

AI in de Zorg: De Governance Gap

Wat wij tegenkomen in de markt — en waar de oplossing ligt

HES Consultancy International | Mei 2026 | hes-consultancy.nl n.a.v. Nictiz AI-radar voor Databeschikbaarheid v1.0

De Nictiz AI-radar brengt voor het eerst in kaart welke AI-systemen in de Nederlandse zorg worden ingezet en hoe volwassen ze zijn. Dat is een cruciale eerste stap. Maar de radar roept ook een dringende vervolgvraag op: wie bewaakt of deze systemen veilig, compliant en verantwoord draaien?

1 Wat wij tegenkomen in de markt

- **AI-adoptie versnelt, governance blijft achter**
Zorginstellingen zetten AI in voor spraakherkenning, medisch samenvatten en triaging. De technologie is TRL 7-9 (marktrijp), maar de governance-infrastructuur is vaak TRL 2-3 (verkennend). Er ontstaat een steeds grotere kloof tussen wat technisch kan en wat organisatorisch geborgd is.
- **Compliance wordt urgent: augustus 2026**
De EU AI Act verplicht per 2 augustus 2026 volledige compliance voor hoog-risico AI. Vrijwel alle AI-systemen op de Nictiz radar die patientdata verwerken, vallen in deze categorie. Daarnaast gelden NEN 7510-2, NIS2 en de Cyber Resilience Act.
- **Geen zicht op AI-gebruik binnen de organisatie**
CISO's en informatiemanagers hebben vaak geen compleet beeld van welke AI-systemen worden gebruikt, door wie, met welke data, en onder welke voorwaarden. Shadow AI is een groeiend risico.
- **De keten is versnipperd**
EPD-leveranciers, AI-startups, cloudplatforms en interne teams bouwen elk hun eigen AI-laag. Er ontbreekt een centrale governance-laag die audit, dataminimalisatie en toegangscontrole afdwingt.

73%

zorginstellingen
zonder AI-register

< 12

maanden tot
EU AI Act deadline

30+

AI-toepassingen
op Nictiz radar

4

frameworks
tegelijk relevant

2 Oplossingsrichtingen

- ✓ **AI-inventarisatie koppelen aan compliance**
De Nictiz radar biedt de inventarisatie. De logische vervolgstap is per AI-systeem een risicoklasse bepalen (EU AI Act), een NEN 7510 gap-analyse uitvoeren, en een governance-plan opstellen.
- ✓ **Centrale AI-governance laag**
Een technische laag tussen de organisatie en AI-systemen die audit trails, PII-filtering, budgetbewaking en tenant-isolatie afdwingt. Vergelijkbaar met hoe een firewall netwerkverkeer beheert.
- ✓ **Continue monitoring, niet eenmalig assessment**
Compliance is geen checkbox maar een continu proces. AI-modellen veranderen, dreigingen evolueren, regelgeving wordt aangescherpt. Automated compliance monitoring is essentieel.
- ✓ **Incident-readiness voor AI-incidenten**
NIS2 vereist melding binnen 24 uur bij significante incidenten. Organisaties moeten nu oefenen met AI-specifieke scenario's: model bias, datalekage via prompts, adversarial attacks.