Het juiste midden tussen patiëntveiligheid en informatieveiligheid

DE VEILIGHEIDS-PARADOX IN DE ZORG

Samenwerking is een heikel thema voor steeds meer ziekenhuizen en zorginstellingen. Bestuurders zitten in tweestrijd: enerzijds zien zij dat de moderne zorg om informatiedeling vraagt, anderzijds is er de constante vrees voor een lek van medische gegevens. Wat is een goede balans? 7 inzichten uit de praktijk.

Tekst **Albert Vlug, director healthcare bij ICT-dienstverlener CGI**

1. 'Sharing is caring'

Zo luidt een veel gebruikt gezegde onder social mediagebruikers. Vrij vertaald: wie een bericht deelt van een ander, biedt hem of haar daarmee een helpende hand. Het is een gedachte die past bij de steeds vrijere informatiestromen tussen personen, bedrijven en instanties – en bij het idee dat de wereld beter af is met vrij beschikbare informatie. In de zorg geldt dit motto letterlijk. De kwaliteit van zorg wordt namelijk steeds sterker bepaald door de kwaliteit van informatie-uitwisseling; voor continuïteit van zorg is een continue informatievoorziening vereist. Dit besef moet leidend zijn bij elke vorm van databeveiliging. Neem een patiënt die allergisch is gebleken voor bepaalde medicatie: het is in zijn directe belang dat die informatie altijd en overal beschikbaar is voor behandelende artsen.

2. De zorg om privacy is terecht

Want het is waar: vrije uitwisseling van informatie heeft ook een keerzijde – helemaal in de zorg, waar meer dan waar ook met hoogstpersoonlijke informatie wordt gewerkt. Juist met het oog op de privacy van de patiënt is de spreek- en behandelkamer in de loop der tijd

+ 'ALLES DRAAIT OM VERTROUWEN'

min of meer heilig verklaard. Ook het beroepsgeheim van artsen en behandelaars komt daaruit voort. Patiënten weten sindsdien zeker dat zij binnen de muren van een instelling altijd in een vertrouwde omgeving zijn. Dat is een groot goed en mag nooit ter discussie staan. Dat patiënten op social media soms veel soepeler met hun privacy omgaan, doet hieraan geen afbreuk. De waakzaamheid onder bestuurders van ziekenhuizen en zorginstellingen is terecht.

3. Meer informatie-uitwisseling vereist een nieuw paradigma

Op dit moment overheerst de 'silo-benadering'; de (onbewuste) overtuiging dat de organisatie tot aan de muren van de instelling reikt. Bij die muren 'staan' firewalls om ongewenste informatiestromen van en naar de oncontroleerbare buitenwereld tegen te houden. Intern wordt alles met autorisatie geregeld.
Het probleem van deze benadering is dat innovaties erdoor worden geblokkeerd: artsen kunnen hun nieuwe apps niet koppelen met systemen van de zorginstelling en patiënten krijgen alleen informatie van het ziekenhuis te zien. Patiëntparticipatie is zo niet te regelen: de systemen zijn simpelweg niet in staat om patiënten tot bepaalde gegevens toe te laten.

4. De nieuwe meldplicht datalekken is 'slechts' een vorm van handhaving

Helaas zorgt de wet ook voor veel angst: wie zijn informatiebeveiliging niet op orde heeft, riskeert enorme sancties. Ook de boetes voor het niet melden van een (mogelijk) lek zijn fors – de reputatieschade potentieel desastreus. Deze angst werkt vaak verlammend: bestuurders kiezen voor nog zwaardere informatiebeveiliging en knellen hun datastromen daarmee onnodig af.

5. Het juiste beveiligingsniveau begint met een gedegen risicoanalyse

Veel zorginstellingen grijpen al snel naar de 'standaard' lijst van maatregelen voor vergelijkbare organisaties, zonder de eigen risico's ook maar in ogenschouw te nemen. Een juiste analyse heeft de zorgdoelen van de organisatie als vertrekpunt en vervolgt met het wegen en prioriteren van 'gevoelige plekken' in de informatie-uitwisseling met externe partijen. Ook de mening van de patiënt over informatiedeling en informatiebeveiliging zou mee mogen tellen of zelfs leidend moeten zijn. Geeft iemand die heel ziek is geweest bijvoorbeeld zelf aan dat privacy voor hem geen issue is, dan kan een hoge beveiligingsmuur beter achterwege gelaten worden. Dat is in zo'n geval niet meer dan een belemmering.

6. Voldoen aan beveiligingsnormen is slechts een voorwaarde, geen eindstation

De internationale ISO-27001 was jarenlang hét uitgangspunt voor informatiebeveiliging, totdat die norm te algemeen en abstract bleek. Speciaal voor de zorg werd daarom de Nederlandse NEN 7510 opgesteld. Die is sindsdien voor alle zorginstellingen verplicht bij alle uitwisseling van gegevens die gekoppeld zijn aan het burgerservicenummer (BSN). Sommige zorginstellingen huren beveiligingsspecialisten in om aan deze norm te voldoen en laten dat vervolgens door een externe auditor vastleggen. Maar dat is te weinig: het risico is dan wel bestuurlijk afgedekt, maar het besef in de organisatie ontbreekt. Risico's moeten bovendien steeds opnieuw gewogen worden – kansen moeten worden benut. Zo komen er steeds geavanceerdere en slimmere mogelijkheden om niet de organisatie, maar de informatie-uitwisseling zelf te beveiligen. Dat biedt kansen voor intensievere samenwerking in de regio of met de participerende (familie van de) patiënt.

7. Vertrouwen is hét fundament voor samenwerking

Te midden van alle aandacht voor privacy en databeveiliging blijft vaak onuitgesproken waar samenwerking écht om draait: een vertrouwensrelatie. Omdat die vaak ontbreekt, zijn veel artsen en specialisten terughoudend in het delen van persoonlijke gegevens. Laboratoriumtests zijn een mooi voorbeeld. In plaats van te vertrouwen op de testresultaten van een andere instelling of praktijk, kiezen instellingen meestal toch voor een 'extra' eigen test, ongeacht welk offer dat van de patiënt vraagt. Ook een eigen bloeddrukmeting van de patiënt wordt meestal (nog) niet vertrouwd: de diversiteit aan standaarden en bepalingen voor tests en meettechnieken is enorm.
Belangrijke technische stappen voor meer vertrouwen zijn het normeren van apps en betrouwbare apparaten, plus een heldere definitie van standaarden en eenheden. Maar toch: ook al heb je als instelling je digitale 'infrastructuur' en beveiliging op orde, vertrouwen is het échte vertrekpunt voor samenwerking en informatie-uitwisseling. Vertrouwen betekent ook je eigen kracht en zwakte kennen, zodat je samen tot een win-win-win-situatie komt. Het is het laatste punt, en tegelijk het belangrijkste waar bestuurders hun informatiebeleid mee zouden kunnen beginnen. +