27 september 2019

Advies opslag medische data in de cloud

ICTRECHT
adviesbureau

Inhoudsopgave

Inleiding

Voor u ligt het adviesrapport met het resultaat van het onafhankelijke onderzoek naar de wenselijkheid van de opslag van medische data van Nederlandse patiënten bij niet-EU cloudproviders. In dit adviesrapport wordt ingegaan op de risico's die kunnen spelen ten aanzien van opslag van medische data van Nederlandse patiënten in 'de cloud'.[1] Zowel juridische als technische risico's worden daarbij behandeld. Gelet op de vraag of cloudopslag van medische data 'wenselijk' is, reikt dit onderzoek ook verder dan alleen de vraag of cloudopslag van medische data op dit moment volgens de wet is toegestaan. Centraal staan de volgende vragen en daarbij horende antwoorden:

- Aan welke juridische eisen moet een cloudprovider voldoen om te borgen dat medische data van Nederlandse patiënten voldoende beveiligd én met waarborgen voor de privacy kan worden opgeslagen en verwerkt?
- Op basis van deze vereisten; welke risico's bestaan er ten aanzien van de waarborgen voor de privacy in deze situaties bij het gebruik van cloudproviders met een basis in Nederland, de Europese Unie, de Verenigde Staten en overige landen? Zijn er wezenlijke verschillen tussen lokale Nederlandse cloudproviders en providers uit de andere categorieën landen?
- Aan welke technische eisen moet een cloudprovider voldoen om te borgen dat medische data van Nederlandse patiënten voldoende beveiligd én met waarborgen voor de privacy kan worden opgeslagen en verwerkt?
- Op basis van deze vereisten; welke risico's bestaan er ten aanzien van informatieveiligheid in deze situaties bij het gebruik van cloudproviders met een basis in Nederland, de Europese Unie, de Verenigde Staten en overige landen? Zijn er wezenlijke verschillen tussen lokale Nederlandse cloudproviders en providers uit de andere categorieën landen?
- Welk onderscheid moet gemaakt worden tussen cloudproviders met een basis binnen Nederland, de Europese Unie, de Verenigde Staten en overige landen ten aanzien van deze technische- en juridische eisen?

Naast antwoorden op deze vragen bevat dit rapport tevens richtlijnen en adviezen over de keuze van cloudopslag bij medische gegevens. Ten behoeve van de leesbaarheid is achterin dit rapport een definitielijst opgenomen met daarin een uitleg van termen en afkortingen.

Het rapport is opgebouwd uit drie delen. Het eerste deel (A) geeft een algemene samenvatting van de onderzoeksresultaten en het advies. Het tweede deel (B) geeft een nadere onderbouwing van de antwoorden op de onderzoeksvragen. In het derde deel (C) worden diverse aanbevelingen voor (i) cloudproviders, (ii) (potentiële) afnemers van clouddiensten en (iii) overheden op een rij gezet.

Dit rapport is tot stand gekomen door uitvoerige documentstudie en het verzamelen van ervaringen en feiten bij diverse belanghebbenden. Dit zijn zowel cloudproviders als partijen die cloudproviders gebruiken ten behoeve van de opslag en verwerking van medische data en diverse brancheorganisaties. Wij zijn zeer dankbaar voor alle input en feedback van alle geraadpleegde partijen.

[1] Hierbij wordt benadrukt dat dit onderzoek niet is gericht op de vraag of bepaalde specifieke partijen wel of niet voldoen of hebben voldaan aan hun wettelijke verplichtingen.

Deel A. Samenvatting advies

"Data honderdduizenden patiënten in stilte naar Google verhuisd" en "Ook jouw medische data liggen nu bij Google".[2] Met deze koppen vestigde het AD op 30 maart 2019 de aandacht op de wenselijkheid van het gebruik van niet-EU[3] cloudplatforms voor het opslaan van medische data van Nederlandse patiënten. Naar aanleiding daarvan heeft de Minister voor Medische Zorg en Sport aangegeven een onafhankelijk onderzoek te laten doen naar deze wenselijkheid. Hieronder volgen de bevindingen en aanbevelingen die gedurende dat onderzoek naar voren zijn gekomen. Specifieke aandacht is besteed aan de juridische en technische eisen en risico's die van toepassing zijn op de bescherming van medische data.

Een hoog beschermingsniveau voor medische data is wettelijk vereist

Medische data zijn gevoelige persoonsgegevens waarmee zeer zorgvuldig omgegaan dient te worden. Deze gegevens gaan over de gezondheid van mensen en zijn zeer persoonlijk. Verlies, onjuistheid of onbevoegde inzage van medische data kan leiden tot lichamelijk of psychisch letsel en andere vormen van schade of nadeel voor de patiënt. Om vrije toegang tot zorg te waarborgen, is het nodig dat patiënten de zekerheid hebben dat hun medische data veilig zijn. Diverse in Nederland en de EU toepasselijke wetten dwingen dan ook een hoog beschermingsniveau van medische data af.

Cloudplatforms worden steeds meer gebruikt, ook voor de verwerking van medische data

Nederlandse zorginstellingen en andere partijen die medische data van Nederlandse patiënten bezitten, werken steeds vaker met 'de cloud'. Deze term kan de indruk wekken van een ongrijpbaar en abstract technisch concept, maar in de praktijk gaat het gewoon om het uitbesteden van opslag, rekenkracht en doorgifte van data aan een daarin gespecialiseerd bedrijf: een cloudprovider.

De wens vanuit zorgpartijen om 'de cloud in' te gaan is zeer goed te begrijpen. Cloudproviders bieden in het algemeen mogelijkheden voor verwerking én bescherming van medische data die door zorgpartijen zelf niet goed zijn te evenaren. Cloudproviders zijn gespecialiseerd in het aanbieden van zo betrouwbaar en veilig mogelijke systemen voor opslag en verwerking van data. Het zo goed mogelijk beschermen van deze data is in hun bedrijfsbelang. Zij investeren daar veel in en kunnen daarbij substantiële schaalvoordelen bieden.

Zorgverleners en andere partijen die medische data verwerken, kunnen daar hun voordeel mee doen. Gebruik van een goed beveiligde cloudprovider faciliteert zorgverleners ook in het nakomen van hun eigen wettelijke verplichtingen tot het beschermen van medische data. Diverse andere partijen die zeer hoge eisen stellen aan beveiliging, zoals banken, maken ook steeds meer gebruik van cloudplatforms.

Categorieën niet-EU cloudproviders

Veel cloudproviders hebben een vestiging of hoofdkantoor in de Verenigde Staten of in andere landen buiten de EU. Onderzocht is in hoeverre de hoge eisen die in Nederland en de EU zijn gesteld aan het beschermingsniveau van medische data, ook geborgd zijn of kunnen worden bij het inschakelen van dergelijke niet-EU cloudproviders.[4]

---

[2] https://www.ad.nl/binnenland/data-honderdduizenden-patienten-in-stilte-naar-google-verhuisd~af1950a9/ en https://www.ad.nl/binnenland/ook-jouw-medische-data-liggen-nu-bij-google~abcb3f6a/.

[3] Onder EU wordt in de context van dit onderzoek begrepen de Europese Unie plus Noorwegen, Liechtenstein en IJsland, aangezien deze landen ook onder het toepassingsbereik van de AVG vallen.

[4] Niet-EU cloudproviders zijn voor dit onderzoek onderverdeeld in twee categorieën: 1. cloudproviders zonder vestiging in de EU en 2. cloudproviders met vestiging(en) in de EU en tevens vestiging(en) buiten de EU.

Als de AVG aantoonbaar wordt nageleefd, is medische data goed beveiligd

Specifiek waar het gaat om medische data gelden extra strenge wettelijke eisen, met name voortvloeiend uit de AVG. Zo is het verplicht om een risicoanalyse uit te voeren, contractuele afspraken te maken ter bescherming en beveiliging van de data en om aanvullende maatregelen te treffen wanneer medische data buiten de EU kan worden opgeslagen. Als de cloudprovider en afnemer beide aantoonbaar aan dit pakket eisen voldoen, wordt daarmee een hoog niveau van veiligheid gerealiseerd bij de opslag van medische data in de cloud.

Om naleving van de AVG effectief af te kunnen dwingen, is wel vereist dat de cloudprovider ten minste een vestiging of opslaglocatie heeft in de EU. Bij de populaire niet-EU cloudproviders is dit het geval.

Certificeringsmechanismes voor naleving van de AVG en beveiliging

Om compliance en veiligheid aan te tonen, maken cloudproviders in de praktijk gebruik van certificering tegen standaarden. Op dit vlak vindt momenteel veel innovatie plaats, waaronder de ontwikkeling van nieuwe gedragscodes en certificeringsmechanismes die specifiek zien op naleving van de AVG door cloudproviders. Daarbij wordt gestreefd naar controles die zo onafhankelijk, doorlopend (of frequent en onverwacht), volledig en specifiek mogelijk de naleving waarborgen. Hoe dichter dit ideaal wordt benaderd, hoe verder het risico op niet-naleving wordt geminimaliseerd. Het advies aan de minister is dan ook om de ontwikkeling van dergelijke mechanismes zoveel als mogelijk te stimuleren, om de kans op niet-naleving zo ver mogelijk terug te dringen.

Het risico van inzage door buitenlandse autoriteiten

Een bijzonder aspect van clouddienstverlening is dat een cloudprovider onderworpen kan zijn aan meerdere rechtsstelsels. Een Amerikaans bedrijf dat in diens datacenters in de EU medische data van Nederlanders opslaat voor een Amsterdams ziekenhuis, is gehouden aan de AVG maar ook aan bevelen van Amerikaanse autoriteiten tot inzage. Dat is bijvoorbeeld mogelijk in het kader van strafrechtelijk onderzoek en bij geheime bevelen van Amerikaanse geheime diensten. In de afgelopen jaren zijn vele vragen gerezen over de reikwijdte van dergelijk inzagerecht van autoriteiten buiten de EU op (medische en andere) data van partijen in de EU.

De AVG heeft een stevige lijn in het zand getrokken. Het is cloudproviders onder de AVG expliciet verboden om klantdata te verstrekken aan autoriteiten van een land buiten de EU, tenzij de EU of de lidstaat zelf internationale afspraken daarvoor heeft gemaakt met dat land, zoals rechtshulpverdragen waaronder rechtshulpverzoeken gedaan kunnen worden.

De meest gebruikte niet-EU cloudproviders met vestiging in de EU geven allen ook aan dat zij zich zeer terughoudend opstellen ten aanzien van dergelijke verzoeken. Zij hebben beleid vastgesteld om verzoekende autoriteiten waar mogelijk door te verwijzen naar de afnemer van de clouddienst. De afnemer is immers de partij die verantwoordelijk is voor het gebruik, en eventueel afstaan, van de medische data.

Ondanks de waarborgen uit de AVG en het beleid van niet-EU cloudproviders, bestaat de mogelijkheid dat een niet-EU cloudprovider zich voor een lastige keuze ziet. De keuze om óf de AVG na te leven, óf de wetgeving die verplicht tot het verstrekken van data aan autoriteiten buiten de EU. Als de cloudprovider dan kiest om de plicht tot verstrekking van data aan de buitenlandse autoriteiten na te leven, bestaat de mogelijkheid dat deze toegang krijgen tot medische data van Nederlandse patiënten. Het dient voorkomen te worden dat cloudproviders door buitenlandse autoriteiten, in strijd met de AVG, verplicht kunnen worden tot het verstrekken van medische data van Nederlandse patiënten. Derhalve luidt het advies aan de minister om waar mogelijk te faciliteren dat met zoveel mogelijk landen buiten de EU internationale afspraken worden gemaakt waardoor medische data van Nederlandse patiënten ook buiten de EU gelijkwaardig worden beschermd.

Instrumenten voor legale doorgifte naar VS en andere landen buiten de EU onder druk

Te concluderen is dat het gebruik van cloudproviders wenselijk is als de cloudprovider (i) ten minste een vestiging of opslaglocatie in de EU heeft en (ii) iedere vestiging van de cloudprovider buiten de EU zich in een land bevindt waar medische data gelijkwaardig is beschermd als in de EU. De Verenigde Staten, waar de meeste grote niet-EU cloudproviders met vestiging in de EU hun hoofdkantoor hebben, zijn in dit opzicht een bijzonder geval. Er is een speciale regeling getroffen met de VS, genaamd Privacy Shield, om persoonsgegevens bij Privacy Shield gecertificeerde partijen in de VS gelijkwaardige bescherming te geven als in de EU. Er loopt momenteel echter een rechtszaak bij het Hof van Justitie van de EU waarin de gelijkwaardigheid van de bescherming in twijfel wordt getrokken. In dezelfde rechtszaak worden ook de model clauses in twijfel getrokken. Dat zijn modelcontracten die eveneens bedoeld zijn om persoonsgegevens van mensen in de EU te beschermen als deze buiten de EU worden opgeslagen. Het probleem daarmee is echter dat contractuele verplichtingen geen reële bescherming kunnen bieden tegen wettelijke plichten die worden opgelegd door buitenlandse autoriteiten. Door de rechtszaak bestaat een reëel risico dat deze instrumenten binnenkort (opnieuw) herzien of vervangen zullen moeten worden.

Het (afgeleide) verschoningsrecht in de zorg

Een andere belangrijke bescherming van medische data tegen de mogelijkheid van inzage door autoriteiten, naast de AVG, is het verschoningsrecht. Op grond van dit in Nederland vastgelegde recht kunnen zorgverleners niet gedwongen worden tot het verstrekken van (toegang tot) medische data, behalve als de patiënt daar (in overleg met de zorgverlener) zelf toestemming voor heeft gegeven. Cloudproviders hebben een afgeleid verschoningsrecht als zij medische data verwerken ten behoeve van zorgverleners. Cloudproviders dienen zich hier bewust van te zijn en zich op het afgeleide verschoningsrecht te beroepen als zij een vordering ontvangen die betrekking heeft, of waarschijnlijk zou kunnen hebben, op medische data van Nederlandse patiënten. Het is wenselijk om dit als verplichting in een (verwerkers)overeenkomst met de cloudprovider vast te leggen. Het is ook wenselijk dat de minister waar mogelijk faciliteert dat afspraken met andere landen worden gemaakt waardoor autoriteiten van die landen gehouden worden het verschoningsrecht voor medische data van Nederlandse patiënten te respecteren.

Technische maatregelen tegen de belangrijkste risico's bij (niet-EU) cloudproviders

Wanneer een cloudprovider onder de jurisdictie valt van een land waar gelijkwaardige bescherming van medische data, waaronder het (afgeleide) verschoningsrecht, niet zeker is, is het wenselijk om medische data van Nederlandse patiënten te versleutelen voordat deze worden overgedragen aan de cloudprovider.

Deze technische maatregel kan ook andere risico's verder minimaliseren. Hoe veelbelovend de hierboven al genoemde nieuwe certificeringsmechanismes ook zijn, zij zullen het risico op niet-naleving door de cloudprovider niet voor de volle 100 procent kunnen uitsluiten. Door encryptie toe te passen waarbij de sleutel altijd buiten de macht van de cloudprovider wordt gehouden, wordt technisch afgedwongen dat de cloudprovider de data zelf niet kan inzien en ook geen inzage kan verstrekken aan buitenlandse autoriteiten. Versleuteling moet wel met grote zorg en aandacht worden ingebouwd, vereist de nodige expertise en kan ook kosten, belemmeringen of andere nadelen met zich mee brengen. Voor zover zorgverleners en andere partijen hier feitelijk niet goed toe in staat zijn, luidt het advies aan de minister om hierin zoveel mogelijk faciliterend op te treden.

Een andere technische maatregel die in het bijzonder van belang is voor het beschermen van medische data bij cloudopslag, is het gebruik van twee- of meerfactorauthenticatie voor toegang. Tevens dienen er technische maatregelen getroffen te zijn om de goede werking van de toegangsbeveiliging te controleren (logging). Tot slot dient zowel het verkeer van de gebruiker naar de cloudprovider, als de opslag van medische data bij de cloudprovider zelf, versleuteld te zijn om opgeslagen medische data optimaal te kunnen beschermen.

Gebruik van cloudproviders zonder vestiging in de EU is niet aan te raden

Gebruik van een niet-EU cloudprovider die geheel geen vestiging, vertegenwoordiger of opslagcapaciteit heeft in de EU, is niet wenselijk. Het gebruik van dergelijke providers creëert een risico dat de AVG niet van toepassing is of dat handhaving van de AVG in de praktijk niet goed mogelijk is. De AVG is immers alleen van toepassing op organisaties binnen de EU, of organisaties die zich van buiten de EU specifiek richten op personen in de EU. Om naleving van de AVG effectief af te dwingen van een cloudprovider zonder vestiging in de EU, zou bovendien medewerking van de lokale autoriteiten nodig zijn van het land waar de cloudprovider wel is gevestigd. Die medewerking zou tegen het belang van de autoriteiten in dat land kunnen ingaan – als zij juist data van de cloudprovider zouden willen hebben in strijd met de AVG – waardoor niet op dergelijke medewerking gerekend kan worden. Wanneer de AVG niet van toepassing is of praktisch niet goed gehandhaafd kan worden, valt het hoge niveau van juridische bescherming van medische data van Nederlandse patiënten grotendeels weg. Het gebruik van een cloudprovider zonder vestiging of opslaglocatie in de EU, en waarop de AVG niet van toepassing is, wordt daarom afgeraden.

Deel B. Achtergrond en verdieping

1. Juridische eisen aan cloudproviders

1.1 Inleiding en scope

Om tot een antwoord op de hoofdvraag te komen, ten aanzien van de beoordeling van de wenselijkheid van het gebruik van niet-EU cloudplatforms, zijn deelvragen geformuleerd. Deze deelvragen worden in de hieronder volgende hoofdstukken apart behandeld. Het antwoord op de eerste deelvraag vereist een uiteenzetting van toepasselijke juridische kaders:

> *Aan welke juridische eisen moet een cloudprovider voldoen om te borgen dat medische data van Nederlandse patiënten voldoende beveiligd én met waarborgen voor de privacy kan worden opgeslagen en verwerkt?*

Voor de opslag van medische data van Nederlandse patiënten zijn twee soorten juridische regels van belang, die hieronder afzonderlijk uiteengezet worden:

1. De regels die gaan over bescherming en bewaring van medische data, en
2. De regels die gaan over de mogelijkheid van opsporingsdiensten, inlichtingendiensten en andere autoriteiten van overheden om (toegang tot) gegevens te vorderen, waardoor de vertrouwelijkheid van de gegevens wordt beperkt.

1.2 Regels ter bescherming, beveiliging en/of bewaring van medische persoonsgegevens

Ter borging van medische data van Nederlandse patiënten bij cloudproviders dient voldaan te worden aan diverse juridische vereisten. Deze vereisten worden hieronder toegelicht.

AVG en UAVG

Omgang met persoonsgegevens is op Europees niveau gereguleerd in de AVG. Nederland heeft hieromtrent nadere regels vastgelegd in de UAVG. Om te begrijpen of en in hoeverre de AVG en UAVG van toepassing zijn op cloudproviders binnen en buiten de EU, wordt hieronder allereerst ingegaan op de reikwijdte van deze privacywetgeving. Vervolgens wordt ingegaan op algemene relevante eisen ten aanzien van de verwerking van persoonsgegevens door cloudproviders in hun rol als verwerker en de daarbij horende specifieke eisen ten aanzien van de verwerking van medische data.

1.2.1.1 Materiële toepasselijkheid van de AVG en UAVG

De AVG en UAVG zijn van toepassing op geheel of gedeeltelijk geautomatiseerde[5] verwerkingen van persoonsgegevens.[6] Hiervan is al sprake wanneer er bij de verwerking van persoonsgegevens gebruik wordt gemaakt van elektronische apparatuur zoals een computer of server. Dat maakt de materiële toepasselijkheid van de AVG op cloudproviders evident.[7] Zij verwerken medische data door middel van elektronische apparatuur. Het opslaan van medische data door cloudproviders is aan te merken als een verwerking.[8]

[5] Daarnaast is de AVG ook van toepassing op de verwerking van persoonsgegevens die zijn opgenomen in een bestand, of bedoeld zijn om daarin opgenomen te worden. Daar dit ten aanzien van de opslag van medische data in de cloud niet relevant is, blijft dit verder buiten beschouwing.

[6] Zie artikel 2 lid 1 AVG.

[7] Artikel 2 lid 2 en 3 AVG bevat uitzonderingssituaties waarop de AVG niet van toepassing is. Hierbij valt te denken aan activiteiten op het gebied van nationale veiligheid van lidstaten en gemeenschappelijk buitenlands en veiligheidsbeleid van lidstaten. Wanneer dergelijke uitzonderingen aan de orde zijn ten aanzien van de verwerking van medische data bij en door cloudproviders, wordt dit expliciet benoemd in dit rapport.

[8] Zie artikel 4 onder 2 AVG en de definitie van 'verwerking' zoals opgenomen in hoofdstuk 6.

1.2.1.2 Territoriale toepasselijkheid van de AVG en UAVG

De AVG is in territoriaal opzicht van toepassing op verwerkingen van persoonsgegevens die plaatsvinden door organisaties met een vestiging binnen de EU[9]. In de rechtspraak is een vestiging gedefinieerd als iedere duurzame, reële en daadwerkelijke activiteit in een lidstaat, zelfs als deze activiteit slechts gering is. Een rechtspersoon is niet per se noodzakelijk om van een vestiging te kunnen spreken. Onder bepaalde omstandigheden kan bij één enkele vertegenwoordiger reeds sprake zijn van een duurzame vestiging, indien diegene optreedt met een voldoende mate van duurzaamheid en met behulp van de nodige middelen voor de verlening van de betrokken concrete diensten in de desbetreffende lidstaat.[10] Dit maakt de AVG in elk geval toepasselijk op iedere cloudprovider met een rechtspersoon binnen de EU en daarnaast op cloudproviders die andere vormen van duurzame, reële en daadwerkelijke activiteiten hebben in een lidstaat.

De AVG is daarnaast ook van toepassing op cloudproviders die geen vestiging (zoals hierboven gedefinieerd) in de EU hebben, maar wel medische data van Nederlandse patiënten verwerken die zich in de EU bevinden. Dit geldt uitsluitend als:

1. De cloudprovider goederen of diensten aanbiedt aan betrokkenen binnen de EU; of
2. De cloudprovider gedrag monitort van betrokkenen, voor zover dit gedrag binnen de EU plaatsvindt.[11]

De UAVG kent een soortgelijke territoriale bepaling ten aanzien van toepasselijkheid.[12] Het enige verschil is dat deze bepaling spreekt over Nederland, waar de AVG spreekt over de EU.

Kijkend naar de meest populaire cloudproviders die op de Nederlandse markt actief zijn, hebben deze allen rechtspersonen (en dus vestigingen) binnen de EU. Daarmee is de AVG op hen van toepassing. Voor cloudproviders zonder vestiging in de EU dient per geval beoordeeld te worden of de provider goederen of diensten aanbiedt aan betrokkenen binnen de EU en Nederland, dan wel gedrag van hen monitort. Enkel in dat geval is de AVG van toepassing op dergelijke cloudproviders.

1.2.1.3 Verwerkingsverantwoordelijke of verwerker

Indien eenmaal is vastgesteld dat de AVG en/of UAVG van toepassing, is dient de privacyrechtelijke rol van de cloudprovider vastgesteld te worden. De AVG maakt een onderscheid tussen de rol van verwerkingsverantwoordelijke[13] en die van verwerker[14]. Verwerkingsverantwoordelijke is de partij die bepaalt waarom en hoe persoonsgegevens verwerkt worden. Een verwerker verwerkt persoonsgegevens ten behoeve van de verwerkingsverantwoordelijke. Dit onderscheid is van belang, aangezien diverse verplichtingen uit de AVG en UAVG primair voor de verwerkingsverantwoordelijke gelden.

Ter illustratie van deze rolverdeling het volgende voorbeeld. Een ziekenhuis is verwerkingsverantwoordelijke ten aanzien van de medische data zie zij van haar patiënten verwerkt. Wanneer een ziekenhuis een derde partij, zoals bijvoorbeeld een onderzoeks- en analysebureau, de opdracht geeft om deze medische data te analyseren voor onderzoeksdoeleinden, is deze derde partij aan te merken als verwerker.

