

BIND Meeting “Zorgtechnologie veilig borgen”

Borging Ethiek, Privacy, Dataprotectie en Cyberweerbaarheid na implementatie

JAIN

Donderdag 17 september 2026 | 14:30 - 16:00 uur bij Vilans Utrecht

Wanneer slimme technologie in huis wordt gehaald om langer zelfstandig te kunnen blijven wonen, biedt dat grote voordelen. Denk aan sensoren die een seintje geven als er iets mis is, of handige digitale hulpmiddelen die helpen bij de dagelijkse structuur. Maar hoe is er absolute zekerheid dat die apparaten na implementatie betrouwbaar blijven werken, dat er niemand onbevoegd meekijkt en dat privégegevens niet op straat komen te liggen?

Dat is waar deze meeting over gaat: **Systeemregie**. Dit betekent simpelweg dat de touwtjes stevig in handen worden gehouden, zodat technologie de zorg menselijk, ethisch en veilig ondersteunt, zonder de controle over te nemen. Binnen deze BIND staan de volgende onderwerpen centraal:

1. Privacy vanaf het allereerste begin en ethische borging

Privacy is geen vinkje dat pas achteraf wordt gezet als de technologie al af is. Het moet vanaf de allereerste computerregel in het systeem ingebouwd zitten (Privacy-by-Design). Tijdens de bijeenkomst wordt besproken hoe er voor kan worden gezorgd dat alle systemen direct en blijvend voldoen aan de strenge privacyregels in de zorg. De vertaling van de AVG naar tastbare technische systeemspecificaties staat hierbij centraal. Door vooraf en tussentijds heel nauwkeurig te onderzoeken waar de risico's liggen via gerichte DPIA's, worden privacyproblemen opgelost én voorkomen.

2. Een eigen Digitale Kluis via gedecentraliseerde data-architectuur

Nu is het vaak zo dat een technologieleverancier alle gegevens en metingen verzamelt op centrale computers. Dat brengt risico's met zich mee voor de privacy, de dataprotectie en de continuïteit. Het uitgangspunt is dat de gegevens altijd eigendom moeten blijven van de persoon die zorg nodig heeft. De inzet van een gedecentraliseerde data-architectuur biedt de techniek in huis om voor elke bewoner een persoonlijke, superveilig afgesloten Digitale Kluis in te richten. Alle gegevens van de sensoren in huis gaan rechtstreeks naar deze kluis. De cliënt (of de wettelijk vertegenwoordiger) bepaalt zélf wie erin mag kijken. Wil een zorgverlener of een applicatie iets weten? Dan moet er eerst expliciet toestemming worden gevraagd via een herroepbaar opt-in model. Die toestemming kan ook altijd weer heel eenvoudig worden ingetrokken, zodat de dataprotectie écht gewaarborgd is.

3. Digitaal slot op de deur (Cyberweerbaarheid & Risico-afdekking)

Helaas komt het in het nieuws steeds vaker voor dat digitale inbrekers (hackers) computersystemen gijzelen en losgeld eisen. In de zorg mag de monitoring nooit uitvallen, want dat is gevaarlijk. Daarom wordt besproken hoe de digitale beveiliging na implementatie zo wordt ingericht dat systemen altijd blijven werken. Zelfs als het internet uitvalt of als centrale computers worden aangevallen, moeten de slimme netwerken in de woning direct en zelfstandig door kunnen blijven draaien om aan zorgnormen zoals de NEN 7510 te voldoen. Er worden duidelijke criteria vastgesteld voor een veerkrachtige zorginfrastructuur die standhoudt in tijden van crisis.

4. Het vangnet bij incidenten:

Omdat absolute veiligheid nooit voor 100% gegarandeerd kan worden, is een sluitende ketenregie onmisbaar. Als cruciale aanvulling op de technische cyberweerbaarheid wordt besproken hoe een operationeel en financieel vangnet na een cyberincident wordt ingericht. Door de inzet van een gerichte, risico dekkende verzekering worden de continuïteit en eventuele gevolgschade effectief afgedekt als het onverhoopt toch misgaat.

Kortom: Tijdens deze sessie komen techneuten en experts samen om ervoor te zorgen dat slimme technologie in de zorg betrouwbaar is, altijd de privacy en ethische waarden rondom de cliënt respecteert, ijzersterk beveiligd is tegen digitale gevaren én financieel beschermd is via een adequaat vangnet.