ilionx
experts in eenvoud

editie najaar 2026

je hebt NEN 7510 al. wat vraagt de AI Act nog meer van je?

Gap-analyse ISO 42001 naast NEN 7510: een werkboek voor zorgorganisaties

1. waar je staat

Je hebt NEN 7510 ingericht, met een risicoproces, eigenaren, een auditcyclus en een directiebeoordeling. Nu komt de AI Act erbij, en daarmee de vraag of je opnieuw moet beginnen.

Dat hoeft niet, want ISO 42001 is de managementsysteemnorm voor AI en helpt je een groot deel van wat de AI Act vraagt te organiseren. De norm heeft dezelfde opbouw als ISO 27001, en dus als NEN 7510, met dezelfde hoofdstukken en dezelfde logica. Het verschil zit in bijlage A, met 38 controls die specifiek over AI gaan.

We hebben die 38 controls naast NEN 7510 gelegd. Voor een zorgorganisatie die NEN 7510 goed op orde heeft en nog niets specifiek voor AI heeft gedaan, levert dat dit beeld op. We noemen dat in dit werkboek het startpunt.

de 38 controls uit bijlage A van ISO 42001, naast NEN 7510



volledig
NEN 7510 dekt het,
AI-invulling is klein werk

deels
de basis staat,
de AI-invulling vraagt werk

niet
geen tegenhanger
in NEN 7510

figuur 1: het startpunt: hoeveel van de 38 controls NEN 7510 al dekt

Met dit werkboek maak je dezelfde meting voor je eigen organisatie. Per control zie je wat de norm vraagt, wat je waarschijnlijk al hebt en wat je moet toevoegen. Aan het eind weet je welke controls je mist. Dat geeft je genoeg voor een eerste gesprek met je bestuur, al is het te weinig om daarna achterover te leunen.

Let op: Met ISO 42001 regel je beleid en proces, maar daarmee ben je er nog niet. Elke AI-toepassing beoordeel je daarna apart, ook de AI die in ingekochte software zit. Het aantonen dat je leverancier voldoet, blijft jouw taak, ook als deze het systeem zelf heeft gebouwd.

2. zo gebruik je dit werkboek

Je werkt in drie stappen: je vinkt per control, je telt op het overzicht en je kiest je drie aandachtspunten.

1 vink
per control één van drie antwoorden, in hoofdstuk 4

2 tel
zet je vinkjes over op het overzicht en tel per kolom

3 kies
je drie aandachtspunten uit de controls op 'niet'

figuur 2: vinken, tellen, kiezen

stap 1 · vink per control

Bij elke control in hoofdstuk 4 kies je één van drie antwoorden. Ze gaan over de vraag hoe goed jouw organisatie de control vandaag dekt.

antwoord	wanneer je dit kiest
volledig	Je hebt het geregeld en het wordt getoetst. Wat onder 'je voegt toe' staat, is al gedaan of klein werk binnen een proces dat al loopt.
deels	Er staat een basis, meestal vanuit NEN 7510, maar de invulling voor AI vraagt nog echt werk.
niet	Er is niets waar je op kunt voortbouwen.
navragen	Je weet het niet. Kies dan niet en vink navragen aan. Zo zie je straks welke antwoorden je nog moet ophalen, vaak bij je leverancier.

Niet weten of een control is ingericht, is zelf een bevinding. Het is bovendien een bevinding die je bestuur moet horen. Daarom tel je navragen apart.

stap 2 · tel op het overzicht

In hoofdstuk 5 staan alle 38 controls onder elkaar. Zet je vinkjes daar over en tel per kolom, dan komen volledig, deels en niet samen uit op 38.

stap 3 · kies je drie aandachtspunten

Op het overzicht zie je in één keer welke controls op niet staan. Daaruit kies je er drie voor het bestuursblad.

praktisch

op papier	Dit is een werkboek. Print het en zet per control je kruisje, of klik de vakjes aan in de PDF. Tellen doe je zelf, op het overzicht in hoofdstuk 5. Het bestuursblad daarna print je apart, want dat is wat de bestuurskamer in gaat.
tijd	Reken op een paar uur als je de antwoorden paraat hebt en op een week als je ze eerst moet ophalen.
wie	Doe het niet alleen. De negen controls die NEN 7510 niet dekt, liggen grotendeels op het terrein van je functionaris gegevensbescherming. Bij een flink deel van de controls heb je bovendien antwoorden van je leveranciers nodig.

3. wat de zorg anders maakt

Vijf dingen die in de zorg bepalen hoe je dit werkboek invult en die je in een generieke gap-analyse niet tegenkomt.

je hebt twee besturen

De Cyberbeveiligingswet legt de goedkeuring van maatregelen en het toezicht daarop bij de raad van bestuur. Bij AI die patiënten raakt kijkt ook de raad van toezicht mee, dus je uitkomst moet voor allebei te volgen zijn.

er zit een derde rol aan tafel

Naast de CISO en degene die voor AI verantwoordelijk is, heb je de functionaris gegevensbescherming nodig. De negen controls die NEN 7510 niet dekt, liggen grotendeels op diens terrein. Betrek de functionaris daarom bij het ophalen van de antwoorden en niet pas bij de uitkomst.

