

Vertrouwen als onmisbare schakel voor hergebruik van gezondheidsgegevens

Hoe kunnen verifieerbare verklaringen zorgen voor betrouwbare gezondheidsgegevens?

René Hietkamp



Inhoudsopgave

» 1. Inleiding	3
2. Urgentie naar betrouwbare data voor hergebruik	5
2.1 Wet elektronische gegevensuitwisseling in de zorg (Wegiz)	5
2.2 Europese ruimte voor gezondheidsgegevens	6
2.3 Welke gevolgen heeft deze wetgeving voor de zorg?	7
3. Betrouwbaarheid door attestering van attributen	10
3.1 Wat is een verifieerbare verklaring?	10
3.2 Welke gegevens bevat een verklaring?	11
3.3 Hoe wordt een verklaring betrouwbaar?	12
3.4 Borgen van de kwaliteit door verklaringen	13
4. De eerste stappen naar betrouwbare gegevensuitwisselingen	14
4.1 Gegevens beschikbaar maken	14
4.2 Afspraken maken over de werking van het informatiestelsel	15
4.3 Samenwerken om de zorg beter te maken	16
5. Conclusie	16
6. Begrippenlijst	18

1. Inleiding

Elke dag vinden er honderden gevaarlijke incidenten plaats doordat computersystemen van zorgaanbieders geen gegevens van patiënten kunnen uitwisselen. Vaak weten artsen ernstige ongelukken te voorkomen, maar niet altijd. Een paar schrijnende voorbeelden zijn te zien in de 2DOC-documentaire 'dodelijke zorg'.

Om dit soort ongelukken terug te dringen is het essentieel dat informatiesystemen automatisch patiëntgegevens kunnen uitwisselen met andere zorgsystemen. Toch blijkt dat in de praktijk moeilijk. De huidige leveranciers van zorginformatiesystemen laten niet zien dat zij over de innovatiekracht beschikken om de zorg verregaand te automatiseren en om beslissingsondersteuning te bieden voor zorgverleners. Wellicht heeft dit te maken met de angst om als medisch hulpmiddel aangemerkt te worden waardoor kosten oplopen.

De technologische innovatiekloof tussen de zorg en andere sectoren is groot. Zo zijn bijvoorbeeld autoverzekeringen al jaren volautomatisch af te sluiten. Of kun je zonder veel digitale moeite een nieuwe bankrekening openen. De zorg loopt hier al jaren op achter. Om de kloof te dichten moet een zorginstelling over haar eigen gegevens kunnen beschikken en in staat zijn om zelf toepassingen te realiseren op deze gegevens. Moderne architecturen voor informatietechnologie kunnen helpen om de huidige impasse te doorbreken.

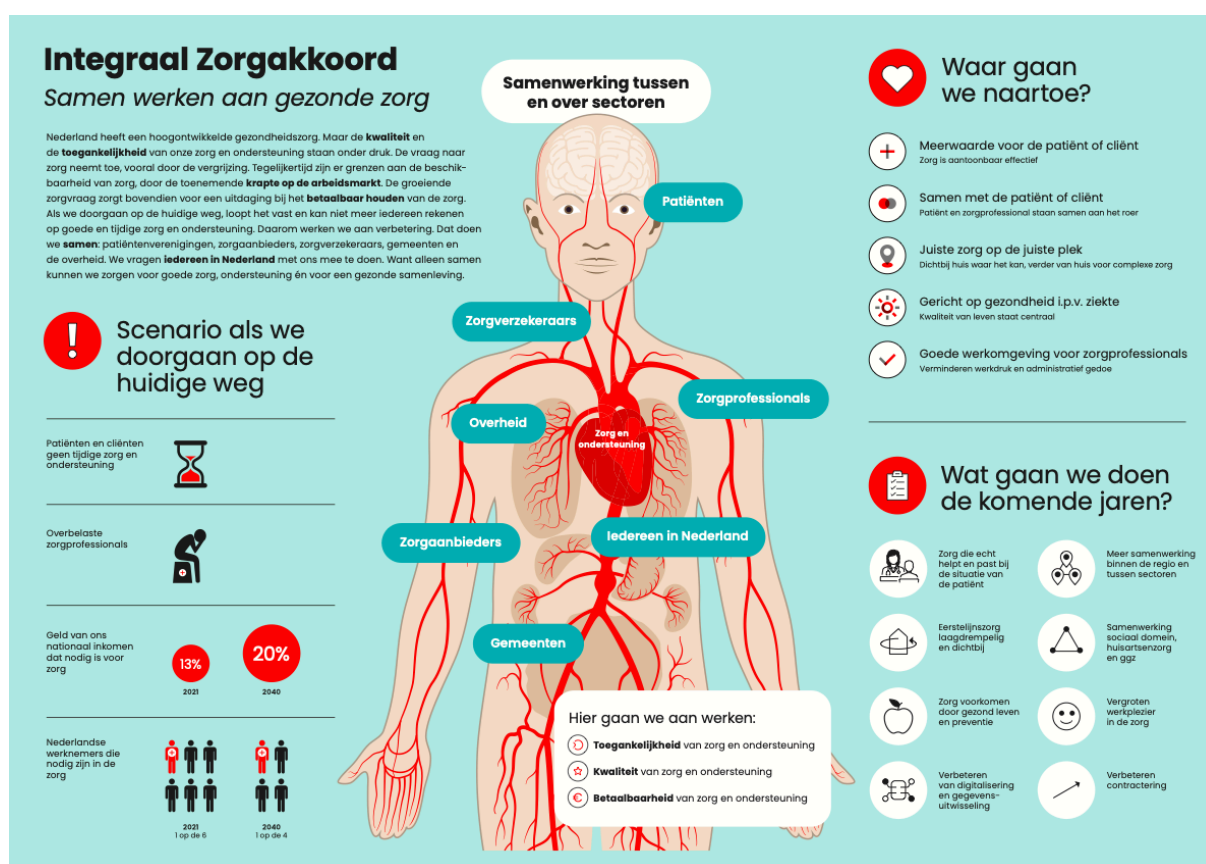
Meer in plaats van minder werk

Om handmatig werk uit te bannen in een sector die al kampt met flinke personeelstekorten, moet zoveel mogelijk werk worden geautomatiseerd. Een zorgverlener mag geen tijd meer kwijt zijn aan het overtypen van gegevens. Een verwijzing moet een eenvoudige druk op de knop zijn. Het zou niet nodig moeten zijn om zelf op zoek te gaan naar informatie in pdf-documenten, zoals nu nog wel vaak het geval is.

De zorgsector moet digitaler, passender en goedkoper worden. Deze ambitie is vastgelegd in [het Integraal Zorgakkoord \(IZA\)](#). In deze overeenkomst staat dat standaardisatie van gegevensuitwisseling leidt tot minder administratieve lasten, minder fouten bij de overdracht en bijdraagt aan secundair gebruik van gegevens. In de huidige situatie betekent hergebruik van gegevens echter meer administratief werk voor zorgverleners, aangezien systemen niet samenwerken en het in de praktijk vaak op overtypen aankomt. Het zou een randvoorwaarde moeten zijn dat verschillende

informatiesystemen geïntegreerd zijn en kunnen samenwerken als één systeem. Systeemwerking wordt dit genoemd.

Het geautomatiseerd uitwisselen van gegevens zou een randvoorwaarde moeten zijn. Om tegemoet te komen aan deze voorwaarde is openheid van zorginformatiesystemen nodig en dat is vooralsnog een groot probleem. Zorgverleners moeten er op kunnen vertrouwen dat hun systemen gevuld worden met betrouwbare gegevens die geschikt zijn voor hun specifieke doel. Zonder dit vertrouwen blijven zorgverleners hun eigen gegevens trouw en wordt er bijvoorbeeld nodeloos opnieuw bloedonderzoek gedaan of wéér een nieuw hartfilmpje gemaakt. Hergebruik blijft in dat geval onmogelijk.



