De toekomst van zorg-IT: Schaalbaar, veilig en soeverein

Whitepaper

Inhoud.

1. Inleiding.

Regie behouden in een tijd van digitale versnelling

De Nederlandse zorg bevindt zich op een kantelpunt. Innovatie en digitalisering volgen elkaar in razend tempo op. Nieuwe technologieën beloven betere zorg, lagere werkdruk en slimmere processen. Denk aan AI die medische dossiers analyseert, algoritmes die behandelplannen optimaliseren of realtime monitoring op afstand. Het klinkt als toekomstmuziek, maar het gebeurt nu al – en het tempo versnelt.

Tegelijkertijd groeit de complexiteit. Wetgeving wordt strenger. **De NIS2-richtlijn**, die vanaf oktober 2024 geldt, verplicht zorgorganisaties om hun digitale weerbaarheid te verhogen. Cyberrisico's nemen toe: ransomware, datalekken en sabotage zijn geen incidenten meer, maar structurele bedreigingen. En onder druk van krappe budgetten en personeelstekorten blijft er weinig ruimte over voor strategische reflectie.

> **De centrale vraag wordt dan ook niet langer: "Wat kunnen we digitaliseren?" maar: "Hoe houden we controle over wat we digitaliseren?"**

Zorgorganisaties willen gebruikmaken van nieuwe technologieën, maar zonder de regie te verliezen. Zonder afhankelijk te worden van buitenlandse cloudproviders. Zonder het risico te lopen dat patiëntdata buiten de muren van de instelling belandt. En zonder opgesloten te raken in systemen die morgen niet meer voldoen aan wetgeving of wensen.

In dit whitepaper schetsen we de contouren van toekomstbestendige zorg-IT. Wat betekent het om écht soeverein te zijn in je digitale keuzes? Welke scenario's dreigen zich af te tekenen als je het niet goed regelt, en hoe voorkom je die valkuilen? Welke rol spelen partnerschappen in het ecosysteem, zoals die tussen ilionx, Bernhoven en Uniserver?

We bieden je inzichten, richtlijnen en een praktische checklist. Maar bovenal: we nodigen je uit om regie te nemen. Want toekomstbestendige zorg begint bij weloverwogen keuzes over je IT-fundament.

2. Digitale zorg in transitie.

Groeiende kansen, groeiende risico's

Dat digitalisering essentieel is, daarover bestaat geen twijfel meer in de zorg. Wat ooit begon met EPD's, is inmiddels uitgegroeid tot een breed landschap van applicaties, cloudoplossingen, slimme medische apparatuur en AI-toepassingen. Volgens rapportages van Nictiz en VWS is het zorg-ecosysteem in korte tijd radicaal veranderd:

- **Ziekenhuizen** zetten in op voorspellende analyses van patiëntdata.
- **GGZ-instellingen** experimenteren met AI om signalen van terugval eerder te. detecteren
- **Thuiszorgorganisaties** gebruiken slimme sensoren voor 24/7 monitoring.

Deze innovaties brengen hoop en mogelijkheden. Maar ze hangen allemaal samen met één cruciaal aspect: data. En daarmee met IT. Het zorglandschap wordt steeds digitaler, maar ook steeds afhankelijker van de infrastructuur erachter.

Vier uitdagingen tekenen zich scherp af

1. Exerne druk vanuit wetgeving en toezicht
   - De komst van **NIS2** verplicht zorginstellingen om risico's in kaart te brengen, incidentmanagement in te richten en te kunnen aantonen dat leveranciers compliant zijn.
   - Het is geen vrijblijvendheid meer. Het is een wettelijke plicht.

2. Exponentiële groei van datavolumes
   - Van hoge resolutie MRI-scans tot videobellen en AI-logbestanden: de hoeveelheid zorgdata verdubbelt in een ongekend tempo.
   - Legacy-systemen en verouderde opslagcapaciteit kunnen dit nauwelijks bijbenen.