je AI komt meestal van je leverancier

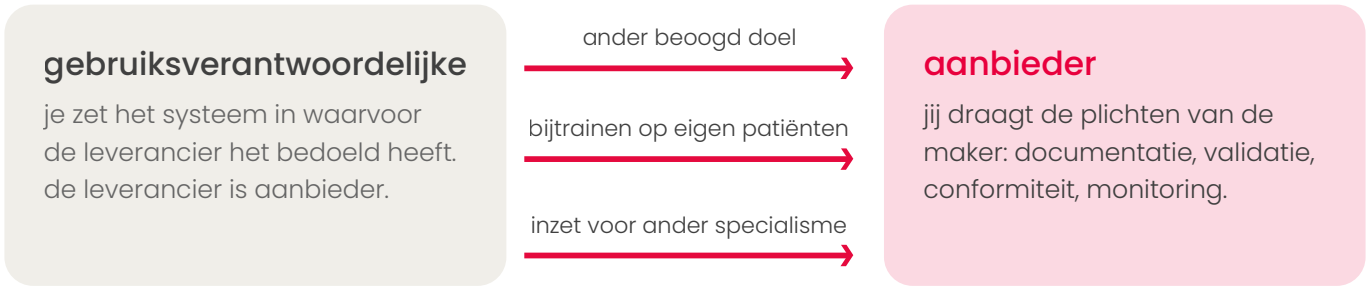
In de zorg bouw je AI zelden zelf. Het zit in een functie van je EPD, in een algoritme in een beeldvormend apparaat of in een module die met een release meekomt. Bij veel controls is het eerlijke antwoord dan dat je het niet weet en het moet vragen. Waar dat speelt, staat de vraag in de regel ‘in de zorg’ uitgeschreven.

sommige AI is ook een medisch hulpmiddel

Is de AI-functie zelf een medisch hulpmiddel of een veiligheidsonderdeel ervan, en moest dat hulpmiddel onder de MDR al langs een notified body, dan is die functie onder de AI Act hoog risico. Dat geldt voor klasse IIa en hoger, en ook voor klasse I-hulpmiddelen die steriel zijn, een meetfunctie hebben of herbruikbaar chirurgisch zijn. Alleen bij een gewoon klasse I-hulpmiddel is dat niet automatisch zo.

De leverancier is dan de aanbieder en jij bent de gebruiksverantwoordelijke. Voor deze categorie gelden de plichten vanaf 2 augustus 2028, acht maanden later dan voor andere hoog-risico AI. Die tijd is alleen nuttig als je nu al kunt aanwijzen welke functies eronder vallen.

Verander je het beoogde doel van zo’n systeem, of train je het bij op je eigen patiënten, dan kun je zelf aanbieder worden, met alle plichten die daarbij horen.

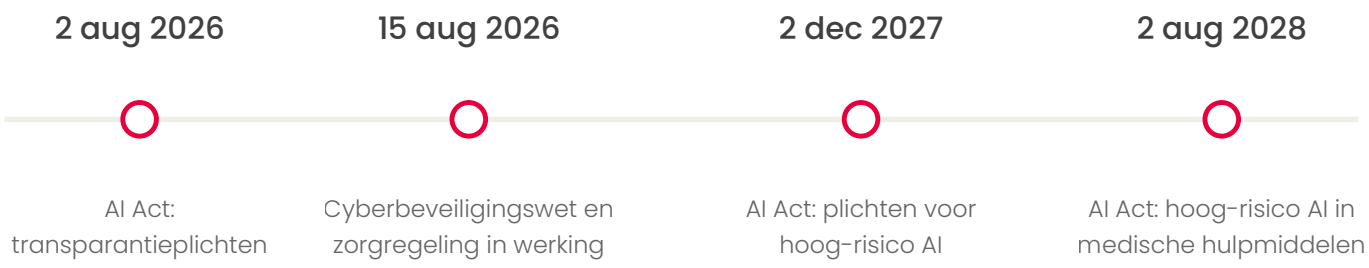


figuur 3: wanneer je van gebruiksverantwoordelijke aanbieder wordt

de Cyberbeveiligingswet heeft een zorgregeling

De Cyberbeveiligingsregeling voor de zorg, in werking sinds 15 augustus 2026, koppelt de zorgplicht aan NEN 7510, zoals de regeling voor de overheid dat met de BIO2 doet. Er komt dus geen apart regime bij, wel eigen loketten: je meldt bij het NCSC, Z-CERT is je CSIRT en de IGJ houdt toezicht.

Of je onder de wet valt, hangt af van je omvang. Vanaf ongeveer vijftig medewerkers ben je een belangrijke entiteit en vanaf tweehonderdvijftig een essentiële. Dat verschil verandert niets aan wat je moet doen, wel aan hoe en hoe vaak de toezichthouder meekijkt.



figuur 4: wat wanneer geldt, na de AI Omnibus van juli 2026

4. de 38 controls

Per control lees je wat de norm vraagt, wat je waarschijnlijk al hebt en wat je moet toevoegen. De regel 'in de zorg' staat er alleen als die iets toevoegt.
Zet onderaan elke control een kruisje bij één van de drie antwoorden. Weet je het niet, kies dan niet en vink ook navragen aan.

A.2 beleid voor AI

A.2.2	AI-beleid
de norm vraagt	Een vastgesteld beleid voor de ontwikkeling en het gebruik van AI, goedgekeurd door het bestuur en bekend bij iedereen die ermee werkt.
je hebt al	Je informatiebeveiligingsbeleid, met de routine voor goedkeuring en communicatie die daarbij hoort.
je voegt toe	Een AI-paragraaf of een apart AI-beleid binnen hetzelfde raamwerk, dus een hoofdstuk erbij in plaats van een nieuw document ernaast.
in de zorg	Leg vast wat AI in je EPD wel en niet mag beslissen zonder dat een zorgverlener meekijkt.

☐ volledig ☐ deels ☐ niet ☐ navragen

A.2.3	afstemming met ander beleid
de norm vraagt	Dat je AI-beleid aansluit op je overige beleid, zoals privacy, informatiebeveiliging, inkoop en HR.
je hebt al	Je governancebeleid en de manier waarop je beleidsstukken op elkaar afstemt.
je voegt toe	Laat de AI-randvoorwaarden ook landen in de andere beleidsstukken, vooral in privacy en inkoop.