Figuur 1 Infographic over integraal zorgakkoord (Bron: Rijksoverheid)

Om vertrouwen te krijgen in gegevens van derden zijn antwoorden nodig op vragen als: door wie of wat zijn de gegevens geregistreerd? Wanneer en met welk doel? De Europese Unie geeft met de nieuwe verordening voor elektronische identificatie en vertrouwensdiensten (eIDAS2) middelen om de betrouwbaarheid en kwaliteit te borgen en de risico's van digitalisering te verkleinen.

Deze verordening past in de Europese ambitie voor een digitaal decennium¹. Deze whitepaper beschrijft hoe eIDAS2 voor zorgverleners de administratieve lasten kan verminderen en de zorg goedkoper kan maken.

2. Urgentie naar betrouwbare data voor hergebruik

De zorg roept heel duidelijk dat het een goede informatievoorziening nodig heeft. Daarom moet de zorg digitaler en gegevens gaan hergebruiken om goedkoper te worden. De schaal en de complexiteit van de huidige problemen met informatietechnologie zijn echter zo groot dat een zorginstelling zelf niet in staat is om deze problemen op te lossen.

Om de ambities te realiseren is wetgeving nodig en zijn landelijke afspraken nodig. De Nederlandse overheid heeft daarom de Wet elektronische gegevensuitwisseling in de zorg (Wegiz) gemaakt en daarom ligt er ook een voorstel voor een Europese ruimte voor gezondheidsgegevens (EHDS). Beiden gaan het hergebruik van gegevens bevorderen. Steeds meer gegevensuitwisselingen, ook steeds meer grensoverschrijdend, betekent dat er meer aandacht nodig is voor de kwaliteit van de gegevens, waaronder de betrouwbaarheid ervan.

2.1 Wet elektronische gegevensuitwisseling in de zorg (Wegiz)

Via de Wegiz kan de minister zorginstellingen verplichten om een bestaande gegevensuitwisseling voortaan elektronisch te doen. Het moet een bestaande gegevensuitwisseling zijn, want bij een uitwisseling die niet bestaat kun je geen verplichting opleggen. Het moet een gegevensuitwisseling zijn die door de zorg zelf gespecificeerd is in een kwaliteitsstandaard.

Kwaliteitsstandaarden zijn voor de Wegiz het fundament om in te vullen welke gegevens uitgewisseld moeten worden. Een NEN-norm beschrijft vervolgens hoe de gegevensuitwisseling wordt uitgevoerd, wie welke verantwoordelijkheid heeft voor welk onderdeel in de uitwisseling. Een voorbeeld is de NEN 7503 voor de elektronische

¹ https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age_nl

verwerking en uitwisseling van gegevens voor het voorschrijven en verstrekken van medicatie.

2.2 Europese ruimte voor gezondheidsgegevens

De verordening voor een Europese ruimte voor gezondheidsgegevens gaat ook de gegevensuitwisselingen bevorderen. Deze verordening hanteert eIDAS2 als uitgangspunt. De impact hiervan is dat de patiënt houder wordt van gezondheidsgegevens via zijn wallet. Denk bij deze wallet aan een betrouwbaardere variant op de Apple of Google-wallet. De verwachting is dat steeds meer gegevensuitwisselingen via de patiënt worden uitgevoerd. Zorginstellingen moeten de gezondheidsgegevens accepteren op basis van de verklaringen uit de wallet.



Figuur 2 Een Europese wallet voor digitale identiteit (Bron: Europese Commissie)

Het huidige voorstel voor een Europese ruimte voor gezondheidsgegevens zal grote gevolgen hebben voor de Nederlandse zorg. Artikel 5 zegt namelijk dat een zorginstelling een aantal categorieën van gegevens elektronisch beschikbaar moeten stellen in de Europese ruimte. Het gaat om de volgende categorieën van gegevens voor het primaire gebruik:

- Patiëntendossiers (de basisgegevensset zorg)
- Recepten voor medicatie
- Verstrekkingen van medicatie
- Medisch beelden en verslagen daarover
- Laboratoriumresultaten
- Ontslagverslagen

Naast bovenstaande categorieën voor primair gebruik van gegevens worden ook categorieën genoemd voor secundair gebruik, met name gericht op wetenschappelijk onderzoek. Ook deze categorieën van gegevens moeten elektronisch beschikbaar worden gesteld door een zorginstelling.

2.3 Welke gevolgen heeft deze wetgeving voor de zorg?

In de huidige praktijk zien we nog weinig aandacht voor kwaliteit van data. De komst van de Wegiz en de Europese ruimte voor gezondheidsgegevens geeft echter aan dat steeds meer data zal worden hergebruikt. Kwaliteit van data is daarom belangrijk. Regels daarover zouden in de kwaliteitsstandaarden opgenomen moeten worden. De zorg moet namelijk zelf vaststellen wat de gewenste kwaliteit van data is. In de ontwikkelingen naar digitalisering en hergebruik zien we de urgentie voor kwaliteit van data terugkomen en de manier hoe dit kan worden vastgesteld.

Door de ontwikkelingen naar digitalisering en hergebruik zijn een aantal gevolgen voor de digitale zorginfrastructuur te ontdekken, namelijk internationalisering, regie op gegevens, datagedreven werken en een 'knowledge-first'-aanpak. Met een zorginfrastructuur bedoelen we de computers en software die door zorgverleners gebruikt worden om data te versturen en te ontvangen.

Het eerste gevolg van de Europese verordening is internationalisering van gegevensuitwisselingen. Een digitale overdracht van een patiënt gaat over landsgrenzen heen. Enerzijds betekent dit dat hergebruik moet worden gemaakt van internationale standaarden en afspraken. Anderzijds zijn er maatregelen voor de betrouwbaarheid van de gegevens nodig. Een uitgangspunt is dat de uitgever van de gegevens onbekend is en niet uit hetzelfde dorp, dezelfde stad of regio afkomstig is. Toch zal een zorgverlener in staat moeten zijn om de kwaliteit te toetsen. Dit is mogelijk door verifieerbare documentatie op te nemen over de herkomst en de integriteit van de gegevens. De zorg heeft, met andere woorden, verifieerbare verklaringen hierover nodig die onweerlegbaar zijn. De ingrediënten voor deze verklaringen komen uit eIDAS2.

Een tweede gevolg is regie op gegevens door de patiënt. De patiënt heeft bij een gegevensuitwisseling de regie en is veelal houder van zijn eigen gezondheidsgegevens. Enerzijds vanuit idealisme en privacy, maar anderzijds ook vanuit een pure logistieke en financiële noodzaak. Het koppelen van alle zorginstellingen in een digitale zorginfrastructuur op een internationale schaal is erg duur en complex. Dat de patiënt de gegevens zelf meeneemt is daarom een beter alternatief. Dit betekent echter dat de gezondheidsgegevens niet meer vertrouwd kunnen worden op basis van de gebruikte digitale zorginfrastructuur van zorgverleners zelf. Omdat gegevens niet meer via een

vaststaande zorginfrastructuur worden ontvangen moet de betrouwbaarheid beoordeeld kunnen worden op basis van de bijgesloten documentatie.

