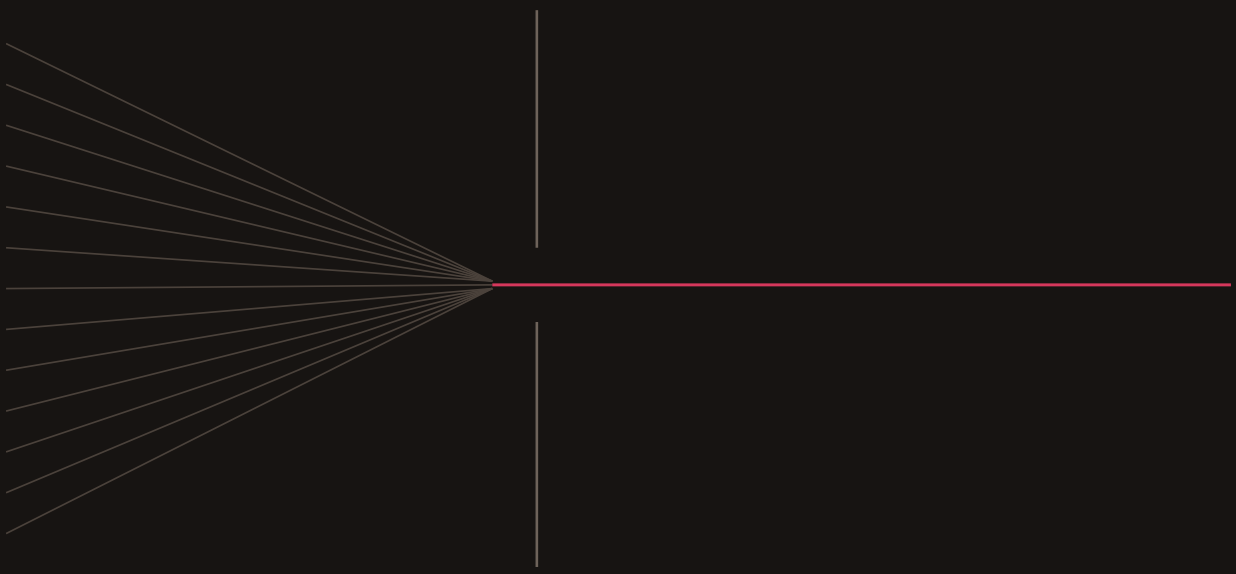
inforeports

WHITEPAPER
VERSIE 1.0



AI in de BI van het ziekenhuis: van experiment naar verantwoorde inrichting

00

Managementsamenvatting

AI is het ziekenhuis al binnen. Medewerkers gebruiken het op eigen initiatief, ook op plekken waar gevoelige gegevens rondgaan. De vraag die daarmee op tafel ligt: hoe geeft het ziekenhuis dit gebruik bewust vorm? Goed ingezet doet AI werk dat nu blijft liggen of te veel tijd kost, van het samenvatten van vrije tekst tot het versnellen van ontwikkelwerk.

Deze whitepaper beschrijft hoe AI verantwoord is in te zetten op de BI-omgeving van het ziekenhuis. De belangrijkste inzichten:

AI in de BI-omgeving betekent twee verschillende dingen: AI die helpt bouwen aan rapportages en datamodellen, en AI die met de data werkt. Het risico verschilt sterk, dus de regels moeten dat ook doen.

Beleid en data governance geven houvast: ze leggen vast welke gegevens waarheen mogen, wie eigenaar is, wie waarover besluit en hoe gebruik wordt vastgelegd. Daarmee is per aanvraag te beoordelen wat verantwoord is.

Veiligheid ligt het stevigst vast in de techniek. Standaard draait het werk op een AI-model in de eigen omgeving van het ziekenhuis. Per taak staat in code vastgelegd of gegevens naar buiten mogen, en elke aanroep wordt geregistreerd.

Een lokaal model draait op een eigen server, in huis of gehost binnen de EU, gekoppeld aan het netwerk van het ziekenhuis. Gevoelige data blijft standaard binnen; wat bij uitzondering naar buiten gaat, ligt per taak vast en wordt geregistreerd.

AI in de BI van het ziekenhuis moet gezien worden als een applicatie, met eigen beheer: van gebruikers en rechten tot koppelingen, monitoring en probleemoplossing.

De implementatie kan gefaseerd verlopen en aansluiten op de behoefte en kennisontwikkeling van de gebruikers, begeleid door de applicatiebeheerder AI. InfoReports heeft tooling ontwikkeld waarmee AI op een veilige manier toegepast kan worden op de data van het ziekenhuis, en helpt bij de inrichting, het beheer en de benodigde hardware, waarbij de inrichting, de toepassingen en de data van het ziekenhuis zelf zijn en blijven.

Inhoud

JURIDISCH KADER

Over de juridische onderwerpen in deze whitepaper. Deze whitepaper raakt aan wetgeving zoals de AVG, de CLOUD Act, de Cyberbeveiligingswet en de Europese AI-verordening. De tekst beschrijft die op hoofdlijnen en is geen juridisch advies. Wat de regels betekenen voor een specifieke situatie vraagt een eigen beoordeling; daarvoor is overleg met de functionaris gegevensbescherming of een gespecialiseerde jurist de aangewezen weg.

01

HOOFDSTUK 01

Waarom nu

In vrijwel elk ziekenhuis wordt al met AI gewerkt. Medewerkers zijn het zelf gaan gebruiken: een arts die een brief laat herschrijven, een beleidsadviseur die een rapport laat samenvatten, een BI-ontwikkelaar die code laat controleren. Handig en snel.

Dat gebruik ontstaat sneller dan de afspraken eromheen. Welke gegevens gaan er in zo'n vraag mee? Naar welke aanbieder gaat dat, en wat gebeurt daar met de invoer? Wie heeft er zicht op wat er in totaal naar buiten gaat? In veel organisaties staan die vragen nog open, terwijl het gebruik intussen doorloopt en groeit.

Voor de BI-omgeving weegt dat extra zwaar. Het datawarehouse is de plek waar veel van de organisatie samenkomt: gegevens uit het ZIS/EPD, en daarnaast personeelsgegevens, verzuim, salarissen en de financiën van het ziekenhuis zelf. Patiëntgegevens springen er qua gevoeligheid uit, maar de rest doet er weinig voor onder: ook een verzuimlijst of een salarisoverzicht mag de organisatie niet verlaten. In deze whitepaper heet dit alles samen gevoelige gegevens.

Het houdt bovendien niet op bij het datawarehouse: ook elders op het netwerk staan gevoelige gegevens, in documenten, verslagen en aparte registraties. Juist daar liggen veel taken waar AI direct bruikbaar voor is: vrije tekst samenvatten, vragen over documenten beantwoorden, een analyse maken van een tabel die het datawarehouse nooit haalt. De inzet van AI kan zich dus uitstrekken over de hele omgeving waar gevoelige gegevens staan. Maar tegelijkertijd is dat ook de omgeving waar de meeste grip op die gevoelige data noodzakelijk is.