☐ volledig ☐ deels ☐ niet ☐ navragen

A.2.4	herziening van het AI-beleid
de norm vraagt	Dat je het AI-beleid periodiek beoordeelt en bijstelt.
je hebt al	Je managementreview en de reviewcyclus van je ISMS.
je voegt toe	Zet AI als vast punt op de agenda van die cyclus, met eigen criteria zoals nieuwe systemen, incidenten en veranderde wetgeving..

☐ volledig ☐ deels ☐ niet ☐ navragen

A.3 interne organisatie

A.3.2	rollen en verantwoordelijkheden voor AI
de norm vraagt	Dat per AI-systeem duidelijk is wie eigenaar is, wie beslist en wie toezicht houdt.
je hebt al	Rollen, bevoegdheden en functiescheiding zoals je die voor informatiebeveiliging hebt belegd.
je voegt toe	Een eigenaar per AI-systeem, met naam, en een afspraak over wie een AI-uitkomst mag overrulen. Daarmee leg je ook de basis voor het menselijk toezicht dat de AI Act vraagt.
in de zorg	Bij AI die patiënten raakt is de eigenaar zelden iemand van IT en meestal een medisch verantwoordelijke. Leg dat vast voordat het eerste incident het voor je beslist.

☐ volledig ☐ deels ☐ niet ☐ navragen

A.3.3	melden van zorgen
de norm vraagt	Een kanaal waar medewerkers zorgen over AI-gebruik kwijt kunnen, ook als er geen beveiligingsincident is.
je hebt al	Je meldproces voor incidenten en je klokkenluidersregeling.
je voegt toe	Breid het meldpunt uit naar AI, voor onjuiste uitkomsten, twijfel over gebruik of een oneerlijke behandeling. Laat medewerkers ook weten dat melden mag.
in de zorg	Een verpleegkundige die een AI-advies niet vertrouwt, moet dat kwijt kunnen zonder een beveiligingsformulier in te vullen.

☐ volledig ☐ deels ☐ niet ☐ navragen

A.4 middelen voor AI-systemen

A.4.2	documentatie van middelen
de norm vraagt	Een overzicht van alles wat een AI-systeem nodig heeft, zoals data, tools, rekencapaciteit en mensen.
je hebt al	Je assetmanagement en het register dat daarbij hoort.
je voegt toe	Neem AI-systemen als aparte categorie op in je register, met per systeem de middelen die erbij horen.
in de zorg	Vergeet de AI niet die meekomt met je EPD, je PACS of een medisch apparaat. Die staat zelden als AI geregistreerd, omdat niemand die functie als AI heeft ingekocht.

☐ volledig ☐ deels ☐ niet ☐ navragen

A.4.3	gegevensbronnen
de norm vraagt	Per AI-systeem vastgelegd welke data erin gaat, waar die vandaan komt en wie er eigenaar van is.
je hebt al	Je informatieclassificatie en het eigenaarschap van gegevens.
je voegt toe	Voeg de herkomst toe. Je classificatie zegt hoe gevoelig data is, maar niet waar ze vandaan komt of dat ze geschikt is om een model op te trainen.

☐ volledig ☐ deels ☐ niet ☐ navragen

A.4.4	tooling
de norm vraagt	Een overzicht van de AI-tools en -platforms die in je organisatie worden gebruikt.
je hebt al	Je technologiebeheer en softwareregister.
je voegt toe	Inventariseer AI-tools apart, ook de functies in platforms waar je al een licentie op hebt, want daar zit het meeste gebruik dat nergens geregistreerd staat.
in de zorg	Vraag het aan de afdelingen en niet alleen aan IT. Een planner die roosters laat voorstellen door een AI-functie, ziet dat zelf niet als tool.

☐ volledig ☐ deels ☐ niet ☐ navragen

A.4.5	systeem- en rekencapaciteit
de norm vraagt	Dat de systemen en rekencapaciteit voor AI in beeld zijn en worden beheerd.
je hebt al	Je capaciteits- en beheerprocessen.
je voegt toe	Voeg AI-eisen toe: waar het model draait, wie die omgeving beheert en wat er gebeurt als ze wegvalt.

☐ volledig ☐ deels ☐ niet ☐ navragen

A.4.6	mensen
de norm vraagt	Dat de mensen die AI ontwikkelen, beheren of gebruiken daarvoor bekwaam zijn.
je hebt al	Je bewustwordingsprogramma en competentiebeheer.
je voegt toe	Benoem en train AI-competenties. De AI Act noemt dit AI-geletterdheid en vraagt je daar aantoonbaar werk van te maken voor iedereen die met AI werkt.
in de zorg	Dit gaat ook over de zorgverlener die een AI-advies krijgt. Weet die waar het systeem goed in is en waar het de mist in kan gaan?

☐ volledig ☐ deels ☐ niet ☐ navragen

A.5 impactbeoordeling

A.5.2	proces voor impactbeoordeling
de norm vraagt	Een vast proces om per AI-systeem de impact te beoordelen voordat het in gebruik gaat, en opnieuw als er iets verandert.
je hebt al	Geen directe tegenhanger. Wel je risicomethodiek en, via de AVG, het DPIA-proces.
je voegt toe	Een AI-impactbeoordeling naast de DPIA, in hetzelfde ritme. De vraag is alleen anders: wat gebeurt er met mensen, naast wat er met hun gegevens gebeurt.
in de zorg	Voor een deel van de hoog-risico AI, zoals systemen die mee bepalen wie welke zorg krijgt, vraagt de AI Act een grondrechteneffectbeoordeling. Dat is dit proces met een wettelijke naam.