Wanneer het bureau vervolgens op haar beurt een derde partij inschakelt, bijvoorbeeld een cloudprovider, om te assisteren bij de opslag van medische data van het ziekenhuis, is de cloudprovider aan te merken als subverwerker.

[9] Zie artikel 3 lid 1 AVG.

[10] Zie HvJ EU 1 oktober 2016, C-230/14 (Weltimmo).

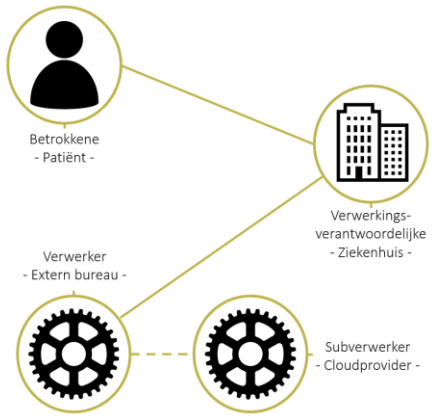
[11] Zie artikel 3 lid 2 AVG.

[12] Zie artikel 4 UAVG.

[13] Zie artikel 4 onder 7 AVG.

[14] Zie artikel 4 onder 8 AVG.

In onderstaande afbeelding wordt dit geïllustreerd.



Kenmerkend voor een verwerker, of subverwerker, is dat deze geen zelfstandige beslissingen neemt ten aanzien van de verwerking van persoonsgegevens. Dit is voorbehouden aan de verwerkingsverantwoordelijke. Zo is het de verwerkingsverantwoordelijke die bepaalt welke persoonsgegevens er voor welk doel verwerkt worden en hoe lang deze verwerking dient te duren. Een cloudprovider mag medische data die zij voor een ziekenhuis opslaat, bijvoorbeeld niet gebruiken voor doeleinden die het ziekenhuis niet zelf heeft toegestaan.

Gelet op de aanleiding van dit rapport, waarin cloudproviders als verwerker of subverwerker een rol spelen bij de verwerking van medische data, zal het uitgangspunt in dit rapport ook zijn dat cloudproviders als verwerker of subverwerker van medische data fungeren. De eisen die de AVG en UAVG stellen aan cloudproviders in de rol als verwerkingsverantwoordelijke zullen derhalve niet belicht worden. Uiteraard worden deze eisen wel besproken wanneer deze relevant zijn voor de klant/gebruiker (bijvoorbeeld een ziekenhuis) van de cloudprovider, of wanneer het risico bestaat dat een cloudprovider ondanks uitdrukkelijke instructies toch handelingen verricht die voorbehouden zijn aan een verwerkingsverantwoordelijke.

Alvorens een cloudprovider wordt geselecteerd om de opslag van medische data te faciliteren, dient er door de verwerkingsverantwoordelijke een DPIA uitgevoerd te worden waarin onder andere de rolverdeling nauwkeurig wordt onderzocht. Het vastleggen van deze rolverdeling in een verwerkersovereenkomst is een wettelijke verplichting[15], maar de naleving van deze verplichting, en andere verplichtingen uit de verwerkersovereenkomst, dient daadwerkelijk door de verwerkingsverantwoordelijke gecontroleerd, geverifieerd en gehandhaafd te worden. Onderstaand voorbeeld illustreert dit.

[15] Zie artikel 28 lid 3 AVG.

Een partij wordt door ziekenhuis A ingeschakeld om analytisch onderzoek te verrichten op de bloeduitslagen van haar patiënten, om zodoende bepaalde trends in kaart te brengen. De onderzoekende partij treedt hier op als verwerker voor ziekenhuis A. De medische data mag uitsluitend gebruikt worden voor onderzoek ten behoeve van ziekenhuis A. De onderzoekende partij doet dit echter ook voor ziekenhuis B en C. Om landelijke trends in kaart te brengen en de trends van ziekenhuis A, B en C af te zetten tegen die landelijke trends, vergelijkt de onderzoekende partij de bloeduitslagen van de patiënten van alle ziekenhuis met elkaar. Als dit gebeurt zonder dat de ziekenhuizen hier weet van hebben, of instructies toe hebben gegeven, is dit niet toegestaan. Voor deze verwerking treedt de onderzoekende partij niet langer op als verwerker, maar is deze zelfstandig verwerkingsverantwoordelijke geworden. Als deze handeling niet als zodanig in de verwerkersovereenkomst is benoemd, en daarom niet is toegestaan, schendt de onderzoekende partij haar verplichtingen uit de verwerkersovereenkomst. Als verwerkingsverantwoordelijke is het ziekenhuis richting haar patiënten verantwoordelijk voor deze schending.

1.2.1.4 Rechtmatig, behoorlijk en transparant

Als verwerkingsverantwoordelijke dient een organisatie zorg te dragen voor naleving van de basisbeginselen van de AVG.[16] Om privacy als grondrecht te borgen, stelt de AVG dat iedere verwerking van persoonsgegevens rechtmatig, behoorlijk en transparant dient te geschieden. Het belang van naleving van deze basisbeginselen wordt benadrukt door het feit dat niet naleving hiervan kan resulteren in een boete van de hoogste categorie, te weten € 20.000.000 of 4% van de totale wereldwijde jaaromzet van de overtreder.[17]

Het feit dat deze verplichtingen bij de verwerkingsverantwoordelijke rusten, wil niet zeggen dat verwerkers hiervan gevrijwaard zijn. Om te kunnen voldoen aan deze basisbeginselen, dient de verwerkingsverantwoordelijke immers te kunnen vertrouwen op haar verwerkers. Zij moet in kunnen staan voor de gehele keten. Aan betrokkenen dient uitgelegd te kunnen worden waarom, waar en door wie hun medische data worden verwerkt[18]. Dit principe wordt elders in de AVG nader uitgewerkt.[19]

De eisen uit de AVG spelen een aanzienlijke rol wanneer medische data van Nederlandse patiënten bij een cloudprovider onder gebracht worden. Een verwerkingsverantwoordelijke kan uitsluitend aan deze eisen voldoen wanneer cloudproviders volledig transparant zijn over de verwerkingen die zij uitvoeren bij het opslaan van data.

1.2.1.5 Doelbinding

De verwerking van persoonsgegevens dient welbepaald en uitdrukkelijk omschreven te worden. Iedere verwerking moet daarnaast een gerechtvaardigd doel dienen, waarbij persoonsgegevens uitsluitend in lijn met dat doel verwerkt mogen worden.[20] Ook dit zijn principes die door de verwerkingsverantwoordelijke gewaarborgd dienen te worden. Principes die echter tevens door verwerkers nageleefd moeten worden. Zoals benoemd in paragraaf 1.2.1.3, is het verwerkers niet toegestaan zelfstandig doelen te bepalen ten aanzien van de medische data die zij van verwerkingsverantwoordelijken hebben ontvangen.

1.2.1.6 Informatieplicht

Op de verwerkingsverantwoordelijke rust de verplichting om betrokkenen te informeren over gegevensverwerkingen. Zo ook ten aanzien van medische data en de omgang daarmee door verwerkers. Gebruikelijk is dat dit door middel van een (online) privacyverklaring

[16] Zie artikel 5 AVG.

[17] Zie artikel 83 AVG.

[18] Zie ook paragraaf 1.2.1.6.

[19] Zie artikel 12, 13 en 14 AVG.

[20] Zie artikel 5 lid 1 sub b AVG.

plaatsvindt. Belangrijkste punt ten aanzien van deze informatieverplichting, in het licht van dit rapport, is dat (categorieën van) verwerkers in de privacyverklaring genoemd dienen te worden alsmede het land waar deze verwerkers zich bevinden (mits dat buiten de EU is).[21]

Om te kunnen voldoen aan deze informatieplicht dienen verwerkingsverantwoordelijken van hun cloudproviders inzicht te krijgen in de locaties waar de medische data worden verwerkt. Immers, als dit buiten de EU is, dient dit in de privacyverklaring genoemd te worden. Daarbij dient tevens opgenomen te worden welke waarborgen er zijn getroffen ten aanzien van een zorgvuldige omgang van medische data buiten de EU.[22] Hiermee samenhangt tevens de verplichting van een als verwerker opererende cloudprovider om een register van verwerkingen bij te houden.[23]

Wanneer een ziekenhuis gebruik maakt van een Amerikaanse cloudprovider dient dit in de privacyverklaring genoemd te worden. Wanneer daarbij medische data door het ziekenhuis via die provider in de VS worden verwerkt, dient hiervan eveneens melding gemaakt te worden. Daarbij dient ook benoemd te worden dat, en of, die partij bijvoorbeeld Privacy Shield gecertificeerd is en daarmee voldoet aan het vereiste van passende waarborgen inzake doorgifte van gegevens buiten de EU.

1.2.1.7 Verwerkersovereenkomst

De relatie tussen een verwerkingsverantwoordelijke en verwerker dient geformaliseerd te worden middels een verwerkersovereenkomst[24].[25] De AVG schrijft voor wat er in een verwerkersovereenkomst vastgelegd dient te worden. Voor de opslag van medische data bij cloudproviders zijn er twee specifieke onderwerpen uit de verwerkersovereenkomst die extra aandacht verdienen.

Het eerste onderwerp ziet op het benoemen van de soorten persoonsgegevens in de verwerkersovereenkomst. Aangezien dit een verplicht onderdeel is van een verwerkersovereenkomst[26], dient bij aanvang van de dienstverlening van de cloudprovider duidelijk gemaakt te worden dat er medische data worden verwerkt. Algemene bewoordingen in een verwerkersovereenkomst kunnen uitkomst bieden ("cloudprovider verwerkt alle soorten persoonsgegevens die bij het gebruik van de clouddienst door verwerkingsverantwoordelijke verstrekt worden"). Dit biedt echter onvoldoende houvast ten aanzien van het tweede verplichte, en voor dit rapport relevante, onderwerp in de verwerkersovereenkomst.

Het tweede onderwerp betreft de beveiliging van persoonsgegevens. De te nemen beveiligingsmaatregelen, die afgestemd dienen te zijn op de soorten persoonsgegevens en daarmee samenhangende risico's, dienen in de overeenkomst benoemd te worden. Derhalve dient een cloudprovider voor ingebruikname van de clouddienst op de hoogte te zijn van het feit dat er medische data worden verwerkt.

Aangezien de AVG de inhoud van een verwerkersovereenkomst in grote mate voorschrijft, zijn er diverse standaardmodellen in de omloop. Ten aanzien van verwerking van medische data heeft bijvoorbeeld de vereniging Brancheorganisaties Zorg (BoZ) een standaardmodel ontwikkeld.[27] Het risico bestaat echter dat het niet voor alle zorgpartijen mogelijk is om dit standaardmodel te sluiten met cloudproviders. Zo verwijzen de voorwaarden van diverse

[21] Zie artikel 13 lid 1 sub e en f AVG.

[22] Zie ook paragraaf 1.2.1.10.

[23] Zie artikel 30 lid 2 AVG.

[24] Of andere rechtshandeling, maar gelet op de leesbaarheid wordt de term verwerkersovereenkomst gehanteerd.

[25] Zie artikel 28 lid 3 AVG.

[26] Zie artikel 28 lid 3 AVG.

[27] Zie https://www.brancheorganisatieszorg.nl/nieuws_list/modelverwerkersovereenkomst-voor-de-zorgsector/.

cloudproviders naar hun eigen verwerkersovereenkomst en wijzen tegelijkertijd ieder ander model van de hand.[28]

Naast de twee bovengenoemde onderwerpen, dient iedere verwerkersovereenkomst in ieder geval de volgende onderwerpen te behandelen als het gaat om verplichtingen voor verwerkers ten aanzien van medische data:

- Het waarborgen van vertrouwelijkheid van persoonsgegevens;
- Het treffen van passende beveiligingsmaatregelen;
- Bijstand verlenen aan het gehoor geven aan uitoefenen van rechten van betrokken;
- Bijstand verlenen wanneer de verwerkingsverantwoordelijke een DPIA uit dient te voeren;
- Bijstand verlenen bij eventuele datalekken;
- Het na afloop van de verwerkersovereenkomst, en in overleg met de verwerkingsverantwoordelijke, retourneren en/of vernietigen van persoonsgegevens.

1.2.1.8 Beveiliging

Privacywetgeving kent van oudsher geen specifieke opsomming van te nemen beveiligingsmaatregelen. Dit wordt veroorzaakt door het feit dat de techniek zich in een razendsnel tempo ontwikkelt. Een tempo dat door de wetgevers niet bijgehouden kan worden. Opname van een concrete encryptiestandaard in de AVG kan ervoor zorgen dat de AVG aangepast moet worden als die concrete encryptiestandaard door de technologische ontwikkelingen wordt achterhaald en niet langer veilig is. Daarom ontbreekt een dergelijke concrete opsomming ook in de AVG en UAVG. Gekozen is voor een technologie neutrale formulering waarbij het aan de verwerkingsverantwoordelijke en verwerker is om op ieder moment aan te kunnen tonen dat de getroffen beveiligingsmaatregelen passend zijn.[29] De basisbeginselen van de AVG verwijzen specifiek naar het waarborgen van integriteit en vertrouwelijkheid van de gegevensverwerking.[30] Dit is dan ook de uiteindelijke doelstelling van het treffen van passende beveiligingsmaatregelen. Het beveiligingsbegrip is samen te vatten als het borgen van de beschikbaarheid, integriteit en vertrouwelijkheid. In paragraaf 3.4 wordt daar uitgebreider op ingegaan.

Om de passendheid te beoordelen dient er rekening gehouden te worden met de stand van de techniek, de kosten van de beveiligingsmaatregelen, de aard, omvang en context van verwerkingsdoeleinden en daarbij horende risico's. Gelet op de gevoeligheid van medische data, dient er ten aanzien van die data een strikter pakket aan beveiligingsmaatregelen genomen te zijn dan wanneer het gaat om gewone persoonsgegevens. De AVG noemt enkele voorbeelden van maatregelen[31] die bij kunnen dragen aan een passend beveiligingsniveau:

- Pseudonimisering en versleuteling (encryptie);
- Het permanent garanderen van de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssytemen;
- Het tijdig kunnen herstellen van de beschikbaarheid en toegang tot persoonsgegevens bij incidenten;
- Het hebben van een procedure om de beveiligingsmaatregelen periodiek te testen, beoordelen en evalueren op het gebied van doeltreffendheid.

Bij de beoordeling of een cloudprovider, als verwerker, zorg kan dragen voor passende informatiebeveiliging, dient derhalve altijd in kaart gebracht te worden in hoeverre voldaan kan worden aan bovenstaande punten. Hoewel dit geen maatregelen zijn die de AVG in alle

[28] Zie bijvoorbeeld artikel 16.13 Google Cloud Platform Agreement https://cloud.google.com/terms/.

[29] Zie artikel 32 AVG.

[30] Zie artikel 5 lid 1 sub f AVG.

[31] Zie artikel 32 lid 1 AVG.

gevallen verplicht stelt, zijn dit wel maatregelen die ten aanzien van de verwerking van medische data in ieder geval onderzocht dienen te zijn. Het onderzoeken van deze maatregelen wordt in de AVG verder verplicht gesteld door uitvoering te geven aan het principe van privacy by design[32], het hebben en hanteren van een gegevensbeschermingsbeleid[33] en het uitvoeren van DPIA's[34]. Dit zijn allen instrumenten die ingezet dienen te worden bij het beveiligen van medische data.

1.2.1.8.1 Privacy by design

Waar bij het vaststellen van de mate van beveiliging een gedeelde verantwoordelijkheid bestaat voor de verwerkingsverantwoordelijke en verwerker, kent de AVG daarnaast een specifiek beveiligingsprincipe dat aan de verwerkingsverantwoordelijke toegeschreven wordt. Het principe van privacy by design.[35] Dit principe houdt in dat de verwerkingsverantwoordelijke vóór ingebruikname van nieuwe systemen onderzoek doet naar de mate van beveiliging. Bij het selecteren van een cloudprovider om opslag van medische data te faciliteren, dient de verwerkingsverantwoordelijke bovengenoemde risico's mee te laten wegen bij het bepalen van de mate van beveiliging. De verwerkingsverantwoordelijke dient cloudproviders tevens te stimuleren om hier rekening mee te houden.[36] De AVG benoemt expliciet de verplichting tot het toepassen van het principe van privacy by design bij openbare aanbestedingen. Bij het uitschrijven van de aanbesteding dient het principe in aanmerking genomen te worden. Concreet kan daarbij gedacht worden aan maatregelen zoals het standaard hanteren van meerfactorauthenticatie bij het verkrijgen van toegang tot de clouddienst, encryptie van data at rest en in transit en logging van toegang tot de dienst. Deze maatregelen worden specifieker en concreter uitgewerkt in hoofdstuk 3.

1.2.1.8.2 Gegevensbeschermingsbeleid

Vergelijkbaar met het principe van privacy by design, en het bovengenoemde algemene beveiligingsprincipe uit de AVG, is het ook aan de verwerkingsverantwoordelijke die medische data verwerkt om beleid te hebben waarin is omschreven hoe de beveiliging van deze data wordt gewaarborgd. De Autoriteit Persoonsgegevens heeft dit expliciet benoemd in haar verkennend onderzoek in april van dit jaar.[37] Dit is lijn met de uitleg die de AVG geeft aan de mate waarin het hebben van een gegevensbeschermingsbeleid verplicht is. Expliciet wordt het voorbeeld van risico's ten aanzien van medische data genoemd. Wanneer het risico bestaat op verlies van vertrouwelijkheid van door het beroepsgeheim beschermde persoonsgegevens, waar medische data onder vallen, en wanneer bijzondere persoonsgegevens worden verwerkt, waar medische data eveneens onder vallen[38], is dit een zwaarwegend argument om een gegevensbeschermingsbeleid te hanteren.

Onderdeel van een dergelijk gegevensbeschermingsbeleid dient tevens een uitbestedingsbeleid te zijn. De verwerkingsverantwoordelijke dient zelf beleid te hebben om risico's in kaart te brengen wanneer onderzoek wordt gedaan naar de opslag van medische data bij een cloudprovider.

[32] Zie artikel 25 lid 1 AVG.

[33] Zie artikel 24 AVG.

[34] Zie artikel 35 AVG.

[35] Zie artikel 25 lid 1 AVG.

[36] Zie overweging 78 AVG.

[37] Zie https://autoriteitpersoonsgegevens.nl/nl/nieuws/zes-aanbevelingen-voor-een-privacybeleid.

[38] Zie overweging 75 AVG.

1.2.1.8.3 DPIA

Naast het hebben van een eigen intern gegevensbeschermingsbeleid en het naleven van het principe van privacy by design, dient voorafgaand aan het inschakelen van een cloudprovider voor de opslag van medische data een DPIA uitgevoerd te worden.[39] Hoewel deze verplichting rust bij de verwerkingsverantwoordelijke[40], is de verwerker verplicht om bijstand te verlenen bij het uitvoeren van de DPIA[41]. Deze bijstand kan bestaan uit het delen van informatie, bijvoorbeeld ten aanzien van concrete beveiligingsmaatregelen die een cloudprovider treft, maar ook informatie ten aanzien van opslaglocaties en de (on)mogelijkheden voor buitenlandse autoriteiten om toegang te verschaffen tot de opgeslagen medische data.

Voor het uitvoeren van DPIA's zijn diverse standaardmodellen beschikbaar. Zoals bijvoorbeeld een model ontwikkeld voor de Rijksoverheid[42] en een model ontwikkeld door GGZ Nederland[43].

1.2.1.9 Meldplicht datalekken

Indien beveiliging wordt doorbroken kan het zo zijn dat hiervan melding moet worden gemaakt bij de AP, en in sommige gevallen ook bij patiënten.[44] Deze meldplicht datalekken legt aan de verwerkingsverantwoordelijken de verplichting op om open en transparant te zijn inzake ingrijpende incidenten. Omdat een datalek zich niet altijd bij de verwerkingsverantwoordelijke voor hoeft te doen, kent de AVG ook een expliciete bepaling die ervoor zorgt dat een verwerker melding van datalekken bij de verwerkingsverantwoordelijke doet.[45]

Richtlijnen/beleid toezichthouder (AP)

De vertaling van de eerdergenoemde juridische vereisten naar de Nederlandse informatiebeveiligingspraktijk is te vinden in de richtsnoeren van de AP[46] en, specifiek voor het gebruik van de cloud in de zorg, in een praktijkgids.[47] De richtsnoeren zijn in 2013 opgesteld door de AP, toen nog het CBP. Ondanks dat deze zijn gepubliceerd ver voordat de AVG in werking trad, worden de richtsnoeren nog altijd gebruikt als startpunt voor de uitleg van wat als passende beveiligingsmaatregelen moeten worden gezien.

Verder moet opgemerkt worden dat de praktijkgids gericht is op het gebruik van de cloud voor het verwerken van medische persoonsgegevens zoals onderdeel van een patiëntdossier. Het gaat hier om het dossier zoals bedoeld in de WGBO waarbij het beroepsgeheim geldt. Voorgaande is relevant omdat voor bepaalde systemen andere regels kunnen gelden dan in de praktijkgids opgenomen. In de praktijkgids staat dat toestemming van de betrokkene niet nodig is voor opslag in de cloud. Dit is juist, echter voor opname in een uitwisselingssysteem (dat draait in de cloud) is wel toestemming nodig.

---

[39] Zie artikel 35 lid 3 sub b AVG. Hoewel dit artikel spreekt over grootschalige verwerkingen, heeft de AP aangegeven verwerkingen door onder andere ziekenhuizen en apotheken altijd als grootschalig te zien. Bij zorginstellingen die niet als dusdanig aan te merken zijn heeft de AP een grens van 10.000 patiënten aangehouden. Bij meer dan 10.000 patiënten is er sprake van een grootschalige verwerking.

[40] Zie artikel 35 lid 1 AVG.

[41] Zie artikel 28 lid 3 sub f AVG.

[42] Zie https://www.avghelpdeskzorg.nl/documenten/brochures/2018/10/4/invulformat-rijksmodel-dpia.

[43] Zie https://www.ggznederland.nl/themas/privacywetgeving.

[44] Zie artikel 33 en 34 AVG.

[45] Zie artikel 28 lid 3 sub f AVG.

[46] Richtsnoeren beveiliging van persoonsgegevens, 2013, https://autoriteitpersoonsgegevens.nl/nl/nieuws/cbp-publiceert-richtsnoeren-beveiliging-van-persoonsgegevens.

[47] Praktijkgids patiëntgegevens in de cloud, 2017, https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/praktijkgids_patientgegevens_in_de_cloud_def.pdf

In de richtsnoeren stelt de AP in het algemeen dat beveiligingsmaatregelen passend zijn indien deze in overeenstemming zijn met de stand der techniek en indien de maatregelen proportioneel zijn gezien de te beschermen gegevens. Algemene uitspraken over welke concrete maatregelen passend zijn, kunnen niet worden gedaan. Dat hangt af van de omstandigheden van het geval en is ook afhankelijk van de ontwikkeling van de techniek.
Daarbij stelt de AP dat het treffen van passende beveiligingsmaatregelen in juridische zin, in samenhang moet worden gezien met de praktijk van de informatiebeveiliging en de daarbij gehanteerde ICT-beveiligingsrichtlijnen.

Besluit elektronische gegevensverwerking door zorgaanbieders
Voor het elektronisch verwerken van gegevens in de zorg ten behoeve van de dossiervoering, oftewel voor het gebruik maken van een zorginformatiesysteem of uitwisselingssysteem, zijn expliciete regels vastgesteld. Dit, omdat de huidige regelgeving onvoldoende toereikend was en omdat het maatschappelijk gewenst was aanvullende maatregelen te nemen.[48] De regels zijn neergelegd in de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg en het Besluit elektronische gegevensverwerking door zorgaanbieders. Voor de opslag in de cloud zijn met name de regels uit het Besluit elektronische gegevensverwerking door zorgaanbieders relevant.

