Naar aanleiding van Webinar 'Veiligheid & Privacy' 14 november 2019

FAQ Privacy compliance

Wilco Brouwers, Baker Tilly, 4 december 2019

1. Het gebruik van veilige elektronische identificatiemiddelen (eID) is een belangrijke voorwaarde voor de toepassing van E-health, omdat je als zorginstelling zeker moet weten wie inlogt, voordat je digitale zorg aanbiedt. Wat betekent dit nu precies en zijn er al relevante pilots?

Dit is een heikel vraagstuk wat volop in ontwikkeling is. Verschillende regelingen leggen de lat ook anders, maar algemene lijn is dat je moet zorgen dat voor gezondheidsgegevens niet alleen gebruikersnaam-wachtwoord maar ook een extra factor zoals SMS of app-verificatie (Google of Microsoft authenticator) gevraagd wordt. Let op: SMS brengt extra communicatiekosten met zich mee!

Achtergrond:

In de brief van 4 oktober 2018 van de AP aan VWS is over het gewenste betrouwbaarheidsniveau in de zorg het volgende aangegeven:

“In het verleden heeft de AP regelmatig aangegeven dat bij patiëntauthenticatie in het kader van de uitwisseling van gegevens over gezondheid in beginsel dient te worden uitgegaan van een “hoog betrouwbaarheidsniveau” en dat in gevallen waar het gaat om gegevens waarop het medisch beroepsgeheim van de zorgverlener rust het ‘hoogste betrouwbaarheidsniveau” vereist is. In de terminologie van de eIDAS-verordening wil dit zeggen dat bij patiëntauthenticatie minimaal niveau “substantieel” vereist is. Als het gaat om gegevens waarop het medisch beroepsgeheim van de hulpverlener rust, is betrouwbaarheidsniveau “hoog” vereist.”

De AP erkent in de brief ook het probleem dat het middel “substantieel “ en “hoog” op dit moment nog niet redelijke schaal beschikbaar is en vereist daarom voor dit moment het hoogst mogelijke betrouwbare middel, te weten 2-factor (naam, wachtwoord en sms of app). Zodra middelen op niveau substantieel, en uiteindelijk hoog, beschikbaar zijn moet dit alsnog worden toegepast.

2. Welke gegevens mag je wel/niet in een applicatie opslaan zonder aan alle NEN eisen te hoeven voldoen (bv alleen geboortedatum of alleen emailadres)?

In de regel tref je de ‘zwaardere’ NEN eisen voor het totale systeem waarin zowel normale als bijzondere persoonsgegevens opgeslagen liggen. Dus is het onderscheid tussen gegevens die normaal zijn en bijzonder in de praktijk niet zo relevant, want je kan de beveiligingsmaatregelen vaak niet splitsen.

Voor de hand liggende gegevens zijn iemands naam, adres en woonplaats. Maar ook telefoonnummers en postcodes met huisnummers zijn persoonsgegevens die in de regel niet als gevoelig worden beschouwd.

Gevoelige gegevens als iemands ras, godsdienst of gezondheid worden bijzondere persoonsgegevens genoemd. Deze zijn door de wetgever extra beschermd.

Meer informatie over de definitie van persoonsgegevens is te vinden in artikel 4 van de AVG.

3. Waar moeten apps aan voldoen om te mogen gebruiken en hoe controleren we of ze veilig zijn?

Apps moeten allereerst als verwerkingen gewoon voldoen aan de AVG vereisten. Dus aan de hand van een risico analyse maatregelen treffen op gebied van authenticatie van de gebruiker (certificaat of 2 factor)), dataminimalisatie, versleuteling van verbindingen en

Sommige medische apps doen meer dan alleen algemene informatie verschaffen of helpen bij het verbeteren van de productiviteit in de zorg. Een steeds groter aantal apps helpen patiënten bij het diagnosticeren, monitoren of behandelen van hun aandoening. Als dit het geval is, is de kans groot dat volgens de Europese wet- en regelgeving de app geclassificeerd wordt als een medisch hulpmiddel, en de daarbij behorende CE-keurmerk nodig heeft. De eisen hieraan worden per 26 mei 2020 in de nieuwe Europese "Verordening betreffende medische hulpmiddelen" nog strenger.

4. Hoe ga je om met partijen die (nog) niet aan de/ alle standaardveiligheidseisen kunnen voldoen (NEN 7510, 7512, 7513) en is het redelijk en nodig om deze eisen meteen en bij aanvang aan alle partijen te vragen, of kan er onderscheid worden gemaakt naar de rol van de partij /afhankelijk van de dienst die zij leveren?