☐ volledig ☐ deels ☐ niet ☐ navragen

A.5.3	documentatie van impactbeoordelingen
de norm vraagt	Dat je de uitkomsten van impactbeoordelingen vastlegt en terug kunt vinden.
je hebt al	Geen directe tegenhanger.
je voegt toe	Een impactregister, of een vaste plek in je bestaande risicoregister. Houd het bij één plek en niet bij een los bestand per project.

☐ volledig ☐ deels ☐ niet ☐ navragen

A.5.4	impact op individuen en groepen
de norm vraagt	Beoordelen wat een AI-systeem doet met de mensen over wie het beslist of adviseert, en of het voor sommige groepen anders uitpakt.
je hebt al	Geen directe tegenhanger. Controls rond privacy raken het zijdelings.
je voegt toe	Een analyse die bij de mens begint: welke uitkomsten kan dit systeem geven, voor wie, en wat gebeurt er als het misgaat. Bias en oneerlijke uitkomsten horen daar expliciet bij.
in de zorg	In de zorg is die mens de patiënt. Een model dat voor één groep patiënten stelselmatig slechter uitpakt, zie je niet terug in je beveiligingsrapportage, terwijl je RvT het wel als incident zal zien.

☐ volledig ☐ deels ☐ niet ☐ navragen

A.5.5	maatschappelijke impact
de norm vraagt	Beoordelen of een AI-systeem gevolgen heeft buiten de directe gebruikers, voor de samenleving, het milieu of de sector.
je hebt al	Geen directe tegenhanger.
je voegt toe	Een korte maatschappelijke toets per systeem. Voor de meeste toepassingen is die snel gedaan, voor een paar kost de toets echt denkwerk.
in de zorg	Denk aan triage- of prioriteringssystemen. Wie krijgt eerder zorg, en wie beslist dat eigenlijk?

☐ volledig ☐ deels ☐ niet ☐ navragen

A.6 levenscyclus van AI-systemen

A.6.1.2	doelstellingen voor verantwoorde ontwikkeling
de norm vraagt	Vastgelegde doelstellingen voor hoe je AI verantwoord ontwikkelt, zoals eerlijk, veilig, uitlegbaar en betrouwbaar.
je hebt al	Je uitgangspunten voor veilige ontwikkeling.
je voegt toe	Formuleer AI-doelstellingen die verder gaan dan beveiliging. Wat vind je een goede uitkomst, en hoe meet je dat?

☐ volledig ☐ deels ☐ niet | ☐ navragen

A.6.1.3	proces voor verantwoord ontwerp en ontwikkeling
de norm vraagt	Een ontwikkelproces waarin die doelstellingen zijn ingebouwd, met vaste controlemomenten.
je hebt al	Je ontwikkelbeveiliging en de secure development lifecycle.
je voegt toe	Maak ethiek, bias en uitlegbaarheid vaste stappen in je ontwikkelproces. Dat geldt ook als je niet zelf bouwt en alleen configureert.

☐ volledig ☐ deels ☐ niet | ☐ navragen

A.6.2.2	vereisten voor AI-systemen
de norm vraagt	Dat je per AI-systeem de eisen vastlegt: functioneel, ethisch, juridisch en technisch.
je hebt al	Je beveiligingseisen bij aanschaf en ontwikkeling.
je voegt toe	Voeg AI-eisen toe aan je eisenlijst, vooral bij inkoop: wat moet een leverancier aantonen voordat je tekent?
in de zorg	Zit de AI in een medisch hulpmiddel, vraag de leverancier dan om de MDR-klasse en het bewijs daarvan. Doe dat voordat je tekent.

☐ volledig ☐ deels ☐ niet | ☐ navragen

A.6.2.3	documentatie van ontwerp en specificatie
de norm vraagt	Dat ontwerp en specificatie van elk AI-systeem zijn vastgelegd.
je hebt al	Je documentatiebeheer.
je voegt toe	Leg de AI-inhoud erbij vast: welk model, welke data en welke beperkingen. Bij ingekochte systemen is dit precies wat je van je leverancier vraagt.

☐ volledig ☐ deels ☐ niet ☐ navragen

A.6.2.4	verificatie en validatie
de norm vraagt	Dat je toetst of een AI-systeem doet wat het moet doen, voordat het in gebruik gaat.
je hebt al	Je testproces.
je voegt toe	Test op wat bij AI misgaat, zoals scheve uitkomsten, gevoeligheid voor vreemde invoer en gedrag buiten de situatie waarvoor het bedoeld is. Een functionele test vangt dat niet.
in de zorg	Test op je eigen populatie. Een model dat elders goed presteert, kan bij jouw patiënten anders uitpakken.

☐ volledig ☐ deels ☐ niet ☐ navragen

A.6.2.5	ingebruikname
de norm vraagt	Een beheerste overgang naar productie, met een expliciet besluit vooraf.
je hebt al	Je wijzigingsbeheer.
je voegt toe	Neem AI-criteria op in dat go/no-go-besluit: impactbeoordeling gedaan, eigenaar benoemd, logging aan en toezicht geregeld.

☐ volledig ☐ deels ☐ niet ☐ navragen

A.6.2.6	gebruik en monitoring
de norm vraagt	Dat je tijdens gebruik in de gaten houdt of het systeem blijft doen wat het hoort te doen.
je hebt al	Je monitoring, je herhaalde risicobeoordeling en je incidentproces.
je voegt toe	Bepaal wat afwijkend gedrag bij AI is, zoals prestaties die langzaam teruglopen, uitkomsten die stelselmatig scheef zijn en gebruik buiten het bedoelde doel. Je huidige detectie ziet dat niet.
in de zorg	Een model dat langzaam slechter wordt, geeft geen alarm. Iemand met een naam moet er periodiek naar kijken.

