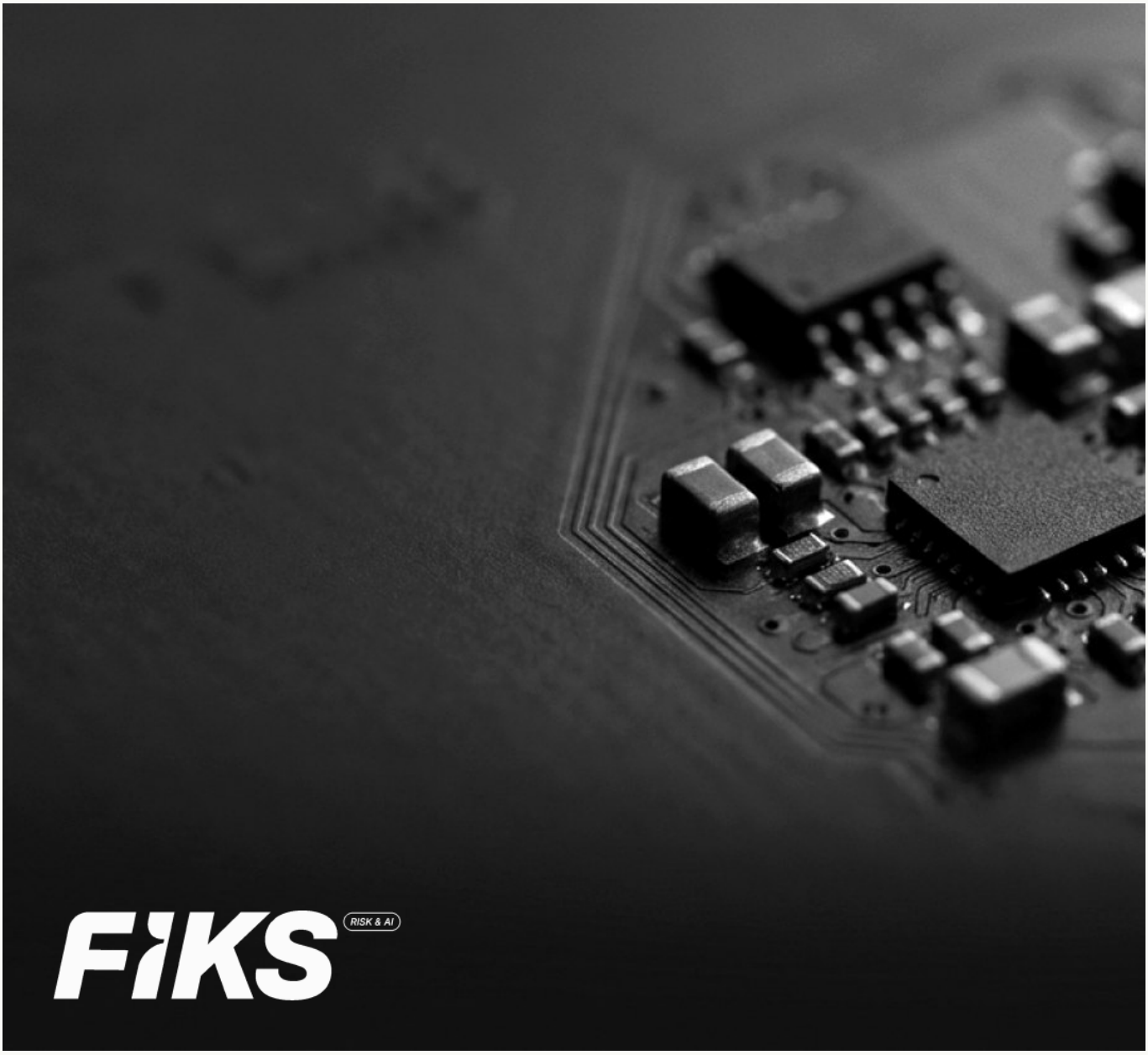
U moet aantonen dat uw patiëntgegevens veilig zijn. Wie regelt het?



Als zorgaanbieder werkt u dagelijks met gezondheidsgegevens van patiënten en cliënten. U moet kunnen laten zien dat die gegevens goed beveiligd zijn: aan de Inspectie Gezondheidszorg en Jeugd, de Autoriteit Persoonsgegevens, zorgverzekeraars en uw patiënten zelf. Denk aan wie toegang heeft tot het EPD, hoe inzage wordt vastgelegd en wat er gebeurt als een medewerker van functie verandert of uit dienst gaat. Het opzetten en bijhouden van informatiebeveiliging volgens NEN 7510 komt vaak boven op de zorg en het dagelijkse werk.

In het kort

Fiks Risk & AI helpt u een managementsysteem voor informatiebeveiliging (ISMS) in te richten dat voldoet aan NEN 7510, met het **NEN 7510-certificaat** als resultaat. Onze specialisten doen het uitzoekwerk, stellen de documentatie op en bereiden u voor op de certificeringsaudit. De afgesproken beheersmaatregelen voeren we samen met uw team in.