In de praktijk val je dan terug op de wettelijke plicht van de verantwoordelijke (uitbestedende) partij om vast te stellen dat passende technische en organisatorische maatregelen getroffen zijn en dit in een verwerkersovereenkomst vast te leggen. Denk aan:

- minimum niveau beveiliging: servers patches, anti virus beveiliging, admin rechten
- data versleuteld opslaan en verbindingen beveiligd (Https)
- datalekken afspraak maken

o.a. pagina 46 en 47 van het privacy control framework van NOREA biedt een goede checklist (zie www.norea.nl).

5. Wat betreft NEN7512: dit gaat over hoe de beveiliging voor communicatie tussen het platform en andere platform leveranciers moet zijn. Vraag is of dit alleen gaat over techniek of dat dit een functionaliteit is die in de oplossing ingebouwd moet worden?

NEN 7512 gaat in breedte in op beheersing van gegevensuitwisseling, vanaf risicoanalyse en op maat maken van de maatregelen tot aan het maken en toezien op afspraken en overeenkomsten. Dus ook procedureel. Hoewel de maatregelen veelal ingaan op identificatie en beveiliging, encryptie, logging etc. zitten er ook wel 'functionele' normen in over bijvoorbeeld de manier waarop incidenten geregistreerd worden en back-ups gemaakt kunnen worden. Maar het merendeel gaat inderdaad wel in op de techniek achter de communicatie.

6. Wat betreft NEN7513: dit gaat vooral over logging van behandelaars / gebruikers van het systeem. Is het dan voldoende om functie scheiding toe te passen voor gebruikers die ook bij medische gegevens kunnen en elke keer onderbouwing te vragen waarom ze een persoon willen inzien, tenzij ze vooraf in groep zitten die hen behandeld? Dan kunnen we veel oplossen door functioneel te specificeren welke acties gelogd moeten worden.

NEN 7513 gaat inderdaad uit van proportionele op risico's afgestemde logging (want je kan nu eenmaal niet alles loggen). Wel is het zo dat in 6.2.1 van de norm wordt gesteld dat alle gebeurtenissen op een patiëntdossier zouden moeten worden gelogd.

In het begin van de norm staat vermeld dat hieraan een risicoanalyse vooraf gaat en je dan bepaald voor welke deelterreinen en/of systemen de norm gevolg gaat worden.

Het uitsluiten van het 'deelterrein' van de behandelaren die al een wettelijke grondslag hebben om gegevens in te zien past daar inderdaad binnen. Mits de toebedeling aan die groep goed geborgd is natuurlijk.

7. Als de zorginstelling de opdracht geeft voor de bouw van een applicatie en uiteindelijk ook eigenaar (applicatie wordt NEN7510 gehost waarbij de applicatiebouwer alleen technisch applicatie beheer uitvoert, is er dan nog sprake van een sub verwerker ?

Ja, ook dan is de applicatiebouwer die beheer blijft uitvoeren een sub verwerker. Je bent als IT dienstverlener eigenlijk bijna altijd 'bewerker': je 'verwerkt' ten behoeve van de verantwoordelijke zonder onder het gezag van de verantwoordelijke te zijn onderworpen.

Verwerken = verzamelen, ordenen, bewaren, afschermen van data. Bij technisch applicatiebeheer hoort vaak ook sleutelen aan afscherming, databeheer etc. Natuurlijk maakt het voor de zwaarte van de afspraken wel degelijk uit of jij alleen beperkt beheer uitvoert of ook actiever met de data werkt. Maar een verwerkersovereenkomst – hoe beperkt ook – is wel raadzaam.

8. Bij samenwerkingsverbanden met een heel groot bereik van de oudere zelfstandige wonende inwoner, op welke wijze kunnen toestemming/ akkoord vastleggen van de inwoner dat zij benaderd kunnen worden?

Eerste vraag is – zoals in webinar toegelicht – of je toestemming als grondslag nodig hebt. Toestemming is lastig, vastlegging moet eenduidig, informeren moet heel duidelijk en de betrokkene mag ook altijd later weer intrekken. Is het niet mogelijk dat je vanuit een samenwerkingsverband een partij kiest die al een grondslag heeft om een betrokkene te benaderen / informeren zonder dat deze eerst toestemming moet geven?

