Innovatie in de zorg? Basis op orde!

Een van de uitdagingen waarvoor de zorg gesteld staat, is het beheersen van de uitgaven en het borgen van de toegankelijkheid en betaalbaarheid op de lange termijn. Om deze uitdaging aan te gaan, worden in toenemende mate innovatieve manieren van zorg toegepast. De meeste innovaties zijn digitale zorgtoepassingen waarmee veel voordelen kunnen worden behaald. Bijvoorbeeld omdat deze toepassingen bijdragen aan het verbeteren van de zorg, administratieve lasten verlagen en mensen meer inzicht geven in hun eigen gezondheid. Er is dan ook alle reden dat digitale zorgtoepassingen met veel enthousiasme worden ontvangen.

Een wezenlijk kenmerk van veel digitale zorg is dat hiermee gezondheidsgegevens worden verwerkt. Op deze verwerkingen zijn de kaders van de wetgeving rondom gegevensbescherming van toepassing, zoals het medisch beroepsgeheim en de AVG. Een veel gehoorde verzuchting is dat 'de privacy' innovatieve toepassingen in de weg staat.

Deze beperkte blik op gegevensbescherming is veelal het gevolg van het niet volledig kunnen overzien van de gevolgen van de betreffende wetgeving. Maar het kan ook het gevolg zijn van onvoldoende begrip van wat een organisatie moet doen om de voordelen van digitale zorg maximaal te benutten. Dat wil zeggen: hoe de hiermee samenhangende dataverwerkingen op een verantwoorde en duurzame manier kunnen plaatsvinden. Dat is jammer, want dit kan ertoe leiden dat de voordelen van digitale zorg onvoldoende worden benut.

Noodzakelijke voorwaarde

Tijd dus voor omdenken. Er kan veel meer dan in eerste instantie wordt gedacht. Gegevensbescherming staat niet in de weg bij het toepassen van digitale zorg. Integendeel, mits goed georganiseerd, is het een noodzakelijke voorwaarde voor een verantwoord en toekomstbestendig gebruik van (complexe) digitale zorg. Tel hierbij op dat het belang van gegevensbescherming alleen maar toeneemt door de voortschrijdende 'dataficering' en kunstmatige intelligentie (AI). Het is vanuit dit perspectief een must om grip te krijgen én te houden op digitale zorg. Dat kan alleen als de basis op orde is.

Wat is er nodig voor een goede basis? In de eerste plaats een andere blik op gegevensbescherming: het is geen op zichzelf staand element maar grijpt in op alles wat met data te maken heeft binnen een organisatie. Gegevensbescherming vereist dan ook een overkoepelende strategie en beleid en een organisatorisch inbedding. Zo gaat gegevensbescherming echt deel uitmaken van de planning- en controle-cyclus. Met daarnaast de noodzakelijke aandacht voor het vertrouwensmodel bestaande uit identificatie, authenticatie, autorisatie, logging, communicatie en toezicht.

Actuele voorbeelden

Onlangs berichtten media over een zorgaanbieder bij wie hulpverleners patiëntgegevens (corona-testgegevens) via WhatsApp deelden met personen die niet bij de behandeling waren betrokken. Daarmee werd het medisch beroepsgeheim, als belangrijkste basisvereiste, doorbroken. Een ander belangrijk basisvereiste op grond van de AVG is dat gezondheidsgegevens voldoende dienen te worden beveiligd. Hieraan voldeed deze zorgaanbieder ook niet, waardoor er sprake was van een datalek. Op grond van het besluit elektronische gegevensbescherming (behorende bij de Wet aanvullende bepalingen verwerking persoonsgegevens zorg) dienen zorgaanbieders bovendien te voldoen aan NEN-normen, zoals NEN 7510: 2017. De zorgaanbieder verklaarde hieraan te voldoen, maar stond niet in het bijbehorende NEN-register.

De recente diefstal, het datalek en de handel in gezondheidsgegevens bij de GGD tonen eveneens aan dat gezondheidsgegevens waardevol zijn en een gegevensbescherming vergt die op orde is.

Veel andere zorgaanbieders geven aan te willen innoveren met behulp van AI. Tegelijkertijd blijken deze zorgaanbieders in de praktijk nog niet te voldoen aan het basisvereiste dat gegevens gelogd dienen te worden op grond van de NEN-7513. Basaler is dat deze zorgaanbieders zelfs nog blijken te werken met een fax.

Risico's in kaart

Voor de goede basis is verder onontbeerlijk dat bekend is welke digitale toepassingen worden gebruikt en in voorbereiding zijn. Voorafgaand aan het gebruik, worden de risico's in kaart gebracht met een gegevensbeschermingseffectbeoordeling (Data Protection Impact Assessment, DPIA). Kortom, gegevensbescherming staat digitale zorgtoepassingen, ook innovatieve toepassingen met bijvoorbeeld kunstmatige intelligentie, niet in de weg als de basis maar op orde is!

In een volgend nummer van ICT&health ga ik verder op dit thema in middels een drieluik, samen met mederedactieraadslid prof.dr. Maurice van den Bosch (vanuit het perspectief van zorgbestuurder als bestuursvoorzitter van het OLVG en prof. dr. Daniel Hommes (vanuit medisch innovatieperspectief als CEO van Dear Health). ■

Theo Hooghiemstra is bestuurder van MedMij en oprichter van Hooghiemstra & Partners.