Het abonnement omvat de nulmeting, de inrichting van het ISMS, de auditvoorbereiding en het onderhoud na certificering. De audit zelf wordt uitgevoerd door een onafhankelijke, geaccrediteerde certificerende instelling. U krijgt een **certificeringsgarantie**, onder de voorwaarden die we op pagina 6 beschrijven.

Duidelijke afspraken tussen IT en bestuur

Uw IT- of informatiebeveiligingsverantwoordelijke kent de systemen en processen. NEN 7510 vraagt daarnaast nadrukkelijk om betrokkenheid van het bestuur of de directie: die stelt het beleid vast, wijst rollen en verantwoordelijkheden toe en beoordeelt periodiek of het ISMS werkt.

Daarom betrekken we het bestuur vanaf de start. Samen bepalen we het toepassingsgebied van het ISMS en wie waarover beslist. Uit de nulmeting en de risicoanalyse volgt een werkplan waarin staat wat er moet gebeuren, wie het oppakt en wanneer het klaar moet zijn.



Waarom NEN 7510?

Zorgaanbieders moeten aantoonbaar zorgen voor een veilige verwerking van gezondheidsgegevens. Die plicht volgt uit de AVG, de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (Wabvpz) en het Besluit elektronische gegevensverwerking door zorgaanbieders, dat NEN 7510 aanwijst als norm. Certificering is niet wettelijk verplicht, maar wel de gangbare manier om aan te tonen dat u voldoet.

NEN 7510 bestaat uit twee delen. Deel 1 beschrijft de eisen aan het managementsysteem, deel 2 de beheersmaatregelen, ingedeeld in de thema's Mens, Fysiek, Technologie en Organisatie. Sinds 15 augustus 2026 geldt ook de Cyberbeveiligingswet (Cbw). Een zorgorganisatie die aan NEN 7510:2024 voldoet, voldoet volgens VWS ook aan de zorgplicht uit de Cbw; registratie en meldplicht vragen wel aparte aandacht. In de nulmeting adviseren we u of uw organisatie onder de Cbw valt.

Wabvpz en Besluit gegevensverwerking

Aantoonbaar veilige verwerking van gezondheidsgegevens

Cyberbeveiligingswet

Valt uw organisatie ook onder de Cbw?

Specialisten die het werk uit handen nemen

De dienst is bedoeld voor zorgaanbieders die aan NEN 7510 moeten voldoen en daarvoor onvoldoende capaciteit of kennis in huis hebben, zoals huisartsenpraktijken, GGZ-aanbieders, thuiszorgorganisaties en klinieken. Onze specialisten plannen het werk, voeren het uit en houden het bij. Uw team levert de benodigde informatie en beslist mee over de beheersmaatregelen.

Een vraag van de zorgverzekeraar, aandacht van de toezichthouder of de overstap naar de nieuwe versie van de norm kan de aanleiding zijn. Heeft u nog een certificaat op NEN 7510:2017? Dan moet de transitie naar NEN 7510:2024 uiterlijk op 20 februari 2027 zijn afgerond.

De aanleiding

Zorgverzekeraar Toezicht IGJ en AP Transitie naar 2024

Dit zit in het abonnement

Nulmeting	Inrichting ISMS	Auditvoorbereiding	Onderhoud

Nulmeting en risicoanalyse	We bepalen samen het toepassingsgebied, brengen de belangrijkste systemen en informatiestromen in kaart, zoals het EPD en het berichtenverkeer met andere zorgverleners, en toetsen de huidige situatie aan NEN 7510. Op basis van de risicoanalyse maken we een werkplan met prioriteiten.
ISMS inrichten en maatregelen invoeren	We stellen het informatiebeveiligingsbeleid en de verklaring van toepasselijkheid op en helpen uw team de gekozen beheersmaatregelen in te voeren, bijvoorbeeld rond toegangsbeheer, logging van inzage in patiëntdossiers (NEN 7513), leveranciers en bewustwording van medewerkers. Ook maken we een incidentplan dat we samen oefenen, zodat iedereen zijn of haar rol bij een incident of datalek kent. De taken en bewijsstukken houden we overzichtelijk bij. Nieuwe Vogels verzorgt de uitvoering op het gebied van informatiebeveiliging. Privacy- en juridische vragen, zoals verwerkersovereenkomsten en de meldplicht datalekken, leggen we voor aan FIKS Legal.
Auditvoorbereiding	We begeleiden de interne audit en de directiebeoordeling, stellen het bewijsdossier samen en bereiden uw team voor op de certificeringsaudit.
Onderhoud	Na certificering houden we het ISMS, de risicoanalyse en de documentatie actueel, zodat u goed voorbereid bent op de jaarlijkse controle-audits en de hercertificering.