In het besluit is onder andere een aantal verplichte beveiligingsmaatregelen opgenomen die gelden voor een zorginformatiesysteem en/of een uitwisselingssysteem. Met een zorginformatiesysteem wordt het interne digitale systeem bedoeld waarmee dossiers van patiënten worden bijgehouden door een zorgaanbieder, denk hier aan een elektronisch patiënten- of cliëntensysteem. Met een elektronisch uitwisselingssysteem wordt een systeem bedoeld waarmee zorgaanbieders patiëntgegevens kunnen uitwisselen. Belangrijk is om hierbij te vermelden dat het gaat om gegevens die na opname in het systeem door middel van “pull-verkeer” uit het systeem gehaald kunnen worden door een andere zorgaanbieder. Het gaat dus niet om push-verkeer, waarbij de ene zorgaanbieder patiëntgegevens naar de andere zorgaanbieder verstuurt, bijvoorbeeld in het kader van een verwijzing.[49]

In het bovengenoemde besluit wordt vastgesteld dat bij het gebruik van een uitwisselingssysteem en een zorginformatiesysteem (bijvoorbeeld een EPD of ECD) moet worden voldaan aan (de laatste versie van) NEN 7510, NEN 7512 en NEN 7513 door de zorgaanbieder. Verder wordt vastgesteld dat de leverancier van een uitwisselingssysteem minstens elke vijf jaar ge-audit moet worden voor NEN 7510 en NEN 7512.

Aanvullend wordt bepaald dat de netwerkverbinding tussen het zorginformatiesysteem en het uitwisselingssysteem beveiligd moet zijn. Er wordt ook aangegeven dat de provider van de netwerkverbinding geautoriseerd moet zijn op basis van overeenkomstig NEN 7512 vastgestelde criteria.

Verder wordt er expliciet bepaald dat er moet worden voldaan aan de laatste stand van de wetenschap en techniek bij de beveiliging van elektronische gegevensverwerking in de zorg. In de uitleg bij het besluit wordt nog gesproken over NEN 7521, deze is nog in ontwikkeling en daarom nog niet verplicht.

In het kader van de controleerbaarheid van de integriteit van de medische gegevens werd onlangs nog de volgende bewaartermijn vastgesteld. Voor de logging van een zorginformatiesysteem en een uitwisselingssysteem geldt dat deze in ieder geval vijf jaar bewaard moet worden. Het gaat hier om de logging conform (NEN 7510 en) NEN 7513.[50]

[48] Kamerstukken II 2010/11, 27529, 82.

[49] Artikel 1 onder j van de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg.

[50] Artikel 5 lid 2 van het Besluit elektronische gegevensverwerking door zorgaanbieders. Zie tevens: https://zoek.officielebekendmakingen.nl/stcrt-2019-38007.html.

In het besluit wordt niet expliciet ingegaan op de eisen die gelden voor de cloudprovider. De cloudprovider voor opslag van medische data is meestal een toeleverancier van de leverancier van het uitwisselingssysteem of zorginformatiesysteem. Er is hier sprake van een keten. Wel moet de zorgaanbieder bij het gebruik van een zorginformatiesysteem of uitwisselingssysteem kunnen voldoen aan bovengenoemde normen. In paragraaf 3.5 wordt verder ingegaan op wat dit concreet betekent voor de eisen ten aanzien van de beveiliging die geleverd moet worden door de cloudprovider.

Het elektronisch uitwisselen van medische data zal komende jaren verplicht gesteld worden. De minister voor Medische Zorg en Sport wil digitaal het nieuwe normaal maken voor gegevensuitwisseling in de zorg. De reden hiervoor luidt als volgt:

> *"Goede en tijdige informatie-uitwisseling met de patiënt en tussen zorgaanbieders onderling is nodig voor goede kwaliteit van zorg".*[51]

De minister doelt hierbij op uitwisseling tussen zorgaanbieders maar dan bij voorkeur op grond van een bestaande behandelrelatie tussen patiënt en hulpverlener waarbij veronderstelde toestemming voldoende is.

De minister wil de ICT-leveranciers die het elektronisch uitwisselen gaan faciliteren direct binden aan gedetailleerde technische eisen. Hij wil middels nieuwe regelgeving bepaalde certificering verplicht maken. Ten behoeve van deze certificering wordt nu met het Nederlands Normalisatie instituut (NEN) gesproken over de ontwikkeling van een standaard. Buiten bovengenoemde reeds verplichte NEN-standaarden, zullen er dus nieuwe standaarden ontwikkeld worden en wettelijk verplicht worden gesteld.

1.2.1.10 Export buiten de EU algemeen

Zoals omschreven in paragraaf 1.2.1.1 kent de AVG een territoriaal en materieel toepassingsgebied. Verwerking van persoonsgegevens binnen dat gebied valt onder de bescherming van de AVG. Om de bescherming van persoonsgegevens ook buiten de EU te kunnen waarborgen, kent de AVG een regime voor internationale doorgiften.[52] Wanneer een verwerkingsverantwoordelijke of verwerker persoonsgegevens buiten de EU brengt, dient, naast bovengenoemde voorwaarden, voldaan te zijn aan aanvullende voorwaarden. De reden achter deze voorwaarden is terug te herleiden tot het feit dat de AVG gezien kan worden als zeer strenge wetgeving op het gebied van bescherming van persoonsgegevens. Vanuit dat gedachtegoed is het niet wenselijk dat afgedaan wordt aan deze strenge bescherming wanneer persoonsgegevens buiten de EU gebracht worden.

Er zijn diverse juridische mogelijkheden om ook buiten de EU een passend beveiligingsniveau te waarborgen:

- Het beschermingsniveau van een land of organisatie is als adequaat aangemerkt door de Europese Commissie;
- Er zijn passende waarborgen genomen, zoals bijvoorbeeld het sluiten van een modelovereenkomst of het naleven van goedgekeurde gedragscodes of certificeringsmechanismes;
- De doorgifte is gereguleerd in bindende bedrijfsvoorschriften;
- Er is voldaan aan één van de voorwaarden uit artikel 49 AVG voor specifieke situaties, waaronder toestemming voor doorgifte.

[51] https://www.rijksoverheid.nl/documenten/kamerstukken/2019/07/12/kamerbrief-over-derde-brief-elektronische-gegevensuitwisseling-in-de-zorg.

[52] Zie artikel 44 en verder AVG.

Opgemerkt dient te worden dat doorgifte van persoonsgegevens op grond van een gerechtelijk bevel uit een derde land, verboden is.[53] Dit artikel is een antwoord vanuit Europa op een rechtszaak[54] die tijdens het opstellen van de AVG speelde. Op basis van Amerikaanse wetgeving werd de Amerikaanse entiteit van Microsoft verplicht om bij haar Europese dochter in Ierland persoonsgegevens op te halen van een gebruiker van Microsoft-diensten.

Uitzondering op het verbod zijn internationale overeenkomsten tussen het verzoekende derde land en een EU-lidstaat, die de doorgifte toestaan. Zo geldt er tussen de VS en Nederland al sinds 1981 een verdrag waarin dit is vastgelegd[55] en is er sinds eind 2001 een verdrag van kracht tussen 50 landen waarin afspraken zijn gemaakt over de bestrijding van strafbare feiten verbonden met elektronische netwerken.[56] Daarin is specifiek een bepaling opgenomen die cloudproviders verplicht stelt om informatie over haar gebruikers af te staan als daartoe een gerechtelijk bevel is uitgevaardigd.[57]

Met dit verbod, en het daarbij horende systeem van internationale afspraken en verdragen om het verbod voor legitieme doeleinden te doorbreken, wordt beoogd bescherming te bieden tegen derde landen die wetten stellen om de bescherming van persoonsgegevens te doorbreken. In de praktijk kan dit tot spanningen leiden wanneer op een cloudprovider toepasselijke wetgeving deze verplicht om gegevens af te staan, maar de AVG dit verbiedt.

Bovenstaande spanning ontstaat wanneer een cloudprovider is gevestigd, en medische data van Nederlandse patiënten opslaat, in een land waarmee Nederland of de EU geen internationale overeenkomst heeft die ziet op de uitwisseling van data. Wanneer de cloudprovider op basis van nationale wetgeving van dat land verplicht is om medische data van een Nederlandse patiënt te overhandigen aan het vestigingsland, houdt meewerken aan een dergelijk verzoek een schending van de AVG in.

1.2.1.11 Adequaatheidsbesluit

De Europese Commissie heeft voor een aantal landen een adequaatheidsbesluit genomen.[58] Dat wil zeggen dat de volgende landen een adequaat beschermingsniveau bieden als het gaat om de zorgvuldige omgang met persoonsgegevens: Andorra, Argentinië, Canada (voor commerciële organisaties), Faeröer Eilanden, Guernsey, Isle of Man, Israël, Japan, Jersey, Nieuw-Zeeland, Zwitserland, Uruguay en de VS (Privacy Shield).

Het Privacy Shield is een specifieke adequaatheidsbeoordeling[59] van de Europese Commissie voor Amerikaanse organisaties. Deze adequaatheidsbeoordeling bestaat uit een overeenkomst tussen de EU en VS met als doel het borgen van afdoende bescherming van persoonsgegevens door Amerikaanse partijen. Door middel van een certificeringsmechanisme kunnen Amerikaanse organisaties aangeven zorgvuldig om te gaan met persoonsgegevens. Het Privacy Shield is de opvolger van de Safe Harbor regeling. Deze regeling had hetzelfde doel, maar is in 2015 ongeldig verklaard.[60] Reden hiervoor was de schending van afspraken door gecertificeerde organisaties toen bleek dat zij op grote schaal persoonsgegevens aan Amerikaanse autoriteiten (zoals de NSA en FBI) verstrekten. Hoewel

[53] Zie artikel 48 AVG.

[54] Zie onder andere Case 14-2985, Document 286-1, 07/14/2016, 1815361, Microsoft vs. United States.

[55] Zie Verdrag tussen het Koninkrijk der Nederlanden en de Verenigde Staten van Amerika aangaande wederzijdse rechtshulp in strafzaken.

[56] Zie Verdrag inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken.

[57] Zie artikel 18 Verdrag inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken.

[58] Zie https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en. Met daarbij de kanttekening dat deze besluiten niet van toepassing zijn op opsporing en handhaving door overheden.

[59] Zie Uitvoeringsverordening (EU) 2016/1250.

[60] Zie HvJ EU 6 oktober 2015, C-362/14.

het Privacy Shield momenteel een juridisch geldig instrument is om persoonsgegevens buiten de EU te brengen, is het de vraag of dit instrument stand zal houden in een rechtszaak waar ook deze regeling ter discussie is gesteld. De zaak tegen Privacy Shield wordt gevoerd door dezelfde persoon (Max Schrems) die eerder ook de zaak aanspande waardoor de voorganger Safe Harbor ongeldig werd verklaard.[61]

Het Privacy Shield wordt jaarlijks geëvalueerd door de Europese Commissie.[62] Tijdens de laatste beoordeling, in december 2018, is vastgesteld dat het Privacy Shield in juridisch opzicht nog steeds gezien wordt als een passend mechanisme om persoonsgegevens in de VS te (laten) verwerken. Tijdens deze, inmiddels tweede, evaluatie is specifiek aandacht besteed aan de toegang tot persoonsgegevens door Amerikaanse overheidsdiensten.[63] De Europese Commissie heeft vastgesteld dat de aanpassing aan de FISA, begin 2018, geen nadelige gevolgen heeft gehad voor het Privacy Shield.

De argumentatie van Schrems is daarentegen dat de bestaande Amerikaanse wetgeving waaronder in het verleden al geheime programma's voor massasurveillance zoals PRISM en Upstream zijn geautoriseerd (artikel 702 FISA), nog steeds massasurveillance toestaat die zich niet verdraagt met het Europese privacyrecht. De Ierse High Court concludeerde voor de verwijzing van de zaak naar het Hof van Justitie van de EU dat er inderdaad massale verwerking van gegevens door Amerikaanse autoriteiten plaatsvindt. Een ander bezwaar van Schrems is dat onvoldoende rechtsmiddelen openstaan tegen inzage van data door Amerikaanse autoriteiten. Er is voor dit doeleinde weliswaar een ombudspersoon in het leven geroepen onder Privacy Shield, maar volgens Schrems is deze niet voldoende onafhankelijk om te voldoen aan hetgeen is vereist onder artikel 47 van het Handvest van de grondrechten van de EU. De Ierse privacytoezichthouder is dat met Schrems eens.[64]

Bij de tweede evaluatie van Privacy Shield is ook de CLOUD Act besproken. Onder de CLOUD Act kunnen Amerikaanse autoriteiten data vorderen van cloudproviders die in de VS zijn gevestigd, ook als het gaat om data die niet in de VS zijn opgeslagen. Zelfs als een zorgverlener een overeenkomst aangaat met de vestiging van een cloudprovider in de EU en als opslaglocatie een land of gebied in de EU kiest, bestaat daardoor de mogelijkheid dat een Amerikaanse autoriteit via de vestiging in de VS data verkrijgt. Daar kan zich ook medische data van Nederlandse patiënten tussen bevinden. De CLOUD Act biedt ook de mogelijkheid dat andere overheden met de Amerikaanse overheid een overeenkomst sluiten waardoor autoriteiten van deze andere overheden rechtstreeks data kunnen vorderen van een Amerikaanse cloudprovider.[65] Aan dergelijke overeenkomsten worden door de CLOUD Act echter voorwaarden gesteld die voor de Europese Commissie afdoende zijn om te stellen dat de CLOUD Act geen bedreiging vormt voor het Privacy Shield.

Ten aanzien van het gebruik van in de VS gevestigde cloudproviders bij de opslag van medische data, kan derhalve gesteld worden dat in ieder geval voldaan wordt aan artikel 45 AVG wanneer de cloudprovider is aangesloten bij het Privacy Shield. Daarmee staat echter nog niet vast dat de medische data ook volledig veilig en in lijn met de AVG opgeslagen kan worden. Daartoe dient tevens voldaan te zijn aan de andere verplichtingen uit de AVG, zoals hierboven omschreven. Denk daarbij onder andere aan het sluiten van een verwerkersovereenkomst, het verschaffen van transparantie richting betrokkenen en het zorgen voor adequate beveiliging van de medische data.

---

[61] Zie https://noyb.eu/cjeu-case/?lang=nl.

[62] Zie https://europa.eu/rapid/press-release_IP-18-6818_nl.htm.

[63] https://ec.europa.eu/info/sites/info/files/report_on_the_second_annual_review_of_the_eu-us_privacy_shield_2018.pdf en https://ec.europa.eu/info/sites/info/files/staff_working_document_-_second_annual_review.pdf

[64] The High Court, 12 april 2018, No. 4809, http://www.europe-v-facebook.org/sh2/ref.pdf

[65] § 2713(5) CLOUD Act: "DISCLOSURE TO QUALIFYING FOREIGN GOVERNMENT", https://www.congress.gov/bill/115th-congress/senate-bill/2383/text.

1.2.1.12 Modelcontract

Waar het Privacy Shield uitsluitend geldt voor gegevensopslag in de VS, bieden de modelcontracten[66] een breder toepassingsbereik. Een breder bereik, aangezien deze modelcontracten niet alleen toepasselijk zijn op export van gegevens naar de VS, maar naar ieder land dat buiten de EU valt. De modelcontracten kunnen gezien worden als instrument om in een land buiten de EU toch passende waarborgen te treffen voor de bescherming van persoonsgegevens. De Europese Commissie heeft drie varianten van de modelcontracten goedgekeurd als exportmechanisme. Twee versies waarbij de verwerkingsverantwoordelijke zich in de EU bevindt en gegevens doorgeeft aan een verwerkingsverantwoordelijke buiten de EU. De derde versie, voor dit rapport het meest relevant, is een versie waarbij de verwerkingsverantwoordelijke zich in de EU bevindt en gegevens deelt met een verwerker buiten de EU.

Het modelcontract kan gezien worden als een speciale vorm van een verwerkersovereenkomst. Door ondertekening van het modelcontract verklaart de verwerker die de data importeert onder andere:

- Dat er geen nationale wetgeving is die de verwerker verhindert om aan zijn verplichtingen te voldoen onder het modelcontract;
- Dat de verwerker de persoonsgegevens adequaat zal beveiligen;
- Dat de verwerker de verwerkingsverantwoordelijke informeert over, en toestemming vraagt voor, het inschakelen van subverwerkers.

Het gebruik van het modelcontract kent echter verschillende risico's. Ten eerste bestaat er geen door de Europese Commissie goedgekeurde variant van het modelcontract voor de situatie waarin een verwerker zich in de EU bevindt en gegevens deelt met een (sub)verwerker buiten de EU. In de situatie waarin een ziekenhuis verwerkingsverantwoordelijke is en gegevens opgeslagen worden bij een niet-EU cloudprovider, is dit geen probleem. Het modelcontract kan echter niet worden gebruikt als juridische oplossing wanneer een ziekenhuis de opslag van medische data uitbesteedt aan een EU cloudprovider, die daarbij de hulp inschakelt van een dienstverlener die buiten de EU is gevestigd. In dat geval is er sprake van een situatie waarin een in de EU gevestigde verwerker persoonsgegevens laat verwerken door een niet in de EU gevestigde subverwerker. In dergelijke situaties dient er een ander juridisch instrument gezocht te worden om de export van medische data te legitimeren. Hoewel het vinden van een ander instrument niet onmogelijk is, kan bovengenoemde situatie wel een risico vormen wanneer betrokken partijen de modelcontracten niet op de juiste manier inzetten en daarmee niet voldoen aan de AVG.

Ten tweede wordt de effectiviteit van het modelcontract momenteel in twijfel getrokken door Max Schrems. Hoewel Europese privacytoezichthouders in het modelcontract de mogelijkheid wordt geboden om bepaalde verwerkingen te verbieden wanneer adequate omgang met persoonsgegevens niet gegarandeerd kan worden[67], is Max Schrems van mening dat de toezichthouders dit mechanisme niet daadwerkelijk gebruiken. En daarmee, zo vindt Schrems, wordt de effectiviteit van de modelcontracten ondermijnd. Door het Ierse Hooggerechtshof zijn naar aanleiding van de mening van Schrems diverse vragen aan het Hof van Justitie van de EU gesteld.[68] De hoorzitting heeft op 9 juli 2019 plaatsgevonden, maar antwoorden op de vragen worden niet eerder dan eind 2019 of begin 2020 verwacht. In potentie zou het Hof van Justitie van de EU de geldigheid van de modelcontracten in kunnen trekken. Hoewel die conclusie op dit moment allerminst zeker is, vergt het gebruik van modelcontracten wel extra aandacht.

[66] Zie artikel 46 lid 2 sub c AVG.

[67] Zie artikel 4 lid 1 van het modelcontract tussen een verwerkingsverantwoordelijke en verwerker.

[68] The High Court, 12 april 2018, No. 4809, http://www.europe-v-facebook.org/sh2/ref.pdf.

Ten derde vormt het gebruik van de modelcontracten een juridisch risico aangezien de huidige modellen dateren van vóór de AVG. Dit tast de geldigheid van de huidige contracten niet aan, maar zorgt wel voor een noodzaak tot extra alertheid bij de gebruikers. Wanneer de huidige modelcontracten worden herzien en in lijn met de AVG worden gebracht, zullen gebruikers hun eerder gesloten contracten moeten aanpassen. Momenteel wordt vanuit Europa gewerkt aan het vernieuwen van de modelcontracten.[69] Het is echter nog niet te zeggen wanneer deze vernieuwing volledig is doorgevoerd.

1.2.1.13 Gedragscode

De AVG voorziet in de mogelijkheid dat gedragscodes en certificeringsmechanismes worden gecreëerd om naleving van de AVG te faciliteren en aan te tonen. Dergelijke mechanismes zijn op dit moment van schrijven nog in ontwikkeling en nog niet goedgekeurd door privacytoezichthouders. Specifiek voor clouddiensten zijn al diverse gedragscodes[70] ontwikkeld. In ieder geval één daarvan is al aangemeld bij de (Belgische) privacytoezichthouder ter goedkeuring. De beslissing op deze aanvraag moet op moment van schrijven echter nog worden genomen. Belangrijk om op te merken is in dit verband wel dat de gedragscode niet specifiek ziet op de opslag van medische data in de cloud, al zou dit in de toekomst wellicht wel als een specifieke module toegevoegd kunnen worden. Certificering onder een dergelijke gedragscode zou onder andere als voordeel kunnen hebben dat de onafhankelijkheid van het certificeringsorgaan (beter) is gewaarborgd, de scope van de certificering specifiek is afgestemd op de AVG en er wordt voorzien in controles op momenten die niet vooraf bekend zijn voor de gecontroleerde partij. Er wordt ook al gewerkt aan manieren om te proberen in meer doorlopende vormen van controle te voorzien.[71] Het is echter nog niet zeker hoe ver dit ideaal in de praktijk werkelijk benaderd kan worden.

1.2.1.14 Bindende bedrijfsvoorschriften

Een andere mogelijkheid tot het realiseren van een stelsel van passende waarborgen wordt geboden door bindende bedrijfsvoorschriften. Dit zijn beleidsregels die binnen een concern of groep van ondernemingen gelden. In deze beleidsregels worden de randvoorwaarden vastgelegd waarbinnen persoonsgegevens van de ene entiteit van het concern, naar een andere entiteit gestuurd mogen worden. Ook wanneer de ene entiteit zich binnen de EU bevindt en de andere buiten de EU. Alvorens bindende bedrijfsvoorschriften echter kunnen dienen als instrument om internationale gegevensverkeer te legitimeren, dienen de voorschriften door de bevoegde privacytoezichthouder goedgekeurd te worden.[72]

Ten aanzien van de opslag van medische data bij cloudproviders kunnen bindende bedrijfsvoorschriften uitkomst bieden bij het creëren van passende waarborgen ter bescherming van persoonsgegevens. Het is echter aan de betreffende cloudprovider om dergelijke bedrijfsvoorschriften op te stellen, wanneer de provider zowel vestigingen binnen als buiten de EU heeft en medische data tevens deelt tussen de vestigingen.

1.2.1.15 Specifieke afwijkingen

Wanneer een adequaatheidsbesluit, modelcontracten en bindende bedrijfsvoorschriften niet aanwezig zijn, biedt de AVG gronden die export van persoonsgegevens buiten de EU rechtvaardigen voor specifieke situaties.[73] Geen van deze specifieke situaties zal hoogstwaarschijnlijk van toepassing kunnen zijn op de stelselmatige opslag van medische data bij cloudproviders buiten de EU.

---

[69] Zie https://europa.eu/rapid/press-release_SPEECH-19-2999_en.htm.

[70] Zie bijvoorbeeld https://eucoc.cloud, https://cispe.cloud/code-of-conduct/.

[71] Zie bijvoorbeeld https://www.sec-cert.eu/.

[72] Zie artikel 57 lid 1 sub s AVG.

[73] Zie artikel 49 AVG.

1.2.1.16 Toezicht en handhaving

Naleving van de AVG wordt uitgevoerd door nationale privacytoezichthouders. In Nederland is dit de Autoriteit Persoonsgegevens. Op naleving van de AVG vindt toezicht en handhaving plaats.[74] Hoewel handhaving veelal pas het nieuws haalt wanneer dit bestaat uit het opleggen van boetes[75], zijn de bevoegdheden van toezichthouders omvangrijker. Deze bevoegdheden lopen uiteen van het uitvragen van informatie, het uitdelen van waarschuwingen tot het verbieden van bepaalde vormen van verwerkingen.[76]

Het grensoverschrijdende karakter van steeds meer verwerkingen heeft in de AVG geleid tot een 'one-stop-shop' mechanisme. Indien een cloudprovider in meerdere landen binnen de EU is gevestigd, wordt er één toezichthouder aangesteld die toeziet op de verwerkingen. Hoofdregel is dat de nationale toezichthouder van het land waar de hoofdvestiging van de cloudprovider zich bevindt, bevoegd is om toezichthoudend en handhavend op te treden.[77] Voor cloudproviders die in het geheel niet in de EU zijn gevestigd geldt een ander systeem. Wanneer zij zich wel op de Europese markt richten[78] is de AVG op hen van toepassing en zijn zij verplicht om een vertegenwoordiger in de EU aan te wijzen.[79] De toezichthouder van het vestigingsland van die vertegenwoordiger is bevoegd om toezichthoudend en handhavend op te treden. Indien de AVG van toepassing is op een verwerking, kent de AVG ook een sluitend systeem om een competente toezichthouder aan te wijzen.

Het is echter wel de vraag in hoeverre het wenselijk is om medische data op te slaan bij een cloudprovider zonder vestiging in de EU. Hoewel de AVG een sluitend systeem kent voor toezicht en handhaving, kan de uitvoering daarvan in de praktijk moeilijk blijken. Een privacytoezichthouder zou bijvoorbeeld moeite kunnen hebben betaling van een opgelegde boete af te dwingen als er geen substantiële bedrijfsmiddelen op EU-grondgebied bestaan.