01

VERVOLG

Die grip is geen doel op zich. Wie de inzet goed inricht, krijgt werk gedaan dat nu blijft liggen of te veel tijd kost: vrije tekst waar niemand meer aan toekomt, uitzoekwerk dat dagen duurt, ontwikkelwerk dat sneller kan. Deze opbrengst is de reden om de grip te regelen; de inrichting zorgt dat het verantwoord kan, en dat het verantwoord blíjft kunnen als het gebruik groeit.

Deze whitepaper gaat over de vraag hoe een ziekenhuis AI op die omgeving inzet op een manier die het kan verantwoorden: met een inrichting waarin per geval duidelijk is wat er kan en waarom. De onderdelen daarvan komen stuk voor stuk aan bod: beleid en data governance, gegevensbescherming, architectuur, hardware, beveiliging, beheer en de mensen die ermee werken.

02

HOOFDSTUK 02

Twee soorten AI in de BI-omgeving

"AI inzetten op de BI" is een verzamelterm, die uiteenvalt in twee heel verschillende soorten gebruik, elk met een eigen risicoprofiel.

Het eerste is AI die de BI-ontwikkelaar helpt met bouwen: een assistent die meedenkt over het inlaadproces van gegevens (ETL), het datamodel of het rapportontwerp. Die werkt met structuur, logica en code: tabelnamen, relaties, berekeningen. De gevoelige gegevens zelf komen daar niet aan te pas. Het risico voor gevoelige data is laag, en de winst zit in het tempo: ontwikkelwerk gaat sneller, en een klein BI-team kan meer aan.

Het tweede is AI die met de data werkt. Vragen stellen aan de inhoud, vrije tekst laten samenvatten, een tabel laten analyseren. Hier ontmoet gevoelige data het AI-model: het taalmodel dat de vraag leest en het antwoord maakt. Dit is waar het grootste risico zit, en waar de rest van deze whitepaper vooral over gaat.

Het onderscheid lijkt scherp, maar vervaagt in de praktijk sneller dan gedacht. Een ontwikkelaar die een query laat verbeteren, plakt er al gauw een stukje uitvoer bij om te laten zien wat er misgaat, en in die uitvoer staan echte gegevens; misschien herleidbaar op personen, misschien ook niet. Het onderscheid houdt dus alleen stand als ook de overgang bewaakt wordt: bouwen gebeurt met testdata of met structuur zonder inhoud, en zodra er echte gegevens in beeld komen, gelden de regels van de tweede soort.

02

VERVOLG

Met die kanttekening erbij is het onderscheid goed bruikbaar om per soort de juiste afspraken te maken. Voor de bouwkant volstaan drie: werk met testdata of met structuur zonder inhoud, plak geen echte uitvoer in een extern hulpmiddel, en gelden zodra er toch echte gegevens in beeld komen de regels van de tweede soort. Daarmee kan het ontwikkelwerk snel blijven zonder dat het langs elke afweging in deze whitepaper moet. Voor de datakant zijn de voorwaarden nodig die in de volgende hoofdstukken aan bod komen.

Naast deze twee soorten is er AI die het ziekenhuis al in huis heeft via bestaande leveranciers: een assistent in de kantoorsoftware, AI-functies in het EPD of in de rapportagetools. Die vallen onder de contracten en voorwaarden van die leveranciers, en de vragen uit deze whitepaper gelden er onverkort voor: welke gegevens gaan erin, waar worden ze verwerkt, en wie kan erbij? Hoe serieus die vragen zijn, bleek in 2026, toen de Autoriteit Persoonsgegevens een voorgenomen inzet van zo'n assistent in de kantoorsoftware bij de gemeente Haarlemmermeer beoordeelde: in de voorgelegde vorm zou die de AVG schenden, en de inzet mocht pas starten na aanvullende maatregelen.[2] Ook wat kant-en-klaar geleverd wordt, is dus niet vanzelf geregeld. Bij AI van leveranciers hangt het antwoord op die vragen af van wat de leverancier prijsgeeft en toestaat. Deze whitepaper gaat over het deel waar het ziekenhuis die antwoorden zelf in de hand heeft: de AI die het ziekenhuis zelf inricht, op de eigen data en de eigen infrastructuur. "Eigen infrastructuur" betekent daarbij exclusief voor het ziekenhuis, of die infrastructuur nu in huis staat of gehost wordt; hoofdstuk 7 werkt dat uit.

03

HOOFDSTUK 03

De rol van beleid en data governance

Zolang afspraken ontbreken, beantwoordt iedere medewerker de vragen uit hoofdstuk 1 zelf, per keer, naar eigen inzicht. AI-beleid heeft in dit verhaal dan ook een duidelijke functie: het geeft medewerkers en leidinggevenden houvast bij keuzes die anders steeds opnieuw worden gemaakt. Werkbaar AI-beleid hoeft geen dik document te zijn, maar het beantwoordt wel minimaal drie vragen.

1 **Welke gegevens mogen waarheen.** De basis is een dataclassificatie: een indeling van gegevens in categorieën, bijvoorbeeld openbaar, intern, vertrouwelijk en patiëntgerelateerd, met per categorie de toegestane bestemmingen: een model in eigen huis, een aanbieder binnen de EU onder voorwaarden, een aanbieder buiten de EU onder aanvullende voorwaarden, of helemaal niet buiten de eigen systemen. Zo'n classificatie maakt het beleid toepasbaar op nieuwe situaties zonder dat elke situatie apart beschreven hoeft te worden. Veel ziekenhuizen hebben er al een voor de informatiebeveiliging; het AI-beleid kan daarop voortbouwen.

2 **Wie mag wat.** Welke AI-toepassingen staan open voor welke groepen medewerkers: mag een controller een tabel laten analyseren, mag een kwaliteitsmedewerker teksten laten samenvatten? Het beleid beantwoordt dit eenmalig, langs de dataclassificatie en de gebruikersgroepen die er al zijn. Nieuwe taken zijn daarna binnen die kaders in te richten, zonder aparte besluitronde per geval.

Hier hoort ook het gebruik buiten de eigen omgeving bij: een publieke chatbot in de browser. Het beleid geeft daar antwoord op met dezelfde dataclassificatie: wat openbaar of intern is mag daarheen, de rest niet. Zo'n antwoord werkt beter naarmate er binnen de muren een bruikbaar alternatief staat, want een verbod zonder alternatief verplaatst het gebruik alleen naar plekken waar niemand het ziet.

03

VERVOLG

3 **Hoe wordt het vastgelegd.** Welk gebruik wordt geregistreerd, waar staat die registratie, en wie kijkt ernaar? Vastlegging maakt het mogelijk om achteraf na te vertellen wat er is gebeurd, met welke gegevens en met welk model. Dat is nodig bij vragen van een toezichthouder, en minstens zo waardevol voor de organisatie zelf: het maakt zichtbaar hoe het gebruik zich ontwikkelt en waar het beleid moet meegroeien.