3. Exponentiële groei van datavolumes
   - Z-CERT registreerde in 2023 een sterke toename van cyberincidenten in de zorg.
   - De sector wordt gezien als kwetsbaar én winstgevend doelwit.

4. Verlies van grip door technologische versnippering

- Veel zorginstellingen werke met een mix van publieke cloud, on-premise servers en shadow IT.
- Dit leidt tot een lappendeken aan systemen die moeilijk te beheren én te beveiligen zijn.

> **De belofte van technologie is groot. Maar zonder solide fundament wordt die belofte een risico.**

Daarom groeit de vraag naar schaalbare, veilige én soevereine oplossingen. Niet alleen om vandaag te voldoen aan compliance-eisen, maar vooral om morgen nog wendbaar te zijn in een snel veranderend zorglandschap.

In de volgende hoofdstukken duiken we dieper in drie scenario's voor de toekomst van zorg-IT – en hoe je daarin het verschil maakt.

3. Toekomstscenario's voor zorginstellingen.

Drie wegen, drie uitkomsten

3.1 Scenario 1: Vendor lock-in en technologische versnippering

Een gefragmenteerd IT-landschap leidt tot vendor lock-in: afhankelijkheid van een beperkt aantal leveranciers. Volgens de ACM beperkt deze 'geslotenheid' de uitwisseling van gegevens, remt innovatie en verhoogt overstapkosten. Zorginkopers bevestigen dat zonder standaardisatie, overstappen vaak technisch onmogelijk of prohibitief duur is.

Gevolgen:

- **Verlies van onderhandelingsmacht:** leveranciers bepalen tarieven en upgrades.
- **Beperkte interoperabiliteit:** koppelingen tussen systemen zijn complex.
- **Hogere kosten en minder innovatie:** door gebrek aan concurrentie.

Cyberrisico's:
Z-CERT constateert een wereldwijde stijging van 73% in ransomware-incidenten in de zorg in 2023 én waarschuwt voor aanvallen via leveranciers ('supply chain'). Dit illustreert hoe versnippering tot kwetsbaarheid leidt en herstel vertraagt.

3.2 Scenario 2: Alles naar hyperscalers

Veel organisaties kiezen voor hyperscalers (AWS, Azure, Google Cloud). Schaalbaar en innovatief, maar er kleven risico's aan:

1. **Onzekerheid over datalocatie:** datacenters buiten de EU vallen mogelijk onder regelgeving als de Amerikaanse CLOUD Act.
2. **Verlies van datacontrole:** toegang door buitenlandse overheden is soms juridisch mogelijk.
3. **Lock-in bij hyperscalers:** overstappen naar een andere cloud wordt technisch en contractueel lastig.

De AIVD en Europese Commissie waarschuwen dat overmatige afhankelijkheid van niet-Europese cloudleveranciers de digitale soevereiniteit in gevaar brengt. In de zorg, onder AVG én beroepsgeheim, is dit extra relevant.

3.3 Scenario 3: Soevereine infrastructuur als fundament

In dit scenario kiest de zorginstelling voor een private of co-managed cloudomgeving, gehost in Nederland. Dit biedt het beste van twee werelden: veiligheid en compliance aan de ene kant, flexibiliteit en toekomstbestendigheid aan de andere.

Voordelen:

- **Nationale datalocatie:** Data wordt opgeslagen in Nederlandse datacenters en valt onder de AVG en NIS2.
- **Beheerd door betrouwbare partijen:** vaak met bewezen ervaring in de zorgsector en aantoonbare certificeringen (ISO 27001, SOC 2).
- **Toegankelijk voor ketenpartners:** samenwerking en datadeling worden eenvoudiger, juist omdat je zelf de regie houdt.