☐ volledig ☐ deels ☐ niet ☐ navragen

A.6.2.7	technische documentatie
de norm vraagt	Technische documentatie per AI-systeem die bruikbaar is voor toezichthouders en auditors.
je hebt al	Je documentatiebeheer.
je voegt toe	Maak modeldocumentatie verplicht: wat het is, hoe het getraind is en welke beperkingen bekend zijn. Voor hoog-risico AI schrijft de AI Act de inhoud voor.

☐ volledig ☐ deels ☐ niet ☐ navragen

A.6.2.8	logboeken van AI-systemen
de norm vraagt	Dat een AI-systeem vastlegt wat het doet, wanneer en op basis waarvan, en dat je die logs bewaart en beschermt. Voor hoog-risicosystemen vraagt de AI Act een bewaartermijn van minimaal zes maanden.
je hebt al	Logging en monitoring uit NEN 7510, inclusief bewaartermijnen en de beveiliging van logs.
je voegt toe	Logs op het niveau van de AI-toepassing zelf, naast de logs van het platform eromheen.
in de zorg	Zit de AI in je EPD, vraag je leverancier dan of je die logs krijgt en hoe lang ze bewaard worden. Doe dat voordat je hier een kruisje zet.

☐ volledig ☐ deels ☐ niet ☐ navragen

A.7 data voor AI-systemen

A.7.2	data voor ontwikkeling en verbetering
de norm vraagt	Dat je beheerst welke data je gebruikt om AI-systemen te ontwikkelen, te trainen en te verbeteren.
je hebt al	Je databeheer.
je voegt toe	Behandel trainingsdata als aparte categorie. Wie mag welke data gebruiken om een model te trainen of bij te trainen, en wie keurt dat goed?
in de zorg	Bijtrainen op eigen patiëntdata kan je onder de AI Act van gebruiksverantwoordelijke tot aanbieder maken. Neem dat besluit bewust, voordat iemand het gewoon doet.

☐ volledig ☐ deels ☐ niet ☐ navragen

A.7.3	verzameling van data
de norm vraagt	Dat je data voor AI beheerst verzamelt: rechtmatig, voor een bepaald doel en vastgelegd.
je hebt al	Je regels voor het verzamelen en verwerken van gegevens, grotendeels vanuit de AVG.
je voegt toe	Leg de herkomst vast. Dat je data mag gebruiken is één vraag, waar ze vandaan komt en onder welke voorwaarden is een tweede.

☐ volledig ☐ deels ☐ niet ☐ navragen

A.7.4	kwaliteit van data
de norm vraagt	Dat de data die een AI-systeem gebruikt goed genoeg is voor het doel: juist, volledig, actueel en representatief.
je hebt al	Je datakwaliteitsbeheer.
je voegt toe	Neem representativiteit op als criterium. Of de data past bij waarvoor je het systeem inzet, is een inhoudelijke vraag en geen beveiligingsvraag.
in de zorg	Een model dat getraind is in een academisch ziekenhuis, kan in een regionaal ziekenhuis andere uitkomsten geven. Zorg dat je weet op welke patiënten het model getraind is.

☐ volledig ☐ deels ☐ niet ☐ navragen

A.7.5	herkomst van data
de norm vraagt	Dat je van de data die een AI-systeem gebruikt kunt aantonen waar ze vandaan komt en wat ermee gebeurd is.
je hebt al	Geen directe tegenhanger.
je voegt toe	Een lineage-proces, met per dataset de bron, de bewerkingen en de verantwoordelijke. Begin bij de systemen die beslissingen over mensen ondersteunen.
in de zorg	Voor AI in je EPD is dit een vraag aan je leverancier die je waarschijnlijk nog niet stelt. Zet de vraag op de agenda van je volgende leveranciersoverleg.

☐ volledig ☐ deels ☐ niet ☐ navragen

A.7.6	voorbereiding van data
de norm vraagt	Dat het bewerken, labelen en omzetten van data voor AI is vastgelegd en beheerst.
je hebt al	Geen directe tegenhanger.
je voegt toe	Beschrijf het voorbereidingsproces: wie labelt, volgens welke regels en wie dat controleert.
in de zorg	Labels in de zorg zijn medische oordelen, dus wie ze zet, bepaalt wat het model leert.

☐ volledig ☐ deels ☐ niet ☐ navragen

A.8 · informatie voor belanghebbenden

A.8.2	informatie voor gebruikers
de norm vraagt	Dat gebruikers van een AI-systeem weten wat het doet, wat het niet kan en hoe ze het moeten gebruiken.
je hebt al	Je gebruikersdocumentatie.
je voegt toe	Voeg AI-transparantie toe: dat het AI is, wat de beperkingen zijn en hoe je de uitkomst leest. Houd het kort en zet het op de plek waar het systeem gebruikt wordt.
in de zorg	Hier is de zorgverlener die een AI-advies krijgt de gebruiker. Die moet weten wanneer het systeem ernaast kan zitten.

☐ volledig ☐ deels ☐ niet ☐ navragen

A.8.3	externe rapportage
de norm vraagt	Dat je over AI-gebruik kunt rapporteren aan wie daar recht op heeft, zoals toezichthouders, klanten en het publiek.
je hebt al	Je communicatieprocessen.
je voegt toe	Een rapportageprotocol voor AI: wat meld je aan wie, en wanneer. De AI Act en de Cyberbeveiligingswet hebben elk hun eigen meldplicht.