Niet in het abonnement: de audit zelf	Fiks Risk & AI voert de certificeringsaudit nadrukkelijk **niet** zelf uit. De audit wordt uitgevoerd door een onafhankelijke certificerende instelling die door de Raad voor Accreditatie (RvA) is geaccrediteerd voor NEN 7510. Wij werken samen met een vaste auditpartner die wij u kunnen voorstellen. De kosten van de audit worden apart begroot en zijn voor uw rekening.

Certificering met garantie

Wij garanderen dat uw organisatie de audit doorstaat en het **NEN 7510-certificaat** behaalt. Dat is een stevige toezegging, en daar staat een stevige inzet van uw organisatie tegenover. De garantie geldt alleen als u aan alle onderstaande voorwaarden voldoet:

- u voert alle maatregelen uit die wij adviseren, volledig en binnen de termijnen uit het werkplan;
- u levert de gevraagde informatie en bewijsstukken tijdig en volledig aan;
- u stelt een vaste contactpersoon beschikbaar en zorgt dat bestuur en betrokken medewerkers meewerken;
- u wijkt niet zonder overleg met ons af van de afgesproken aanpak.

Kortom: wij bepalen wat er moet gebeuren, u zorgt dat het gebeurt.

Als de audit niet slaagt

Haalt u de audit onverhoopt niet terwijl aan de voorwaarden is voldaan, dan passen wij ons advies, de documentatie en het bewijsdossier aan op de bevindingen van de auditor en begeleiden we de heraudit **zonder extra advieskosten**.

Het doorvoeren van ontbrekende of onjuiste technische maatregelen blijft de verantwoordelijkheid van uw organisatie. De kosten van de certificerende instelling voor de heraudit zijn voor uw rekening.

Wat het certificaat aantoont

Het certificaat toont aan dat uw ISMS binnen het afgesproken toepassingsgebied voldoet aan NEN 7510. Of u ook aan alle toepasselijke wettelijke verplichtingen voldoet, zoals de AVG of de Cyberbeveiligingswet, vraagt een afzonderlijke beoordeling.

Uw inzet en de kosten

Uw inzet

Van uw organisatie vragen we een vaste contactpersoon en voldoende tijd om informatie aan te leveren en maatregelen door te voeren. Hoeveel tijd dat is, schatten we in tijdens de nulmeting en leggen we vast in het werkplan.

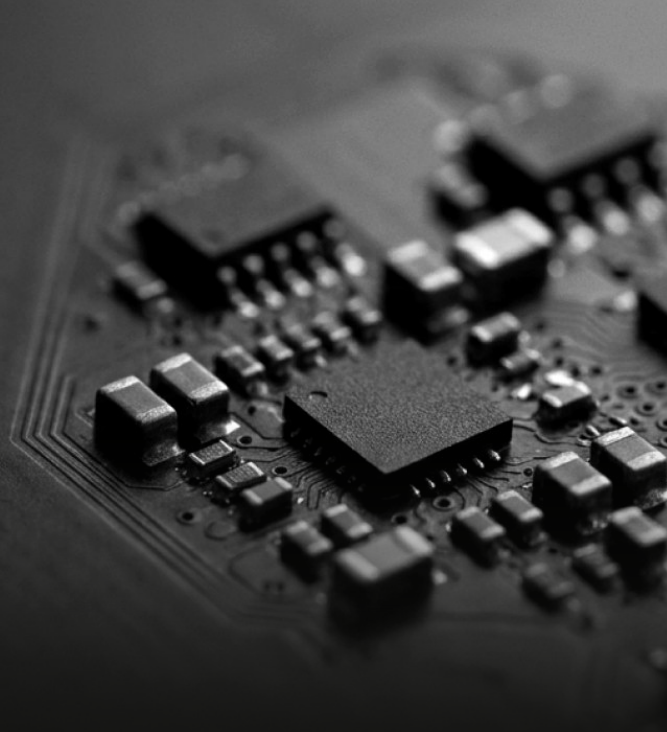
Wij verzorgen de planning en bewaken de voortgang. Besluiten over budget en verantwoordelijkheden blijven bij uw bestuur of directie.

De kosten

Abonnement	NEN 7510-certificering (NEN 7510-1:2024)
Prijs	Op basis van uw omvang, het aantal locaties en het toepassingsgebied
Niet inbegrepen	De certificeringsaudit (via onze auditpartner, apart begroot), licenties, technisch beheer en de afhandeling van een daadwerkelijk incident

Offerte

De exacte werkzaamheden, prijs, looptijd en opzegtermijn vindt u in de offerte.



Vragen over dit voorstel?

Wij lichten de offerte graag toe. Nodig daarvoor bij voorkeur uw IT-verantwoordelijke en de collega die over het budget beslist uit, zodat we ook de planning en haalbaarheid kunnen bespreken.

Wie wij zijn

Fiks Risk & AI is een samenwerking van RSafe, Nieuwe Vogels en FIKS Legal. Nieuwe Vogels voert de informatiebeveiliging uit, FIKS Legal adviseert over privacy en juridische vragen en RSafe is uw aanspreekpunt.



Rob Buddingh
Fiks Risk & AI

robb@rsafe.eu
+31 6 1208 5538