1.3 Regels waardoor de vertrouwelijkheid kan worden beperkt

Het recht op bescherming van de persoonlijke levenssfeer is niet onbeperkt. Er kunnen zich situaties voordoen waarin, na een zorgvuldige belangenafweging, een ander recht prevaleert. Hierbij valt bijvoorbeeld te denken aan opsporing van strafbare feiten.

Wetboek van Strafvordering

In Nederland kunnen opsporingsambtenaren (zoals politieagenten) gegevens vorderen van aanbieders van communicatiediensten.[80] Cloudproviders vallen hieronder.[81] Hierbij spelen wel diverse waarborgen en voorwaarden waaraan moet zijn voldaan. In het algemeen geldt hoe groter de inbreuk op privacy, hoe zwaarder de waarborgen en voorwaarden.
Zowel bij het opstellen van de bevoegdheden door de wetgever als bij het uitoefenen van de bevoegdheden door de politie, moeten fundamentele rechten worden gerespecteerd. Het recht op privacy wordt bijvoorbeeld beschermd door artikel 10 Gw, artikel 8 EVRM en artikelen 7 en 8 van het Handvest van de Grondrechten van de EU.

---

[74] Zie bijvoorbeeld 'Haga beboet voor onvoldoende interne beveiliging patiëntendossiers' https://autoriteitpersoonsgegevens.nl/nl/nieuws/haga-beboet-voor-onvoldoende-interne-beveiliging-pati%C3%ABntendossiers.

[75] Zie bijvoorbeeld https://edpb.europa.eu/news/national-news_en.

[76] Zie artikel 58 AVG.

[77] Zie artikel 56 lid 1 AVG.

[78] Zie paragraaf 1.2.1.2.

[79] Zie artikel 27 AVG.

[80] 126n, 126na, 126nd, 126ng Sv.

[81] 138g Sv. Onder aanbieder van een communicatiedienst wordt verstaan de natuurlijke persoon of rechtspersoon die in de uitoefening van een beroep of bedrijf aan de gebruikers van zijn dienst de mogelijkheid biedt te communiceren met behulp van een geautomatiseerd werk, of gegevens verwerkt of opslaat ten behoeve van een zodanige dienst of de gebruikers van die dienst.

Daaruit vloeien de eisen voort waaraan voldaan moet worden bij het vaststellen en uitoefenen van opsporingsbevoegdheden. Dergelijk ingrijpen moet:

- Een wettelijke basis hebben;
- Een legitiem doel dienen dat expliciet bij wet is omschreven, en
- Noodzakelijk zijn in een democratische samenleving (het ingrijpen moet proportioneel zijn aan het doel en mag niet verder gaan dan een ander alternatief waarmee het doel ook bereikt kan worden).

Artikel 8 EVRM werkt rechtstreeks, zodat iedere burger er een beroep op kan doen bij de rechter. Als een zaak bij de nationale rechter is uitgeprocedeerd (dat wil zeggen: tot aan de hoogste nationale rechter, zoals de Hoge Raad), kan ook een zaak worden aangespannen bij het Europees Hof voor de Rechten van de Mens (EHRM) in Straatsburg. Dit stelsel geeft een belangrijke en wezenlijke bescherming aan burgers tegen overmatige en ongerechtvaardigde inbreuken op hun privacy. Ook in verband met de mogelijkheid van inzage door autoriteiten in medische data van burgers is deze bescherming van groot belang. Dit is ook terug te zien in het stelsel van bevoegdheden die (in het Wetboek van Strafvordering) zijn toegekend aan opsporingsambtenaren.

Hoe meer impact een opsporingsbevoegdheid heeft op de privacy van betrokkenen, hoe zwaarder de eisen die daaraan worden gesteld. Voor ernstigere delicten (misdrijven) waar hogere straffen voor kunnen worden opgelegd, kunnen zwaardere opsporingsbevoegdheden worden ingezet, die een grotere impact kunnen hebben op de privacy van de betrokkene (vaak de verdachte, maar er kunnen ook andere betrokkenen zijn). Bevoegdheden die een kleinere impact hebben op de privacy, kunnen bij minder ernstige delicten worden ingezet.

Bevoegdheden met een grotere impact worden veelal voorbehouden aan hogere opsporingsambtenaren (zoals de officier van justitie) en mogen pas worden ingezet na voorafgaande toetsing door de rechter(commissaris). Het type (persoons)gegevens dat voor opsporing kan worden gevorderd is van belang voor de impact en de vereisten waaraan moet zijn voldaan om de bevoegdheid uit te kunnen oefenen.

Artikel 126n Sv geeft bijvoorbeeld een brede bevoegdheid om gegevens te vorderen van wie ook maar gegevens heeft, maar die bevoegdheid strekt zich niet uit tot bijzondere persoonsgegevens, zoals medische data.

WIV

De Wet op de inlichtingen en veiligheidsdiensten is een Nederlandse wet die, kortweg, omschrijft wat de bevoegdheden zijn van de AIVD (en MIVD) op het gebied van nationale veiligheid. De WIV biedt geen grondslag voor deze diensten om op grote schaal medische data te verzamelen. Meer specifiek verbiedt de wet het verwerken van medische data in beginsel expliciet. Slechts wanneer de verwerking onvermijdelijk is, is dit onder strikte voorwaarden toegestaan en na toestemming van de minister van Binnenlandse zaken en Koninkrijksrelaties en de onafhankelijke Toetsingscommissie Inzet Bevoegdheden (TIB).[82]

Verschoningsrecht

Artsen en andere zorgverleners hebben in verband met hun medische beroepsgeheim een verschoningsrecht.[83] Dat wil zeggen dat zij niet hoeven te voldoen aan vorderingen om medische data te verstrekken. Partijen die diensten verlenen aan verschoningsgerechtigde hulpverleners en daarbij medische persoonsgegevens opslaan of daar toegang toe hebben, hebben een afgeleid verschoningsrecht. Cloudproviders hebben een afgeleid verschoningsrecht wanneer zij medische data opslaan voor of namens verschoningsgerechtigde zorgverleners.

[82] Zie artikel 19 lid 3 en 4 WIV.

[83] Zie artikel 218 Sv.

Wanneer de cloudprovider weet dat een vordering tot het verstrekken van (toegang tot) gegevens betrekking heeft op medische data, kan (en hoort) de cloudprovider te weigeren om aan de vordering te voldoen op grond van een afgeleid verschoningsrecht.[84] De cloudprovider slaat de medische persoonsgegevens immers als (sub)verwerker op ten behoeve van of namens een verschoningsgerechtigde verwerkingsverantwoordelijke. Van de cloudprovider kan en mag niet worden verwacht dat deze zelfstandig kan besluiten of het verschoningsrecht, dat niet absoluut is, in het betreffende geval buiten toepassing moet blijven of niet.

Wanneer een cloudprovider een vordering ontvangt tot het verstrekken van (toegang tot) medische data, zal de cloudprovider (als afgeleid verschoningsgerechtigde) de vrager moeten doorverwijzen naar diens klant.

[84] Zie bijvoorbeeld HR 12-02-2013, ECLI:NL:HR:2013:BV3004.

2. Juridische risico's ten aanzien van bescherming van medische data bij cloudproviders

2.1 Inleiding en scope

Nu bovenstaand juridisch kader is geschetst, is duidelijk waarmee rekening gehouden dient te worden wanneer er medische data van Nederlandse patiënten op worden geslagen bij een clouddienst. Nu dit kader helder is, wordt ingegaan op de volgende deelvraag:

> *Welke risico's bestaan er ten aanzien van de waarborgen voor de privacy in deze[85] situaties bij het gebruik van cloudproviders met een basis in Nederland, de Europese Unie, de Verenigde Staten en overige landen? Zijn er wezenlijke verschillen tussen lokale Nederlandse cloudproviders en providers uit de andere categorieën landen?*

Om tot een antwoord op deze vraag te komen wordt hieronder allereerst ingegaan op risico's die voor alle cloudproviders gelden. Ongeacht het land van vestiging. Daarna zal specifieker gekeken worden naar de verschillen tussen cloudproviders met een vestiging in Nederland en de EU, en daarbuiten.

Al in 2012 constateerde de voormalig artikel 29 werkgroep (thans de EDPB) dat het gebruik van clouddiensten risico's met zich meebrengt ten aanzien van adequate gegevensbescherming.[86] Toen was de conclusie dat het gebruik kon zorgen voor gebrek aan controle en transparantie. Hieronder wordt onderzocht in hoeverre deze bevindingen nog steeds relevant zijn.

2.2 Juridische risico's algemeen

Niet naleving wet- en regelgeving door cloudprovider

Uitgaande van een goedwerkend stelsel van wet- en regelgeving om de medische data van Nederlandse patiënten te beschermen, is een eerste risico ten aanzien van deze bescherming het niet naleven van een cloudprovider van deze toepasselijke wet- en regelgeving. Deze niet naleving kan zich in uiteenlopende verschijningsvormen voordoen. Zo kan een cloudprovider niet, of niet voldoende, meewerken aan de wettelijke verplichte DPIA. Daardoor kan er geen volledige inschatting gemaakt worden van de aanwezige risico's en kan er op basis van een onvolledig beeld besloten kan worden om medische data bij een cloudprovider onder te gaan brengen.

Meer nog dan in de precontractuele fase, doen de risico's zich uiteraard voor wanneer de medische data eenmaal is ondergebracht bij een cloudprovider en deze zich vervolgens niet aan de geldende wet- en regelgeving houdt. Denk hierbij aan het niet, of niet tijdig, melden van datalekken, het niet continu monitoren en verbeteren van beveiliging of geen bijstand verlenen ten behoeve van de uitvoering van rechten van betrokkenen. Niet-naleving door de cloudprovider kan leiden tot schade of andere nadelige gevolgen voor betrokkenen. Als de medische data bijvoorbeeld nodig is voor een juiste en tijdige toekenning van een behandeling, kan onbeschikbaarheid of onjuistheid van de data zelfs leiden tot lichamelijk en/of psychisch letsel. Voor de zorgverlener kan niet-naleving door de cloudprovider leiden tot reputatieschade, een waarschuwing van een toezichthouder of een boete.

Hoewel er zowel civielrechtelijk, bijvoorbeeld wegens niet nakomen van de verwerkersovereenkomst, als bestuursrechtelijk, bijvoorbeeld door handhavend optreden van de AP, opgetreden kan worden tegen een schending van wet- en regelgeving door een

[85] Zie paragraaf 1.1.

[86] Zie Advies 05/2012 over cloud computing, 1 juli 2012, p. 2.

cloudprovider, is het kwaad daarmee al geschiedt. De bescherming van privacy van Nederlandse patiënten is daarmee immers al doorbroken.
De cloudprovider staat uiteraard wel bloot aan sterke prikkels om diens verplichtingen wel zo goed mogelijk na te leven, omdat de cloudprovider door niet-naleving zelf ook reputatieschade, een waarschuwing of boete van de toezichthouder en civiele aansprakelijkheid naar de afnemer en/of de betrokkenen op kan lopen.

Verder dient te worden opgemerkt dat het niet naleven van wet- en regelgeving ook als risico in acht genomen dient te worden bij het opslaan van medische data van Nederlandse patiënten bij een on premise oplossing. Denk aan de situatie waarbij een onbevoegde toegang krijgt tot deze data. Zo kan een situatie zoals zich heeft voorgedaan in het HagaZiekenhuis[87] zowel gebeuren bij een cloudprovider als bij een on-premise oplossing.

Aan de ene kant betekent het inschakelen van een cloudprovider per definitie een extra partij die potentieel de verplichtingen inzake de verwerking en bescherming van medische data niet na zou kunnen leven, en daarmee een extra risico, maar aan de andere kant zijn cloudproviders juist gespecialiseerd in het aanbieden van zo veilig en betrouwbaar mogelijke systemen voor dataverwerking. Ook certificeringsmechanismes zoals besproken in 3.5 kunnen helpen het risico op niet-naleving (aanzienlijk) terug te dringen.

Gebrek aan transparantie
Hoewel dit vanzelfsprekend ook een niet naleving van wet- en regelgeving is, verdient een dreigend gebrek aan transparantie extra aandacht. Al in 2012 constateerde de artikel 29 werkgroep risico's[88]:

- Onduidelijkheid over de volledig keten waarin de verwerking plaatsvindt. De AVG heeft hier inmiddels echter verandering in gebracht. De AVG verplicht iedere, als verwerker opererende cloudprovider, om volledig transparant te zijn over de keten;[89]
- Het verspreiden van persoonsgegevens op verschillende geografische locaties binnen de EU;
- Het verspreiden van persoonsgegevens op verschillende geografische locaties buiten de EU, waarbij de mogelijkheid bestaat dat daar locaties tussen zitten die geen adequaat beschermingsniveau bieden.

Ondanks nieuwe verplichtingen uit de AVG, zijn deze risico's nu nog steeds reëel. Een afnemer van clouddiensten dient op ieder moment inzichtelijk te hebben waar en hoe de medische data op is geslagen. Deze informatie dient zowel in de eigen privacyverklaring terug te vinden te zijn, als wanneer betrokkenen een verzoek tot inzage of bijvoorbeeld verwijdering van hun gegevens indienen. Wanneer cloudproviders niet volledig zijn in hun informatievoorziening richting afnemers, levert dit direct risico op voor de afnemer ten aanzien van zijn verplichtingen onder de AVG.

Gebrek aan controle
Inherent aan het uitbesteden van opslagdiensten aan een cloudprovider is het weggeven van exclusieve controle over de persoonsgegevens. En meer specifiek de medische data van Nederlandse patiënten. Waar bij een on premise oplossing een zorgverlener direct controle uit kan oefenen op de hard- en software, wordt dit bij het inschakelen van een cloudprovider volledig uit handen gegeven. Door de toenmalig artikel 29 werkgroep werden op dit vlak in 2012 de volgende risico's omschreven[90]:

- Gebrek aan beschikbaarheid als gevolg van een vendor lock-in;
- Gebrek aan integriteit door het gebruik van gedeelde bronnen;

[87] Zie ook paragraaf 1.2.1.13.

[88] Zie Advies 05/2012 over cloud computing, 1 juli 2012, p. 7.

[89] Zie artikel 28 lid 2 AVG.

[90] Zie Advies 05/2012 over cloud computing, 1 juli 2012, p. 6 en 7.

- Gebrek aan vertrouwelijkheid indien opsporingsinstanties handhavingsverzoeken rechtstreeks aan de cloudprovider richten;
- Gebrek aan mogelijkheden om te interveniëren door de complexiteit van de keten waar de cloudprovider onderdeel van uitmaakt;
- Gebrek aan het geven van goede uitvoering aan rechten van betrokkenen
- Gebrek aan afscherming van gegevens.

Ook voor deze risico's geldt dat ze nog steeds reëel zijn, zij het wel minder aanwezig dan in 2012. Technologische ontwikkelingen zorgen voor toenemende mate van beveiliging en dus afscherming van gegevens, het risico op vendor lock-in ten aanzien van medische data neemt in het algemeen af door dataportabiliteit[91] onder de AVG en cloudproviders zijn door de AVG eveneens gedwongen om goede uitvoering aan rechten van betrokkenen te geven.[92]

Geen juridische onderhandelruimte

De in Nederland populaire cloudproviders die clouddiensten aanbieden, werken met hun eigen set aan gebruiks- en algemene voorwaarden, inclusief verwerkersovereenkomsten.[93] Inherent aan cloudproviders is de weerstand als het gaat om het afwijken van deze voorwaarden voor individuele gebruikers. Immers, het schaalvoordeel wordt gehaald door voor alle gebruikers dezelfde diensten tegen dezelfde voorwaarden aan te bieden. Wanneer een cloudprovider wordt geselecteerd dienen de daarbij horende voorwaarden zeer nauwkeurig bestudeerd en beoordeeld te worden. Bij nadelige bepalingen voor de verwerkingsverantwoordelijke, nadelige bepalingen voor de medische data van Nederlandse patiënten of zelfs bepalingen die strijdig zijn met Nederlandse, of andere toepasselijke wetgeving, is het aan de verwerkingsverantwoordelijke om dit bespreekbaar te maken bij de cloudprovider.

Al in 2010 gaf de voormalig artikel 29 werkgroep aan dat het argument waarin wordt gesteld dat er vanwege het verschil in omvang van een cloudprovider tegenover een afnemer geen juridische onderhandelingsruimte is, geen legitiem excuus is[94]:

> *"ook de onevenwichtigheid in de contractuele macht van een kleine voor de verwerking verantwoordelijke ten opzichten van grote dienstverleners niet [behoort] te worden beschouwd als een rechtvaardiging voor de voor de verwerking verantwoordelijke om contractbepalingen te accepteren die niet in overeenstemming met de wetgeving voor gegevensbescherming zijn"*

Vanzelfsprekend speelt dit risico minder bij cloudproviders die zich flexibel opstellen ten aanzien van de gebruikte juridische voorwaarden. In dat geval is er meer ruimte voor de verwerkingsverantwoordelijke om eigen voorwaarden te stellen. Zo kan er voor de verwerkersovereenkomst bijvoorbeeld aansluiting gezocht worden bij in de medische branche werkbare modellen, zoals de BoZ verwerkersovereenkomst.[95]

Toegang tot medische data door opsporingsinstanties

Ongeacht de opslaglocatie van medische data, bestaat het risico dat opsporingsinstanties de data op kunnen vragen. Dat risico geldt zowel voor on premise als voor cloudoplossingen. Het enige verschil daarin is dat het bevel van een opsporingsinstantie bij een on premise

[91] Zie artikel 20 AVG.

[92] Zie artikel 28 lid 3 sub e AVG.

[93] Zie bijvoorbeeld http://www.microsoftvolumelicensing.com/DocumentSearch.aspx?Mode=3&DocumentTypeId=46, https://cloud.google.com/terms/ en https://aws.amazon.com/blogs/security/aws-gdpr-data-processing-addendum/.

[94] Zie Advies 1/2010 over de begrippen "voor de verwerking verantwoordelijke" en "verwerker", 16 februari 2010, p. 31.

[95] Zie ook paragraaf 1.2.1.7.

oplossing aan de verwerkingsverantwoordelijke zelf gericht zal zijn, waar dat in het geval van een cloudoplossing richting de cloudprovider, de verwerker, gericht kan worden. In dat laatste geval kan er bij de verwerkingsverantwoordelijke een gevoel ontstaan dat er minder controle over de eigen medische data is wanneer een cloudprovider kan besluiten om gehoor te geven aan een bevel. Uit het onderzoek is gebleken dat de in Nederland populaire cloudproviders, in hun rol als verwerker, erg strikt zijn. Zij geven geen gehoor aan verzoeken van overheden, tenzij zij daartoe wettelijk verplicht worden. Ook proberen zij waar mogelijk de verzoeker door te verwijzen naar de afnemer van de clouddienst, omdat die verantwoordelijk is voor de data. [96]

Het in Nederland geldende (afgeleide) verschoningsrecht voor medische data lijkt op dit moment nog weinig op het netvlies te staan van cloudproviders. Dit kan dan ook een aandachtspunt zijn voor zorgverleners die clouddiensten willen gebruiken voor opslag en eventuele verdere verwerking van medische data. De zorgverlener zou aan de cloudprovider kunnen laten weten dat de klantdata medische data bevat die onder het verschoningsrecht valt. De zorgverlener zou daarbij ook van de cloudprovider kunnen proberen te vergen dat deze zich op het afgeleide verschoningsrecht beroept in het geval de cloudprovider ooit een verzoek of vordering zou ontvangen ten aanzien van de klantdata van de zorgverlener. Op deze manier kan het risico op inzage van medische data tot een minimum worden beperkt.

2.3 Juridische risico's Nederland en de EU

Wanneer de gegevensverwerking zich uitbreidt van Nederland naar andere landen binnen de EU, ontstaat een grensoverschrijdende situatie. Hoewel de EU in een steeds grotere mate van harmonisatie voorziet in de wetgeving van lidstaten, bestaan er ook nog altijd belangrijke verschillen tussen de rechtsstelsels van EU-lidstaten. Deze verschillen kunnen juridische risico's veroorzaken.

Afwijkingen in geldende (privacy)wetgeving

Hoewel de AVG de wetgeving van alle EU-landen op gebied van privacy gelijk heeft getrokken, bevat de AVG ook specifieke mogelijkheden voor landen om af te wijken. Om deze reden heeft bijna iedere EU-lidstaat inmiddels toch nationale wetgeving aangenomen om de AVG nader te implementeren.[97] Daardoor kunnen er op specifieke punten toch afwijkingen bestaan tussen de regels die in de lidstaten van toepassing zijn op de verwerking en bescherming van medische data. De mogelijkheden voor het verwerken van medische data voor wetenschappelijk onderzoek kunnen bijvoorbeeld per lidstaat verschillen. Dit kan ook tot gevolg hebben dat medische data van Nederlandse patiënten net niet helemaal op gelijke manier juridisch is beschermd in een andere EU-lidstaat als in Nederland. Deze verschillen betreffen eerder subtiele nuances dan aanzienlijke afwijkingen. Daardoor blijven de risico's die eventueel voort kunnen vloeien uit deze verschillen beperkt.

Onzekerheid of (afgeleide) verschoningsrecht helder is geregeld

Een voorbeeld daarvan is het (afgeleide) verschoningsrecht voor medische data. In Nederland is helder dat zorgverleners en de (cloud)dienstverleners die zij inschakelen voor de verwerking van medische data niet gedwongen kunnen worden tot het verstrekken van medische data van Nederlandse patiënten. Het is niet geheel zeker of dit in alle andere EU-landen wel even duidelijk is geregeld. Op basis van in de hele EU geldende wetgeving waaronder de AVG maar ook het EVRM en het Handvest van de grondrechten van de EU zijn goede argumenten te geven waarom het (afgeleide) verschoningsrecht inderdaad zo zou moeten zijn of worden geregeld, maar dat geeft nog niet zoveel zekerheid als een specifieke regeling. Alvorens medische data van Nederlandse patiënten op te slaan bij een

[96] Zie onder andere https://www.amazon.com/gp/help/customer/display.html?nodeId=GYSDRGWQ2C2CRYEF, https://transparencyreport.google.com/user-data/overview en https://www.microsoft.com/en-us/corporate-responsibility/lerr.

[97] Voor een overzicht, zie https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeetingDoc&docid=30306.

cloudprovider die elders in de EU is gevestigd dan Nederland, is het dus van belang om na te gaan of het (afgeleide) verschoningsrecht in dat land wel bestaat en gelijkwaardig is aan dat in Nederland. Als de cloudprovider (een) vestiging(en) heeft in (een) land(en) waar het (afgeleide) verschoningsrecht niet gelijkwaardig is aan dat in Nederland, is het wenselijk om maatregelen te treffen om het risico op inzage door buitenlandse autoriteiten zo ver mogelijk terug te dringen. Daarbij kan bijvoorbeeld worden gedacht aan encryptie van de medische data op zodanige manier dat de sleutel altijd buiten de macht van de cloudprovider blijft (zie ook hoofdstuk 3).

E-evidence verordening

Een ontwikkeling die van belang is in verband met het risico op inzage door buitenlandse autoriteiten, is dat de EU werkt aan een e-evidence verordening[98], waarmee de autoriteiten van iedere EU-lidstaat rechtstreeks data zullen kunnen vorderen van cloudproviders gevestigd in eender welke EU-lidstaat, ongeacht waar de data is opgeslagen. Dit zou een substantiële verruiming kunnen betekenen van het risico dat buitenlandse autoriteiten medische data van Nederlandse patiënten kunnen inzien, tenzij ook het (afgeleide) verschoningsrecht voor medische data in de hele EU op gelijkwaardige wijze wordt geregeld als in Nederland. Het is aan te raden dat er vanuit de Nederlandse overheid nauwlettend op wordt toegezien dat de e-evidence verordening geen materiële verslechtering oplevert van de juridische bescherming van de medische data van Nederlandse patiënten.