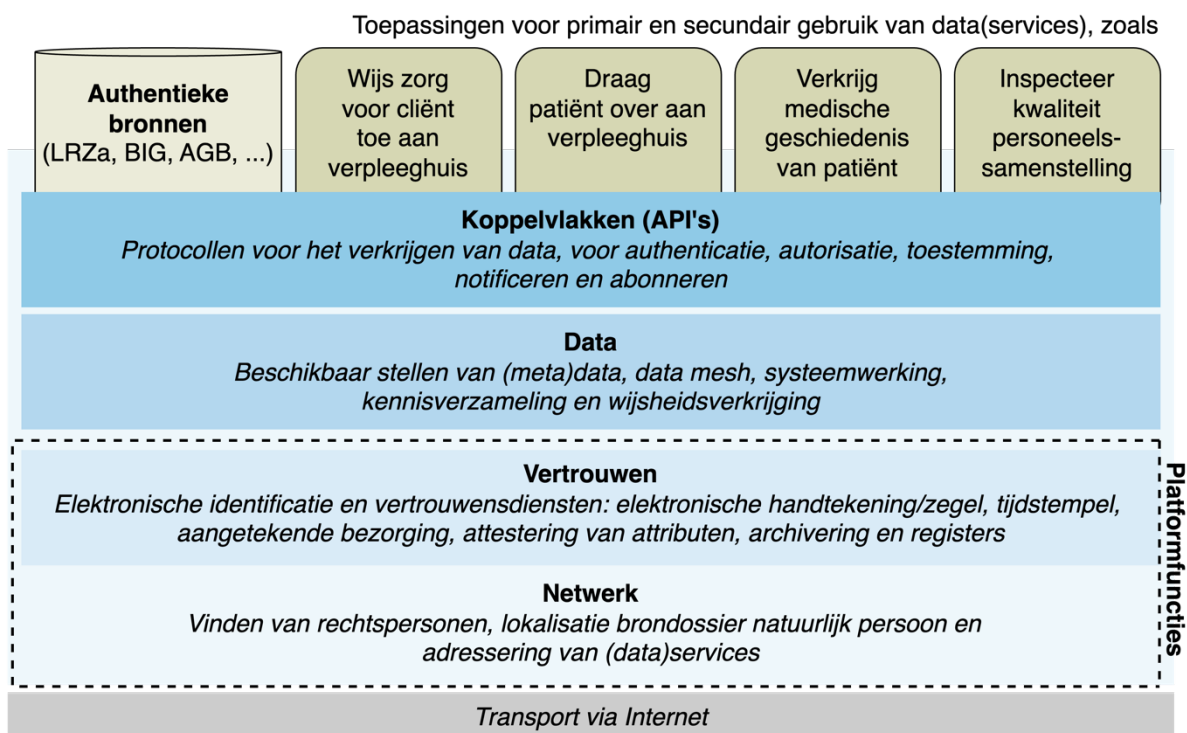
Een derde gevolg gaat over datagedreven werken, oftewel: over het toepassen van de gegevens. Gegevens worden niet alleen gebruikt voor het verkrijgen van een patiëntbeeld, maar ook voor het maken van beleid, voor onderzoek en innovatie en voor beslissingsondersteuning bij diagnose, behandeling en advisering. Foutieve gegevens hebben daarom een steeds grotere impact. Het is dan ook noodzakelijk dat de kwaliteit van gegevens hoog is en dat verificatie van herkomst, integriteit en kwaliteit geautomatiseerd kan worden.

Een vierde gevolg gaat over hoe de gegevensuitwisseling tot stand komt. Gegevens worden steeds vaker hergebruikt waardoor het te duur is om iedere gegevensuitwisseling als maatwerk te behandelen. Een verandering is daarom nodig. Deze verandering is overigens afkomstig uit de hoek van de gegevensanalyse. Zowel binnen gegevensuitwisseling als gegevensanalyse worden op dit moment gegevensverzamelingen gemaakt voor een specifiek doel. Voor gegevensuitwisselingen worden bijvoorbeeld berichten (ook wel resources genoemd) gespecificeerd voor een koppeling tussen zorginstellingen. Voor een andere koppeling worden opnieuw berichten gespecificeerd. Ook komt het voor dat dezelfde berichten worden hergebruikt, maar dat de betekenis van de data in de berichten anders is.

Om dit maatwerkprobleem op te lossen wordt een kennislaag over de informatielaag heen gelegd. Deze aanpak heet 'knowledge-first'. Dit is een aanpak die bijvoorbeeld in KIK-V (Keteninformatie Kwaliteit Verpleeghuiszorg) wordt gebruikt en uitgebreid gaat worden naar andere zorgsectoren. In deze context zijn gegevens de ruwe binaire gegevens, zoals een datum, nummer of een tekst. Informatie betekent dat de gegevens ingedeeld zijn in berichten (of entiteiten) en voorzien zijn van een label zoals geboortedatum of naam. Generiek wordt gesproken over kennis als informatie onderling verbonden is met andere informatie, dat de informatie interpreteerbaar is, dat verbanden beredeneerd kunnen worden en dat over deze kennis *queries* uitgevoerd kunnen worden. Door de kennislaag is gegevensuitwisseling geen maatwerk meer, maar is het mogelijk om gegevens daadwerkelijk voor meerdere toepassingen te gebruiken.

Ook vanuit de internationalisering zien we de 'knowledge-first'-aanpak terug. De standaarden in deze aanpak ondersteunen namelijk dat gegevens kunnen worden verzonden in combinatie met de betekenis van de gegevens. Een randvoorwaarde voor het borgen van de kwaliteit van data bij hergebruik.

Een antwoord op al deze ontwikkelingen is het netwerkmodel voor gegevensuitwisseling in de zorg. In dit model is een vertrouwenslaag opgenomen om tot een betrouwbare uitwisseling te komen. De vertrouwenslaag is gebaseerd op eIDAS2 en is niet uniek voor de zorg. De vertrouwenslaag is onderdeel van een zeer brede internationale ontwikkeling. De verklaring dat elektronische gegevens in een dossier betrouwbaar zijn, oftewel de attestering van attributen, staat binnen deze laag in de schijnwerpers omdat het afspraken over vertrouwen koppelt aan een individuele gegevensuitwisseling, zodat gegevens betrouwbaar uitgewisseld kunnen worden.



Figuur 3 Netwerkmodel voor gegevensuitwisseling in de zorg (Bron: Info Support)

3. Betrouwbaarheid door attestering van attributen

Eén van de vertrouwensdiensten uit eIDAS2 is attestering van attributen. Attestering van attributen, de verklaring dat elektronische gegevens uit een dossier betrouwbaar zijn, heeft als doel hergebruik van gegevens te realiseren. Het is een protocol om gegevens betrouwbaar uit te kunnen wisselen.

Om betrouwbaarheid te realiseren worden gegevens uitgegeven in verifieerbare verklaringen. Een houder neemt de verklaringen op in een digitale portemonnee, beter bekend onder de noemer wallet. De wallet is een onderdeel van de aanpassingen aan eIDAS2. Dit hoofdstuk gaat verder in op de werking van de verifieerbare verklaringen.

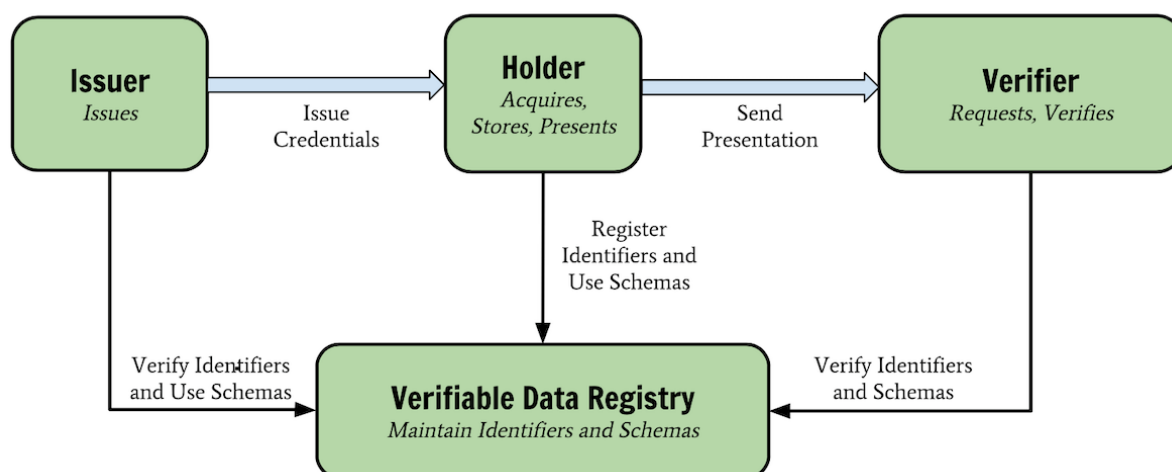
3.1 Wat is een verifieerbare verklaring?