De drie vragen worden beantwoord bij het opstellen van het beleid, met de functionaris gegevensbescherming aan tafel, en daarna periodiek herijkt: bijvoorbeeld jaarlijks, of eerder als er iets wezenlijks verandert. Het beleid leunt daarbij op de data governance die het ziekenhuis al heeft. Daar hoort data-eigenaarschap bij: voor veel gegevens is belegd wie er inhoudelijk over gaat, van zorgadministratie tot financiën, en die eigenaren worden betrokken bij de afspraken over het gebruik van hun gegevens in AI-taken. Het AI-beleid sluit zo aan op wat er al is, zonder een nieuwe structuur op te tuigen.

Data governance omvat daarnaast datakwaliteit, en die krijgt met AI extra gewicht. Een model dat op het datawarehouse werkt, neemt de kwaliteit van dat warehouse één op één mee in zijn antwoorden. In een rapportage valt een onvolkomenheid nog op bij wie de cijfers kent; een taalmodel verpakt diezelfde onvolkomenheid in een vloeiend geformuleerd antwoord. Werk aan datakwaliteit betaalt zich met AI dus dubbel uit.

03

VERVOLG

Beleid en techniek versterken elkaar hierbij. Afspraken op papier werken zolang iedereen ze kent en volgt; een inrichting die de afspraken technisch afdwingt, garandeert de naleving ervan. Andersom geeft het beleid richting aan wat er technisch wordt ingesteld: de configuratie is de vertaling van wat de organisatie heeft besloten. De hoofdstukken 6 en 7 beschrijven hoe die technische kant eruitziet.

PRAKTIJKVOORBEELD

Zo ziet dat er in de praktijk uit. Een kwaliteitsmedewerker wil een reeks anamneses laten samenvatten. In de AI-omgeving van het ziekenhuis kan dat meteen: de teksten in de chat plakken en om een samenvatting vragen. Niets houdt dat tegen, en dat hoeft ook niet, want het draait op het lokale model: de gegevens blijven binnen en het gebruik wordt geregistreerd. Een ingerichte taak komt in beeld zodra er meer nodig is: een vaste toepassing met eigen instellingen, gekoppeld aan de bron zelf, voor grotere aantallen, voor een vaste werkwijze binnen de afdeling, of om de kracht van een extern model te mogen gebruiken. De applicatiebeheerder AI richt zo'n taak in binnen de kaders die het beleid al heeft vastgelegd: de dataclassificatie bepaalt welk model en welke bestemming zijn toegestaan, en de toegang loopt via het bestaande accountbeheer, waar de rollen aan de bestaande groepen worden gekoppeld.

04

HOOFDSTUK 04

AI en de AVG

De AVG is techniekneutraal en geldt bij elke verwerking van persoonsgegevens, met of zonder AI.[1] Ook een model dat volledig binnen het ziekenhuis draait, verwerkt persoonsgegevens zodra die in een vraag of in een bron zitten. Een lokale opzet verandert de verplichtingen dus niet. Wat er altijd geregeld moet zijn: een grondslag en een duidelijk doel, een verwerkingsregister waarin ook de AI-verwerkingen staan, bij verwerkingen met een hoog risico een gegevensbeschermingseffectbeoordeling (DPIA), en een privacyverklaring die klopt met wat er gebeurt. In een ziekenhuis, waar gezondheidsgegevens tot de bijzondere persoonsgegevens horen, is dat hoge risico snel aan de orde. De functionaris gegevensbescherming, in hoofdstuk 3 al aan tafel bij het beleid, heeft hier zijn wettelijke rol.

De Autoriteit Persoonsgegevens heeft dit terrein recent concreet ingevuld. In juli 2026 publiceerde de AP een AVG-handreiking voor ontwikkelaars van generatieve AI en een praktisch hulpmiddel voor organisaties die generatieve AI willen invoeren, gebaseerd op een voorafgaande raadpleging over Microsoft 365 Copilot.[2] Het advies daarin is voor elk ziekenhuis bruikbaar: onderzoek eerst of generatieve AI gebruikt kan worden zonder persoonsgegevens te verwerken. Dat sluit aan op het onderscheid uit hoofdstuk 2: aan de bouwkant kan dat vrijwel altijd, bij het werken met data lang niet altijd.

04

VERVOLG

Veel organisaties zoeken een deel van het antwoord in een zakelijk AI-abonnement, vaak "enterprise" genoemd, waarbij de aanbieder toezegt invoer niet te gebruiken om modellen te trainen. Dat is een zinvolle stap, met een beperking die vaak wordt overgeslagen: de gegevens gaan nog steeds naar buiten, de aanbieder wordt daarmee een verwerker waar een verwerkersovereenkomst mee nodig is, en de toezegging gaat over trainen; over bewaartermijnen en over wie er verder bij kan, is daarmee nog weinig gezegd.

Daar komt een hardnekkig misverstand bij: dat gegevens veilig te delen zijn zodra de namen eruit zijn. Herleidbaarheid zit zelden alleen in de naam. Een zeldzame diagnose in combinatie met een geboortejaar en een postcodegebied wijst al snel één persoon aan. Wie gegevens naar buiten laat gaan, moet dus preciezer werken dan namen weglakken; hoofdstuk 6 laat zien hoe dat vorm krijgt.

De conclusie van dit hoofdstuk is overzichtelijk. De verplichtingen van de AVG gelden hoe dan ook, en een inrichting waarin het werk binnen de eigen omgeving gebeurt, maakt het naleven een stuk eenvoudiger: er is geen doorgifte aan een externe AI-aanbieder, en de kring van systemen en mensen die de gegevens zien blijft klein. De registratie die verderop in deze whitepaper terugkomt, levert bovendien het overzicht dat de AVG toch al vraagt.

05

HOOFDSTUK 05

Soevereiniteit: wie heeft de zeggenschap

Naast de privacyvraag uit het vorige hoofdstuk is er een tweede vraag: die van de soevereiniteit, de zeggenschap over de gegevens. De rijksoverheid omschrijft datasoevereiniteit als het waarborgen van controle over de locatie, de verwerking en de toegang tot informatie.[3] In de kern gaat het om vier vragen: wie bepaalt waar de gegevens staan, wie kan erbij, onder welk recht valt dat, en wie kan ingrijpen als het erop aankomt? Die vragen staan los van de privacyvraag uit het vorige hoofdstuk: een verwerking kan volledig aan de AVG voldoen terwijl de zeggenschap bij een buitenlandse partij ligt.