Een concreet voorbeeld is de samenwerking tussen Bernhoven, ilionx en Uniserver. Samen bouwden zij een infrastructuur waarbij Bernhoven zelf de regie behoudt over haar digitale zorgomgeving. Zonder afhankelijk te zijn van buitenlandse cloudleveranciers. Zonder concessies te doen aan compliance of flexibiliteit. Daarmee bewijst dit project dat soevereine cloudoplossingen vandaag al praktisch inzetbaar zijn in de Nederlandse zorg.

3.4 Samenvattend

Scenario.	Kenmerken.	Gevolgen.
Lock-in & versnippering	Gefragmenteerde IT, vendor lock-in	Hogere kosten, weinig interoperabiliteit, groot cyber-risico
Hyperscalers	Schaalbaar, maar externe afhankelijkheid	Compliance-risico's, juridisch onzeker, migratie vastlopers
Soevereine infrastructuur	Nederlandse private cloud, open standaarden	Maximale regie over data, veilig, toekomstbestendig

4. Wat betekent een soevereine cloudoplossing in de zorg?

Zorgorganisaties verwerken en beheren grote hoeveelheden gevoelige informatie: medische dossiers, behandelplannen, identiteitsgegevens, communicatie tussen zorgverleners. Deze data is essentieel voor goede zorgverlening, maar vormt ook een aantrekkelijk doelwit voor cyberaanvallen en commerciële exploitatie. Dat maakt de vraag wie er toegang heeft tot die data, waar het staat en onder welke wetgeving het valt, belangrijker dan ooit.

Een soevereine cloudoplossing biedt hiervoor een structureel antwoord. Het concept draait om controle – over data, infrastructuur, toegang, compliance en continuïteit. In dit hoofdstuk onderzoeken we wat dat concreet betekent voor zorginstellingen, en waarom die controle steeds fundamenteler wordt in een digitaal zorglandschap.

4.1 Gegevensopslag en -verwerking binnen de EU

Bij een soevereine cloud worden alle data opgeslagen en verwerkt in datacenters binnen Nederland of de Europese Unie. Hierdoor valt de data uitsluitend onder de Europese wetgeving, zoals de AVG en NIS2. De opslaglocatie is niet alleen geografisch relevant, maar ook juridisch bepalend: het voorkomt dat buitenlandse wetgeving, zoals de Amerikaanse CLOUD Act, alsnog toegang afdwingt tot gevoelige informatie.

Voor zorginstellingen betekent dit:

- Volledige naleving van privacywetgeving, zonder uitzonderingsgronden
- Geen onduidelijkheid over waar data zich bevindt
- Verkleining van juridische en reputatierisico's

4.2 Beheer binnen de Europese rechtsorde

Naast dataverwerking speelt ook het operationeel beheer een sleutelrol. In een soevereine cloud ligt die verantwoordelijkheid bij een Europese partij, met lokale aanwezigheid, contracten en juridische binding. Dat voorkomt dat ondersteuning of beheer onbedoeld buiten de EU plaatsvindt.

Voor zorginstellingen betekent dit:

- Lokale SLA's en support in het Nederlands of Engels
- Duidelijke eigendomsstructuren en toegangspaden
- Juridische bescherming volgens EU-regelgeving

Voor bestuurders betekent dit: geen verrassingen in contractuele aansprakelijkheid of toezicht – en volledige transparantie richting raad van toezicht, IGJ en andere toezichthouders.

4.3 Volledige controle over toegang, encryptie en integriteit

Een publieke cloudomgeving biedt vaak minder grip op wie wanneer toegang heeft tot welke informatie. Bij een soevereine oplossing ligt de nadruk op transparantie en controle.

Concrete maatregelen:

- Role-Based Access Control (RBAC) en multifactor-authenticatie
- Encryptie met eigen sleutelbeheer (eventueel via lokale HSM)
- Volledige audittrails en monitoring binnen nationale infrastructuur
- Datasegregatie en zero-trust design als uitgangspunt

Hierdoor is toegang tot medische informatie altijd herleidbaar én onderbouwbaar – cruciaal bij audits, incidentonderzoek of compliancetoetsing.