Een verifieerbare verklaring of kortweg een verklaring is gebaseerd op de open standaard van het World Wide Web Consortium (W3C). De standaard is onder technici beter bekend als '*verifiable credentials*'. W3C is de belangrijkste internationale standaardisatieorganisatie voor het internet. In het Nederlands is de standaard bekend onder meerdere namen. In deze whitepaper wordt bijvoorbeeld de naam verklaring gehanteerd, maar de naam referentie, legitimatie, certificaat, getuigschrift, geloofsbrief en attest worden ook vaak gebruikt.

Niet iedere verklaring heeft hetzelfde betrouwbaarheidsniveau nodig. Het doel waarvoor het gegeven gebruikt wordt bepaald het betrouwbaarheidsniveau. Voor een bioscoopkaartje is een laag niveau bijvoorbeeld voldoende. De uitgever stelt de gegevens beschikbaar en heeft daarbij een bepaald doel voor ogen. Dat doel komt mogelijk niet overeen met het doel van de andere partij. Een match tussen het doel van de uitgever en het doel van de andere partij, de verificateur, is daarom nodig.

De standaard gaat uit van een vertrouwensdriehoek tussen een uitgever, houder (in het geval van de zorg een patiënt) en een afhankelijke partij, de verificateur. Elke rol in deze driehoek kan worden ingevuld door een natuurlijk persoon, een rechtspersoon of een ding. Allen gebruiken applicaties om hun rol te kunnen vervullen. De houder heeft bijvoorbeeld een wallet tot zijn beschikking waarin hij de verifieerbare verklaringen kan

bewaren. De houder staat in het midden van de vertrouwens-driehoek en heeft regie over de uitwisseling van gegevens tussen uitgever en verificateur. Door gegevens uit een verklaring te overleggen aan een verificateur kan de houder iets over zichzelf bewijzen.



Figuur 4 Rollen in de standaard voor verifieerbare verklaringen (Bron: W3C)

In de vertrouwensdriehoek vertrouwen de uitgever en de houder elkaar, de houder vertrouwt de verificateur en de verificateur vertrouwt de uitgever. Dat laatste gaat niet vanzelf, omdat beide partijen elkaar mogelijk niet kennen. De verificateur baseert zijn vertrouwen daarom op een vertrouwd elektronisch register en de afspraken van dat register. In het elektronische register wordt bijvoorbeeld geregistreerd wie welke verklaring mag uitgeven en hoe de elektronische zegel van de uitgever kan worden geverifieerd. Het elektronische register is een vertrouwensdienst in eIDAS2.

Het concept met een wallet en verklaringen is ook bekend onder de noemer 'self-sovereign identity', omdat de houder autonoom regie heeft op het delen van gegevens over zijn identiteit.

3.2 Welke gegevens bevat een verklaring?

Een verifieerbare verklaring bevat gegevens over de identiteit van een persoon, een rechtspersoon of een ding. Identiteit is breder dan alleen het burgerservicenummer of een naam. Volgens *Stanford Encyclopedia of Philosophy* verwijst persoonlijke identiteit meestal naar eigenschappen waaraan we een speciaal gevoel van gehechtheid of eigendom voelen. Iemands persoonlijke identiteit bestaat uit die eigenschappen die hij of zij aanneemt om zich te definiëren als een persoon of zich te maken tot de persoon die hij of zij is en die zich van anderen onderscheidt. Ook een ziekte of aandoening

behoort tot iemands identiteit, net als iemands werk, inkomen, opleiding, levenssituatie etc.

3.3 Hoe wordt een verklaring betrouwbaar?

Met alleen de verificatie van een elektronische zegel of handtekening kan een afhankelijke partij een verklaring nog niet vertrouwen. Deze partij weet immers niets over de uitgever en wie of wat die uitgever is. Het vertrouwen daarin kan opgebouwd worden met andere verklaringen, maar voor die verklaringen geldt dezelfde vraag: kan de uitgever vertrouwd worden?

Het vertrouwen kan gerealiseerd worden met afspraken. De afspraken zijn in een afsprakenstelsel vastgelegd door een 'assurance community'. Wetgeving kan in deze ook gezien worden als een afsprakenstelsel met een wettelijke status. Een afspraak is bijvoorbeeld dat een recept alleen mag worden voorgeschreven door een bevoegde zorgverlener. Dat een zorgverlener bevoegd is zou geverifieerd kunnen worden door een verklaring te maken van een getuigschrift. De verificateur kan deze dan verifiëren aan de hand van de lijst van aangewezen getuigschriften en modules voorschrijfbevoegdheid. Een verklaring maken van de voorschrijfbevoegdheid zelf is vaak niet verstandig, omdat regels hierover kunnen veranderen. Afspraken zijn daarom nodig over het gebruik van de verklaring.

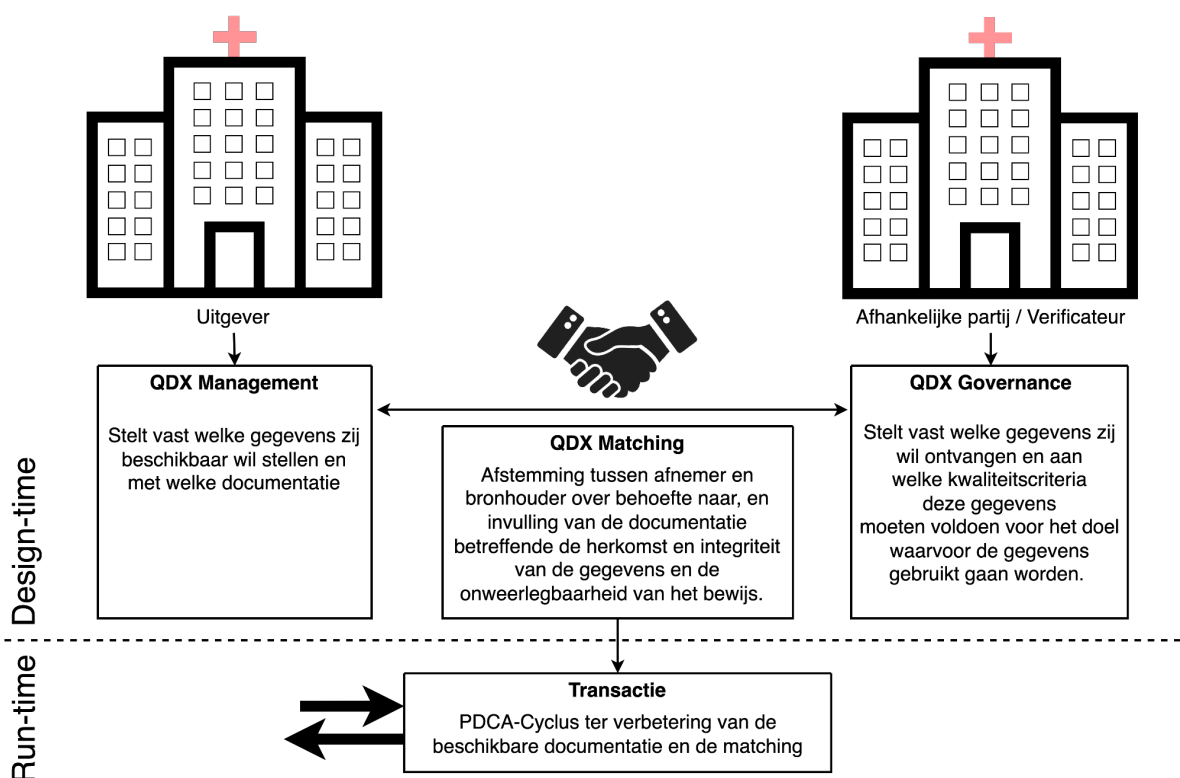
Een getuigschrift uit het bovenstaande voorbeeld mag uitgegeven worden door een post-HBO-opleiding tot verpleegkundige. Deze instelling moet geregistreerd zijn in een vertrouwd elektronisch register als uitgever van het getuigschrift. Uiteraard kan de instelling ook een verklaring hebben dat zij door het Ministerie van Onderwijs, Cultuur en Wetenschap erkend is als post-HBO-opleiding. Het Ministerie van Onderwijs, Cultuur en Wetenschap zou in dit voorbeeld geregistreerd moeten zijn als vertrouwde uitgever van de erkenning. Het elektronische register speelt al met al een essentiële rol in het vertrouwen, evenals de afspraken wie in het register geregistreerd mogen worden als uitgever van welke verklaringen.