In de praktijk krijgt deze vraag minder aandacht dan de privacyvraag, terwijl hij zwaar weegt. Beslissend is wie de aanbieder bezit: het recht van het land van het moederbedrijf reikt mee tot aan de gegevens. Het bekendste voorbeeld is Amerikaans: een aanbieder met een Amerikaans moederbedrijf valt onder Amerikaans recht, ook als de vennootschap, het personeel en de datacentra volledig binnen de EU zitten. Zo'n aanbieder kan onder de CLOUD Act verplicht worden gegevens af te geven aan de Amerikaanse overheid, ook als die gegevens in een datacentrum binnen de EU staan. Microsoft bevestigde dat medio 2025 onder ede, tijdens een hoorzitting van de Franse Senaat: de directeur juridische zaken van Microsoft Frankrijk kon daar geen garantie geven dat gegevens uit de EU buiten het bereik van een Amerikaans bevel blijven.[4] Ook de nieuwe "soevereine" cloudvarianten die Amerikaanse aanbieders sindsdien lanceren, veranderen daar weinig aan, want het eigendom verandert niet mee. Het eigendom van de aanbieder weegt dus zwaarder dan de plek van de server.

05

VERVOLG

Afhankelijkheid gaat bovendien verder dan de vraag wie bij de gegevens kan. Een aanbieder kan ook verplicht worden de toegang tot de dienst zelf af te sluiten, bijvoorbeeld door sancties of exportmaatregelen. Daar bestaan inmiddels praktijkvoorbeelden van, waarbij diensten van de ene op de andere dag niet meer beschikbaar waren voor bepaalde klanten of regio's. Voor een ziekenhuis dat AI in het dagelijkse werk opneemt, is ook die vorm van afhankelijkheid een afweging waard. Een uitgebreide analyse van beide kwesties, met AWS in Europa als casus, is te vinden in het dossier soevereiniteit van Metagora.[5]

FIGUUR 1 · DE LADDER VAN ZEGGENSCHAP

05

VERVOLG

Soevereiniteit vraagt overigens niet dat alle gegevens op eigen servers staan; het vraagt dat de grip juridisch, technisch en organisatorisch geregeld is. Zeggenschap is daarmee een ladder. Eigen hardware in het eigen netwerk staat bovenaan: eigen rechtsmacht, fysieke controle, en geen aanbieder die de toegang kan afsluiten. Een aanbieder waarvan eigendom en recht binnen de EU liggen, staat daar vlak onder en regelt de zeggenschap juridisch ook goed; wat daar overblijft is gewone leveranciersafhankelijkheid, met continuïteit en overstapbaarheid als aandachtspunten. Voor veel ziekenhuizen is dat in de praktijk ook de begaanbare route: een server bij een aanbieder in Nederland of elders in de EU, via een VPN-verbinding gekoppeld aan het eigen netwerk, geeft vrijwel dezelfde grip zonder dat het ziekenhuis zelf hardware hoeft te huisvesten. Een aanbieder met een moederbedrijf buiten de EU staat onderaan de ladder, ook in een EU-regio en ook in een soevereine variant; de Amerikaanse voorbeelden hierboven zijn de bekendste, maar de redenering geldt voor elk recht buiten de EU. De dataclassificatie uit hoofdstuk 3 bepaalt welk niveau voor welke categorie gegevens volstaat; de inrichting uit het volgende hoofdstuk werkt op elk van de bovenste treden.

06

HOOFDSTUK 06

Inrichting: de architectuur bepaalt wat kan

De hoofdstukken hiervoor eindigen steeds op hetzelfde punt: de afspraken moeten ergens worden waargemaakt. Dat kan op papier, met richtlijnen en goede wil, en het kan in de techniek. Een richtlijn beschrijft de gewenste keuze; een systeem dat de keuze afdwingt, sluit andere keuzes uit.

Het antwoord daarop is een AI-gateway: één doorgang waar al het AI-verkeer van de BI-omgeving doorheen loopt. AI-mogelijkheden duiken op in steeds meer losse gereedschappen, elk met eigen instellingen en eigen voorwaarden. Eén centrale doorgang betekent één plek waar de regels staan, één plek waar geregistreerd wordt, en één plek om te controleren. Welke gateway een ziekenhuis ook kiest, hij moet vier afspraken afdwingen.

FIGUUR 2 · DE GATEWAY ALS ÉÉN DOORGANG

1 **Standaard blijft alles binnen.** Het werk draait op een taalmodel in de eigen omgeving van het ziekenhuis. Voor veel taken, zoals het samenvatten van vrije tekst of het beantwoorden van vragen over documenten, is zo'n lokaal model ruim voldoende. Gevoelige gegevens verlaten het huis niet.

06

VERVOLG

2 **Vrijgave per taak, vastgelegd in code.** Een taak is hier een afgebakende toepassing met eigen instellingen: het samenvatten van meldingen, het beantwoorden van vragen over protocollen, het aanvullen van omschrijvingen in een rapportage. Per taak ligt vast welke modellen gebruikt mogen worden en welke gegevens erin mogen; binnen die vrijgave kan een gebruiker kiezen met welk toegestaan model hij werkt. "Vastgelegd in code" betekent hier: een instelling in een bestand onder versiebeheer, die een gebruiker niet zelf kan wijzigen, die na te lezen is, en waarvan te zien is wie hem wanneer heeft aangepast. De gateway kan naast het datawarehouse ook andere bronnen aansluiten via één standaardmanier van koppelen, en elke aangesloten bron valt onder dezelfde vrijgaveregels. Sommige taken hebben de kracht van een groot extern model nodig; of dat mag, staat in de configuratie van de taak en ligt daarmee buiten het keuzemoment van de individuele gebruiker. En wie met het gewone ziekenhuisaccount inlogt, krijgt nooit toegang tot externe modellen; dat recht geeft de beheerder alleen bewust en gericht uit. Een gevoelige samenvatting van vrije tekst blijft gesloten voor de cloud.

3 **Pseudonimisering met vaste regels.** Stuurt een analysetaak gegevens naar een extern model, dan worden gevoelige waarden in de tekst vooraf vervangen volgens vaste, controleerbare regels die per taak zijn vastgelegd. Een taak die naar buiten mag zonder zulke regels, weigert het systeem als configuratiefout. Welke waarden vervangen moeten worden, is een inrichtingskeuze per taak; hier komt het misverstand uit hoofdstuk 4 terug, want herleidbaarheid zit zelden alleen in de naam. Vaste regels vangen dat combinatierisico nooit volledig; de eerste en belangrijkste keuze blijft daarom of een taak überhaupt naar buiten mag, en de pseudonimisering is de tweede verdedigingslinie. Er hoeft geen AI zelf te oordelen over wat gevoelig is: dat besluit is al genomen en in regels gegoten, en die regels zijn na te lezen en te controleren.

06

VERVOLG

4 **Alles wordt geregistreerd.** Elke aanroep wordt vastgelegd: welke taak, welk model, hoeveel gegevens, in een register waarin elke regel aan de vorige vastzit, zodat aanpassing achteraf zichtbaar wordt. Toezichthouders vragen daarom, en de organisatie heeft er zelf het meest aan: bij een vraag of een incident is te achterhalen wat er is gebeurd, en het gebruik per taak is te volgen in de tijd.