Als toch toestemming nodig is, dan staat op de AVG helpdesk voor de zorg een kernachtige samenvatting met voorbeelden analoog en digitaal: https://www.avghelpdeskzorg.nl/onderwerpen/toestemming

9. Hoe kunnen we met alle samenwerkingsorganisaties rondom SET / en de inwoner informatie en kennis delen end daarbij AVG technisch correct werken?
En in het verlengede daarvan, idealiter zou het verband een soort van registratiesysteem moet aanleggen en bijhouden waar meerde partner organisaties gebruik van kan maken, hoe borgen we daar de privacy?

Zoals in webinar behandeld is het advies om bij een nieuwe samenwerkingsorganisatie eerst een goede data inventarisatie en een privacy impact assessment te maken.

Met de data inventarisatie en PIA heb je taak, doel en noodzaak van het verzamelen en delen van gegevens in beeld en pas dan volgt de vraag: mogen we de gegevens delen en onder welke voorwaarden ?

Regelmatig blijkt gaandeweg dat het mogelijk is om mensen de juiste zorg te bieden, zonder dat hun privacy in het geding is. Of dat het privacyvraagstuk beperkt is.

10. Als bij innoveren met eHealth nog niet alle privacy en veiligheid gedurende het project volledig is gewaarborgd: Welke best practices zijn bekend om toch zo min mogelijk geremd te worden in het innovatie proces?

Daar waar de risico's redelijk groot blijven rest niet veel anders dan de betrokkenen te informeren en om toestemming te vragen. In pilots is het ook vaak nog nodig vanwege het experimenteel karakter. Daar is het aantal deelnemers vaak ook nog beperkt en toestemming nog wel werkbaar.

Als de verwerking opschaalt, dan is het zaak om met een goede data inventarisatie en privacy impact assessment (zie webinar) in ieder geval als verantwoordelijke goed de risico's te kennen en hierover ook in een actieplan te volgen hoe deze worden opgelost.

Het blijft dan een kunst om met alle partijen in een samenwerkingsverband vast te stellen en te onderbouwen waarom je vind dat je goed genoeg je best doet om privacy compliance te borgen zonder het proces ernstig te remmen.

Vragen gesteld tijdens de Webinar

11. Je hebt het over 'verwerking' maar geldt dat ook voor 'gegevens delen' met verschillende organisaties (tweede lijn, eerste lijn, zorgverzekeraars)

Ja.

Volgens art. 4 lid 2 AVG is het verwerken van persoonsgegevens: 'elke bewerking of elk geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedures, 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.'

Het begrip 'verwerken' is erg ruim en betekent eigenlijk alles wat met persoonsgegevens gedaan wordt.

12. Indien de zorg via beeldverbinding uitgevoerd wordt, bijvoorbeeld 4-ogen controle medicatie. Wat moet er dan aan gegevens aangegeven worden waarvoor akkoord op gegeven moet worden door een cliënt?

Zie eerdere antwoord over toestemming: is er geen andere grondslag op basis waarvan de beeldverbinding en de controle worden verricht? Is er geen behandelrelatie of andere overeenkomst? Als dit niet het geval is, is het laatste redmiddel toestemming en dan slaat de toestemming eigenlijk op alle bijzondere persoonsgegevens (dus alle gezondheidsgegevens).

13. Check of we in zee gaan met betrouwbare partij. Dient iedere organisatie hier achteraan te gaan? Of kan er voor leveranciers die vanuit dit traject worden aangesloten al een en ander worden georganiseerd? Bijv. dat die partij/leverancier al een PIA bij zichzelf heeft uitgevoerd en dit openbaar maakt; zoals hoe zij omgaan met beveiliging, bewaartermijnen etc.

Het heeft de voorkeur dat niet elke partij weer moet vast stellen hoe zorgvuldig een leverancier is. Dit kan de leverancier dan aantonen via een zelfverklaring of self assessment in de vorm van een PIA, maar beter nog is een onafhankelijke toets (audit) op de AVG wetgeving of tenminste op algemene beveiligingsnormen als de 27001 en 7510.

14. Wij zijn een platform voor zorgprofessionals (ZZP'ers) en bieden daarin een digitale werkomgeving, inclusief ECD. Als een zorgverlener iets download op eigen computer, valt dit onder de verantwoordelijkheid van ons of van de ZZP'er (is namelijk ook een organisatie)?

Op het moment dat de zorgverlener ZZP'er iets op zijn eigen omgeving heeft neergezet bepaalt hij/zij vervolgens het doel en de middelen waarmee deze data wordt bewerkt (ervan uitgaande dat deze omgeving niet onder jullie beïnvloeding valt). En ja, dan is de ZZP'er zelf de verantwoordelijke.