Het elektronische register is voor het vertrouwen een randvoorwaarde en is daarom een vertrouwensdienst in eIDAS2. Iedere lidstaat in Europa zal de verantwoordelijkheid krijgen voor de juiste inrichting van het afsprakenstelsel in het register. Aanvullend kunnen assurance communities ook zelf een vertrouwd elektronisch register kiezen en inrichten op basis van de afspraken in de community. Een assurance community bestaat uit partijen die gezamenlijk een doel nastreven waarbij vertrouwen een belangrijk onderdeel is. Deze partijen maken gezamenlijk afspraken over de verklaringen die gehanteerd worden. Een voorbeeld van een assurance community is het afsprakenstelsel KIK-V (Keteninformatie Kwaliteit Verpleeghuiszorg) waarin de

deelnemers afspraken hebben gemaakt over een gevalideerde vraag. De deelnemers van ieder afsprakenstelsel vormen in principe een assurance community.

3.4 Borgen van de kwaliteit door verklaringen

Afspraken over de kwaliteit van gegevens zijn nodig tussen uitgevers van gezondheidsgegevens en de gebruikers van deze gegevens. Een zorginstelling kan een afhankelijke partij zijn in een gegevensuitwisseling of kan uitgever zijn van gezondheidsgegevens. Beide rollen vereisen andere activiteiten om de kwaliteit van de gegevens te borgen. In het rapport *Een nieuw perspectief voor vertrouwensmodellen in de zorg* laat TNO zien welke activiteiten iedere rol moet uitvoeren om tot een gekwalificeerde uitwisseling van gegevens te komen (zie onderstaand figuur). Een gekwalificeerde uitwisseling is gedefinieerd als een uitwisseling van gegevens die geschikt is voor het doel van de afhankelijke partij.



Figuur 5 Gekwalificeerde gegevensuitwisseling (Bron: TNO, gemodificeerd door auteur)

De uitgever en de afhankelijke partij stemmen onderling af welke gegevens nodig zijn en welke documentatie beschikbaar is. Het is niet verstandig dat iedere zorginstelling dit afzonderlijk doet. Het zou onderdeel moeten zijn van de afspraken in een kwaliteitsstandaard. Het zijn namelijk afspraken om goede zorg voor een patiënt te borgen en te continueren. Een zorginstelling blijft in de uitvoering echter zelf verantwoordelijk voor het beschikbaar stellen van de documentatie, evenals verificatie van de kwaliteit van gegevens bij hergebruik.

De documentatie van gezondheidsgegevens zal antwoord geven op de vragen waarom en hoe de gegevens zijn geproduceerd, waar, wanneer en door wie. Hiervoor is waarschijnlijk bewijs nodig dat onweerlegbaar is. Een verifieerbare verklaring is dan ook het middel waarmee de vragen beantwoord kunnen worden.

4. De eerste stappen naar betrouwbare gegevensuitwisselingen

In deze whitepaper is beschreven hoe verklaringen een rol kunnen spelen in de betrouwbaarheid van gegevensuitwisselingen en de kwaliteit van gegevens in het algemeen. Het is echter noodzakelijk dat eerst een aantal beperkingen overwonnen worden, voordat gegevensuitwisseling succesvol geïmplementeerd kan worden. Een zorginstelling moet bijvoorbeeld eerst weer over haar gegevens kunnen beschikken. Een scheiding tussen de gegevens en de toepassingen die gebruik maken van gegevens is daarom nodig. Een monolithische architectuur van een zorginformatiesysteem van één leverancier past niet meer en belemmert innovatie.

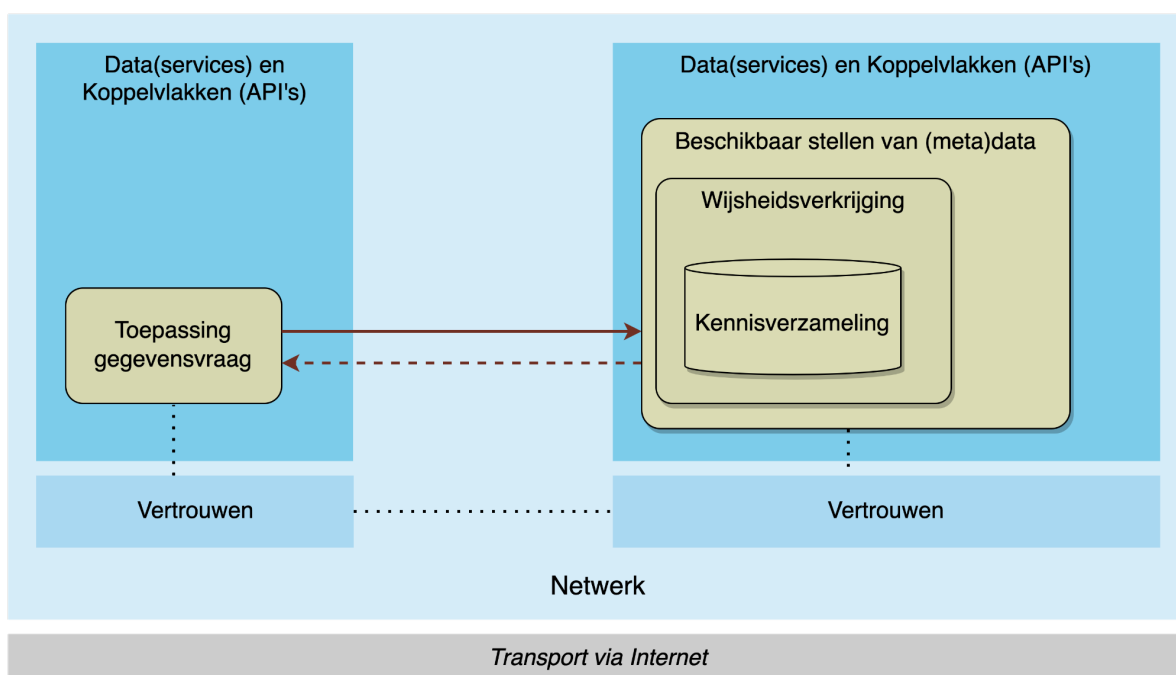
4.1 Gegevens beschikbaar maken

Een eerste stap is om gegevens beschikbaar te stellen voor hergebruik door verschillende toepassingen. Dat zijn zowel interne toepassingen als toepassingen van andere zorginstellingen. De koppelvlakken voor interne en externe toepassingen kunnen verschillen, maar de gegevens komen vanuit dezelfde bron.