4.4 Onafhankelijkheid van leveranciers en lock-in vermijden

Een soevereine cloud is doorgaans opgebouwd met open standaarden en modulaire technologie. Dit maakt zorginstellingen minder afhankelijk van specifieke leveranciers, en vergemakkelijkt overstap of integratie.

Dit betekent:

- Geen verplichte koppeling aan specifieke softwareleveranciers
- Ondersteuning voor standaarden als HL7, FHIR en ZIB
- Eenvoudigere integratie met EPD's, portalen, analytics of AI-oplossingen

In plaats van vast te zitten aan één platform, houdt de zorgorganisatie regie over haar IT-architectuur – inclusief keuzemogelijkheid in partners.

4.5 Klaar voor NIS2 en toekomstige ketenverantwoordelijkheid

De aankomende NIS2-richtlijn maakt het noodzakelijk om risico's, beveiliging en leveranciersmanagement aantoonbaar op orde te hebben. Dit geldt niet alleen voor ziekenhuizen, maar ook voor ICT-dienstverleners, softwareleveranciers en datacenters in de zorgketen.

Een soevereine cloud sluit hier naadloos op aan:

- Security by design: beveiliging is ingebouwd, niet toegevoegd
- Ketenverantwoordelijkheid: duidelijke afspraken over taken, bevoegdheden en controle
- Snelle incidentrapportage en herstelprocedures op lokaal niveau

Deze aanpak maakt compliance geen eenmalige exercitie, maar een structureel beheersbaar proces.

Samenvattend

Een soevereine cloudoplossing is gericht op controle, transparantie en naleving van wetgeving. Door te kiezen voor data-opslag en -beheer binnen de Europese rechtsorde, kunnen zorgorganisaties risico's verkleinen en ruimte creëren voor digitale vernieuwing – zonder dat zij afhankelijk worden van externe, niet-Europese partijen.

De elementen die dat mogelijk maken, zoals lokale hosting, juridisch beschermde toegang, open standaarden en strikte toegangscontrole, vormen samen het fundament onder een toekomstbestendige digitale zorgomgeving.

In het volgende hoofdstuk laten we zien hoe deze principes in de praktijk worden toegepast in een samenwerking tussen zorginstelling, softwarepartner en cloudspecialist.

5. Praktijkcase: Bernhoven.

Grip op digitale regie bij Bernhoven

Het ziekenhuis Bernhoven stond voor de uitdaging om het beheer van zijn EPD-omgeving te moderniseren én te verduurzamen. De vraag: hoe behoud je regie over patiëntdata, terwijl je de technologische slag ook daadwerkelijk maakt? De samenwerking tussen Bernhoven, ilionx (EPD-beheer) en Uniserver (private cloud) biedt een concreet antwoord

5.1 Doel en uitgangspunten

Doelstelling.	Beschrijving.
Datasoevereiniteit	Patiëntdata blijft binnen Nederlandse/EU-wetgeving
Technisch beheer	ilionx beheert het EPD (ChipSoft HiX) binnen het cloudplatform
Regie & controle	Bernhoven bepaalt wie toegang heeft en hoe data wordt gemonitord
Compliance	Voldoen aan NIS2, AVG en NEN 7510 door ontwerp, structuur en protocollen

Bernhoven koos voor deze opzet om technologische modernisering te realiseren, maar zonder afhankelijkheid van hyperscalers of leveranciersbepaalde infrastructuur.

5.2 Technische architectuur en rolverdeling

1. Private cloudplatform (Uniserver)
   - Gehost in een Nederlands datacenter
   - Lokale encryptie en sleutelbeheer
   - RBAC, auditlogging, multilayer security

2. EPD-beheer (ilionx)
   - Exploitatie van ChipSoft HiX binnen deze omgeving
   - Applicatiebeheer en updates verzorgd door ilionx

3. Regie door Bernhoven
   - Bepaalt wie welke rollen in het systeem krijgt
   - Beheert toegangsrechten
   - Krijgt inzicht via auditlogs en security-tools

Deze heldere scheiding maakt dat elke partij zich kan richten op zijn sterkte: Uniserver verzorgt het technisch fundament, ilionx brengt klinische en functionele know-how, en Bernhoven houdt de regie op data en compliance.