INFOREPORTS

De invulling van InfoReports. InfoReports heeft de vier afspraken uit dit hoofdstuk gebouwd in de InfoReports AI Gateway, samen met de inrichting en het beheer eromheen. De hoofdstukken hierna gaan uit van die invulling, en wat er staat is evengoed te gebruiken als toets voor elke andere oplossing die een ziekenhuis overweegt. Meer over de InfoReports AI Gateway staat op inforeports.nl/aanbod/ai-gateway.

Deze inrichting geeft de vraag "mag dit?" een antwoord dat te laten zien is: zo staat het ingesteld, dit blijft binnen, dat gaat onder deze voorwaarden naar buiten, en hier staat het logboek. De waarde die in het datawarehouse ligt, komt zo binnen bereik van AI, terwijl het ziekenhuis de controle over zijn gegevens houdt.

Daarbij hoort één kanttekening: de techniek dwingt alleen af wat door de gateway loopt. Voor gebruik daarbuiten, zoals een publieke chatbot in de browser, blijft de combinatie nodig die eerder aan bod kwam: een beter alternatief binnen de muren, duidelijke afspraken in het beleid, en waar de organisatie dat wil aangevuld met maatregelen op de werkplek.

07

HOOFDSTUK 07

Hardware en infrastructuur

Lokaal als standaard roept meteen een praktische vraag op: waar draait dat dan? Een eigen taalmodel heeft rekenkracht nodig, en wel van een ander soort dan de servers die er al staan. Concreet gaat het om een server met videokaarten (GPU's) die zijn gebouwd voor AI-rekenwerk. Die kan op twee plekken staan, in lijn met de ladder uit hoofdstuk 5: in het eigen netwerk van het ziekenhuis, of gehost bij een aanbieder in Nederland of elders in de EU, via een VPN-verbinding gekoppeld aan dat netwerk. In beide gevallen is de machine exclusief voor het ziekenhuis, gekocht of gehuurd als dedicated server, en valt het werk onder EU-recht.

Voor de taken waar het hier om gaat volstaat in de regel één goed gekozen machine, afgestemd op het aantal gebruikers dat tegelijk werkt; groeit die groep, dan groeit de capaciteit mee. De modellen die erop draaien zijn vrij beschikbaar en de afgelopen jaren sterk verbeterd: voor samenvatten, vragen beantwoorden en tekst verwerken zijn ze ruim toereikend, en ze draaien volledig op de eigen machine. Bij Nederlandstalige medische vrije tekst zijn de grote commerciële modellen op dit moment sterker. Juist daarvoor bestaat de vrijgaveroute per taak uit hoofdstuk 6: waar dat verschil telt en de gegevens het toelaten, kan een taak gericht naar buiten.

De keuze voor een eigen machine levert drie dingen op. Ten eerste de zekerheid uit hoofdstuk 5: gevoelige gegevens blijven in eigen huis of bij een aanbieder binnen de EU, onder EU-recht. Ten tweede voorspelbare kosten: de machine staat er en doet zijn werk, zonder afrekening per aanroep die oploopt naarmate het gebruik groeit. Ten derde onafhankelijkheid: een prijswijziging, koerswijziging of zelfs een afsluiting bij een grote AI-aanbieder, zoals beschreven in hoofdstuk 5, verandert niets aan wat er op de eigen machine draait.

07

VERVOLG

Een eigen machine betekent natuurlijk ook eigen verantwoordelijkheid voor de beveiliging ervan. Of de server nu in huis staat of via een VPN-verbinding aan het netwerk hangt, hij krijgt een afgeschermde plek: een gescheiden netwerksegment, toegang voor een klein aantal beheerders, en een vast ritme van updates voor het systeem en de modellen erop. De beveiliging van deze omgeving is onderdeel van de informatiebeveiliging van het ziekenhuis als geheel, met dezelfde eisen en dezelfde controles als voor andere systemen die met gevoelige gegevens werken.

Daar komt de zorg voor de machine zelf bij: kiezen, inrichten, onderhouden en op tijd vervangen. Serverbeheer hoort bij het reguliere werk van een ICT-afdeling; wat hier bijkomt is gespecialiseerde kennis van het AI-platform zelf, zoals de modelserver en de Linux-omgeving eromheen, en de capaciteit om dat naast het bestaande werk te doen. Die kennis en capaciteit zijn zelden standaard aanwezig, en hoeven dat ook niet te zijn. InfoReports faciliteert de aanschaf of huur en de inrichting van deze hardware en neemt het technisch beheer op zich; de gegevens en de inrichting op die machine zijn en blijven van het ziekenhuis. Wie technisch beheer voert op een omgeving met gevoelige gegevens, is daarmee verwerker in de zin van de AVG; die rol en de bijbehorende afspraken liggen vast in een verwerkersovereenkomst. In hoofdstuk 9 komt terug hoe de rolverdeling in de organisatie belegd wordt.

08

HOOFDSTUK 08

Applicatiebeheer van AI

Over de vraag of AI mag, wordt veel geschreven. Over de vraag wie het daarna beheert, veel minder. Toch is dat waar het na de invoering om draait: een AI-toepassing is een applicatie, en applicaties hebben beheer nodig. Dat vraagt een eigen rol, de applicatiebeheerder AI.

En er verandert nogal eens iets. Taalmodellen krijgen updates, worden vervangen of verdwijnen. De aanbieder van een extern model wijzigt zijn prijzen of voorwaarden, wat de taken raakt die daarvan gebruikmaken. Een nieuwe versie van een model geeft op dezelfde vraag een ander antwoord dan de vorige.

Die laatste verandering laat het verschil met klassiek applicatiebeheer het duidelijkst zien. Na een modelwisseling levert dezelfde samenvattingstaak opeens langere teksten, of blijft een veld leeg dat eerst altijd gevuld was. Een rapportage die daarop doorbouwt, klopt ongemerkt niet meer, en dat valt pas op als iemand het mist. Bij klassieke software is een update vooral een technische gebeurtenis; bij AI is het ook een inhoudelijke, omdat het gedrag van een model niet vastligt in regels die na te lezen zijn.

Goed applicatiebeheer voor AI omvat daarom meer dan bij een gemiddelde applicatie. Een overzicht van wat er belegd moet zijn:

INHOUD EN KWALITEIT

Eigenaarschap: wie is verantwoordelijk voor de toepassing, inhoudelijk en technisch, en hoe sluit dat aan op het data-eigenaarschap uit hoofdstuk 3?

Beheer van taken en instructies: de instructies en hulpmiddelen die de AI per taak gebruikt, moeten worden bijgehouden, verbeterd en getest, net als code.

Versiebeheer van modellen: welk model draait er, sinds wanneer, en wat draaide er daarvoor?

Kwaliteitsbewaking: een vaste set testvragen met gewenste uitkomsten, die na elke wijziging opnieuw wordt doorlopen. Wijkt het gedrag af, dan komt dat bij het beheer boven tafel in plaats van bij de gebruiker.

08

VERVOLG

Wijzigen en accepteren: wie geeft akkoord dat een nieuwe taak of een nieuw model live gaat, waar wordt dat eerst beproefd, en hoe worden gebruikers over een wijziging geïnformeerd?