De ontwikkelingen voor het beschikbaar stellen van gegevens wijzen op dit moment specifiek richting een API-strategie op basis van de FAIR-dataprincipes. Volgens de FAIR-dataprincipes hoort bij het beschikbaar stellen van de gegevens ook het beschikbaar stellen van metadata, oftewel de documentatie over de gegevens. Dit is overigens andere of aanvullende documentatie dan de documentatie over de herkomst,

integriteit, onweerlegbaarheid en betekenis van de gegevens waarover we eerder in deze whitepaper schreven.

De FAIR-dataprincipes geven aan dat de gegevens beschreven moeten zijn in een formele, toegankelijke, gedeelde en breed toepasbare taal voor kennisrepresentatie. Juist omdat interpretatie van de gegevens van belang is voor hergebruik. Praktisch kan het principe vertaald worden naar gebruik van de semantische webstandaarden van W3C. Deze standaarden worden ook gebruikt voor verklaringen. Deze standaarden zijn nodig om betekenis en data met elkaar te verbinden in een gegevensuitwisseling, zodat de ontvanger van de gegevens altijd de betekenis kan interpreteren (de 'knowledge-first'-aanpak).



Figuur 6 Gegevens beschikbaar stellen voor gegevensuitwisseling (Bron: Info Support)

4.2 Afspraken maken over de werking van het informatiestelsel

Afspraken zijn nodig om te komen tot een informatiestelsel in de zorg. Het is bijvoorbeeld nodig om afspraken te maken over de werking van het stelsel, wie de bron is voor welke gegevens en hoe die gegevens beschikbaar worden gesteld. Daarnaast is een spin in het web nodig voor de volledige medische geschiedenis van een patiënt. Deze rol zou ingevuld kunnen worden door de patiënt zelf of door de huisarts. Met de komst van eIDAS2 en de Europese ruimte voor gezondheidsgegevens is de verwachting dat de rol van de patiënt toeneemt. De patiënt zal meer en meer de houder worden van zijn eigen gezondheidsgegevens. De verwachting is dat big tech zal bijdragen aan functionaliteit voor preventie en monitoring van gezondheid. Een patiënt zelf zijn

medicatiebewaking laten doen, zou bijvoorbeeld een volgende stap kunnen zijn. Dit zou kunnen als recepten als verifieerbare verklaringen beschikbaar komen.

De gezondheidsgegevens zullen in de vorm van verifieerbare verklaringen in de wallet van een patiënt zijn opgenomen. Een verklaring zou bijvoorbeeld de Europese patiëntsamenvatting kunnen zijn. De patiënt kan deze verklaring uitwisselen met een zorginstelling, zodat zijn zorgverlener de gegevens kan inzien. Op basis van het voorstel voor de Europese ruimte voor gezondheidsgegevens moet een zorginstelling in staat zijn deze verklaringen te accepteren en te verifiëren. Dezelfde verklaringen kunnen ook gebruikt worden voor een directe gegevensuitwisseling tussen zorginstellingen.

4.3 Samenwerken om de zorg beter te maken

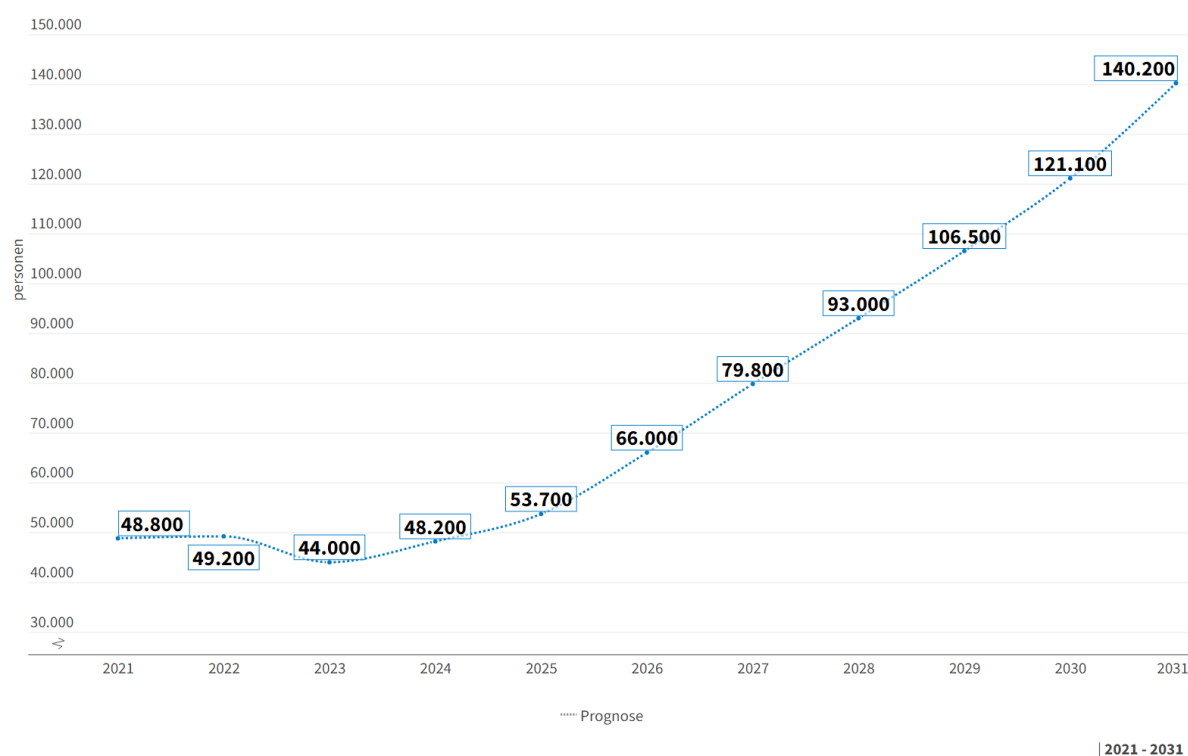
Iedere zorginstelling moet haar informatievoorziening voorbereiden op eIDAS2, op de Europese ruimte voor gezondheidsgegevens en op de Wet elektronische gegevensuitwisseling. Alle zorginformatiesystemen zouden de uitgifte en verificatie van verklaringen moeten ondersteunen. Beter is echter om het gezamenlijk te doen.

Softwareleveranciers bouwen nu gezamenlijk aan Nuts, een verzameling standaarden voor een decentraal open source-platform voor het aanbieden van vertrouwensdiensten. Via het platform kunnen verklaringen uitgegeven en geverifieerd worden. Een platform is nodig om tot een vertrouwde gegevensuitwisseling te komen. Het zou mooi zijn als dit initiatief door meer organisaties ondersteund zou worden, ook met financiële middelen. Juist om te voorkomen dat de ontwikkeling door een enkele partij gedomineerd wordt. Het platform moet de komende jaren nog verder worden uitgebreid. Met de komst van eIDAS2 zal bijvoorbeeld ook ondersteuning gegeven moeten worden aan de European Blockchain Services Infrastructure (EBSI).

5. Conclusie

Er zijn nog veel problemen te overwinnen in de zorg voordat de informatievoorziening op orde is. Informatievoorziening zorgt in de huidige situatie alleen maar voor extra administratieve lasten en ondersteunt een zorgverlener niet. De druk op zorgverleners lijkt alleen maar toe te nemen door het Integraal Zorgakkoord (IZA), door de Wet elektronische gegevensuitwisseling (Wegiz) en de komst van een Europese ruimte voor gezondheidsgegevens (EHDS). Terwijl er al een groot personeelstekort is. Volgens de huidige prognoses (zie figuur 7) zal het personeelstekort alleen maar toenemen, waardoor de huidige manier van werken niet houdbaar is.

