Boardroom memo

Aan: Bestuur Vanguard Healthcare
Van: Viresh Sheoratan, Muazma Anwar
Datum: 11 februari 2026
Onderwerp: Belangrijkste wettelijke en ketenrisico's

Vanguard Healthcare verwerkt veel medische persoonsgegevens. Dat zijn bijzondere persoonsgegevens en die moeten extra goed beveiligd worden. Tegelijk is de organisatie sterk afhankelijk van digitale systemen zoals het EZPD, cloudoplossingen en externe leveranciers. Daardoor kunnen cyberproblemen direct invloed hebben op privacy, wetgeving en zorgcontinuïteit.

Top 3 wettelijke risico's (AVG/NIS2)

Risico 1: Onbevoegde toegang tot patiëntgegevens

Binnen Vanguard is MFA nog niet overal verplicht en autorisaties zijn niet altijd actueel. Er is ook al een phishing-incident geweest. Hierdoor kunnen onbevoegde personen toegang krijgen tot medische dossiers. Dit is een groot risico onder de AVG (Algemeen verordening persoonsgegevens) en ook onder NIS2 (Cyberbeveiligingswet).

Risico 2: Uitval EZPD

In de casus staat dat het EZPD tijdelijk onbeschikbaar was geweest door een storing bij de cloudleverancier. Als het EZPD uitvalt, kunnen zorgprocessen vertragen of stilvallen. Dat is niet alleen een technisch probleem, maar ook een risico voor patiëntveiligheid en wettelijke verplichtingen rond continuïteit, NIS2.

Risico 3: Onvoldoende aantoonbare beveiligingsaanpak

De IT-afdeling werkt vooral operationeel, er is geen volledig ISMS en monitoring is beperkt. Daardoor ontbreekt vaak een bewijs op papier en systemen. Dit vergroot het risico op problemen bij audits en toezicht vanuit AVG/NIS2.

Top 2 ketenrisico's

Ketenrisico 1: Storing bij cloudleverancier, EZPD onbeschikbaar

Vanguard is afhankelijk van externe partijen voor hosting en beheer van belangrijke systemen. Als een leverancier storing heeft, raakt dat direct de zorgverlening bij Vanguard. Ten slotte, EZPD wordt onbeschikbaar.

Ketenrisico 2: Te zwakke afspraken met leveranciers

In de casus staat dat contracten en afspraken historisch gegroeid zijn en niet altijd aantoonbaar aansluiten op actuele AVG/NIS2 eisen. Als beveiligingseisen niet scherp in contracten staan, is het lastiger om leveranciers aan te sturen en verantwoording af te leggen na incidenten.

Conclusie

De belangrijkste prioriteiten voor Vanguard zijn: Toegang beter beveiligen: MFA overal en autorisaties opschonen. Continuïteit van kritieke systemen verbeteren, verlaagde afhankelijkheidsrisico, leveranciersafspraken aanscherpen en aantoonbaar maken.