☐ volledig ☐ deels ☐ niet ☐ navragen

A.8.4	communicatie van incidenten
de norm vraagt	Dat je AI-incidenten binnen de geldende termijnen meldt aan de juiste partijen.
je hebt al	Je incidentmanagement, inclusief de meldplicht uit de Cyberbeveiligingswet.
je voegt toe	Voeg AI-scenario's toe aan je incidentproces. Een model dat stelselmatig verkeerde uitkomsten geeft is een incident, ook als er niets gehackt is.
in de zorg	Is de AI onderdeel van een medisch hulpmiddel, dan geldt ook de meldplicht uit de MDR. Spreek vooraf af wie welke melding doet, want één incident kan dan via twee routes gemeld moeten worden.

☐ volledig ☐ deels ☐ niet ☐ navragen

A.8.5	informatie voor belanghebbenden		
de norm vraagt	Dat mensen over wie een AI-systeem beslist of adviseert dat weten, en begrijpen wat het voor hen betekent.		
je hebt al	Je informatieplicht en verwerkingsregister vanuit de AVG.		
je voegt toe	Mensen moeten weten dat ze met AI te maken hebben en waar de rol van het systeem ophoudt. De transparantieplichten uit de AI Act gelden sinds augustus 2026, ook voor systemen die geen hoog risico zijn.		
in de zorg	Hier is de patiënt de belanghebbende. Hoe vertel je dat een AI heeft meegekeken, en wie doet dat?		
☐ volledig	☐ deels	☐ niet	☐ navragen

A.9 · gebruik van AI-systemen

A.9.2	processen voor verantwoord gebruik
de norm vraagt	Vastgelegde regels voor hoe AI-systemen in je organisatie gebruikt mogen worden.
je hebt al	Geen directe tegenhanger. Je acceptable-use-beleid komt in de buurt.
je voegt toe	Een AI-gebruiksbeleid: wat mag, wat niet en wat je doet als iemand AI gebruikt die niet is goedgekeurd.
in de zorg	Wees concreet over generatieve AI in de spreekkamer. Mag een arts een ontslagbrief laten voorbereiden, en met welke tool?

☐ volledig ☐ deels ☐ niet ☐ navragen

A.9.3	doelstellingen voor verantwoord gebruik
de norm vraagt	Doelstellingen voor het gebruik van AI die passen bij je waarden en verplichtingen.
je hebt al	Geen directe tegenhanger.
je voegt toe	Benoem waarom je AI inzet en waar de grens ligt. Dat klinkt abstract, tot de eerste discussie over een concrete toepassing begint.

☐ volledig ☐ deels ☐ niet ☐ navragen

A.9.4	beoogd gebruik
de norm vraagt	Per AI-systeem vastgelegd waarvoor het bedoeld is, en waarvoor niet.
je hebt al	Geen directe tegenhanger.
je voegt toe	Een registratie van de use case per systeem. Wijk je af van het beoogde doel, dan verschuiven je verplichtingen onder de AI Act.
in de zorg	Dit is de grens waarachter je van gebruiksverantwoordelijke aanbieder kunt worden. Een systeem voor het ene specialisme inzetten bij een ander, kan die grens al overschrijden.

☐ volledig ☐ deels ☐ niet ☐ navragen

A.10 · relaties met derden

A.10.2	toewijzing van verantwoordelijkheden
de norm vraagt	Dat in de keten duidelijk is wie waarvoor verantwoordelijk is: de leverancier, jij en eventuele andere partijen.
je hebt al	Je leveranciersbeheer.
je voegt toe	Maak contractuele afspraken over AI. De AI Act verdeelt de plichten per rol, zoals aanbieder en gebruiksverantwoordelijke, dus moet op papier staan welke rol wie heeft.
in de zorg	Bij AI in een medisch hulpmiddel is de fabrikant de aanbieder en ben jij de gebruiksverantwoordelijke, zolang je het gebruikt zoals het bedoeld is.

☐ volledig ☐ deels ☐ niet ☐ navragen

A.10.3	leveranciers
de norm vraagt	Dat je leveranciers van AI-systemen beoordeelt en afspraken maakt over hun verplichtingen.
je hebt al	Je leveranciersbeheer en verwerkersovereenkomsten, plus de aandacht voor de toeleveringsketen uit de Cyberbeveiligingswet.
je voegt toe	Een AI due diligence: is de leverancier aanbieder onder de AI Act, is het systeem hoog risico en welke documentatie en logs krijg je? Je huidige contract regelt beveiliging, niet deze kwalificatie.
in de zorg	Voor je EPD-leverancier komt dit neer op één gesprek. De vragen staan in hoofdstuk 6 van dit werkboek.

☐ volledig ☐ deels ☐ niet ☐ navragen

A.10.4	klanten
de norm vraagt	Dat je je eigen klanten of afnemers duidelijk maakt welke AI je gebruikt en wat ze daarvan mogen verwachten.
je hebt al	Je contractmanagement.
je voegt toe	Leg afspraken over AI vast. Voor een zorgorganisatie is de klant meestal de patiënt of een ketenpartner, zie ook A.8.5.