De manier waarop we naar zorg kijken zal moeten veranderen. De manier van werken zal moeten veranderen. IZA, maar ook het Programma Wonen, Ondersteuning en Zorg voor Ouderen (WOZO) laat zien dat een transitie van de zorg in gang is gezet. Maar de zorg heeft ook een digitale transitie nodig om de informatievoorziening te moderniseren en te automatiseren. Iedere zorginstelling zou een gevoel van urgentie moeten hebben om haar administratieve lasten te verlagen. Deze urgentie speelt naast de urgentie om betere zorg te leveren door betere informatie over de patiënt. Informatietechnologie is nodig om werk uit handen te nemen van zorgverleners. Het is nodig om beslissingsondersteuning te bieden in de vele duizenden protocollen waar een zorgverlener mee te maken heeft. Maar ook om hergebruik te kunnen maken van kennis die door de patiënt, zorgverleners of anderen al is verzameld.



*Figuur 7 Verwachte arbeidsmarkttekort zorg en welzijn (exclusief kinderopvang)
(Bron: ABF Research)*

De Europese ruimte voor gezondheidsgegevens en eIDAS2 bieden kansen. Een wallet en het uitgeven van verifieerbare verklaringen biedt bijvoorbeeld de mogelijkheid om de patiënt een grotere rol te laten spelen in de gegevensuitwisseling, zodat een zorgverlener een volledig patiëntbeeld kan verkrijgen. Het biedt ook de mogelijkheid om gegevens betrouwbaar uit te wisselen met een hoge kwaliteit om de informatievoorziening te kunnen automatiseren. Het biedt het noodzakelijke vertrouwen en het geeft de mogelijkheden om hergebruik te maken van gegevens, zodat uiteindelijk informatie kan gaan werken voor zorgverleners.

6. Begrippenlijst

Wat is vertrouwen?

In deze whitepaper bedoelen we met vertrouwen het menselijk vertrouwen dat we hebben in een gegeven, oftewel een stukje data. Menselijk vertrouwen is echter niet iets wat gerealiseerd kan worden met een checklist. Een persoon bepaalt uiteindelijk altijd zelf of hij of zij iets vertrouwt. Daarom gaat het in deze whitepaper enkel over de maatregelen die je kunt nemen om betrouwbare gegevens te creëren. Betrouwbaarheid stelt eisen aan de mate van onweerlegbaarheid van het bewijs over de herkomst en integriteit van de gegevens.

Wat betekent herkomst, integriteit en onweerlegbaarheid?

Herkomst van gegevens geeft antwoord op vragen als waar, waarom, wanneer, door wie en hoe zijn de gegevens geproduceerd? Herkomst gaat dus verder dan alleen de oorsprong van een gegeven. Herkomst van gegevens is belangrijk, omdat patiënten vaker reizen of zelf een keuze maken voor een zorgverlener. Patiënten komen daardoor vaker op zorglocaties waar ze nog niet bekend zijn, vanuit andere regio's of vanuit andere landen met mogelijk andere eisen aan de kwaliteit van de gegevens.

De herkomst wordt geregistreerd als documentatie over een gegeven. De context van het gegeven bepaalt welke documentatie over de herkomst nodig is. Op basis van deze documentatie kunnen zorgverleners elkaars data bekijken en geautomatiseerd vaststellen of de data betrouwbaar hergebruikt kan worden. Neem bijvoorbeeld het lichaamsgewicht dat een diëtiste vastlegt. Dan moet er ook vastgelegd worden waar, wanneer, hoe, onder welke omstandigheden en met welke apparatuur het gewicht is vastgesteld. Alleen dan kan bijvoorbeeld een anesthesist de betrouwbaarheid verifiëren en besluiten tot hergebruik van het gegeven.

Naast herkomst van data is integriteit cruciaal. Het doel van gegevensintegriteit is onbedoelde veranderingen in data voorkomen. Je hebt specifieke technieken die de integriteit van een gegeven bewaken en gedurende de hele levenscyclus zorgen dat het gegeven is opgeslagen zoals het bedoeld was. Als je het gegeven oproept, is deze dus altijd hetzelfde als toen deze oorspronkelijk werd vastgelegd. De documentatie over het gegeven bevat daarom documentatie over de integriteit en de mogelijkheid tot verificatie hiervan.

De onweerlegbaarheid bepaalt uiteindelijk het niveau waarop de herkomst en integriteit kan worden vastgesteld. De onweerlegbaarheid kan laag, substantieel of hoog zijn en is

gebaseerd op de niveaus in de verordening voor elektronische identificatie en vertrouwensdiensten (eIDAS). Het betrouwbaarheidsniveau van de vertrouwensdiensten is in de documentatie opgenomen.

Wat is kwaliteit van gegevens?

Er zijn vele definities te vinden over kwaliteit van gegevens. In het algemeen stellen al deze definities dat de kwaliteit hoog is als de gegevens geschikt zijn voor het doel waarvoor de gegevens moeten worden gebruikt. Een gebruiker van de gegevens moet dus weten welk doel hij voor ogen heeft en welke eisen aan de gegevens gesteld moeten worden om dat doel te realiseren. Betrouwbaarheid is een van de eisen aan de kwaliteit van gegevens.

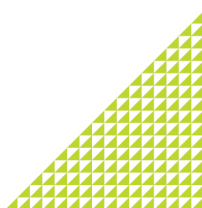
Terug naar het voorbeeld met het meten van het gewicht van een patiënt. De eisen aan iemands gewicht zijn anders voor een diëtiste dan voor een revalidatiearts. Daarom is documentatie en beleid nodig over hoe het gewicht is gemeten om te bepalen of het hergebruikt kan worden. Denk aan welk moment van de dag de weging is gedaan en of de patiënt met of zonder kleding is gewogen. Maar denk ook aan zaken als: welk apparaat is gebruikt voor de weging, bijvoorbeeld een klasse III gekeurde weegschaal. Voor de kwaliteit van de gegevens is het belangrijk dat ook zorgverleners van andere instanties de betekenis en de geldigheid van de gegevens kunnen interpreteren en beoordelen.

De zorgverlener die de gegevens wil hergebruiken zal moeten aangeven wat zijn beleid is voor hergebruik en welke documentatie nodig is. Voorwaarden aan de betrouwbaarheid, herkomst, integriteit en betekenis zijn allen onderdeel van de eisen die bepalen of de gegevens geschikt zijn voor het doel. Als de gegevens aan deze eisen voldoen, dan is er sprake van een gekwalificeerde gegevensuitwisseling voor hergebruik (bron: TNO Eindrapport – Een nieuw perspectief voor vertrouwensmodellen in de zorg).

Beleed opstellen voor gegevens zal voornamelijk landelijk worden gedaan, maar ook een zorginstelling kan (aanvullend) beleid opstellen voor specifieke toepassingen. Op landelijk niveau zijn de kwaliteitsstandaarden het instrument om beleidsafspraken te maken over de kwaliteit van gegevens. In de praktijk worden deze echter niet expliciet beschreven.

Wat is een kwaliteitsstandaard?

Een kwaliteitsstandaard is een beschrijving van een zorgproces. Het beschrijft de activiteiten die nodig zijn om goede zorg te verlenen. Hierbij hoort ook het registreren en raadplegen van informatie. Een kwaliteitsstandaard wordt getoetst en geregistreerd



in het register door Zorginstituut Nederland. De kwaliteitsstandaarden zijn voor de Wet elektronische gegevensuitwisseling in de zorg (Wegiz) het fundament om te bepalen welke gegevens uitgewisseld moeten worden en welke eisen zorgverleners hieraan stellen. Een NEN-norm (afspraken tussen Nederlandse marktpartijen onderling), beschrijft vervolgens hoe de gegevensuitwisseling technisch moet worden uitgevoerd.