Uitfaseren: taken die niemand meer gebruikt worden opgeruimd, inclusief de bijbehorende rechten en koppelingen.

GEBRUIKERS

Gebruikersbeheer: wie krijgt toegang tot welke taken, en wat gebeurt er bij vertrek of functiewisseling?

Training en ondersteuning: hoe leren gebruikers met AI werken, bij de start en bij nieuwe taken, en waar kunnen ze terecht met vragen over het gebruik?

Rechten: welke taak mag bij welke gegevens, aansluitend op de rechtenstructuur die er voor het datawarehouse al is. AI mag nooit meer zien dan de gebruiker zelf mag zien; dat vraagt dat de rechten tot op databaseniveau zijn ingericht.

Functiescheiding: wie een taak mag inrichten die gegevens naar buiten stuurt, en wie daarop meekijkt. Een tweede paar ogen op die vrijgaven is een kleine maatregel met veel effect.

TECHNIEK EN KOPPELINGEN

Koppelingen met bronnen: welke databases en systemen zijn aangesloten, wie beheert die koppelingen, en wat gebeurt er als een bron wijzigt?

Monitoring: draaien de koppelingen, halen de taken hun antwoorden op tijd op, en wie ziet het als er iets hapert?

Probleemoplossing: waar melden gebruikers een storing of een vreemde uitkomst, en wie pakt dat op?

Continuïteit en herstel: wat gebeurt er als de server uitvalt, hoe snel moet de omgeving weer draaien, en welke back-up hoort daarbij? Bij één machine hoort daar een expliciete keuze bij: wat is een acceptabele stilstand, en is er een terugvaloptie nodig, bijvoorbeeld een tweede machine of het tijdelijk stilleggen van de AI-taken.

Beveiligingsincidenten: hoe wordt een vermoedelijk datalek of beveiligingsincident gemeld, aan wie binnen de organisatie, en wat betekent dat voor de meldplichten die het ziekenhuis toch al kent.

08

VERVOLG

STURING EN VASTLEGGING

Leverancierscontact: wie onderhoudt het contact met de leverancier van de software, de hostingpartij en eventuele externe modelaanbieders, over updates, storingen en contracten? Leg daarbij vast hoe en hoe lang van tevoren een modelwissel wordt aangekondigd, zodat de testset vooraf kan draaien in plaats van achteraf.

Gebruik en kosten: wie gebruikt wat, hoeveel, en past dat nog bij de afspraken? Voor taken die naar een extern model mogen, horen daar limieten per taak of per gebruiker bij, zodat het verbruik begrensd is.

Het logboek zelf: hoe lang wordt de registratie bewaard, waar staat die, wie mag erin kijken en op welke grond? Registratie van AI-gebruik op patiëntgegevens is zelf een verwerking van persoonsgegevens; zonder afspraken hierover wordt de sterkste maatregel een nieuw risico.

Dit hoeft geen zware bureaucratie te worden. Voor een BI-omgeving gaat het om een overzichtelijk aantal taken en modellen. De registratie uit hoofdstuk 6 dekt daarbij het gebruik en de herleidbaarheid; de vaste testset en de kostenafspraken zijn het werk van de applicatiebeheerder AI zelf. Waar het om gaat is dat die er op vaste momenten en volgens een vaste werkwijze naar kijkt.

09

HOOFDSTUK 09

Beheer en beveiliging in de dagelijkse praktijk

Naast het applicatiebeheer van de AI zelf is er de vraag waar dit alles in de organisatie thuishoort en hoe de beveiliging op orde blijft.

De organisatorische plek eerst. AI op de BI-omgeving ligt op het snijvlak van het BI-team en ICT. Het BI-team kent de data, de taken en de gebruikers; ICT kent het netwerk, de servers en de beveiliging. In de praktijk werkt een eenvoudige verdeling het best: het functionele beheer bij de applicatiebeheerder AI, meestal gepositioneerd bij het BI-team, het technische beheer bij ICT of bij een partner, en één iemand die eindverantwoordelijk is voor het geheel. Meestal is dit een uitbreiding van het functioneel beheer dat er voor het datawarehouse en de rapportagetool al is, en geen nieuwe functie: dezelfde persoon kent de bronnen, de rechtenstructuur en de gebruikers, en de AI-taken sluiten daarop aan. Belangrijker dan de precieze verdeling is dat die er is, en dat hij op papier staat.

Dan de beveiliging. Naast de klassieke onderdelen, zoals de netwerkbeveiliging uit hoofdstuk 7, brengt AI eigen risico's mee. Het bekendste: gebruikers kunnen via slim geformuleerde vragen proberen het model iets te laten doen waarvoor het niet is bedoeld, bijvoorbeeld gegevens ophalen waar hun taak niet voor is ingericht. Het antwoord daarop zit in de plek waar de grens ligt: bij de database zelf. Een instructie aan het model is met een slimme vraag te omzeilen; de database is dat niet. Mits de rechten op databaseniveau zijn ingericht, tot en met de filtering per gebruiker, geeft die fysiek geen rijen buiten iemands bereik, laat hij alleen leesopdrachten door en dwingt hij dat op de opdracht zelf af. Die inrichting is een voorwaarde. Staat hij, dan blijft AI binnen de rechten die de gebruiker al had, en levert een handige vraag geen extra toegang op.

09

VERVOLG

Deze voorwaarde verdient aandacht, want ze is niet overal ingevuld. In veel omgevingen is de autorisatie geregeld in de rapportagelaag, en niet in de database eronder. Ligt de filtering per gebruiker daar niet, dan blijven taken mogelijk die op een vaste, afgebakende selectie werken, of die draaien onder de rechten van een gedeeld account met een beperkte set gegevens. Wat dan niet kan, is een gebruiker vrij laten vragen aan een brede bron. Het inrichten van rechten op databaseniveau is daarmee vaak de eerste stap, en soms een project op zichzelf; het is werk dat losstaat van AI en dat ook zonder AI waarde heeft.

Daarnaast zijn er twee verwante risico's. Een instructie kan ook verstopt zitten in de inhoud die het model leest, bijvoorbeeld in een melding of een document; ook dan kan het model niets wat buiten de leesrechten en de instellingen van de taak valt. Leesrechten beschermen wel de vertrouwelijkheid, maar niet de juistheid: een verstopte instructie kan ook een subtiel onjuiste samenvatting opleveren van gegevens waar de gebruiker gewoon bij mag. Daarom vraagt het aansluiten van nieuwe bronnen een bewuste afweging, en blijft het toetsen van uitkomsten uit hoofdstuk 11 van belang. En wie gegevens zelf in een gesprek plakt, gaat om de databasegrens heen; daarvoor gelden de afspraken uit hoofdstuk 3, met als vangnet dat ook chatverkeer binnen de gateway standaard op het lokale model draait en geregistreerd wordt. De registratie doet ook hier de rest: afwijkend gebruik is terug te zien en te bespreken.