☐ volledig ☐ deels ☐ niet ☐ navragen

5. je uitkomst

Zet in het overzicht op het volgende blad je antwoorden uit hoofdstuk 4 onder elkaar. Je telt per kolom en ziet meteen waar je gaten zitten.

wat je uitkomst betekent

Je belangrijkste uitkomst is de lijst controls op niet, want dat zijn je gaten. Je drie getallen leg je naast het startpunt. Dat is geen norm en geen gemiddelde. Het laat zien waar een organisatie staat die NEN 7510 op orde heeft en nog niets aan AI heeft gedaan. Het verschil tussen jouw getallen en die van het startpunt vertelt je waar je zit.

zo lees je je drie getallen

als je ziet	dan betekent dat
meer dan 10 op volledig	Je hebt al werk gemaakt van AI. Kijk bij die controls of het ook getoetst wordt, anders is het eerlijker om ‘deels’ te kiezen.
meer dan 9 op niet	Er ontbreekt ook iets in je NEN 7510-basis, of je weet te weinig over de AI die je gebruikt. Begin daar, want op dat aandachtspunt bouwt de rest.
veel op navragen	Je antwoorden liggen vaak bij je leveranciers. Het gesprek met je EPD-leverancier is dan je eerste stap, met de vragen uit hoofdstuk 6.
ongeveer 10, 19 en 9	Je staat op het startpunt. In de 19 controls op deels zit het meeste werk en in de 9 op niet het meeste risico.

het overzicht

control	volledig	deels	niet	navragen
A.2.2 AI-beleid	☐	☐	☐	☐
A.2.3 afstemming met ander beleid	☐	☐	☐	☐
A.2.4 herziening van het AI-beleid	☐	☐	☐	☐
A.3.2 rollen en verantwoordelijkheden voor AI	☐	☐	☐	☐
A.3.3 melden van zorgen	☐	☐	☐	☐
A.4.2 documentatie van middelen	☐	☐	☐	☐
A.4.3 gegevensbronnen	☐	☐	☐	☐
A.4.4 tooling	☐	☐	☐	☐
A.4.5 systeem- en rekencapaciteit	☐	☐	☐	☐
A.4.6 mensen	☐	☐	☐	☐
A.5.2 proces voor impactbeoordeling	☐	☐	☐	☐
A.5.3 documentatie van impactbeoordelingen	☐	☐	☐	☐
A.5.4 impact op individuen en groepen	☐	☐	☐	☐
A.5.5 maatschappelijke impact	☐	☐	☐	☐
A.6.1.2 doelstellingen voor verantwoorde ontwikkeling	☐	☐	☐	☐
A.6.1.3 proces voor verantwoord ontwerp en ontwikkeling	☐	☐	☐	☐
A.6.2.2 vereisten voor AI-systemen	☐	☐	☐	☐
A.6.2.3 documentatie van ontwerp en specificatie	☐	☐	☐	☐
A.6.2.4 verificatie en validatie	☐	☐	☐	☐
A.6.2.5 ingebruikname	☐	☐	☐	☐
A.6.2.6 gebruik en monitoring	☐	☐	☐	☐
A.6.2.7 technische documentatie	☐	☐	☐	☐
A.6.2.8 logboeken van AI-systemen	☐	☐	☐	☐
A.7.2 data voor ontwikkeling en verbetering	☐	☐	☐	☐
A.7.3 verzameling van data	☐	☐	☐	☐
A.7.4 kwaliteit van data	☐	☐	☐	☐
A.7.5 herkomst van data	☐	☐	☐	☐
A.7.6 voorbereiding van data	☐	☐	☐	☐
A.8.2 informatie voor gebruikers	☐	☐	☐	☐
A.8.3 externe rapportage	☐	☐	☐	☐
A.8.4 communicatie van incidenten	☐	☐	☐	☐
A.8.5 informatie voor belanghebbenden	☐	☐	☐	☐
A.9.2 processen voor verantwoord gebruik	☐	☐	☐	☐
A.9.3 doelstellingen voor verantwoord gebruik	☐	☐	☐	☐
A.9.4 beoogd gebruik	☐	☐	☐	☐
A.10.2 toewijzing van verantwoordelijkheden	☐	☐	☐	☐
A.10.3 leveranciers	☐	☐	☐	☐
A.10.4 klanten	☐	☐	☐	☐
totaal (samen 38)	☐	☐	☐	☐

Volledig, deels en niet tellen samen op tot 38. Navragen tel je apart.

het bestuursblad

Deze pagina vul je in nadat je hebt geteld. Print de pagina apart en neem die mee naar de raad van bestuur of de raad van toezicht.

mijn drie getallen

volledig	deels	niet

Ter vergelijking: een organisatie met NEN 7510 die nog niets aan AI heeft gedaan, zit op 10, 19 en 9.

mijn drie grootste aandachtspunten

Kies uit de controls waar je 'niet' hebt aangekruist. Heb je er meer dan drie, geef dan voorrang aan AI die patiënten raakt (A.5, A.7.4 tot en met A.7.6 en A.9.4) en aan controls die je nog moet navragen bij je leverancier.

	control	wat ontbreekt	eigenaar
1			
2			
3			

wat ik mijn bestuur in één zin vertel

Vul de zin aan. De zin is bewust kort, zodat die in een bestuursnotitie of op één dia past.

Van de 38 AI-controls hebben we er _____ geregeld, _____ half en _____ nog niet.
Bij _____ weten we het nog niet en vragen we het na. Het grootste aandachtspunt zit in _____,
daar beginnen we mee met _____ als eigenaar.
Op _____ meten we opnieuw.