Wat is de verordening voor Elektronische identificatie en vertrouwensdiensten?

De Europese verordening Elektronische identificatie en vertrouwensdiensten bestaat al sinds 2014 onder de noemer eIDAS (electronic IDentification And trust Services). Met behulp van eIDAS moet een Europese digitale interne markt ontstaan waarin partijen elektronisch transacties met elkaar kunnen uitvoeren. De eerste versie van eIDAS voldeed echter niet aan alle verwachtingen, omdat de burger geen eigen rol en regie had in deze verordening. Daarom wordt er nu gewerkt aan een verbeterde versie. Deze herziening staat bekend als eIDAS2.

In een Europese digitale interne markt kan een transactie van gegevens op ieder moment met iedere andere organisatie plaatsvinden, niet alleen met overheidsinstellingen maar ook met private ondernemingen. Ook in de zorg moet iedere zorgverlener een patiënt binnen de geldende regels kunnen overdragen aan iedere andere zorgverlener. De zorgsector is met een zogenoemde transactie niet uniek in eisen aan vertrouwen. Hergebruik van eIDAS ligt daarom voor de hand en is daarom ook verplicht voor de zorgsector via de Wet digitale overheid.

In het huidige eIDAS zijn vijf vertrouwensdiensten beschreven. Voor ieder van deze vertrouwensdiensten beschrijven we hieronder kort de waarde.

1. Met een *elektronische handtekening* van een natuurlijk persoon wordt onweerlegbaar bewezen dat een persoon de transactie heeft ondertekend. Onweerlegbaarheid betekent dat de elektronische handtekening cryptografisch zo sterk is, dat deze zal standhouden in een geschil en door de rechter erkend zal worden als geldig bewijs.
2. Rechtspersonen zetten geen handtekening, maar plaatsen een zegel. Een *elektronisch zegel* voor rechtspersonen geeft het onweerlegbare bewijs dat een rechtspersoon de transactie heeft verzegeld.
3. Een *elektronisch tijdstempel* om het tijdstip van de transactie onafhankelijk en onweerlegbaar vast te stellen. Hiermee is het tijdstip van de transactie bewijsbaar.
4. Voor een transactie kan een *elektronisch aangetekende bezorging* nodig zijn van elektronische gegevens. Hiermee is bewijsbaar dat de elektronische gegevens zijn bezorgd.

5. De *authenticatie van websites*² voor browsers geeft zekerheid over de juistheid van de organisatie en het domein van de website. Met deze vertrouwensdienst kan vertrouwen worden verkregen in de website waarop de transactie wordt uitgevoerd.

Het voorstel van eIDAS2 voegt drie vertrouwensdiensten toe.

1. *Elektronische archivering* van elektronische gegevens en digitale documenten waarmee onder andere de integriteit en de juistheid van een document gegarandeerd kan worden gedurende de volledige bewaartermijn.
2. Een *elektronisch register* moet partijen bewijs geven over een vaststaand, niet veranderbaar, controlespoor voor de volgorde van transacties en gegevensbestanden.
3. Een vertrouwensdienst voor *elektronische attestering van attributen*. Hiermee kan onweerlegbaar bewijs worden overhandigd over kenmerken van een natuurlijk persoon, een rechtspersoon of van een ding.

Naast de vertrouwensdiensten wordt eveneens een Europese portemonnee voor digitale identiteit geïntroduceerd. De portemonnee is beter bekend onder de Engelse naam *Digital Identity Wallet*. In deze wallet, die doet denken aan een betrouwbaardere variant op de Apple of Google-wallet, zal een elektronische identiteit van een natuurlijk persoon of rechtspersoon kunnen worden opgenomen. Maar ook andere data op basis van de vertrouwensdienst voor elektronische attestering van attributen. De data worden gebundeld uitgegeven in de vorm van een elektronische verklaring zoals een bankpas, rijbewijs, bioscoopkaartje, boardingpass of diploma. Ieder van deze elektronische verklaringen heeft een verifieerbare referentie naar de uitgever van de verklaring.

Burgers kunnen de wallet gebruiken om bijvoorbeeld betalingen te doen, aan boord te gaan van een vliegtuig of om een auto te huren. Op hun beurt zullen organisaties in staat moeten zijn om de gegevens uit de wallet te verifiëren en de betrouwbaarheid ervan vast te stellen. De wallet wordt naar verwachting voor de zorgsector verplicht via de Wet digitale overheid. Voor zeer grote online platforms, voor de big tech dus, wordt acceptatie van de wallet eveneens verplicht.

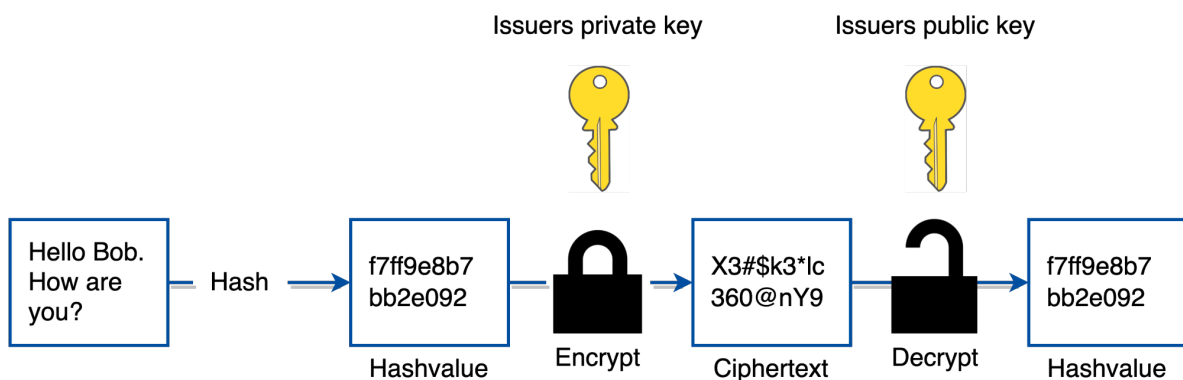
Zowel het Europese parlement als uiteenlopende private partijen werken aan een verdere verbetering van het huidige voorstel. Naar verwachting zal eIDAS2 in 2023 van kracht worden. In de reductie van administratieve lasten kan eIDAS2 nu al helpen. Denk bijvoorbeeld aan het uitgeven van een patiëntenpas. Hierbij kan hergebruik worden

² In deze whitepaper gaan we uit van transacties die niet in een browser worden uitgevoerd. De vertrouwensdienst voor authenticatie van websites zal in deze whitepaper daarom niet verder worden behandeld.

gemaakt van de huidige elektronische identificatiemiddelen zoals DigiD in voorbereiding op eIDAS2. De patiënt zou bijvoorbeeld door middel van selfservice een patiëntenpas kunnen ontvangen in de vorm van een verklaring.

Hoe kan een verklaring van een uitgever worden geverifieerd?

Een verklaring wordt verifieerbaar door de elektronische zegel van de uitgever. Een elektronische zegel is in de praktijk een versleutelde hashwaarde van de gegevens in een verklaring. De hashwaarde is eenrichtingsverkeer. Dit betekent dat de hashwaarde berekend kan worden op basis van de gegevens, maar dat de gegevens niet herleid kunnen worden uit de hashwaarde. De hashwaarde wordt met de private sleutel van de uitgever versleuteld. Een verificateur kan met de publieke sleutel van de uitgever verifiëren dat de gegevens afkomstig zijn van de uitgever. Er is technisch geen verschil tussen een elektronische handtekening en een elektronische zegel. Een handtekening kan echter alleen door een natuurlijk persoon worden gezet en een zegel door een rechtspersoon.



Figuur 8 Werking elektronische handtekening/zegel (Bron: Internet)