10

HOOFDSTUK 10

Het wettelijk en normatief kader

AI op de BI-omgeving valt niet in een leeg vak. Naast de AVG uit hoofdstuk 4 en de zeggenschapsvraag uit hoofdstuk 5 zijn er de normen voor informatiebeveiliging in de zorg, de Cyberbeveiligingswet en de Europese AI-verordening. De inrichting uit de vorige hoofdstukken sluit daarop aan.

Informatiebeveiliging: NEN 7510 en verwante normen. NEN 7510 is de norm voor informatiebeveiliging in de zorg, opgezet rond een managementsysteem: risico's in kaart, maatregelen kiezen, uitvoeren, controleren en bijstellen. Een AI-toepassing die gevoelige gegevens raakt, valt binnen de reikwijdte daarvan en hoort dus in de risicoanalyse, de maatregelenset en de auditcyclus, als systeem naast de andere systemen. De inrichting uit deze whitepaper levert daarvoor bouwstenen:

ONDERDEEL VAN DE NORM	WAT DE INRICHTING LEVERT
Toegangsbeveiliging	rechten per taak en per gebruiker, tot op databaseniveau; toegang via het bestaande accountbeheer
Registratie en herleidbaarheid	vastlegging van elke aanroep, met taak, model en omvang, in een register waarin aanpassing zichtbaar wordt
Beperking van gegevensstromen	lokaal als standaard, vrijgave per taak, pseudonimisering bij uitgaand verkeer
Wijzigingsbeheer	het beheer uit hoofdstuk 8: versies, acceptatie, testen en uitfaseren
Leveranciersbeheer	vastgelegde afspraken met hosting- en modelaanbieders, en een verwerkersovereenkomst waar die nodig is
Monitoring en incidenten	zicht op werking en gebruik, en een route voor storingen en beveiligingsincidenten

10

VERVOLG

Let op de formulering: een product voldoet niet aan NEN 7510, want de norm certificeert een organisatie en haar managementsysteem. Een inrichting levert de bouwstenen waarmee het ziekenhuis de beheersmaatregelen kan aantonen. Twee verwante normen horen in beeld: NEN 7513 over het vastleggen van acties op elektronische patiëntdossiers, dat raakt aan de registratie uit hoofdstuk 6, en NEN 7512 voor de beveiliging van koppelingen.

Cyberbeveiliging: de Cyberbeveiligingswet. Sinds 15 augustus 2026 gelden de Cyberbeveiligingswet en de Wet weerbaarheid kritieke entiteiten, waarmee Nederland de Europese NIS2-richtlijn heeft ingevoerd; in de zorg houdt de Inspectie Gezondheidszorg en Jeugd toezicht.[7] De wet brengt een registratieplicht, een zorgplicht, een meldplicht voor significante incidenten en bestuurlijke eindverantwoordelijkheid voor cyberrisico's, uitdrukkelijk ook in de keten van leveranciers.[8] De maatregelen sluiten aan op wat er al is: aantoonbaar voldoen aan NEN 7510 of een gelijkwaardig niveau. Voor de AI-omgeving volgt daaruit dat dezelfde zorgplicht geldt als voor de andere systemen, met continuïteit en incidentafhandeling als expliciete onderdelen, en dat het ziekenhuis van partijen die eraan meewerken mag vragen wat het zelf moet aantonen: hoe de beveiliging is geregeld, hoe incidenten worden gemeld, en hoe de dienstverlening overdraagbaar is als de samenwerking eindigt.

De AI-verordening. De Europese AI-verordening wordt stapsgewijs van kracht; sinds augustus 2026 gelden de transparantieverplichtingen.[6] De zware eisen gelden voor systemen met een hoog risico, en of daarvan sprake is hangt af van het toepassingsgebied: de verordening wijst die gebieden aan in bijlagen, waaronder AI in medische hulpmiddelen. Die verplichtingen zijn in juli 2026 uitgesteld naar december 2027 en augustus 2028.[9] AI die rapportages helpt bouwen of teksten samenvat onder menselijk toezicht valt in de regel buiten die categorieën, maar de toets is de toepassing, niet de mate van zelfstandigheid.

10

VERVOLG

De lichtere verplichtingen gelden voor vrijwel elke organisatie: medewerkers moeten weten dat ze met AI werken, de organisatie moet kunnen uitleggen waar AI wordt ingezet, en er moeten maatregelen zijn die de AI-kennis van medewerkers ondersteunen (AI-geletterdheid). Eén punt verdient aandacht bij de functionaris gegevensbescherming: wie zelf taken en instructies bouwt op een bestaand model, is meestal gebruiksverantwoordelijke, maar kan in bepaalde gevallen als aanbieder worden aangemerkt, met zwaardere verplichtingen.

De regels rond AI zijn in beweging en de precieze eisen per situatie vragen om een eigen beoordeling. Voor alle drie de kaders geldt dezelfde strekking: wie het eigen AI-gebruik kan laten zien en uitleggen, staat er goed voor. Wie de inrichting uit deze whitepaper volgt, heeft daarvoor de basis al staan, tot en met een machineleesbare uitdraai van welke taak naar welk model gaat en welke bronnen zijn aangesloten.

11

HOOFDSTUK 11

De mensen: vakmanschap verandert, verdwijnt niet

De gebruikers van AI op de BI-omgeving vormen een bredere groep dan het BI-team alleen. Iedereen die met veel data werkt en daarbij put uit onder meer het datawarehouse krijgt ermee te maken: controllers, de DBC-helpdesk, kwaliteitsmedewerkers, capaciteitsplanners. Voor al deze mensen geldt hetzelfde uitgangspunt: AI is een versterker. Het neemt repetitief werk weg, versnelt het uitzoekwerk en maakt meer mogelijk met dezelfde bezetting. Een versterker versterkt wel wat erin gaat. De kwaliteit van de uitkomst hangt af van wie het gereedschap bedient en welke context die meegeeft.

Voor de BI-teams zelf komt daar de bouwkant uit hoofdstuk 2 bij: AI die het ontwikkelwerk versnelt, waardoor een klein team meer aankan.

Het werk verandert daardoor meer dan dat het verdwijnt. Het accent verschuift van zelf uitvoeren naar goed opdrachten geven: vooraf uitdenken wat er moet gebeuren, de goede informatie meegeven, en beoordelen of het resultaat klopt en in het grote geheel past. Dat beoordelen vraagt tijd en vakkennis. Een model levert altijd een antwoord, ook als het antwoord onjuist is, en het verschil zien tussen een overtuigend antwoord en een juist antwoord is waar de vakinhoudelijke kennis van het team het verschil maakt.

Die vakkennis moet ergens vandaan blijven komen, en daar zit een aandachtspunt dat verder gaat dan de BI-omgeving. Vakkennis groeit door het eenvoudige werk zelf te doen. Organisaties die al het eenvoudige werk aan AI geven, halen daarmee ook de plek weg waar nieuwe mensen het vak leren, en staan over een paar jaar zonder ervaren beoordelaars. Het eenvoudige werk slim verdelen tussen AI en mensen in opleiding betaalt zich daarom op termijn terug.