Grensoverschrijdende geschillen met een cloudprovider

Verschillen in wetgeving tussen EU-lidstaten hoeven niet per definitie specifiek aan privacy gerelateerd te zijn om toch gevolgen te kunnen hebben voor de bescherming van medische data van Nederlandse patiënten. Zo zal een geschil over betaling kunnen resulteren in het niet beschikbaar zijn van medische data, wanneer de cloudprovider besluit om de diensten tijdelijk te blokkeren. Wanneer de afnemer, bijvoorbeeld een ziekenhuis, en de cloudprovider in verschillende lidstaten van de EU zijn gevestigd, zullen eventuele geschillen automatisch een grensoverschrijdend karakter krijgen. Dit kan betekenen dat juridische geschillen beslecht moeten worden op basis van een ander rechtsstelsel of dat er rekening gehouden dient te worden met specifieke procedurele regels die in Nederland niet gelden. Dit kan leiden tot hogere juridische kosten voor de verwerkingsverantwoordelijke, of een vermindering van de rechtsmiddelen en feitelijke mogelijkheden voor de verwerkingsverantwoordelijke om naleving door de cloudprovider af te dwingen.

2.4 Juridische risico's buiten de EU

Zodra gebruik wordt gemaakt van een cloudprovider met een vestiging buiten Nederland of de EU, wordt de medische data blootgesteld aan bevoegdheden van de autoriteiten in ieder land waar de cloudprovider gevestigd is.

Conflicterende verplichtingen AVG en buitenlandse wetgeving

Wanneer een cloudprovider is gevestigd in een land buiten de EU waarmee Nederland geen internationale overeenkomsten of afspraken heeft gemaakt, is dat een aanzienlijk risico. Een aanzienlijk risico omdat daarmee de mogelijkheid bestaat dat de cloudprovider verstrikt raakt in op hem toepasselijke wet- en regelgeving. In dat geval dicteert de AVG[99] dat het de cloudprovider niet toegestaan is de data af te staan, terwijl nationale wetgeving diezelfde cloudprovider kan verplichten om de data op basis van die wetgeving juist wel af te staan. Derhalve dient dit risico in iedere DPIA die wordt uitgevoerd alvorens een cloudprovider wordt ingeschakeld, zwaar mee te wegen.

[98] https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2018/06/22/verordening-europese-verstrekkings-en-bewaringsbevelen-voor-e-evidence/verordening-europese-verstrekkings-en-bewaringsbevelen-voor-e-evidence.pdf

[99] Zie artikel 48 AVG.

CLOUD Act

Diverse populaire cloudproviders hebben een hoofdkantoor in de Verenigde Staten. Sinds 2018 maakt de CLOUD Act deel uit van de Amerikaanse wetgeving. Zoals vermeld in paragraaf 1.2.1.11 bestaat door de CLOUD Act de mogelijkheid dat Amerikaanse autoriteiten de Amerikaanse vestiging kunnen opdragen om data te verstrekken die door of namens de vestiging in de EU wordt opgeslagen voor een klant in de EU. Dat zou ook een zorgverlener kunnen zijn, die de clouddiensten gebruikt voor opslag van medische data van Nederlandse patiënten.

Op grond van artikel 48 van de AVG is het cloudproviders met een vestiging in de EU uitdrukkelijk verboden om gehoor te geven aan verzoeken of bevelen van autoriteiten van landen buiten de EU, behalve als deze zijn gebaseerd op een internationale overeenkomst, zoals een rechtshulpverdrag, tussen de EU of een lidstaat (zoals Nederland) en het land buiten de EU. Wanneer een cloudprovider gehoor zou geven aan een vordering van een Amerikaanse autoriteit die op basis van de CLOUD Act rechtstreeks aan de Amerikaanse vestiging van de cloudprovider is gericht, in plaats van aan de autoriteiten van het vestigingsland in de EU (doorgaans Ierland) tot het verstrekken van klantdata waaronder zich medische data van Nederlandse patiënten bevinden, dan zou de cloudprovider in overtreding zijn van de AVG. Op deze overtreding is het hoge boetemaximum van de AVG (20.000.000 euro of 4% van de wereldwijde jaaromzet) van toepassing.[100]

Cloudproviders die zich voor tegengestelde verplichtingen zien staan, hebben op grond van de CLOUD Act de mogelijkheid om bezwaar te maken tegen een vordering als de cloudprovider meent dat de klant waarvan gegevens worden gevorderd geen Amerikaanse persoon is en niet in de Verenigde Staten woonachtig of gevestigd is en er een aanmerkelijk risico zou bestaan dat de cloudprovider door verstrekking wetgeving van een 'qualifying foreign government' zou schenden.[101] Voordat cloudproviders hier een beroep op kunnen doen in het kader van artikel 48 van de AVG bij verzoeken die betrekking hebben op klanten in de EU, zal de EU of lidstaat dus eerst een 'qualifying foreign government' moeten worden.

De CLOUD Act schept daarnaast de mogelijkheid dat de autoriteiten van 'qualifying foreign governments' ook zelf rechtstreeks verzoeken of vorderingen kunnen sturen aan Amerikaanse cloudproviders voor het verkrijgen van data. Dergelijke overeenkomsten zullen dan wel moeten voorzien in waarborgen ter bescherming van privacy en andere fundamentele rechten.[102] In het kader van de evaluatie van Privacy Shield wordt daarbij ook vermeld dat diverse burgerrechtenorganisaties de eisen die in de CLOUD Act worden gesteld voor het sluiten van dergelijke overeenkomsten niet voldoende vinden. De Europese Commissie heeft zelf in de CLOUD Act echter geen aanleiding gevonden om Privacy Shield niet langer toereikend te beschouwen voor de bescherming van persoonsgegevens.

De European Data Protection Board (EDPS) heeft in februari 2019 een opinie uitgebracht over het voornemen van de Europese Commissie en de Raad om tot een internationale overeenkomst te komen met de VS inzake de toegang tot elektronisch bewijs door (opsporings)autoriteiten.[103] De beleving dat de werkwijze van het inzetten van rechtshulpverdragen in toenemende mate te belemmerend en tijdrovend is voor een effectieve opsporing van criminaliteit, wordt ook daarin als breed gedragen onderschreven. Tegelijkertijd ziet de EDPS risico's wanneer autoriteiten van het ene land rechtstreeks toegang kunnen krijgen tot data van burgers van een ander land en stelt daarom voor dat in internationale overeenkomsten wordt afgesproken dat de autoriteiten van het andere land wel betrokken worden. Dit is in lijn met de opvatting van de Nederlandse regering in verband

[100] Zie artikel 83 lid 5 sub c AVG.

[101] Zie § 2713(2) CLOUD Act: "MOTIONS TO QUASH OR MODIFY", https://www.congress.gov/bill/115th-congress/senate-bill/2383/text.

[102] Zie § 2523 CLOUD Act.

[103] https://edps.europa.eu/sites/edp/files/publication/19-04-02_edps_opinion_on_eu_us_agreement_on_e-evidence_en.pdf.

met de voorgestelde e-evidence verordening. Specifiek in het kader van de bescherming van medische data van Nederlandse patiënten, kan hierbij nog worden opgemerkt dat de toenemende mogelijkheden voor rechtstreekse grensoverschrijdende toegang tot data door autoriteiten tegelijkertijd een noodzaak en een kans bieden om afspraken te maken waardoor het (afgeleide) verschoningsrecht ten aanzien van medische data van Nederlandse patiënten ook door buitenlandse autoriteiten zal worden gerespecteerd.

FISA en NSL

In 2013 is veel ophef ontstaan toen Edward Snowden via de media (Glenn Greenwald en Laura Poitras namens the Guardian) de klok luidde over massale ongerichte spionage door de NSA en FBI. Documenten over de geheime 'PRISM' en 'Upstream' programma's toonden aan dat Amerikaanse autoriteiten via Amerikaanse (cloud)providers toegang kregen tot grote hoeveelheden data van personen over de hele wereld.

De wetgeving op basis waarvan dergelijke programma's zijn geautoriseerd is sectie 702 FISA. Op basis daarvan kunnen Amerikaanse inlichtingendiensten zoals de NSA en ook de FBI informatie vergaren over 'doelwitten'. Dit zijn personen waarvan de inlichtingendiensten het van belang achten voor de nationale veiligheid om informatie over te vergaren. Ook zogenaamde national security letters, NSL's, dienen dat doel. Volgens rapporten van de Amerikaanse inlichtingendiensten waren er in 2016 ongeveer 106.000 doelwitten geselecteerd en in 2017 ongeveer 130.000.[104] Uit transparantierapporten van drie populaire cloudproviders met hoofdkantoor in de VS blijken aanzienlijke verschillen in de hoeveelheid verzoeken die zij rapporteren. Een provider gaf aan dat zij in de periode van januari tot en met juni 2018 ieder tussen de 500 en 999 verzoeken ontving van Amerikaanse inlichtingendiensten ten aanzien van tussen de 97.000 en 97.499 accounts. Een andere provider gaf aan dat zij in dezelfde periode tussen de 0 en 499 verzoeken ontving over tussen de 13.000 en 13.499 accounts. Een derde provider is later dan de andere providers begonnen met het rapporteren van dergelijke statistieken en geeft slechts aan dat er van januari tot en met juni 2018 sprake was van tussen de 0 en 249 verzoeken op basis van FISA.[105]

Er zijn verschillende manieren waarop naar de transparantierapporten gekeken kan worden. Enerzijds is 130.000 doelwitten een zeer aanzienlijk aantal. Ook de bevoegdheden en technische capaciteiten van Amerikaanse inlichtingendiensten om informatie over de doelwitten te vergaren zijn aanzienlijk. Anderzijds lijken de twee cloudproviders die de meeste verzoeken hebben ontvangen ieder ruim een miljard accounts te hebben. Puur op basis van de percentages zou dat betekenen dat, mits de rapportages juist zijn, er een kans van 0,013% bestaat dat een willekeurig account onderwerp is van spionage door de Amerikaanse inlichtingendiensten. De kans dat specifiek de medische data van Nederlandse patiënten door Amerikaanse inlichtingendiensten zou worden ingezien is op basis van de beschikbare statistieken moeilijk in te schatten. Deze statistieken maken namelijk geen onderscheid tussen de soorten gebruikte diensten en gooien consumentendiensten om e-mails mee te sturen en agenda's bij te houden op een hoop met de zakelijke IaaS-, PaaS- en SaaS-diensten die door zorgverleners gebruikt kunnen worden. Een probleem hierbij is ook dat de juistheid van de statistieken moeilijk te controleren lijkt.

Los van de statistieken kan ook worden geargumenteerd dat massale surveillance zoals uitgevoerd door de Amerikaanse inlichtingendiensten zich simpelweg niet verdraagt met Europese fundamentele rechten. Op basis van artikel 48 AVG lijkt het voldoen aan dergelijke verzoeken overigens ook verboden. Gelet op het geheime karakter van de verzoeken en de naleving ervan, is het wel sterk de vraag of dergelijke niet-naleving aan het licht zou komen.

[104] https://www.dni.gov/files/documents/icotr/2018-ASTR----CY2017----FINAL-for-Release-5.4.18.pdf.

[105] https://transparencyreport.google.com/user-data/us-national-security?hl=en, https://www.microsoft.com/en-us/corporate-responsibility/us-national-security-orders-report, https://d1.awsstatic.com/certifications/Information_Request_Report_June_2018.pdf.

In 2017 werd bij herautorisatie van 702 FISA een einde gemaakt aan de mogelijkheid van zogenaamde 'about' verzameling, waarbij communicatie werd verzameld waarin het doelwit werd genoemd maar waar het doelwit zelf niet aan deelnam. De overige bevoegdheden werden echter ongemoeid gelaten.

Al met al lijkt de werkelijke kans dat medische data van willekeurige Nederlandse patiënten door Amerikaanse inlichtingendiensten worden ingezien in het algemeen (zeer) gering. Of dat ook geldt voor prominentere personen, zoals de premier of andere belangrijke ambtsbeklederS, kan de vraag zijn. Volgens diverse nieuwsberichten werden bijvoorbeeld telefoons van Duitse president Angela Merkel en Franse president Francois Hollande door de NSA afgeluisterd.[106] Hoe dan ook doet de enkele mogelijkheid van spionage afbreuk aan het benodigde vertrouwen dat medische data geheim zullen blijven. Om die reden kan het dan ook als wenselijk worden beschouwd dat (i) zoveel mogelijk wordt gefaciliteerd dat internationaal wordt onderhandeld om medische data uit te sluiten van spionagebevoegdheden en (ii) technische maatregelen te treffen om de mogelijkheid van inzage in medische data zo ver mogelijk te minimaliseren, waaronder het toepassen van encryptie waarbij de sleutel te allen tijde buiten de macht van de cloudprovider wordt gehouden.

Exportinstrumenten

Inherent aan de opslag van medische data bij een cloudprovider buiten de EU, is de verplichting tot het hanteren van de juiste exportinstrumenten om ook buiten de EU een passend beschermingsniveau op juridisch gebied te realiseren.

Zoals omschreven in paragraaf 1.2.1.10 zijn hier meerdere instrumenten voor beschikbaar. De geldigheid van twee van deze instrumenten wordt momenteel echter beoordeeld door het Hof van Justitie van de EU. De mogelijkheid bestaat dat de model clauses en het Privacy Shield ongeldig worden verklaard. Daarmee ontstaat het risico dat een verwerkingsverantwoordelijke en cloudprovider gezamenlijk zorg moeten dragen om op een andere manier een passend beschermingsniveau te realiseren wanneer medische data van Nederlandse patiënten buiten de EU wordt gebracht.

Wanneer een cloudprovider als subverwerker optreedt[107], doet zich ten aanzien van de model clauses een aanvullend risico voor. Wanneer de Europese verwerker een cloudprovider buiten de EU inschakelt, treedt de verwerker op als data-exporteur en de cloudprovider als data-importeur. De versie van de model clauses die voor deze situatie bestaat is echter nooit door de Europese Commissie goedgekeurd. Dat betekent dat model clauses in deze situatie niet kunnen dienen als passende waarborg. Een alternatieve waarborg zou het Privacy Shield kunnen zijn als de betreffende cloudprovider in de VS is gevestigd. Een ander alternatief zou mogelijk zijn als de cloudprovider zich in een land bevindt waar door de Europese Commissie een adequaatheidsbesluit over is genomen.[108] Bevindt de subverwerkende cloudprovider zich niet in de VS of een land met een adequaat beschermingsniveau, dan dient de verwerker zich te beroepen op een ander exportmechanisme zoals beschreven in paragraaf 1.2.1.10 en verder.

Ook van andere bestaande exportmechanismes die partijen zelf kunnen implementeren kan echter niet worden verwacht dat deze effectief zijn tegen het risico op verstrekking van gegevens aan autoriteiten. Wanneer een vestiging van een cloudprovider wettelijk verplicht is om gegevens aan een autoriteit te verstrekken, zal de cloudprovider deze plicht immers simpelweg moeten naleven. Zo bezien is de enige mogelijkheid om dit risico werkelijk tegen te gaan, dat de EU en/of EU-lidstaten internationale afspraken maken met andere landen waardoor de medische data van Nederlandse patiënten worden beschermd tegen inzage

[106] https://nos.nl/artikel/2158544-merkel-ik-wist-niets-van-duitse-hulp-aan-nsa-bij-afluisteren.html.

[107] Zoals geschetst in het voorbeeld en de afbeelding in paragraaf 1.2.1.3.

[108] Zie paragraaf 1.2.1.12.1.

door buitenlandse autoriteiten, bijvoorbeeld door het respecteren van het (afgeleide) verschoningsrecht.

3. Technische eisen aan cloudproviders

3.1 Inleiding en scope

Nu de juridische eisen en risico's in kaart zijn gebracht, volgt een verdieping op de technische eisen aan de hand van de volgende vraag:

> *Aan welke technische eisen moet een cloudprovider voldoen om te borgen dat medische data van Nederlandse patiënten voldoende beveiligd én met waarborgen voor de privacy kan worden opgeslagen en verwerkt?*

De technische eisen aan cloudproviders vloeien voort uit de juridische eisen zoals hiervoor behandeld. Technische eisen zijn in feite een interpretatie van het 'passende' beveiligingsniveau zoals vereist onder de AVG, specifiek toegespitst op techniek. Zoals aangegeven, is de wetgeving zelf echter techniekneutraal. Er zijn simpelweg te veel situaties en factoren mogelijk om een lijst technische maatregelen te maken en voor te schrijven die voor alle soorten gegevens, verwerkingen en bijbehorende risico's passend zou zijn. Vanwege de snelle technologische ontwikkelingen zou een dergelijke lijst ook zeer snel verouderd zijn. Voortdurend worden nieuwe manieren en technieken gevonden om binnen te dringen in systemen en voortdurend worden systemen en technieken aangepast om daarop te anticiperen en reageren. Ook de beveiligingsrichtsnoeren van privacytoezichthouders zien (daarom) juist op de processen om te komen tot passende beveiliging en schrijven geen specifieke technische maatregelen of vooraf gedefinieerde risicoklassen (meer)[109] voor.

Ook voor een situatie zoals opslag en verwerking van medische data in de cloud, is het niet goed mogelijk een lijst technische maatregelen of eisen te formuleren die passend zijn voor alle mogelijke vormen van opslag en verwerking van medische data in de cloud. Zoals ook elders uit dit rapport blijkt, bestaan er vele verschillende soorten medische data en een breed spectrum van gevoeligheid (van het feit of iemand lenzen draagt of verkouden is tot iemands vingerafdruk, complete DNA, ziektes, benodigde behandeling of medicijnen, etc). Ook zijn er vele verschillende vormen van opslag (en eventuele verdere verwerking) in de cloud mogelijk, waarbij de risicoprofielen zoals aangegeven kunnen verschillen afhankelijk van de landen waar de cloudprovider een juridische entiteit heeft, de landen waar datacenters staan, welke entiteiten feitelijk toegang hebben of kunnen krijgen tot data en of dat afhankelijk is van de locatie waar de data is opgeslagen of niet.

Ook de verwerkingen, doeleinden en samenhangende risico's kunnen zeer verschillend zijn. Een ziekenhuis zou zelf ook andere technische eisen kunnen stellen aan een cloudprovider dan een partij die in opdracht van ziekenhuizen de kwaliteit en efficiëntie van behandelingen analyseert. De data, verwerkingen, doeleinden en risicoprofielen kunnen immers anders zijn.

Gezien een lijst met 'one-size-fits-all' technische eisen in de praktijk niet goed haalbaar is, wordt gewerkt met beveiligingsstandaarden die meer zien op het proces om tot passende beveiliging te komen, zoals ISO 27001. Specifiek voor verwerking van persoonsgegevens door cloudproviders is ISO 27018 ontwikkeld. Om op een efficiënte manier aan te tonen dat informatie passend is beveiligd, passen cloudproviders in de praktijk deze normen toe en laten zich tegen deze normen certificeren door daartoe gespecialiseerde partijen. Zoals

[109] In het document 'Achtergrondstudies en Verkenningen 23' (https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/av/av23.pdf

) van de Registratiekamer (de voorloper van het CBP, wat weer de voorloper was van de AP) werden bepaalde risicoklassen in het algemeen aangeduid en specifieke maatregelen genoemd om deze te mitigeren. De richtsnoeren van het CBP uit 2013 stapten hier echter vanaf en sloten meer aan bij algemene industriestandaarden om tot passende beveiliging te komen, zoals ISO 27001. Deze focussen meer op het proces dan specifieke risico's en maatregelen.

elders ook omschreven bieden certificeringen een belangrijke aanwijzing van passende beveiliging maar kunnen zij geen absolute garanties bieden.

De Autoriteit Persoonsgegevens heeft een lijst van technische[110] en organisatorische[111] voorbeeldmaatregelen op haar website genoemd om partijen op weg te helpen bij vaststellen van een passend beveiligingsniveau.

Technisch:

- Logische en fysieke (toegangs-)beveiliging en beveiliging van apparatuur (denk niet alleen aan kluizen en portiers, maar ook aan firewalls en netwerksegregatie);
- Technisch beheer van de (zo beperkt mogelijke) autorisaties en bijhouden van logbestanden;
- Beheer van technische kwetsbaarheden (patch management);
- Software, zoals browsers, virusscanners en operating systems up-to-date houden;
- Back-ups maken waarmee u de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig kunt herstellen. Overweeg of u dubbele systemen nodig heeft zodat het geheel goed blijft functioneren wanneer een onderdeel uitvalt;
- Automatisch verwijderen van verouderde gegevens;
- Versleuteling van gegevens;
- Hashing. Organisaties kunnen hashing gebruiken als methode om persoonsgegevens te pseudonimiseren;
- Minder gegevens op uw servers verwerken en meer gegevensverwerkingen laten plaatsvinden op de apparatuur van de gebruiker zelf, zoals een smartphone.

Organisatorisch:

- Toewijzen van verantwoordelijkheden voor informatiebeveiliging;
- Bevorderen van beveiligingsbewustzijn bij bestaande en nieuwe medewerkers;
- Opstellen van procedures om op gezette tijdstippen de beveiligingsmaatregelen te testen, te beoordelen en te evalueren;
- Regelmatige controle van de logbestanden;
- Opstellen van een protocol voor de afhandeling van datalekken en beveiligingsincidenten;
- Sluiten van geheimhoudings- en verwerkersovereenkomsten;
- Beoordelen of u dezelfde doelen kunt behalen met minder persoonsgegevens;
- Minder mensen in uw organisatie toegang geven tot persoonsgegevens;
- Per verwerking het besluitvormingsproces en de achterliggende overwegingen vastleggen.

3.2 Omschrijving clouddiensten

Zoals ook elders aangegeven, is het belangrijk om te redeneren vanuit risico's ten aanzien van de data, meer specifiek de beschikbaarheid, integriteit en vertrouwelijkheid (BIV). Om dat in de technische context van cloud en medische data te kunnen doen, is het nodig een goed begrip te hebben van de onderdelen en ketens waaruit clouddiensten bestaan.

Een clouddienst (zie ook de definitie in de lijst) is in essentie een hoeveelheid digitale opslag- en rekencapaciteit, die via het internet kan worden bediend en benaderd. De afnemer configureert, gebruikt en bedient deze opslag- en rekencapaciteit op afstand, meestal via het

[110] Zie https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/algemene-informatie-avg/verantwoordingsplicht#wat-zijn-voorbeelden-van-technische-beveiligingsmaatregelen-6385.

[111] Zie https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/algemene-informatie-avg/verantwoordingsplicht#wat-zijn-voorbeelden-van-organisatorische-beveiligingsmaatregelen-6384.

internet.[112] Dit wordt ook wel 'Infrastructure-as-a-Service' (IaaS) genoemd. Dit soort diensten geeft de klant de mogelijkheid om op afstand een virtuele computer (virtual machine) op te starten en te bedienen, waarbij de klant zelf kan instellen hoeveel opslag- en rekencapaciteit de virtuele machine moet of mag hebben (dit kan ook variabel zijn, afhankelijk van het gebruik). De virtuele opslag- en rekencapaciteit wordt feitelijk geleverd door fysieke machines (servers) die draaien in datacenters (gebouwen die speciaal zijn gebouwd om servers zo efficiënt, betrouwbaar en veilig mogelijk te laten draaien) en aan elkaar zijn verbonden door netwerken en (virtualisatie)software.

Kiezen van de locatie voor opslag en verdere verwerking
De techniek hierachter maakt het ook mogelijk om als cloudprovider functies aan te bieden waarmee de klant zelf kan kiezen in welk datacenter of welke datacenters de fysieke machines moeten draaien die worden gebundeld tot één virtuele machine. Dit kan bijvoorbeeld van belang zijn om de latency (vertraging) te beperken. Hoe dichter data bij degene die erbij moet is opgeslagen, hoe korter de wachttijden.[113] Cloudproviders die op meer verschillende plaatsen datacenters hebben staan, kunnen daarmee in het algemeen ook een grotere mate van zekerheid bieden dat uitval van één datacenter (bijvoorbeeld vanwege een ramp) niet leidt tot onbeschikbaarheid van de virtuele machines en de daarin opgeslagen data. In dit opzicht zal het ook een voordeel zijn als cloudproviders in meerdere landen datacenters hebben. En meerdere datacenters op verschillende locaties per land of per 'beschikbaarheidsregio' kan in dit opzicht nog meer voordelen bieden.

