben de voorkeur.		
Beschrijving:	Bij het uitgifte- of verificatieproces is het belangrijk om controlemomenten in te bouwen. Bij voorkeur zijn dit bestaande momenten om de zorgconsument en de uitvoeringsinstantie zo veel mogelijk te ontlasten. Hierbij moet gedacht worden aan de inschrijving voor behandeling in het ziekenhuis of het ophalen van een nieuwe digitale sleutel bij het gemeentehuis.		

T.10	Type eis:	Relevant voor onderdeel:	Bron:
	Technisch	Uitgiftemethode middel	F.10, 2008-3027
Samenvating:	Voorregistratie is wenselijk.		
Beschrijving:	Om de administratieve belasting zo veel mogelijk te beperken dient indien mogelijk gebruik gemaakt te worden van bestaande registraties. Als voorbeeld kan hierbij gedacht worden aan de voor een groot deel van de Nederlanders al bekende DigiD-registratie van gebruikersnamen.		

T.11	Type eis:	Relevant voor onderdeel:	Bron:
	Technisch	Uitgiftemethode middel	F.1, 2008-3027
Samenvatting:	Gebruik of activering van het toegangsmiddel kan worden teruggekoppeld.		
Beschrijving:	Gebruik of activering van het middel kan aan de gebruiker worden teruggekoppeld via een ander kanaal (bijvoorbeeld post, e-mail). Hierdoor wordt het moeilijker om ongemerkt een middel voor een andere persoon aan te vragen en te gebruiken. Mogelijke invulling kan zijn een melding van gebruik via e-mail of sms aan de zorgconsument.		

T.12	Type eis:	Relevant voor onderdeel:	Bron:
	Technisch	Toegangsmethode	F.1, F.5, NEN 7512, 2008-3027
Samenvatting:	Alleen identificatoren met registratieniveau 3 conform NEN 7512 worden toegepast.		
Beschrijving:	De NEN norm 7512 onderscheidt 3 versleutelingsniveaus: 0 = geen versleuteling, 1 = versleutelde verbinding en 2 = versleuteld bericht. Volgens het communicatiescenario beschreven in bijlage A van de NEN7512 norm moet bij de raadpleging van dossiers door cliënten worden voldaan aan versleutelingsniveau 2. Door de versleuteling van een bericht wordt het volledige kanaal tussen zender en ontvanger afgedekt. De verzender gebruikt een publieke sleutel van de geadresseerde om het bericht te versleutelen. De geadresseerde maakt het leesbaar met de bijbehorende privésleutel.		

T.13	Type eis:	Relevant voor onderdeel:	Bron:
	Technisch	Toegangsmiddel	F.2, F.3, F.7, F.9
Samenvatting:	Het toegangsmiddel kan gebruikt worden om toestemming voor inzage te geven.		
Beschrijving:	Om toestemming te kunnen geven voor bepaalde handelingen (bijvoorbeeld toegang, transport, wijzigingen, etc.) is het noodzakelijk dat zorgconsumenten berichten kunnen ondertekenen om zo onweerlegbaar aan te kunnen tonen dat de zorgconsument afzender is van het bericht of op een andere wijze toestemming kunnen geven.		

T.14	Type eis:	Relevant voor onderdeel:	Bron:
	Technisch	Toegangsmethode	F.6, Zorgpas Eemland
Samenvatting:	De toegangsmethode beschikt over de mogelijkheid om medische gegevens in het geval van nood beschikbaar te maken.		
Beschrijving:	Om medische gegevens in het geval van nood beschikbaar te maken voor zorgverleners, dient de toegangsmethode opslagfunctionaliteit te bieden.		

T.15	Type eis:	Relevant voor onderdeel:	Bron:
	Technisch	Toegangsmethode	F.1
Samenvatting:	Het is mogelijk de digitale medische gegevens vrijwel direct te actualiseren, onafhankelijk van waar deze zich bevinden.		
Beschrijving:	Om te kunnen zorgen voor voldoende actuele gegevens is het noodzakelijk dat gegevens direct – tijdens of vlak na de behandeling of testuitslag – kunnen worden gesynchroniseerd. Op deze wijze beschikt de zorgconsument over recente informatie en kan ook informatie direct worden teruggekoppeld naar de zorgverlener.		

T.16	Type eis:	Relevant voor onderdeel:	Bron:
	Technisch	Toegangsmethode	F.8
Samenvatting:	De oplossing maakt gebruik van een gestandaardiseerde wijze van communiceren (en opslag).		
Beschrijving:	Om te kunnen voldoen aan de wens gegevens eenduidig uit te kunnen wisselen is het aan te raden een gestandaardiseerde communicatie- en opslagwijze toe te passen.		

T.17	Type eis:	Relevant voor onderdeel:	Bron:
	Technisch	Toegangsmethode	F.10
Samenvatting:	De oplossing kan gebruikt worden om het BSN van de zorgconsument te verifiëren.		
Beschrijving:	Het is wettelijk verplicht het BSN van de zorgconsument te controleren. Om de koppeling tussen de oplossing, BSN en zorgconsument te kunnen maken moet het mogelijk zijn om na te gaan of het BSN van de zorgconsument het juiste is. Hiervoor is het overigens technisch niet strikt noodzakelijk om het BSN op het middel op te slaan.		

B. Betrokken onderzoekers PwC

175 Dit onderzoek is uitgevoerd door de volgende adviseurs van PwC Advisory:

- Otto Vermeulen
- Adri de Bruijn
- Cas de Bie
- Anneke van Mourik
- Bart Witteman
- Yvonne Mennen