5.3 Belangrijkste voordelen en lessons learned

Transparante governance
Heldere afspraken over wie wat doet, ondersteund door technische hulpmiddelen zoals audits en logging.

Data in zicht
Bernhoven heeft realtime inzicht in datastromen en toegangslogs – essentieel voor toekomstige NIS2-verplichtingen.

Flexibel en uitbreidbaar
Bij toekomstige innovaties (denk ketenzorg of AI-toepassingen) kan de cloudomgeving eenvoudig opgeschaald worden, zonder lock-in.

Compliance by design
Veel voorkomende checkstukken (databescherming, certificeringen, incidentmanagement) zijn vanaf de start geborgd.

Strategische investeringskeuze
In plaats van hyperscalerkosten kiest Bernhoven voor lokale beheersbaarheid en juridische rust.

5.4 Verdere aandachtspunten

Samenwerking vraagt disciplines
Naast techniek is het cruciaal dat zorg-ICT'ers, inkoop en compliance samen optrekken. Sluiten governance-modellen hier goed op aan?

Bewustzijn creëren binnen de organisatie
Rollen en toegangsrechten veranderen pas als ook gebruikers, artsen, verpleegkundigen en staf hiervan doordrongen zijn.

Continu evalueren
Techniek, wetgeving en dreigingen veranderen. Regelmatiger toetsmomenten – samen met alle partijen – zijn een voorwaarde voor duurzaamheid.

Samenvattend

De samenwerking tussen Bernhoven, ilionx en Uniserver is een concreet voorbeeld van hoe een soevereine cloudoplossing er in de praktijk uitziet. Niet vanuit abstract begrip, maar met duidelijke rolverdeling, technische beheersbaarheid en regie door de zorgorganisatie zelf. Daarmee is het een stevig fundament voor grensverleggende, en compliant, digitale zorgverlening.

6. Checklist.

Waar moet je op letten bij het kiezen van een cloudoplossing voor jouw zorginstelling?

De keuze voor een cloudoplossing is strategisch. Het raakt aan patiëntveiligheid, compliance, innovatievermogen én de continuïteit van zorg. Toch worden beslissingen over infrastructuur vaak genomen op basis van kosten, technologische beloften of bestaande contracten – terwijl juist regie, transparantie en juridische zekerheid doorslaggevend zijn.

Onderstaande checklist helpt bij het stellen van de juiste vragen aan potentiële leveranciers of partners:

1

Data-opslag & -verwerking

- Wordt alle data opgeslagen en verwerkt binnen Nederland of de EU?
- Is duidelijk onder welke jurisdictie de data valt?
- Is de cloudprovider gecertificeerd (bijv. ISO 27001, NEN 7510, SOC 2)?

2

Toegangscontrole & inzicht

- Is er volledige transparantie over wie toegang heeft tot welke data?
- Zijn toegangsrechten gebaseerd op rollen (RBAC)?
- Kun je zelf auditlogs inzien en monitoren?
- Wordt encryptie toegepast, en wie beheert de sleutels?

3

Compliance & wetgeving

- Voldoet de oplossing aantoonbaar aan AVG, NIS2 en sectorale richtlijnen?
- Zijn er protocollen voor incidentrespons en rapportage?
- Is ketenverantwoordelijkheid vastgelegd in SLA's en verwerkersovereenkomsten?

4

Flexibiliteit & schaalbaarheid

- Kun je applicaties toevoegen zonder afhankelijk te zijn van één leverancier?
- Worden open standaarden ondersteund (zoals HL7, FHIR)?
- Is de omgeving eenvoudig schaalbaar bij piekbelasting of groei?