Zoals wij ook elders hebben aangegeven, is de locatie waar data is opgeslagen echter niet doorslaggevend voor de vraag welke autoriteiten (toegang tot) de data kunnen vorderen. Daarvoor is eerder doorslaggevend of de cloudprovider een entiteit heeft in het betreffende land die feitelijk bij de data kan of daar feitelijk toegang toe kan verschaffen. Als in het betreffende land waar het datacenter staat geen rechtspersoon van de cloudprovider is gevestigd die toegang kan krijgen of verschaffen tot de data, dan zouden de opsporingsautoriteiten van het land waar het datacenter staat eventueel wel fysieke servers in beslag kunnen nemen. Vanwege de encryptie die in het algemeen wordt toegepast door cloudproviders (zie 3.9) en de relatief grote impact van inbeslagname, zal het uitoefenen van deze bevoegdheid in de meeste gevallen niet passend, effectief of proportioneel zijn. De financiële schade die inbeslagname tot gevolg heeft voor de cloudprovider zou wel een prikkel kunnen opleveren voor de entiteit die de gevraagde (toegang tot) data wel kan bieden, al lijkt ook dat geen passende inzet van de bevoegdheid tot inbeslagname.

NCSC
Cloudcomputing in zijn algemeenheid, en de beveiligingsmaatregelen die daarbij horen, zijn in 2012 door het Nationaal Cyber Security Centrum (NCSC) onder de aandacht gebracht middels een whitepaper.[114] Hoewel daarin geen specifieke aandacht is besteed aan de opslag van medische data, is er wel degelijk aandacht besteed aan beveiliging in de breedste zin van het woord. Samengevat dient er volgens het NCSC bij clouddiensten rekening gehouden te worden met de volgende beveiligingsaspecten:

- **Naleving van wet- en regelgeving.** Relevante wet- en regelgeving dient in kaart gebracht te zijn en controleerbaar nageleefd te worden;

[112] Het zou in theorie ook mogelijk kunnen zijn een aparte (glasvezel)verbinding naar een datacenter van de cloudprovider aan te leggen of te huren. Dat zou normaliter zowel voor de capaciteit en beschikbaarheid van de verbinding positief zijn, als voor de vertrouwelijkheid. Omdat dit wel aanzienlijke kosten met zich meebrengt en bijvoorbeeld de vertrouwelijkheid ook met cryptografische maatregelen over het internet is te beschermen (TLS/SSL), zal het gebruik van een aparte lijn niet in alle gevallen 'passend' zijn en ook niet te beschouwen als minimumeis die in alle situaties nageleefd zal moeten worden.

[113] Om data dichter bij de gebruiker op te slaan kan ook gebruik worden gemaakt van content distribution networks. Het gebruik van CDNs kan weer een risico opleveren omdat er een extra partij is (de CDN-provider) met een kopie van de data. De wenselijkheid van het gebruik van CDN-providers voor opslag en verwerking van medische data valt buiten de scope van dit onderzoek.

[114] Zie https://www.ncsc.nl/documenten/publicaties/2019/mei/01/cloudcomputing.

- **Beheersbaarheid van processen en systemen.** Gebruik van een cloudprovider betekent uitbesteden en per definitie controleverlies. Een afnemer dient derhalve heldere afspraken met een cloudprovider te maken teneinde de beheersbaarheid te kunnen blijven borgen;
- **Gegevensbescherming.** De afnemer van clouddiensten is verantwoordelijk voor de bescherming van gegevens bij de cloudprovider;
- **Relatie tot de leverancier.** In 2012 noemde het NCSC de cloudmarkt nog onvolwassen. Uit dit onderzoek is gebleken dat daar inmiddels geen sprake meer van is;
- **Beschikbaarheid van de clouddienst.** Beschikbaarheid is één van de pijlers van BIV. Derhalve dient een afnemer van clouddiensten extra aandacht te besteden aan mogelijke gevolgen van het niet-beschikbaar zijn van een clouddienst;
- **Beheer van gebruikers.** Toegang tot data in de cloud dient beperkt te zijn tot daartoe geautoriseerde personen;
- **Beheer van incidenten.** Verstoringen dienen zo snel en adequaat mogelijk verholpen te worden teneinde de BIV van data te kunnen waarborgen;
- **Beheer van wijzigingen.** Wijzigingen in clouddiensten dienen met zo min mogelijk impact doorgevoerd te worden, zodat de kans op verstoringen zo laag mogelijk blijft;
- **Back-up en recovery.** Een back-up dient zorg te dragen voor herstel van gegevens in geval van verlies of corruptie;
- **Transparantie.** Een cloudprovider dient transparant te zijn over onder andere de geleverde diensten, eventueel ingeschakelde derde partijen en de opslaglocatie van data.

Bij het selecteren van een cloudprovider en het uitvoeren van een DPIA zijn dit onderwerpen die voor een weloverwogen risicoanalyse allen behandeld dienen te worden.

3.3 On premise vs cloud

Enige tijd geleden[115] was het hosten van data in een eigen gecontroleerde omgeving de standaard. Voordelen waren de controleerbaarheid, transparantie en onafhankelijkheid. Wanneer alles in eigen beheer uit wordt gevoerd weet de verwerkingsverantwoordelijke precies waar de data zijn en bestaat er geen (of in ieder geval in veel mindere mate dan bij een clouddienst) afhankelijkheid van een externe partij.

Uit de gesprekken die zijn gevoerd met marktpartijen ten behoeve van dit adviesrapport is echter gebleken dat de verschuiving van on premise naar de cloud in volle gang is. De redenen daarvoor zijn divers, maar beveiliging van data komt telkens als één van de belangrijkste argumenten naar voren in onderzoeken naar on premise en cloudoplossingen.[116] In de clouddienstverleningsmarkt leeft bovendien het idee dat zij beveiliging van data en systemen beter op orde hebben dan de zorgaanbieders zelf, zo blijkt uit diverse gesprekken met brancheorganisaties.

In het algemeen bieden de grotere cloudproviders een hoog beschermingsniveau tegen onbevoegden die zich toegang willen verschaffen tot hun systemen en de daarin opgeslagen data. Diverse varianten van *state of the art* encryptie van data worden standaard toegepast, zowel wanneer deze is opgeslagen ('at rest') als wanneer deze via het internet wordt verstuurd ('in transit'). Ook fysieke toegangsbeveiliging van de datacenters en de systemen om DDoS- en andere soorten aanvallen op de infrastructuur te detecteren en af te weren, worden door technische security-experts in het algemeen als hoogstaand en veilig beschouwd. Tegen risico's als brand of defecte hardware die zou kunnen veroorzaken dat

[115] In 2012 sprak het NCSC nog van een onvolwassen markt van cloudproviders.

[116] Uit de Cloud Adoptie Monitor 2019 van DHPA en Hewlett Packard Enterprise blijkt dat veiligheid, stabiliteit en voorspelbare kosten belangrijke argumenten zijn om te kiezen voor een cloudoplossing.

opgeslagen data onbeschikbaar raken of worden aangetast, bieden zij in het algemeen eveneens een hoog beschermingsniveau. Een dergelijk vergelijkbaar niveau is niet haalbaar in een on premise variant. Daartoe zijn de expertise, mogelijkheden en financiële middelen veelal ontoereikend.

De oorzaak daartoe ligt voor de hand. De primaire taak van een ziekenhuis is het leveren van zorg en niet het zo efficiënt en effectief mogelijk ontwikkelen en gebruiken van IT-diensten. Cloudproviders daarentegen specialiseren zich in het aanbieden van diensten die veiligheid en gebruiksgemak voorop hebben staan.

3.4 BIV en controleerbaarheid

Informatiebeveiliging ten aanzien van medische data in de cloud dient continu gecontroleerd en verbeterd te worden. Het begrip 'informatiebeveiliging' is een verzamelterm van maatregelen die de beschikbaarheid, integriteit en vertrouwelijkheid van, in dit geval, medische data dient te borgen. Daarnaast noemt de AP ook nog controleerbaarheid als vierde aspect. De terminologie is in het kort als volgt samen te vatten:

- **Beschikbaarheid.** Dit houdt in dat geautoriseerde personen op het juiste moment toegang hebben tot de informatiesystemen;
- **Integriteit.** De integriteit van informatie hangt ervan af of de informatie en de verwerking juist, actueel en volledig is;
- **Vertrouwelijkheid.** Informatie is niet langer vertrouwelijk indien er onbevoegd wordt kennisgenomen van de informatie of indien de informatie onbevoegd wordt verstrekt.

De informatiebeveiliging die moet zorgen voor betrouwbaarheid is controleerbaar als met voldoende zekerheid kan worden vastgesteld of er wordt voldaan aan de eisen van beschikbaarheid, integriteit en vertrouwelijkheid.

Volgens het regime van plan-do-check-act, zoals ook terug te vinden in ICT-beveiligingsrichtlijnen, moet, voordat een clouddienst in gebruik wordt genomen voor de verwerking van medische data, een risico-afweging worden gemaakt (dergelijke risico-afweging maakt tevens onderdeel uit van een DPIA). Op basis van de risico-afweging moet het gewenste beveiligingsniveau, dus ook wel de betrouwbaarheidseisen, vastgesteld worden.

Plan-do-check-act is niet bedoeld als een eenmalig iets, maar als een cyclus die geïmplementeerd en herhaald wordt. De afnemer van een clouddienst moet regelmatig controleren of de maatregelen worden nageleefd. Daarnaast dient periodiek gecontroleerd en geëvalueerd te worden of de maatregelen nog voldoen.

3.5 Certificeringen

Op het gebied van informatiebeveiliging bestaan diverse certificeringen.[117] Wereldwijd bekende certificeringen zijn die van de International Organization for Standardization (ISO). ISO is een onafhankelijke NGO die zich specialiseert in het waarborgen van kwaliteit, veiligheid en efficiëntie.[118] Op het gebied van informatiebeveiliging heeft ISO de 27000-serie certificeringen ontwikkeld:[119]

- ISO 27001 voor het beheren van een information security management system (ISMS);
- ISO 27002 voor richtlijnen voor risico-mitigerende maatregelen;
- ISO 27017 voor informatiebeveiliging in de cloud;

[117] Overigens niet te verwarren met certificeringen zoals bedoeld in artikel 42 AVG.

[118] Zie https://www.iso.org/about-us.html#2012_aboutiso_iso_name-text-Anchor.

[119] Zie https://www.iso.org/isoiec-27001-information-security.html.

- ISO 27018 voor het beveiligen van persoonsgegevens in de cloud door verwerkers;
- ISO 27701 voor specifiek op privacy gerichte informatiebeveiliging;
- ISO 27799 voor richtlijnen voor risico-mitigerende maatregelen gericht op de zorg.

Onafhankelijke instellingen toetsen in hoeverre een organisatie aan de normeringen voldoet alvorens een certificaat wordt uitgereikt. Na het behalen van een certificaat wordt vervolgens periodiek getoetst of een organisatie zich nog aan de gestelde eisen houdt.

Hoewel deze normeringen geen zekerheid garanderen ten aanzien van de bescherming van persoonsgegevens, tonen organisaties die conform deze normen gecertificeerd zijn een degelijke mate van volwassenheid aan op het gebied van informatiebeveiliging. Hoewel dergelijke certificeringen een belangrijke aanwijzing geven, betekent het hebben van een certificaat nog niet automatisch dat de beveiliging werkelijk passend is of dat alle verwerking werkelijk in overeenstemming is met wet- en regelgeving, zoals de AVG. Ook het ontbreken van een certificering betekent in het algemeen niet automatisch dat niet is voldaan aan de AVG en andere wetgeving, behalve waar een specifiek certificaat door de wet is voorgeschreven.[120]

Een belangrijk aandachtspunt bij certificering is de scope. Partijen die gecertificeerd willen worden, kiezen zelf op welke diensten of onderdelen van de diensten dit van toepassing is. De exacte scope van een certificaat, of enige beperking daarvan, is niet altijd transparant. Daardoor bestaat het risico dat bepaalde diensten of verwerkingen niet zijn gecontroleerd (en ook niet voldoen), terwijl de aanwezigheid van het certificaat een andere indruk wekt.

Ook is het belangrijk om er bewust van te zijn dat de controles of audits die plaatsvinden bij dergelijke certificeringen momentopnames zijn, waarbij de gecertificeerde partij vaak weet wanneer de controle zal plaatsvinden. Dergelijke controles kunnen dan ook geen absolute zekerheid bieden dat de situatie tussen de controles door niet anders kan zijn dan tijdens de controles.

Geconcludeerd kan worden dat de momenteel bestaande certificeringen in het algemeen een belangrijke aanwijzing geven dat serieus aandacht wordt besteed aan beveiliging. Certificeringen dienen echter niet gezien te worden als garantie dat een bepaalde clouddienst voldoet aan de AVG of dat cloudproviders de opgeslagen data zelf niet zouden kunnen inzien of inzage kunnen bieden aan buitenlandse autoriteiten.

Zorgspecifieke certificeringen

Een bekende zorgspecifieke normering is de NEN 7510. Deze certificering ziet op informatiebeveiliging in de zorg, waarin aandacht wordt besteed aan het uitvoeren van een risicoanalyse. De NEN 7510 normering is een vertaling van ISO 27001, ISO 27002 en ISO 27799. In de normering is een uitgebreide omschrijving van een risicoanalyse opgenomen. In het kort komt het erop neer dat:

1. Op basis van vooraf vastgestelde risicocriteria, bij een herhaalde risicobeoordeling, consistente resultaten voort moeten komen uit de beoordeling;
2. Middels de beoordeling allereerst de risico's geïdentificeerd dienen te worden: welke risico's er zijn op het verlies van vertrouwen, integriteit en beschikbaarheid; en wie de risico-eigenaren zijn;
3. Op basis van het voorgaande vastgesteld moet worden wat de potentiële gevolgen zijn van, en hoe groot de kans is op, de geïdentificeerde risico's;

[120] Certificering tegen een standaard (zoals NEN 7510) is alleen in bepaalde specifieke gevallen wettelijk vereist, bijvoorbeeld voor uitwisselingssystemen voor medische data. Clouddiensten zelf vallen echter niet onder de definitie daarvan, al is het wel mogelijk dat een clouddienst wordt gebruikt voor een uitwisselingssysteem.

4. Tenslotte de resultaten van deze exercitie vergeleken moeten worden met de eerder vastgestelde risicocriteria, en op basis daarvan een volgorde van behandeling vastgesteld wordt.[121]

NEN 7510 beschrijft naast de risicoanalyse eveneens zorgspecifieke beheersmaatregelen voor leverancierrelaties. Er wordt daarbij nogmaals gewezen op de risicobeoordeling, waaronder het risico naar de mogelijke toegang door derden tot de medische data. Daarop dienen beveiligingsmaatregelen afgestemd te worden. Een en ander moet goed worden vastgelegd in een overeenkomst met de leverancier.[122] De verwerkersovereenkomst zoals genoemd in paragraaf 1.2.1.7 kan hiervoor gebruikt worden.
Op deze manier kan de zorgaanbieder voldoen aan NEN 7510, ook bij het gebruik van een cloudprovider voor de opslag van medische data.

Anno 2019 zijn naast NEN 7510 ook andere normen algemeen geaccepteerd in de gezondheidszorg zoals:[123]

- NEN 7512 voor uitwisseling van medische gegevens;
- NEN 7513 voor logging van toegang tot medische gegevens verwerkt in het kader van het dossier;
- Het MedMij-afsprakenstelsel voor de persoonlijke gezondheidsomgeving (PGO).[124]

3.6 Continuïteit van de clouddienst

De beschikbaarheid, integriteit en vertrouwelijkheid van medische data zoals opgeslagen middels een clouddienst is afhankelijk van de kwaliteit van de dienstverlening van de cloudprovider, maar ook van het voortbestaan van die cloudprovider. Indien een cloudprovider failliet gaat, is het onzeker of zijn dienstverlening wordt voortgezet. Of de medische data dan beschikbaar blijft, hangt ervan af van welke maatregelen vooraf zijn getroffen.

Denk hierbij aan maatregelen die door de afnemer zelf genomen kunnen worden, zoals het gebruikmaken van twee verschillende cloudproviders, waarbij bij beide providers de medische data op dusdanige wijze wordt opgeslagen dat deze binnen een aanvaardbare termijn beschikbaar is. Uiteraard mogen deze maatregelen niet ten koste gaan van de integriteit en vertrouwelijkheid. Zo zullen beide cloudproviders moeten voldoen aan de relevante beveiligingsnormen en moet er bij het inrichten van de uitwijkomgeving nagedacht worden over het voorkomen van verlies van data. [125]

DDoS en EDoS
De continuïteit van een clouddienst, en daarmee de beschikbaarheid van medische data die daarin zijn opgeslagen, loopt gevaar in het geval van een Distributed Denial of Service (DDoS) of Economic Denial of Service (EDoS). Het risico bestaat dat kwaadwillenden zoveel verkeer naar een clouddienst sturen dat deze daaronder bezwijkt (DDoS). Daarnaast bestaat het risico dat kwaadwillenden zich toegang verschaffen door middel van identiteitsfraude (bijvoorbeeld phisingmails), of de dienst dusdanig veel bevragen dat de daartoe gereserveerde financiële middelen van de afnemer opraken of, in het ergste geval, waardoor de afnemer in financiële problemen raakt (EDoS). Zowel DDoS als EDoS methoden zijn een

[121] NEN 7510-1 2017 p. 30.

[122] NEN 7510-2:2017, onder 15.1.1 en 15.1.2.

[123] NEN 7521 evenals NTA 7516 zijn nog in ontwikkeling, mogelijk moeten deze in de toekomst aan dit lijstje worden toegevoegd.

[124] Vanaf eind 2019 kan iedere burger een PGO krijgen op kosten van de overheid. Een PGO is bedoeld om medische gegevens in op te slaan, en om deze te delen met een of meerdere zorgaanbieders/hulpverleners. Indien een partij een PGO wil ontwikkelen en op de markt brengen dan kan hij hier subsidie voor krijgen per geleverd PGO, als er wordt voldaan aan het MedMij-afsprakenstelsel (en de leverancier MedMij-deelnemer is).

[125] https://www.faillissementsdossier.nl/nl/faillissement/121806/advanced-infotechnology-management-bv.aspx; https://tweakers.net/nieuws/73054/minister-epd-data-veilig-ondanks-faillissement-infotechnology.html.

bedreiging voor de informatiebeveiliging. Derhalve dient een cloudprovider hierop berekend te zijn en door middel van juist incidentmanagement ook te weten hoe hiermee om te gaan. Dergelijke scenario's dienen door een afnemer van een clouddienst op risico ingeschat te worden.

3.7 Toegangscontroleproces (authenticatie)

Omdat clouddiensten voor de afnemer en de door de afnemer gemachtigde legitieme gebruikers in het algemeen op afstand, via het internet, te bedienen moeten zijn, moet worden gewaarborgd dat alleen de afnemer en diens gemachtigde legitieme gebruikers technisch toegang hebben en niemand anders. Er moet dus via het internet worden geverifieerd of iemand een legitieme gebruiker is. Daar zijn vele verschillende manieren (en combinaties van manieren) voor mogelijk. Hieronder worden de minimale standaarden uiteengezet waar een cloudprovider bij de verwerking van medische data in ieder geval aan dient te voldoen.

Vormen van toegangscontrole

Er kan bijvoorbeeld gebruikgemaakt worden van iets wat alleen de legitieme gebruiker *weet* (zoals een wachtwoord), een *uniek kenmerk* van de legitieme gebruiker (bijvoorbeeld een biometrisch kenmerk zoals vingerafdruk of irisscan), en/of iets dat alleen de legitieme gebruiker *heeft* (zoals een hardwaretoken of smartcard, of een code die per SMS of via een specifieke authenticatie-app wordt verstuurd). Alle vormen van authenticatie hebben voor- en nadelen, geen ervan is perfect. Voor systemen waar een hoge mate van zekerheid is benodigd dat alleen de legitieme gebruiker toegang kan krijgen, wordt in de praktijk tegenwoordig vaak een combinatie van twee of meerdere factoren gebruikt. De beveiligingsstandaarden voor in de zorg NEN 7510 en 7513 schrijven dit ook voor[126]:

- Identiteit van gebruikers wordt vastgesteld op basis van tweefactorauthenticatie;
- Er is een toegangscontrolebeleid;
- Logbestanden worden aangemaakt ter controle van toegekende bevoegdheden;
- Logbestanden worden regelmatig gecontroleerd;
- Gebruikers worden bewust gemaakt van hun eigen verantwoordelijkheid ten aanzien van informatiebeveiliging.

Wachtwoorden

Wachtwoorden worden nog altijd het meest gebruikt voor authenticatie via het internet. Een probleem van wachtwoorden is dat zij vergeten kunnen worden, waardoor een legitieme gebruiker niet bij de data of systemen kan (verlies van beschikbaarheid). Om dat risico weer tegen te gaan, wordt vaak een methode geboden om een wachtwoord te resetten. Dat kan weer een mogelijkheid bieden voor aanvallers om binnen te komen zonder het wachtwoord te kennen (verlies van vertrouwelijkheid en mogelijk ook beschikbaarheid en integriteit, als de aanvaller data kan wijzigen of verwijderen). Het opschrijven van wachtwoorden beperkt het risico van verlies van beschikbaarheid, maar geeft juist weer een aanzienlijk risico van verlies van vertrouwelijkheid, omdat een onbevoegde het wachtwoord dan ergens kan vinden. Opschrijven wordt in het algemeen dan ook sterk afgeraden.

Aanvallers kunnen wachtwoorden ook kraken door *brute force* methodes (alle mogelijke wachtwoorden proberen), *dictionairy attacks* (alle woorden uit woordenboeken eerst proberen) *rainbow tables* (vooraf berekende hashes met hetzelfde algoritme matchen) of raden op basis van voorspelbare patronen van mensen die wachtwoorden moeten kiezen (die bijvoorbeeld zijn af te leiden uit gestolen databases met eerder gebruikte wachtwoorden). In de praktijk worden wachtwoorden gekraakt door zeer geavanceerde tools waarmee de meest waarschijnlijke wachtwoorden het eerst worden geprobeerd, totdat het wachtwoord juist blijkt. Hoe meer karakters het wachtwoord heeft en hoe meer verschillende typen karakters (hoofdletters, kleine letters, cijfers, leestekens) hoe moeilijker

[126] Zie ook het onderzoeksrapport 'Toegang tot digitale patiëntdossiers door medewerkers van het HagaZiekenhuis' van de Autoriteit Persoonsgegevens uit maart 2019.

het te kraken is (minder risico op verlies van vertrouwelijkheid). Maar vaak ook hoe moeilijker te onthouden (meer risico op verlies van beschikbaarheid).

Een andere technische maatregel om risico's bij wachtwoorden te beperken, is *hashing*. Tegenwoordig wordt het algemeen als onverantwoord beschouwd om wachtwoorden in 'plain text' op te slaan. Als een aanvaller toegang krijgt tot een database met 'plain text' wachtwoorden, is de impact daarvan dat de aanvaller alle wachtwoorden direct kent en deze kan misbruiken en ook bij andere diensten kan proberen. Om dit risico te beperken, worden wachtwoorden eerst gehasht. Via een algoritme wordt het wachtwoord veranderd in een lange brij van tekens (een hash). Hashes zijn bedoeld om nooit meer terug te herleiden te zijn tot de oorspronkelijke 'plain text'. In de database van de server wordt alleen de hash opgeslagen. Als de gebruiker een wachtwoord invoert, wordt hetzelfde algoritme gebruikt om een hash te maken. Die wordt vervolgens gecontroleerd. Alleen als het juiste wachtwoord wordt ingevoerd, komt er een hash uit die exact overeenkomt met de opgeslagen hash. Hoe sterk hashing is, hangt af van het toegepaste algoritme. Regelmatig worden hashing-algoritmen gekraakt. Het is belangrijk geen gebruik te maken van algoritmen die kunnen worden gekraakt. Op moment van schrijven worden MD5 en SHA1, hashing-algoritmen die in het verleden veel zijn toegepast, bijvoorbeeld algemeen als kraakbaar en onveilig beschouwd. Het toevoegen van 'salt' – een aantal karakters dat willekeurig wordt gegenereerd en toegevoegd iedere keer dat een wachtwoord wordt aangemaakt – zorgt ervoor dat als twee verschillende gebruikers hetzelfde wachtwoord kiezen, er toch voor iedere gebruiker een andere hash ontstaat. Salt voorkomt dat wachtwoorden met behulp van rainbow tables uit hashes herleid kunnen worden. Voor hashing van wachtwoorden raadt de gezaghebbende Open Web Application Security Project (OWASP) op moment van schrijven Argon2 aan als voorkeuralgoritme, in combinatie met salt. Ook raadt OWASP aan een minimaal aantal karakters af te dwingen bij het aanmaken van een wachtwoord, maar juist geen eisen te stellen aan het type karakters (hoofdletters, kleine letters, etc).[127]

Twee- of meerfactorauthenticatie

Onder security-experts is een vrij brede consensus waar te nemen dat wachtwoorden alleen niet (meer) genoeg zijn om de vertrouwelijkheid te borgen van gegevens waarbij verlies van vertrouwelijkheid aanzienlijke schade of ander nadeel zou veroorzaken. Naast een wachtwoord moet dan een tweede factor worden gebruikt. Volgens Microsoft voorkomt tweefactorauthenticatie 99,9% van de aanvallen op een account.[128]

Ook de andere mogelijke factoren hebben zoals gezegd nadelen. Biometrische kenmerken hebben bijvoorbeeld als nadeel dat deze niet vervangen kunnen worden. Je kunt geen nieuwe vingerafdruk of iris krijgen als aanvallers een hoge resolutie afbeelding daarvan hebben bemachtigd en deze op zo'n manier kunnen reproduceren dat de scanner denkt dat het kenmerk authentiek is. Om deze reden worden biometrische gegevens onder de AVG en UAVG als bijzondere persoonsgegevens aangemerkt en extra beschermd. Het is bijvoorbeeld niet zomaar toegestaan dat een werkgever van een werknemer eist dat deze zich met biometrische kenmerken identificeert. De werkgever moet dan aantonen dat dit noodzakelijk is voor een goede beveiliging en moet maatregelen treffen om het risico voor de werknemer te minimaliseren dat diens biometrische kenmerken bij onbevoegden terecht zouden kunnen komen en misbruikt zouden kunnen worden.