Voor alle gebruikersgroepen betekent de komst van AI concreet: tijd inruimen om ermee te leren werken, afspraken maken over wat wel en niet aan het model wordt overgelaten, en de gewoonte opbouwen om uitkomsten te toetsen voordat ze verder de organisatie in gaan. Samen bepalen deze drie punten of AI het werk daadwerkelijk versterkt.

12

HOOFDSTUK 12

Een begaanbare route

De weg naar verantwoorde AI op de BI-omgeving hoeft niet te beginnen met een groot programma, en vraagt ook geen lange volgorde waarin het één af moet zijn voordat het ander begint. Architectuur, beleid, beheer en de eerste toepassingen zijn naast elkaar op te pakken, en versterken elkaar als ze samen oplopen: de eerste toepassingen leren wat het beleid moet regelen, en het beheer groeit mee met wat er draait.

De fasering zit ergens anders, namelijk bij de gebruiker. Wie begint met AI, start met eenvoudige, duidelijk afgebakende taken, leert wat het gereedschap wel en niet kan, en breidt van daaruit uit. Die begeleiding is het werk van de applicatiebeheerder AI uit hoofdstuk 8: nieuwe gebruikers krijgen toegang tot de taken die bij hun werk passen, worden op weg geholpen, en er is een vaste plek waar vragen en verbeterpunten terechtkomen. Zo groeit het gebruik in een tempo dat de organisatie kan volgen, per persoon en per afdeling.

Twee dingen krijgen daarbij voorrang. De architectuur staat er voordat er taken met gevoelige inhoud gaan draaien; zo hoeft er nooit een uitzondering "voor even" gemaakt te worden. En het beheer is belegd vanaf dag één, want eigenaarschap, rechten en monitoring zijn eenvoudiger vooraf in te richten dan achteraf toe te voegen.

12

VERVOLG

InfoReports begeleidt ziekenhuizen op deze route met een klein team en korte lijnen. De werkwijze is dezelfde als bij al het BI-werk van InfoReports: volledige transparantie, en duidelijkheid over wat van wie is. Alles wat voor het ziekenhuis wordt gemaakt, is van het ziekenhuis: de datamodellen en rapportages, de inrichting van de omgeving, de taken en instructies die per toepassing worden opgesteld, de configuratie en de gegevens. Dat werk is in te zien, over te nemen, aan te passen of door een derde te laten controleren. De gateway zelf is standaardsoftware van InfoReports, die het ziekenhuis in gebruik krijgt; het intellectueel eigendom daarvan blijft bij InfoReports, net als bij andere software die een ziekenhuis afneemt. Ook de taalmodellen worden onder hun eigen licentievoorwaarden gebruikt. Zo is vooraf duidelijk waar het ziekenhuis zelf over gaat en waar niet, en ontstaat er geen black box waarin niemand meer kan nagaan wat er gebeurt. Bij AI op gevoelige data is dat geen detail: controle kunnen houden was de reden om het zo in te richten, dus die controle hoort ook bij de samenwerking zelf.

13

HOOFDSTUK 13

Tot slot

Discussies over AI in de zorg beginnen vaak bij de vraag of het mag. Deze whitepaper heeft die vraag opgedeeld in vragen die te beantwoorden zijn: welke gegevens waarheen mogen, hoe de techniek dat afdwingt, wie het beheert en wat het van de mensen vraagt. Een goed antwoord begint immers met een betere vraag. Zo wordt "mag het?" een vraag die het ziekenhuis zelf kan beantwoorden, en kan onderbouwen.

Wie het zo aanpakt, komt uit bij een inrichting waarin gevoelige gegevens standaard binnen blijven, uitzonderingen per taak in code staan, en alles wat er gebeurt kan worden naverteld. Die inrichting bestaat, draait, en is in werking te zien. Neem contact met ons op voor een demonstratie of een verkennend gesprek over wat dit voor het eigen ziekenhuis betekent, of kijk op inforeports.nl/aanbod/ai-gateway.

Bijlage: bronnen

1 Autoriteit Persoonsgegevens, "Toezicht op AI & algoritmes".
https://autoriteitpersoonsgegevens.nl/uploads/imported/toezicht_op_ai_en_algoritmes.pdf

2 Autoriteit Persoonsgegevens, hulpmiddel generatieve AI en de AVG, met de voorafgaande raadpleging over Microsoft Copilot, juli 2026.
https://www.autoriteitpersoonsgegevens.nl/en/documents/tool-generative-ai-and-the-gdpr-prior-consultation-microsoft-copilot

3 Rijksoverheid, visiedocument "Digitale autonomie en soevereiniteit van de overheid".
https://open.overheid.nl/documenten/c49a2705-3f3d-44be-8a7d-2cecd2183604/file

4 Sénat (Frankrijk), commissie van onderzoek naar de overheidsopdrachten, verslag van de hoorzitting met Microsoft France, 10 juni 2025.
https://www.senat.fr/compte-rendu-commissions/20250609/ce_commande_publique.html

5 Metagora, dossier soevereiniteit: "Waarom het bijna niet uitmaakt of uw data in Amerika staat. AWS Europa als casus voor compliance en sovereignty washing."
https://metagora.nl/dossiers/soevereiniteit/waarom-het-bijna-niet-uitmaakt-of-uw-data-in-amerika-staat-aws-europa-als-casus-voor-compliance-en-sovereignty-washing

VERVOLG

6 Europese Unie, Verordening (EU) 2024/1689 (AI-verordening), geconsolideerde versie.
https://eur-lex.europa.eu/eli/reg/2024/1689/oj

7 Rijksoverheid, "Cyberbeveiligingswet en Wet weerbaarheid kritieke entiteiten vanaf 15 augustus 2026 van kracht", juli 2026.
https://www.rijksoverheid.nl/actueel/nieuws/2026/07/07/cyberbeveiligingswet-en-wet-weerbaarheid-kritieke-entiteiten-vanaf-15-augustus-2026-van-kracht

8 Ministerie van VWS, Data voor gezondheid, dossier Cyberbeveiligingswet.
https://www.datavoorgezondheid.nl/onderwerpen/c/cyberbeveiligingswet

9 Europese Unie, Verordening (EU) 2026/1744 (Digital Omnibus inzake AI), juli 2026.
https://eur-lex.europa.eu/eli/reg/2026/1744/oj

Colofon

InfoReports Business Intelligence B.V., Loenen (Gelderland)

TITEL	AI in de BI van het ziekenhuis: van experiment naar verantwoorde inrichting
VERSIE	1.0
DATUM	Augustus 2026
KVK	08134621
CONTACT	info@inforeports.nl
WEB	inforeports.nl
AI GATEWAY	inforeports.nl/aanbod/ai-gateway
CITEREN ALS	InfoReports (2026). *AI in de BI van het ziekenhuis: van experiment naar verantwoorde inrichting.* Versie 1.0.

Wij geven de regie terug.