5

Regie & contractuele controle

- Heb je zeggenschap over wijzigingen, updates en configuraties?
- Zijn contracten ondergebracht bij een Nederlandse of Europese partij?
- Kun je overstappen zonder technische of juridische belemmeringen?

6

Beheer & ondersteuning

- Wordt de omgeving beheerd door een partij die ervaring heeft in de zorgsector?
- Is support lokaal georganiseerd, in begrijpelijke taal?
- Zijn verantwoordelijkheden en escalaties helder omschreven?

Samenvattend

Een cloudoplossing in de zorg moet méér bieden dan schaalbaarheid of snelheid. Het gaat om vertrouwen, controle, en toekomstbestendigheid. Gebruik deze checklist als leidraad bij nieuwe selecties, heronderhandeling van contracten of een herijking van je IT-strategie.

7. Tot slot.

Regie begint bij de basis

De zorg digitaliseert sneller dan ooit. Nieuwe technologieën beloven efficiëntere processen, betere besluitvorming en minder administratieve druk. Maar tegelijkertijd nemen de risico's toe; van cyberaanvallen tot wetgeving die steeds verder reikt. In deze dynamiek wordt het fundament belangrijker dan de vorm: **zonder controle over data, infrastructuur en toegang is iedere digitale stap een risico.**

De weg naar toekomstbestendige zorg-IT begint daarom bij de vraag:
Hebben wij vandaag de regie die we morgen nodig hebben?

Een soevereine cloudoplossing is daarin geen einddoel, maar een voorwaarde. Een manier om compliance te borgen, innovatie mogelijk te maken en keuzes te blijven maken op je eigen voorwaarden. Door dataverwerking, beheer en juridische controle binnen de Europese kaders te houden, ontstaat ruimte voor samenwerking, groei en vernieuwing.

Het realiseren van zo'n fundament vraagt om samenwerking tussen zorgorganisaties, softwarepartners en cloudspecialisten. Elk met hun eigen rol, maar met een gedeeld belang: veilige, wendbare en veerkrachtige zorg-IT.

> **Toekomstige zorg begint niet bij technologie.**
> **Ze begint bij regie.**

Over ons.

De zorg vraagt om betrouwbare digitale fundamenten. Uniserver helpt zorginstellingen om controle te houden over hun data, infrastructuur en leverancierskeuzes. Als Nederlands cloudspecialist bieden we volledig beheerde, soevereine cloudoplossingen die voldoen aan de strengste eisen op het gebied van veiligheid, compliance en continuïteit.

Onze infrastructuur wordt gehost in Nederlandse datacenters, onder Nederlandse wetgeving, en is aantoonbaar voorbereid op wet- en regelgeving zoals NIS2, de AVG en NEN 7510. Daarmee bieden we een robuust fundament voor moderne zorgapplicaties, EPD's en ketensamenwerking.

Samenwerken in het ecosysteem
Wij werken nauw samen met partijen als ilionx, Equans en zorgsoftwareleveranciers. Door verantwoordelijkheden helder te verdelen, ontstaat een flexibele en beheersbare IT-omgeving. Zo houden zorginstellingen grip op hun digitale toekomst, zonder afhankelijk te zijn van buitenlandse hyperscalers.

Ook klaar voor AI in de zorg
Voor organisaties die verder willen kijken, bieden we ondersteuning bij de veilige inzet van AI. Met Fuse AI, onze private AI-oplossing, kunnen zorginstellingen bijvoorbeeld gestructureerde rapportages en voorspellende analyses mogelijk maken, altijd binnen een streng gereguleerde, soevereine private cloudomgeving. Niet als doel op zich, maar als uitbreiding van een veilig fundament.

Meer weten?
We denken graag met je mee over wat bij jouw zorginstelling past. Van compliance tot cloudstrategie, en van regie tot samenwerking.

Pim Kerstens | p.kerstens@uniserver.nl
+31 6 27 19 05 59