Het gebruik van een tweede factor waarbij de legitieme gebruiker iets heeft, zoals een smartcard of token, heeft als voornaamste nadeel dat de legitieme gebruiker dit kan kwijtraken. In dat geval kan verlies van beschikbaarheid optreden. De kans op verlies van vertrouwelijkheid en integriteit kan ook worden verhoogd als een onbevoegde het verloren

[127] https://cheatsheetseries.owasp.org/cheatsheets/Password_Storage_Cheat_Sheet.html.

[128] https://www.security.nl/posting/621417/Microsoft%3A+MFA+voorkomt+99%2C9+procent+van+aanvallen+op+accounts.

object kan vinden, maar dat risico blijft dan nog steeds beperkt doordat ook nog een andere factor is vereist voor toegang.

3.8 Controle op de werking van toegangscontrole (logging)

Waar met behulp van technische maatregelen de toegang tot medische data afgeschermd kan worden, dient bij het creëren van een passend beschermingsniveau eveneens aandacht geschonken te worden aan de technische controle van de werking van deze maatregelen. Deze technische controle kan uitgevoerd worden aan de hand van logging. Met behulp van een dergelijke techniek kunnen alle handelingen die plaatsvinden omtrent medische data bijgehouden worden. Zo kan inzichtelijk gemaakt worden welk persoon, op welk moment en waar vandaan toegang heeft verkregen tot de medische data. Dit controlemechanisme wordt bijvoorbeeld aanbevolen bij het constateren van datalekken.[129]

In tegenstelling tot algemene toegangscontrole en encryptie, wat preventieve beveiligingsmaatregelen zijn, is logging een reactieve beveiligingsmaatregel. Er wordt niet voorkomen dat onbevoegden toegang krijgen tot medische data. Maar goed geïmplementeerde logging zorgt voor signalering van onvolkomenheden in de beveiliging.

Bij de inrichting van logging dient rekening gehouden te worden met het feit dat loggegevens op zichzelf ook zijn aan te merken als persoonsgegevens. De toegang tot deze loggegevens dient derhalve afgeschermd te worden.

3.9 Encryptie

Naast het beveiligen van de toegang tot een clouddienst middels wachtwoorden en meerfactorauthenticatie, speelt encryptie een belangrijke rol. Zoals genoemd in paragraaf 1.2.1.8 is encryptie expliciet in de AVG opgenomen als mogelijk voorbeeld van een adequate beveiligingsmaatregel. De waarde van encryptie als zodanig is al lang bekend. Niet alleen noemt de AVG het specifiek, ook Amerikaanse gezondheidswetgeving kent het principe al langer.[130]

Encryptietechnologie is simpel gezegd het vervangen van leesbare informatie door onherkenbare informatie. Kenmerkend aan encryptie, in tegenstelling tot bijvoorbeeld hashing, is dat de onherkenbare informatie weer getransformeerd kan worden naar de oorspronkelijke leesbare informatie met behulp van een digitale sleutel.

Encryptie komt in diverse varianten voor. Zo kunnen er grofweg twee vormen van encryptie onderscheiden worden. De eerste is encryptie in transit, of end-to-end encryptie. Deze vorm van encryptie zorgt voor een versleutelde overdracht van data van punt A naar punt B. De tweede vorm is de zogenaamde encryptie at rest. Dat wil zeggen dat data niet alleen tijdens transport, maar ook tijdens opslag is voorzien van encryptie. Technisch is encryptie daarnaast te ontleden in twee hoofdthema's: het cryptografische algoritme om leesbare tekst te coderen en de sleutel om dit te bewerkstelligen en weer ongedaan te maken. Kennis van het onderscheid in encryptietechnologie is van belang bij het herkennen en mitigeren van risico's op dit vlak.

Naast de beveiligingsaspecten van encryptie dient ook rekening gehouden te worden met de praktische uitvoering daarvan. Zo vereist het uitvoeren van encryptie extra rekenkracht, dient daar speciale software voor aangeschaft en geïnstalleerd te worden en dient de betrouwbaarheid van de software continu gecontroleerd te worden.

[129] Zie Richtsnoeren voor de melding van inbreuken in verband met persoonsgegevens krachtens Verordening 2016/679, 6 februari 2018, p. 13.

[130] Zie bijvoorbeeld § 164.312 van The Health Insurance Portability and Accountability Act (HIPAA).

Het moment en de vorm van encryptie verdienen aanvullende aandacht wanneer de techniek in wordt gezet ter bescherming van medische data. Zo bieden de meest populaire cloudproviders standaard hun eigen vormen van encryptie aan. Zij bieden door hun expertise en schaalbaarheid aanzienlijke voordelen op dit gebied. Nadelig is echter het feit dat de encryptiesleutel, en decryptiesleutel, veelal in het bezit van de cloudprovider zijn wanneer deze technieken door hen aangeboden worden. Daardoor bestaat de kans dat cloudproviders gedwongen kunnen worden deze sleutel af te staan, waarmee de vertrouwelijkheid van medische data geschonden kan worden.

Het is echter niet uitsluitend de cloudprovider die zorg kan dragen voor passende encryptie. Een zorgaanbieder kan zelf encryptie toepassen op de medische data, alvorens deze naar de clouddienst wordt overgebracht. Hiermee wordt de kans dat een cloudprovider de medische data zelfstandig kan ontsleutelen aanzienlijk verkleind.

Ten aanzien van het beschermingsniveau van medische data, wat hoog dient te zijn, gecombineerd met het principe van privacy en security by design en de verplichting tot het treffen van passende waarborgen, is de conclusie dat encryptie een verplichte beveiligingsmaatregel is wanneer medische data in een clouddienst op wordt geslagen. De daarbij aanwezige risico's worden in paragraaf 4.2 nader uiteengezet.

4. Technische risico's ten aanzien van bescherming van medische data bij cloudproviders

4.1 Inleiding en scope

Nu hierboven de technische eisen zijn omschreven kan een antwoord worden geformuleerd op de volgende deelvraag:

> *Welke risico's bestaan er ten aanzien van informatieveiligheid in deze situaties[131] bij het gebruik van cloudproviders met een basis in Nederland, de Europese Unie, de Verenigde Staten en overige landen? Zijn er wezenlijke verschillen tussen lokale Nederlandse cloudproviders en providers uit de andere categorieën landen?*

Om tot een antwoord op deze vraag te komen wordt, net zoals bij de beantwoording van de juridische risico's, hieronder allereerst ingegaan op risico's die voor alle cloudproviders gelden. Ongeacht het land van vestiging. Daarna zal specifieker gekeken worden naar de verschillen tussen cloudproviders met een vestiging in Nederland en de EU, en daarbuiten.

Uit het uitgevoerde onderzoek is gebleken dat steeds vaker voor de opslag en verdere verwerking van medische data gebruik wordt gemaakt van cloudoplossingen ten opzichte van de traditionele on premise oplossingen. Belangrijke redenen om voor de cloud te kiezen zijn efficiëntie, gebruiksgemak, flexibiliteit en schaalbaarheid. Ook het beveiligingsniveau dat cloudproviders tegenwoordig kunnen bieden blijkt steeds vaker een argument om voor cloudopslag te kiezen. Juridisch en technisch is algemeen goed verdedigbaar dat cloudopslag van medische data volgens huidige wet- en regelgeving is toegestaan en dat (of omdat) daarbij in de praktijk een passend, hoog niveau van bescherming kan worden bereikt, dat in verhouding staat tot de risico's die deze bijzonder gevoelige gegevens voor betrokkenen vertegenwoordigen. Dat neemt echter niet weg dat er wel degelijk risico's bestaan.

4.2 Technische risico's algemeen

Het voornaamste technische risico bestaat uit het feit dat de beschikbaarheid, integriteit of het vertrouwelijk karakter van de medische data in de cloud (deels) teniet wordt gedaan. De oorzaken hiertoe kunnen zeer uiteenlopend zijn. Denk aan gebrekkige beveiliging in de randapparatuur waarmee de afnemer de cloudprovider benadert, een onbeveiligde verbinding tussen de afnemer en de cloudprovider, niet juist ingestelde autorisaties, inbraak door een hacker of verlies van gegevensdragers.

Onveilige implementatie van encryptie

Het doel van goed gebruik van encryptie is evident. Er wordt beoogd uitsluitend bevoegde personen toegang te geven tot de versleutelde data. Goed uitgevoerde encryptie is daarmee onmisbaar als instrument om de vertrouwelijkheid van medische data te borgen. Kijkend naar de risico's ten aanzien van het gebruik van encryptie zijn er echter diverse soorten risico's waar rekening mee gehouden dient te worden.

Ten eerste staat of valt de effectiviteit van encryptie met het gebruik van een juiste, nog veilige encryptiestandaard. Encryptiestandaarden kunnen verouderen doordat toegenomen rekenkracht van nieuwe hardware het kraken sneller mogelijk maakt, of doordat een fout in de standaard wordt ontdekt.[132] Op basis van de plan-do-check-act cyclus dient derhalve ook het gebruik van de juiste standaard continu gecontroleerd te worden.

[131] Zie paragraaf 3.1.

[132] Zoals bijvoorbeeld het geval was met Hearthbleed in april 2014: https://www.nu.nl/internet/3748811/heartbleed-moet-weten-grootste-internetlek-ooit.html.

Ten tweede bestaat het risico op misbruik, of onzorgvuldig gebruik, van de encryptiesleutel. Inherent aan encryptie als technologie is het feit dat er sleutels bestaan om bestanden te versleutelen en ook weer te ontsleutelen. De kortste weg tot het verkrijgen van data die volgens een recente en veilige encryptiestandaard is versleuteld is immers het verkrijgen van toegang tot de sleutel. Kijkend naar de huidige stand van encryptie bij de meest populaire (EU en niet-EU) cloudproviders is te concluderen dat deze allen standaard encryptie in transit en at rest aanbieden.[133] Allen faciliteren echter zelf de techniek en hebben daarmee de beschikking over de encryptiesleutel. Ook hier geldt het eerder opgemerkte controleverlies van het gebruik van een clouddienst tegenover een on premise oplossing. De sleutel wordt ondergebracht bij een derde partij. Hoewel cloudproviders er vanzelfsprekend baat bij hebben om de encryptie zo goed en veilig mogelijk uit te voeren, bestaat het theoretische risico dat zij door misbruik van de encryptiesleutel onbevoegde toegang tot medische data mogelijk maken.

Ten derde kan een onjuiste implementatie van encryptie de BIV van medische data aantasten wanneer de encryptiesleutel, op wat voor manier dan ook, verloren gaat. Hiermee wordt niet alleen de beschikbaarheid, maar ook de integriteit van de medische data aangetast. Wanneer de data eenmaal goed versleuteld is, is het praktisch niet mogelijk om de encryptie zonder sleutel ongedaan te maken. Daarmee kan de medische data als verloren worden beschouwd. Goede technische inrichting en een managementproces ten aanzien van het beheer van een sleutel maakt dit echter tot een risico met een lage waarschijnlijkheid. Dat neemt niet weg dat het risico wel zeer verstrekkende gevolgen kan hebben wanneer het zich voordoet.[134]

Veroudering van encryptie

Naast onjuiste implementatie en onzorgvuldig beheer van encryptie bestaat een tweede risico waardoor de BIV van medische data aangetast zou kunnen worden. Encryptie (zowel in transit als at rest) zorgt voor het onbegrijpelijk maken van medische data voor onbevoegden die niet over de decryptiesleutel beschikken. Encryptie op zichzelf is echter geen maatregel om onbevoegden de toegang tot data te ontzeggen. Daartoe dienen bijvoorbeeld wachtwoorden, meerfactorauthenticatie en toegangscontrole. Wanneer deze technieken niet juist of volledig worden toegepast bestaat het risico dat onbevoegden toegang krijgen tot databases met versleutelde medische data. En wanneer het hen lukt om de versleutelde data uit de clouddienst te onttrekken, bijvoorbeeld door deze te kopiëren en elders op te slaan, kan er geprobeerd worden om de data zonder sleutel te decrypteren. Wanneer een adequate encryptiestandaard is gebruikt zal dit praktisch onmogelijk zijn. Zoals hierboven echter aangegeven, kunnen standaarden naar verloop van tijd verouderen of gekraakt worden. Een geduldige onbevoegde kan in dat geval alsnog toegang tot versleutelde medische data krijgen zonder de beschikking te hebben over de oorspronkelijke sleutel.[135] Zowel encryptie van een cloudprovider als een eigen laag van encryptie daarbovenop door de afnemer van een cloudprovider beschermen medische data niet tegen dit risico. Daartoe zijn andere maatregelen noodzakelijk, zoals adequate toegangsbescherming.

DDoS en EDoS

Diverse maatregelen dienen genomen te worden om de beschikbaarheid van medische data te waarborgen. Hiermee wordt bijgedragen aan het niveau van informatiebeveiliging. Deze beschikbaarheid wordt aangetast wanneer medische data door overbelasting van een

[133] Zie bijvoorbeeld https://docs.aws.amazon.com/AmazonS3/latest/dev/serv-side-encryption.html, https://cloud.google.com/security/encryption-at-rest/, https://docs.microsoft.com/en-us/azure/security/fundamentals/encryption-overview en https://www.rackspace.com/security/tools/data-protection.

[134] Zie ook Cloud Computing Security Risk Assessment, ENISA, 20 november 2009, p. 41.

[135] Dat het risico reëel is blijkt bijvoorbeeld uit het feit dat Edward Snowden inzichtelijk heeft gemaakt dat de NSA encrypte data op heeft geslagen met het oog op mogelijke toekomstige ontsleuteling: https://www.forbes.com/sites/andygreenberg/2013/06/20/leaked-nsa-doc-says-it-can-collect-and-keep-your-encrypted-data-as-long-as-it-takes-to-crack-it/#36c9f357b07d en https://www.theguardian.com/us-news/the-nsa-files.

clouddienst hinder ondervindt. Ook voor dit risico geldt echter dat de gemiddelde clouddienst hier beter tegen is beveiligd dan een eigen on premise oplossing.

Toegangsproces

Bij het gebruik van iedere clouddienst, dient niet alleen de clouddienst en bijbehorende cloudprovider onder de loep genomen te worden. Minstens zo belangrijk is het managen van het toegangsproces waarmee toegang verkregen kan worden tot de medische data in de cloud. Afnemers van clouddiensten spelen hierbij een belangrijke rol, maar uiteraard de cloudproviders zelf ook. Diverse cloudproviders omschrijven dit proces als een 'shared responsibility'. Een clouddienst kan volgens de beste en meest recente technische processen beveiligd zijn, maar wanneer een gebruiker van de dienst onzorgvuldig omgaat met zijn toegangs- en autorisatiegegevens, kunnen onbevoegden alsnog toegang verkrijgen. Overigens is dit geen risico dat specifiek voor clouddiensten geldt. Ook wanneer medische data on premise op worden geslagen geldt dit als een beveiligingsrisico.

Maatregelen

Er zijn wel technische maatregelen mogelijk om bovenstaande risico's te minimaliseren. Bijvoorbeeld het zelf toepassen van encryptie door de afnemer van de cloudprovider (zoals een ziekenhuis) kan bescherming bieden tegen zowel het risico van inzage door de cloudprovider zelf als door buitenlandse autoriteiten. Om dit goed te kunnen doen is expertise vereist, waarbij bijvoorbeeld goed opgelet moet worden dat betrouwbare algoritmen worden gebruikt, het versleutelingsproces zo wordt ingericht dat de cloudprovider geen sleutels kan onderscheppen (dus in principe vóór overdracht van de data naar de cloudprovider) en dat de encryptiesleutels niet verloren gaan.

Het bewaren van (eveneens goed geëncrypteerde) back-ups (kopieën) bij een andere partij dan de cloudprovider, kan verder bescherming bieden tegen het risico dat data bij de cloudprovider om wat voor reden dan ook onbeschikbaar zou raken. Tegelijkertijd is hiermee een overmatige afhankelijkheid van een specifieke provider ('vendor lock-in') te vermijden. Als de 'back-up-provider' alleen in Nederland of de EU actief is, kan daarmee zelfs het (relatief beperkte) risico van een handelsverbod of vergelijkbare maatregel uit de VS worden weggenomen of geminimaliseerd. Vanuit veiligheidsperspectief zal cloudopslag met dergelijke (extra) maatregelen verreweg te prefereren zijn boven een situatie waar wordt gekozen voor opslag in Nederland maar onvoldoende beveiliging wordt geboden tegen toegang door kwaadwillenden of verlies van data door brand, rampen, defecte apparatuur of andere oorzaken.

Het blijft wel steeds aan de verwerkingsverantwoordelijke om in detail te beoordelen in hoeverre bovengenoemde encryptiemaatregelen in de specifieke situatie haalbaar en passend zijn. Als dergelijke encryptie om vertrouwelijkheid beter te waarborgen juist risico's zou veroorzaken voor de beschikbaarheid of integriteit (juistheid) van de data, bijvoorbeeld vanwege verlies van encryptiesleutels of fouten bij het encrypteren of decrypteren, dan zou bekeken moeten worden of de voordelen wel opwegen tegen de nadelen. Dat zal steeds van de specifieke situatie, data en verwerkingen afhangen.

Ter illustratie de volgende afweging die in ieder geval opgenomen dient te worden in een goed uitgevoerde DPIA wanneer het voornemen bestaat om medische data van Nederlandse patiënten in de cloud op te slaan. Als de data bijvoorbeeld nodig is om patiënten de juiste behandeling en medicijnen toe te dienen, dan lijkt het in het algemeen nog belangrijker om de beschikbaarheid en integriteit van deze gegevens te waarborgen dan de vertrouwelijkheid. In dat geval zou onbeschikbaarheid of onjuistheid immers ziekte, letsel of zelfs dood tot gevolg kunnen hebben, terwijl inzage door een buitenlandse autoriteit, cloudprovider of andere partij weliswaar onwenselijk is maar in het algemeen aanzienlijk minder zware nadelige gevolgen zal hebben. In dat geval mogen ook meer back-up maatregelen worden verwacht.

4.3 Technische risico's Nederland, de EU en buiten de EU

Uit het uitgevoerde onderzoek zijn geen specifieke technische risico's gebleken waarbij een territoriaal onderscheid gemaakt kan worden.

5. Internationaal onderscheid; het vertrouwen in cloudproviders

Welk onderscheid moet gemaakt worden tussen cloudproviders met een basis binnen Nederland, de Europese Unie, de Verenigde Staten en overige landen ten aanzien van deze technische- en juridische eisen?

In voorgaande hoofdstukken is per vraag reeds een internationaal onderscheid gemaakt. Gedurende de uitvoering van dit onderzoek naar de wenselijkheid van het gebruik van niet-EU cloudplatforms voor de opslag van medische data van Nederlandse patiënten en de daarbij horende technische en juridische risico's, is een aanvullende constatering gedaan. Een constatering die niet direct ziet op het beantwoorden van de gestelde vragen, maar die wel degelijk het vermelden waard is. Er blijkt sprake te zijn van een vertrouwenskwestie ten aanzien van niet-EU cloudproviders.

5.1 Vertrouwen

Tijdens het uitgevoerde onderzoek is geconstateerd dat nog altijd niet iedereen overtuigd is van de veiligheid van de internationale cloud voor data die zo gevoelig is als medische data. Belangrijke en legitieme zorgen zijn onder andere (i) in hoeverre cloudproviders de opgeslagen data zelf zouden kunnen inzien en voor andere doeleinden gebruiken, (ii) de mate en situaties waarin (buitenlandse) politie, inlichtingendiensten en andere autoriteiten (toegang tot) de data kunnen opeisen en (iii) in hoeverre kwaadwillenden (zoals hackers) de beschikbaarheid, integriteit of vertrouwelijkheid van de data kunnen aantasten.

Opslag van medische data in de cloud mag geen afbreuk doen aan het *vertrouwen* van patiënten dat hun medische gegevens veilig zijn. Dat vertrouwen is immers nodig om te waarborgen dat zij zich vrij zullen voelen om zorg te zoeken als zij dat nodig kunnen hebben. Uit krantenkoppen als "Ook jouw medische data liggen nu bij Google", blijkt wel dat het vertrouwen in dergelijke providers op dit moment niet optimaal is. De gestelde Kamervragen die aanleiding vormden voor dit rapport bevestigen dat ook, evenals de meningen van diverse zorgpartijen die in dit onderzoek zijn geraadpleegd. Dat raakt ook aan de wenselijkheid van de opslag van medische gegevens bij dergelijke cloudproviders.

5.2 Oorzaken

De oorzaken voor deze vertrouwenskwestie, die gedurende dit onderzoek zijn geconstateerd, zijn hoofdzakelijk terug te voeren naar de angst dat buitenlandse autoriteiten toegang krijgen tot de opgeslagen medische data.

Ondanks state of the art beveiligingsmaatregelen die de in Nederland populaire cloudproviders treffen, juridische toezeggingen dat medische data niet zonder juridische grond wordt afgestaan, sluitende wetgeving in de vorm van de AVG die onrechtmatige toegang verbiedt en een sluitend systeem van handhaving hierop, lijkt vertrouwen één van de oorzaken waarom in sommige gevallen zeer terughoudend om wordt gegaan met de gang naar een clouddienst als het gaat om opslag van medische data.

6. Afkortingen en definities

Autoriteit: iedere publieke autoriteit of overheidsinstantie, bijvoorbeeld de politie/FBI, een toezichthouder (zoals een consumentenautoriteit, privacy-autoriteit of andere toezichthouder), of rechter;

AVG: Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (Algemene verordening gegevensbescherming);

Betrokkene: een geïdentificeerde of identificeerbare natuurlijke persoon;

BIV: beschikbaarheid, integriteit, vertrouwelijkheid;

BW: Burgerlijk wetboek;

CLOUD Act: Clarifying Lawful Overseas Use of Data Act;

Clouddienst: iedere dienst of ieder product waarbij klantdata is of wordt opgeslagen en eventueel verder verwerkt op een samenhangend geheel van digitale opslag- en rekencapaciteit (veelal bestaande uit diverse servers die via een netwerk zijn verbonden en gevirtualiseerd tot een (schaalbaar) geheel) en voor de klant of door de klant gemachtigde gebruikers via het internet beschikbaar worden gehouden;

Cloudplatform: het totaalaanbod van clouddiensten van een cloudprovider;

Cloudprovider: leverancier van een clouddienst of cloudplatform;

DPIA: data protection impact assessment, of gegevensbeschermingseffectbeoordeling, zoals bedoeld in artikel 35 AVG;

Datalek: Een inbreuk in verband met persoonsgegevens zoals bedoeld in artikel 4 onder 12 AVG;

Encryptie: het coderen (versleutelen) van gegevens op basis van een algoritme;

Encryptie at rest: encryptie van gegevens die zijn opgeslagen;

Encryptie in transit: encryptie van gegevens die worden verstuurd;

EDPB: European Data Protection Board (in het Nederlands Het Europees Comité voor gegevensbescherming) de opvolger van de artikel 29 werkgroep, waarin de Europese privacytoezichthouders in zijn verenigd. De EDPB draagt bij aan de consequente toepassing van regels voor gegevensbescherming in de gehele (EU). Ook bevordert de EDPB de samenwerking tussen de privacytoezichthouders in de EU;

EU: Europese Unie. Onder Europese Unie wordt in de context van dit onderzoek begrepen de Europese Unie plus Noorwegen, Liechtenstein en IJsland, aangezien deze landen ook onder het toepassingsbereik van de AVG vallen.