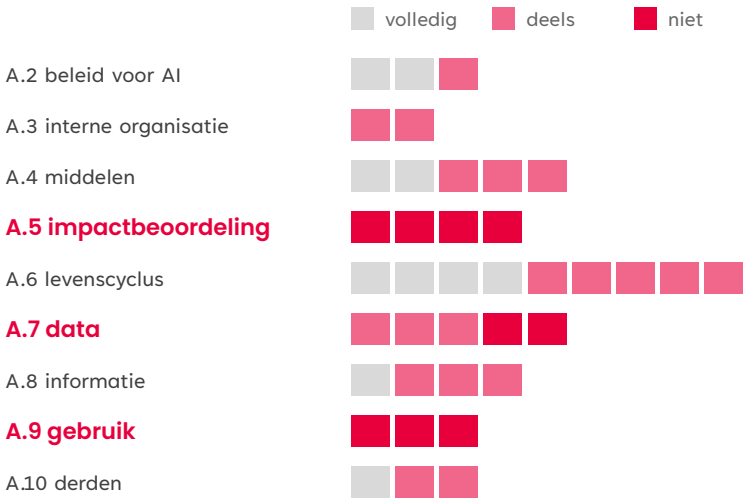
datum van deze meting _____

ingevuld door _____

volgende meting _____

6. de negen die NEN 7510 niet dekt

Negen controls hebben geen tegenhanger in NEN 7510. Ze zitten op drie plekken. Alle drie wegen ze in de zorg zwaarder dan elders.



figuur 5: het startpunt per cluster: de rode blokken zijn de negen zonder tegenhanger

wat het systeem met mensen doet · A.5.2 tot en met A.5.5

NEN 7510 beschermt informatie, terwijl ISO 42001 je vraagt te beoordelen wat een AI-systeem doet met de mensen over wie het beslist. In de zorg zijn dat patiënten. Als een model voor één groep patiënten stelselmatig slechter uitpakt, is dat geen beveiligingsincident, maar je raad van toezicht zal het wel zo behandelen.

waar de data vandaan komt · A.7.5 en A.7.6

NEN 7510 classificeert data en regelt wie erbij mag. ISO 42001 wil daarnaast weten waar trainings- en invoerdata vandaan komen en wat ermee gebeurd is. Voor AI in je EPD ligt dat antwoord bij je leverancier. De kans is groot dat je die vraag nog niet hebt gesteld.

waarvoor je het gebruikt · A.9.2 tot en met A.9.4

ISO 42001 vraagt per systeem vast te leggen waarvoor het bedoeld is en waarvoor niet. Dat lijkt administratie, tot je ziet dat hier de grens ligt waarachter je van gebruiksverantwoordelijke aanbieder wordt. Een model dat je bijtraint op je eigen patiëntenpopulatie, kan die grens al overschrijden.

de vragen aan je leverancier

Voor AI die je niet zelf hebt gebouwd, komen deze negen controls neer op één gesprek met je leverancier. Neem voor dat gesprek deze zes vragen mee.

1. Is dit systeem onder de AI Act hoog risico, en zijn jullie de aanbieder?
2. Valt het ook onder de MDR, en zo ja, in welke klasse?
3. Op welke data is het model getraind, en op welke patiëntenpopulatie?
4. Welke logs krijgen wij, op welk niveau, en hoe lang bewaren jullie ze?
5. Wat is het beoogde gebruik volgens jullie documentatie, en wat gebeurt er als wij daarvan afwijken?
6. Hoe melden jullie een incident aan ons, en binnen hoeveel uur?

7. wat je hierna doet

Een normenkader vertelt je wat je geregeld moet hebben. Het vertelt je niet welke AI er al in je organisatie aanwezig is, wie er eigenaar van is en of je het kunt stopzetten.
Die vraag beantwoord je met een overzicht van je toepassingen, je leveranciers en je risico's. Je kunt daar op twee manieren mee beginnen.

zelf	Met de **preplijst voor AI-agents**: zes voorwaarden voordat een agent je systemen in mag, en een invulbaar register voor je belangrijkste agents.
samen	In een verdiepingsgesprek over **grip op AI**. Neem je ingevulde werkboek mee, dan beginnen we niet bij nul.

wil je je score samen doornemen?

Neem je ingevulde werkboek mee, dan hebben we een mooie basis voor het gesprek. We lopen samen de controls door die jouw aandacht nodig hebben. Ligt het antwoord bij je EPD-leverancier, dan zetten we de vragen klaar.

wil je je score samen doornemen?



Erik Schmitz
Marktdirecteur Zorg

plan een gesprek

over ilionx

ilionx is een IT-kennis- en implementatiepartner. We helpen organisaties vooruit met architectuur, applicatieontwikkeling, security en data, en met de processen en veranderingen die daarbij horen. Dat doen we in teams met verschillende specialisten, samengesteld rond jouw vraag. Zo brengen we eenvoud in een complexe wereld.

Voor security kiezen we per laag de beste tool en verbinden we het geheel in ons eigen SOC in Nederland, 24/7. Onze analisten brengen de signalen uit al je tools samen tot één beeld, onderzoeken wat ze zien en grijpen in. Voor AI brengen we shadow AI in kaart en handhaven we je beleid in de tools die medewerkers en agents gebruiken.

verantwoording

Dit werkboek is gebaseerd op ISO/IEC 42001:2023 (bijlage A), NEN 7510:2024, de EU AI Act (verordening (EU) 2024/1689, zoals gewijzigd door de AI Omnibus, verordening (EU) 2026/1744), de Cyberbeveiligingswet en de Cyberbeveiligingsregeling voor de zorg.

De eerste plichten uit de AI Act gelden sinds februari 2025, de transparantieplichten sinds augustus 2026. De plichten voor gebruiksverantwoordelijken van hoog-risico AI gelden vanaf 2 december 2027, en voor AI in medische hulpmiddelen vanaf 2 augustus 2028. De Cyberbeveiligingswet is op 15 augustus 2026 in werking getreden.

Het startpunt (10, 19 en 9) is een expertoordeel per control voor een zorgorganisatie die NEN 7510 heeft ingericht, vóór AI-specifieke maatregelen. Het werkboek is een zelfbeoordeling en geen audit, certificering of juridisch advies. Tien controls op volledig betekent dat je de risico's kent. Klaar ben je dan nog niet.

Versie 1.5 · editie najaar 2026 · ilionx