EVRM: Europees Verdrag voor de Rechten van de Mens;

FISA: Foreign Intelligence Surveillance Act;

Gw: Grondwet voor het Koninkrijk der Nederlanden van 24 augustus 1815;

Klantdata: alle gegevens die voor, namens of ten behoeve van de klant via de clouddienst worden opgeslagen (en eventueel verder verwerkt);

Medische data: persoonsgegevens die verband houden met de fysieke of mentale gezondheid van een natuurlijke persoon, waaronder gegevens over verleende gezondheidsdiensten waarmee informatie over zijn gezondheidstoestand wordt gegeven. Alsmede persoonsgegevens die verbandhouden met de overgeërfde of verworven genetische kenmerken van een natuurlijke persoon die unieke informatie verschaffen over de fysiologie of de gezondheid van die natuurlijke persoon en die met name voortkomen uit een analyse van een biologisch monster van die natuurlijke persoon. En tevens persoonsgegevens die het resultaat zijn van een specifieke technische verwerking met betrekking tot de fysieke, fysiologische of gedragsgerelateerde kenmerken van een natuurlijke persoon op grond waarvan eenduidige identificatie van die natuurlijke persoon mogelijk is of wordt bevestigd, zoals gezichtsafbeeldingen of vingerafdrukgegevens;

Model clauses: contractuele standaardbepalingen die zijn opgesteld om een waarborg te bieden voor verwerking van persoonsgegevens buiten de EU, zoals bedoeld in artikel 46 AVG;

On premise: ICT-infrastructuur op locatie van de partij (zoals een zorgverlener) zelf;

Persoonsgegevens: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon („de betrokkene"); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon;

Pseudonimisering: het verwerken van persoonsgegevens op zodanige wijze dat de persoonsgegevens niet meer aan een specifieke betrokkene kunnen worden gekoppeld zonder dat er aanvullende gegevens worden gebruikt, mits deze aanvullende gegevens apart worden bewaard en technische en organisatorische maatregelen worden genomen om ervoor te zorgen dat de persoonsgegevens niet aan een geïdentificeerde of identificeerbare natuurlijke persoon worden gekoppeld;

Sv: Wetboek van strafvordering;

UAVG: Wet van 16 mei 2018, houdende regels ter uitvoering van Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming) (PbEU 2016, L 119) (Uitvoeringswet Algemene verordening gegevensbescherming);

Verwerker: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt;

Verwerking van persoonsgegevens: een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens;

Verwerkingsverantwoordelijke: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen,

het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt; wanneer de doelstellingen van en de middelen voor deze verwerking in het Unierecht of het lidstatelijke recht worden vastgesteld, kan daarin worden bepaald wie de verwerkingsverantwoordelijke is of volgens welke criteria deze wordt aangewezen;

WGBO: Wet op de geneeskundige behandelingsovereenkomst;

Wiv: Wet op de inlichtingen- en veiligheidsdiensten.

7. Bronnen

Wet- en regelgeving

- Algemene verordening gegevensbescherming;
- Besluit elektronische gegevensverwerking door zorgaanbieders;
- Burgerlijk Wetboek;
- Clarifying Lawful Overseas Use of Data Act;
- Europees Verdrag voor de Rechten van de Mens;
- Foreign Intelligence Surveillance Act;
- Grondwet voor het Koninkrijk der Nederlanden;
- Handvest van de grondrechten van de Europese Unie;
- Health Insurance Portability and Accountability Act;
- Uitvoeringswet Algemene verordening Gegevensbescherming;
- Verdrag inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken;
- Verdrag tussen het Koninkrijk der Nederlanden en de Verenigde Staten van Amerika aangaande wederzijdse rechtshulp in strafzaken;
- Verordening Europese Verstrekkings- en Bewaringsbevelen voor e-evidence;
- Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg;
- Wet op de geneeskundige behandelingsovereenkomst;
- Wet op de inlichten- en veiligheidsdiensten;
- Wetboek van Strafvordering.

Autoriteit Persoonsgegevens

- Autoriteit Persoonsgegevens, 'Praktijkgids: Patiëntgegevens in de cloud', 7 juli 2017;
- Autoriteit Persoonsgegevens, 'Richtsnoeren: Beveiliging van persoonsgegevens', 1 maart 2013.

WP 29 (EDBP)

- Artikel 29-Werkgroep, 'Advies 04/2014 betreffende de bewaking van elektronische communicatie voor de doeleinden van inlichtingen en openbare veiligheid', 10 april 2014;
- Artikel 29-Werkgroep, 'Advies 05/2012 over cloud computing', 1 juli 2012;
- Artikel 29-Werkgroep, 'Advies 02/2015 over de CSIG-gedragscode inzake cloudcomputing', 22 september 2015;
- Artikel 29-Werkgroep, 'Advies 03/2015 inzake de ontwerprichtlijn betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens', 1 december 2015;
- Artikel 29-Werkgroep, 'Advies 1/2010 over de begrippen "voor de verwerking verantwoordelijke en "verwerker"', 16 februari 2010.

Kamerstukken

- Aanhangsel Handelingen II 2018/19, 2458 (Antwoorden op Kamervragen van het Kamerlid Hijink (SP) over het bericht 'Ook jouw medische data liggen nu bij Google' (2019Z06461));
- Kamerstukken II 2018/19, 27529, 164 (Kamerbrief over data laten werken voor gezondheid);
- Kamerstukken II 2018/19, 27529, 189 (Kamerbrief over elektronische gegevensuitwisseling).

Overige documentatie

- CISPE.Cloud, 'Buying Cloud Services in Public Sector', 3 juni 2019
- EU Data Protection Code of Conduct for Cloud Service Providers, maart 2019;
- European Network and Information Security Agency, 'Cloud Computing Security Risk Assessment', 20 november 2009;
- KNMG, 'Handreiking Beroepsgeheim en politie/justitie', februari 2012;
- Nationaal Cyber Security Centrum, 'Whitepaper NCSC Cloudcomputing & Security', januari 2012;
- National Institute of Standards and Technology, 'The NIST Definition of Cloud Computing, Recommendations of the National Institute of Standards and Technology', 28 september 2011;
- N. Klaassen & D. Bremmer, 'Data honderdduizenden patiënten in stilte naar Google verhuisd', Algemeen Dagblad 30 maart 2019;
- N. Klaassen & D. Bremmer, 'Ook jouw medische data liggen nu bij Google', Algemeen Dagblad 30 maart 2019;
- Patiëntenfederatie Nederland, 'Het Patiëntgeheim: position paper Patiëntenfederatie Nederland', 17 januari 2019.

Geconsulteerde partijen

Bij de uitvoering van het onderzoek zijn de volgende (markt)partijen geconsulteerd:

- Amazon;
- DINL;
- Google;
- ISPConnect;
- Microsoft;
- MRDM;
- National Health Service;
- NVZ;
- OIZ;
- SCOPE;
- Vektis.

Deel C. Aanbevelingen voor cloudproviders, afnemers en overheden

- Transparantie. Wees ten aanzien van al uw clouddiensten volledig transparant over:
    - Geschikt voor medische data? Welke van uw clouddiensten u zelf als geschikt of ongeschikt beschouwt voor de opslag en eventuele verdere verwerking van medische data (en waarom);
    - Beschikbaarheid. De mate waarin de clouddienst in het afgelopen jaar, maand en/of andere periode beschikbaar is geweest;
    - Garanties. De mate waarin u de beschikbaarheid van de clouddienst garandeert;
    - Beveiliging en BIV. De manieren waarop met gebruikmaking van de clouddienst de beschikbaarheid, integriteit en vertrouwelijkheid van klantdata is gewaarborgd. Maak daarbij onderscheid tussen waarborgen die standaard in de dienst zitten en de configuraties of opties die door de gebruiker gekozen kunnen worden;
    - Toegang tot data. In hoeverre u[136] klantdata kunt inzien, decrypteren en/of decrypteerbaar maken, buiten de ondubbelzinnige instructies[137] van de klant. Maak hierbij ook duidelijk:
        - Doeleinden. In hoeverre u dit juridisch zou mogen (bijvoorbeeld om uw diensten te verbeteren) of moeten (bijvoorbeeld om aan vorderingen van politie of inlichtingendiensten te voldoen);
        - Maatregelen cloudprovider. Welke maatregelen u zelf neemt of door de klant in de clouddienst ingesteld kunnen worden om dit technisch onmogelijk te maken en de eventuele beperkingen daarvan;
        - Maatregelen klant zelf. Welke maatregelen door de klant zelf genomen kunnen worden om de mogelijkheid hiervan technisch verder te minimaliseren.
    - Opslaglocaties. Welke mogelijkheden u biedt om te kiezen en te beperken waar klantdata wordt opgeslagen en eventueel verder verwerkt;
    - Garanties mbt opslaglocatie. In hoeverre u garandeert dat klantdata (in ongeëncrypteerde of decrypteerbare vorm) uitsluitend kan worden opgeslagen en eventueel verder verwerkt in het door de klant gekozen gebied;[138]
    - Vestigingslocaties en organisatiestructuur. Uw organisatiestructuur, zoals waar uw hoofdkantoor en dochter- of zusterondernemingen zijn gevestigd, welke beslissingsbevoegdheden deze vestigingen onderling hebben en de eventuele implicaties daarvan voor de veiligheid van klantdata;
    - Wetgeving voor toegang tot data. De wetgeving, in alle landen waar u aan onderworpen bent, die ertoe kan leiden dat enige partij (toegang tot) klantdata (in ongeëncrypteerde of decrypteerbare vorm) kan verkrijgen

[136] Onder 'u' wordt in deze aanbevelingen steeds ook verstaan iedere andere (gelieerde) entiteit binnen dezelfde groep.

[137] Dit wil hier zeggen: een ondubbelzinnige verklaring of handeling waaruit onmiskenbaar de wil van de klant (tot een bepaalde verwerking) blijkt. Enkel het aanvaarden van standaardcontracten en/of -voorwaarden van de cloudprovider is hiervoor niet voldoende.

[138] Behoudens ondubbelzinnige instructies namens de afnemer zelf tot verwerking buiten het gebied (zoals door de afnemer geautoriseerde gebruikers die data benaderen vanuit andere locaties).

zonder inzet van een traditioneel rechtshulpverdrag. Maak daarbij onderscheid in:

- **Verschoningsrecht**. Landen waar u niet gehouden kunt worden tot verstrekking van (toegang tot) medische klantdata vanwege uw afgeleide verschoningsrecht;
- **Geen verschoningsrecht**. Landen waar u geen afgeleid verschoningsrecht hebt of u desondanks toch tot verstrekking van (toegang tot) medische klantdata kunt worden gedwongen. Wijs klanten hierbij ook op eventuele maatregelen die u en/of uw klant zou kunnen nemen om te waarborgen dat u feitelijk geen mogelijkheid zult hebben om klantdata in ongeëncrypteerde of decrypteerbare vorm te verstrekken.

- **Certificeringen en scope**. Uw certificering(en), zoals NEN 7510, 7512, 7513, ISO 27001/2, ISO 27018, ISO 27701, etc, en de scope daarvan;
- **Portabiliteit**. De mogelijkheden en faciliteiten voor portabiliteit, d.w.z. om data uit de clouddienst te migreren naar een andere dienst of omgeving, met zo min mogelijk moeite, tijd, kosten, of andere drempels;
- **Open source**. De mate waarin de diensten bestaan uit open source oplossingen, die ook in andere omgevingen geïmplementeerd kunnen worden;

- **Verwerkersovereenkomst**. Sluit een verwerkersovereenkomst die duidelijk is en overeenstemt met informatie die u elders verstrekt over uw diensten en uw opslag en eventuele verdere verwerking van klantdata;
- **Keuzevrijheid klant gebruik klantdata**. Zorg ervoor dat de klant weet in hoeverre u klantdata zou kunnen gebruiken of inzien om uw diensten te verbeteren of ontwikkelen en bied daarbij een eenvoudige manier aan de klant om dat te voorkomen;
- **Verzoeken om klantdata doorverwijzen naar klant**. Verwijs iedere partij die u om (toegang tot) klantdata verzoekt of dat van u vordert door naar de klant zelf, tenzij dit onmiskenbaar verboden is onder het geldende recht:
  - **Geheimhouding**. Geef daarbij aan dat u de data alleen opslaat voor of namens de klant en de klant (volledige) geheimhouding van u verwacht;
  - **Verschoningsrecht**. Maak daarbij gebruik van het afgeleide verschoningsrecht waar dit van toepassing is. Vraag klanten voor dit doeleinde om aan te geven of zij verschoningsgerechtigde zijn (en zo nodig dat te bewijzen). Neem dit op in de verwerkersovereenkomst voor clouddiensten die specifiek zijn bedoeld voor verwerking van medische data of sta toe dat dit wordt toegevoegd op verzoek van een klant die zorgverlener is;
  - **Notificatie klant**. Als u toch verplicht bent (toegang tot) klantdata te verstrekken, stel de klant daar dan zo snel mogelijk van op de hoogte, tenzij dit onmiskenbaar verboden is onder het geldende recht.
- **Organisatiestructuur**. Als u een vestiging heeft in een land buiten de EU waar autoriteiten niet zijn gebonden aan de beperkingen en waarborgen die in Nederland en elders in de EU gelden voor het opvragen of inzien van klantdata, waaronder in het bijzonder medische data en het gerelateerde (afgeleide) verschoningsrecht, probeer er dan voor te zorgen dat deze vestiging feitelijk geen beschikking kan hebben of verstrekken over de klantdata die voor of namens klanten in de EU wordt verwerkt. Wees daarbij transparant over de mate waarin dit in de praktijk mogelijk is en eventuele risico's;

- Certificering specifiek voor medische data. Overweeg het naleven van en certificeren tegen nieuwe gedragscodes die specifiek zijn of worden ontwikkeld voor cloudplatforms waarin medische data kan worden opgeslagen en eventueel verder worden verwerkt.
- Overige certificeringsmechanismes. Overweeg het bieden van of conformeren aan controlemechanismes die voorzien in controles die zo doorlopend (of frequent en onverwacht) mogelijk zijn en worden uitgevoerd door zo onafhankelijk en deskundig mogelijke partijen, op een zo uniform mogelijke manier.

- Risicoanalyse. Voer een deugdelijke risicoanalyse uit voor de opslag en eventuele verdere verwerking van medische data.
- Alternatieve oplossingen vergelijken. Vergelijk de risico's bij verschillende cloudproviders met elkaar en met alternatieve methoden voor opslag en verdere verwerking van data, zoals on-premise of een combinatie van verschillende methoden ('hybride');
- Houd bij uw risicoanalyse rekening met:
    - Geschikt voor medische data? Of de clouddienst volgens de cloudprovider zelf geschikt is voor opslag en verdere verwerking van medische data;
    - Beschikbaarheid van de dienst. De mate waarin de clouddienst in het afgelopen jaar, maand en/of andere periode beschikbaar is geweest;
    - Garanties. De mate waarin de cloudprovider de beschikbaarheid van de clouddienst juridisch garandeert;
    - Beveiliging en BIV. De manieren waarop de clouddienst de beschikbaarheid, integriteit en vertrouwelijkheid (BIV) van klantdata waarborgt. Let daarbij ook op welke waarborgen standaard in de dienst zitten en welke configuraties of opties door de gebruiker gekozen kunnen worden;
    - (Verwerkers)Overeenkomst. De inhoud van de overeenkomst voor het gebruik van de clouddienst, waaronder in het bijzonder de vereiste verwerkersovereenkomst;
    - Toegang tot data. In hoeverre de cloudprovider klantdata kan inzien, decrypteren en/of decrypteerbaar maken, buiten uw ondubbelzinnige instructies[139]. Let hierbij ook op:
        - Doeleinden. In hoeverre de cloudprovider dit juridisch zou mogen (bijvoorbeeld om de diensten te verbeteren) of moeten (bijvoorbeeld om aan vorderingen van politie of inlichtingendiensten te voldoen);
        - Maatregelen cloudprovider. Welke maatregelen de cloudprovider zelf neemt of in de clouddienst ingesteld kunnen worden om dit technisch onmogelijk te maken en de eventuele beperkingen daarvan;
        - Eigen maatregelen. Welke maatregelen u zelf zou kunnen nemen om de mogelijkheid hiervan technisch verder te minimaliseren.
    - Opslaglocatie kiezen. Welke mogelijkheden de clouddienst biedt om te kiezen en te beperken waar klantdata wordt opgeslagen en eventueel verder kan worden verwerkt;
    - Garanties mbt opslaglocatie. In hoeverre de cloudprovider garandeert dat klantdata (in ongeëncrypteerde of decrypteerbare vorm) uitsluitend kan worden opgeslagen en eventueel verder verwerkt in het door u gekozen gebied;[140]

[139] Dit wil hier zeggen: een ondubbelzinnige verklaring of handeling waaruit onmiskenbaar de wil van de klant (tot een bepaalde verwerking) blijkt. Enkel het aanvaarden van standaardcontracten en/of -voorwaarden van de cloudprovider is hiervoor niet voldoende.

[140] Behoudens ondubbelzinnige instructies namens de afnemer zelf tot verwerking buiten het gebied (zoals door de afnemer geautoriseerde gebruikers die data benaderen vanuit andere locaties).

- Vestigingslocaties en organisatiestructuur cloudprovider. De organisatiestructuur van de cloudprovider, zoals waar het hoofdkantoor en de dochter- of zusterondernemingen zijn gevestigd, welke beslissingsbevoegdheden deze vestigingen hebben en de implicaties daarvan voor de veiligheid van uw data;
- Wetgeving voor toegang tot data. De wetgeving, in alle landen waar de cloudprovider gevestigd is, die ertoe kan leiden dat autoriteiten of enige andere partij (toegang tot) klantdata (in ongeëncrypteerde of decrypteerbare vorm) kan verkrijgen. Maak daarbij onderscheid in:
  - Verschoningsrecht. Landen waar de cloudprovider niet gehouden kan worden tot verstrekking van (toegang tot) medische klantdata vanwege het afgeleide verschoningsrecht;
  - Geen verschoningsrecht. Landen waar de cloudprovider geen afgeleid verschoningsrecht heeft of desondanks toch tot verstrekking van (toegang tot) medische klantdata kunt worden gedwongen. Overweeg in dit geval maatregelen om te waarborgen dat de cloudprovider feitelijk geen mogelijkheid zal hebben om klantdata in ongeëncrypteerde of decrypteerbare vorm te verstrekken.
- Beleid cloudprovider ivm verzoeken tot data. Het beleid van de cloudprovider over hoe wordt omgegaan met verzoeken of vorderingen van autoriteiten tot het verstrekken van (inzage in) klantdata. Ook van belang hierbij is de hoeveelheid verzoeken of vorderingen van autoriteiten die de cloudprovider daadwerkelijk heeft ontvangen in het afgelopen jaar of andere periode die geschikt is om het risico voor de toekomst uit af te leiden.
- Certificeringen en scope. De certificering(en) van de cloudprovider, zoals NEN 7510, 7512, 7513, ISO 27001/2, ISO 27018, ISO 27701, etc, en de scope daarvan;
- Portabiliteit. De mogelijkheden en faciliteiten om data uit de clouddienst te migreren naar een andere dienst of omgeving, met zo min mogelijk moeite, tijd, kosten, of andere drempels;
- Open source. De mate waarin de clouddiensten bestaan uit open source oplossingen, die ook zonder problemen bij andere cloudproviders of in andere omgevingen geïmplementeerd kunnen worden;

- Cloudprovider enkel in EU? Overweeg in hoeverre een cloudprovider die enkel in de EU is gevestigd, aan uw eisen en wensen kan voldoen;
- Cloudprovider buiten EU? Als u een cloudprovider wilt gebruiken die behalve in de EU ook daarbuiten is gevestigd, kies dan bij voorkeur voor een cloudprovider die enkel is gevestigd in landen waar verstrekking van medische data aan autoriteiten geweigerd kan worden door het (afgeleide) verschoningsrecht, of tref (aanvullende) technische maatregelen on te voorkomen dat de cloudprovider medische data kan inzien of inzage kan verstrekken aan anderen;
- Geen cloudprovider zonder vestiging in EU. Gebruik geen cloudprovider die geheel geen vestiging of opslaglocatie heeft in de EU;
- Verwerkersovereenkomst. Sluit een verwerkersovereenkomst met de cloudprovider, waarin onder andere expliciet is bepaald dat de cloudprovider uw klantdata enkel op uw ondubbelzinnige instructies mag verwerken en niet voor eigen of wat voor andere doeleinden dan ook;
- Afspraken over verschoningsrecht. Verg van uw cloudprovider, bijvoorbeeld in de verwerkersovereenkomst, dat deze ieder verzoek of vordering om uw klantdata

afwijst en aan u doorzet, tenzij dit onmiskenbaar niet is toegestaan onder het toepasselijke recht. Verg daarnaast dat de cloudprovider zich beroept op het afgeleide verschoningsrecht om verzoeken of vorderingen voor (toegang tot) *medische* klantdata af te wijzen;

- Twee- of meerfactorauthenticatie. Maak gebruik van twee- of meerfactorauthenticatie voor toegang tot iedere clouddienst waarin medische data wordt verwerkt;
- Logging. Maak ook gebruik van passende logging om alle toegang tot en verwerking van medische data te kunnen controleren;
- Encryptie. Maak gebruik van versleuteling van verkeer tussen de gebruiker en de cloudprovider en versleutelde opslag bij de cloudprovider zelf;
    - Sleutel niet bij cloudprovider? Maak zoveel mogelijk gebruik van cryptografische maatregelen waarbij de sleutel altijd buiten de macht van de cloudprovider blijft, om het risico te beperken of weg te nemen dat de cloudprovider uw klantdata zou kunnen gebruiken of (inzage) aan anderen kan verstrekken buiten uw ondubbelzinnige instructies om:
- Tweede cloudprovider? Overweeg, in geval van zeer hoge eisen aan de beschikbaarheid en integriteit van de medische data die u verwerkt, om gebruik te maken van een tweede cloudprovider voor back-up:
    - Zorg daarbij dan wel dat er zo min mogelijk tijd nodig is om over te stappen en dat in geval van een calamiteit bij de andere cloudprovider geen of zo min mogelijk verlies van beschikbaarheid of integriteit van uw klantdata kan optreden;
    - Overweeg eventueel een provider die alleen actief is in de landen waar u zelf ook actief bent of in elk geval niet in landen waar een risico bestaat op overheidsmaatregelen of sancties die verlies van beschikbaarheid of integriteit van data tot gevolg kan hebben.

Aanbevelingen voor overheden

- Cloud wenselijk mits. Sta het gebruik van clouddiensten voor medische data toe en moedig dat aan, op voorwaarde dat de aanbevelingen in dit rapport worden nageleefd door zowel de aanbieder als de afnemer;
- Internationale afspraken wenselijk ter bescherming medische data. Draag de aanbevelingen in dit rapport internationaal uit en streef na dat zoveel mogelijk landen deze of vergelijkbare aanbevelingen hanteren ter bescherming van medische data;
- Medisch verschoningsrecht. Identificeer landen waar het (afgeleid) medisch verschoningsrecht niet geldt of (te gemakkelijk) doorbroken kan worden door politie, inlichtingendiensten, of andere partijen. Probeer deze landen ertoe te bewegen een vergelijkbaar (afgeleid) verschoningsrecht ten aanzien van medische data te implementeren als geldt in Nederland dan wel de EU;
- Model clauses. Zorg dat nieuwe model clauses worden gemaakt die in overeenstemming zijn met de (U)AVG;
    - Besef dat model clauses geen passende waarborg bieden tegen het specifieke risico van verstrekking van (toegang tot) medische data aan autoriteiten in landen waar politie, inlichtingendiensten en/of andere autoriteiten te brede bevoegdheden hebben om (toegang tot) klantdata te vorderen, of onvoldoende voorzien in onafhankelijke (rechterlijke) controle van of rechtsmiddelen tegen dergelijke bevoegdheden.