Voldoen aan het MedMij Normenkader Informatiebeveiliging

In dit factsheet lees je meer over:

- NEN 7510-certificatietraject
- wat is NEN 7510?
- het Normenkader Informatiebeveiliging MedMij
- toetreden tot MedMij
- doorlooptijd en tijdlijn
- penetratietest

NEN 7510-certificatietraject

Om MedMij-deelnemer te kunnen worden heb je een NEN 7510-certificering nodig en moet je bovendien voldoen aan het aanvullend normenkader informatiebeveiliging. Je certificering moet je laten uitvoeren door een NEN 7510-bevoegde instantie. Die kun je vinden via de NEN 7510-certificerende instellingen. Een certificatietraject bestaat in eerste instantie uit een tweetal audits.

Tijdens de fase 1-audit wordt de opzet van je managementsysteem getoetst, tijdens fase 2 wordt in een serie gesprekken met medewerkers van je organisatie het bestaan en de werking beoordeeld. Om je in de gelegenheid te stellen eventuele bevindingen uit fase 1 op te lossen, liggen deze twee audits doorgaans 4 tot 6 weken uit elkaar.

Het aantal benodigde auditdagen hangt onder meer af van de grootte van je organisatie.

Wat is NEN 7510?

NEN 7510 is een Nederlandse norm, gebaseerd op ISO 27001. Beide normen beschrijven een managementsysteem (plan-do-check-act) voor informatiebeveiliging. Een belangrijk onderdeel van dit managementsysteem is het uitvoeren van een risicoanalyse en het selecteren en implementeren van de benodigde beheersmaatregelen.

NEN 7510 werd specifiek ontwikkeld voor de zorgsector en bevat een aantal zorgspecifieke beheersmaatregelen, gericht op de bescherming van persoonlijke zorggegevens zoals patiëntdata en behandelgegevens.

Organisaties die NEN 7510 succesvol hebben geïmplementeerd, voldoen automatisch aan de eisen uit ISO 27001. Daarom worden beide normen vaak in één adem genoemd. Van auditpartijen ontvang je meestal een offerte voor de certificering van beide normen tegelijk

NEN 7510-normdocumentatie is gratis verkrijgbaar. Kijk hiervoor op de **NEN-website**. Via NEN 7510-1 (Managementsysteem) en NEN 7510-2 (Beheersmaatregelen).

Normenkader informatiebeveiliging MedMij

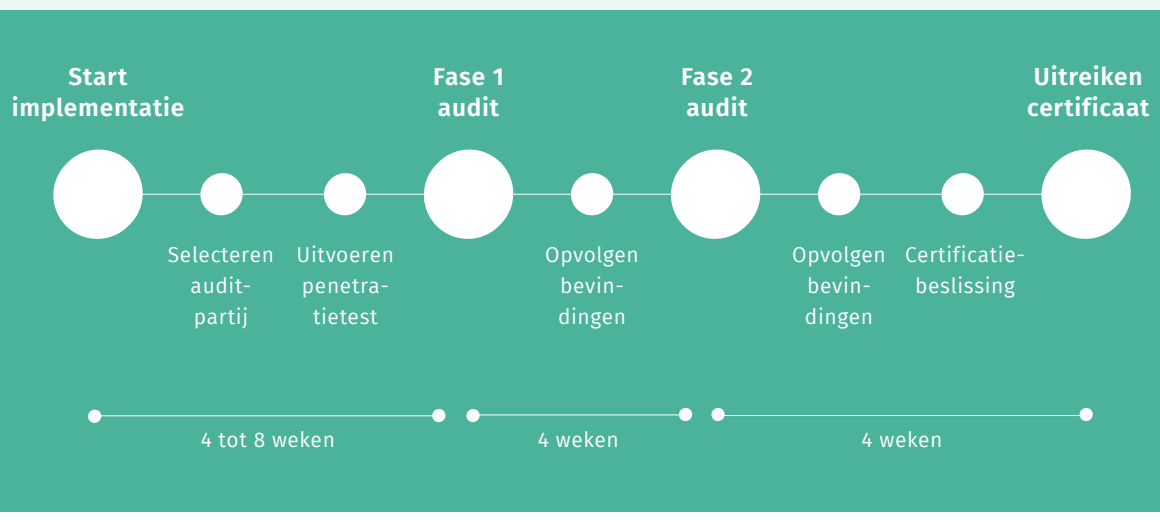
Bij de totstandkoming van het MedMij Afsprakenstelsel werd een risicoanalyse uitgevoerd en besloten voor het beheersen van deze risico's de NEN 7510-beheersmaatregelen te hanteren. In het MedMij Afsprakenstelsel lees je meer over de aanvullende eisen in het **MedMij Normenkader Informatiebeveiliging**.

Doorlooptijd en tijdlijn

Allereerst heeft je organisatie tijd nodig om het managementsysteem op te zetten. Je kunt zelfstandig aan de slag gaan met de NEN 7510-documentatie. Of je kunt hulp inroepen van gespecialiseerde adviseurs, die je met behulp van voorbeelddocumenten werk uit handen kunnen nemen zodat je tijd bespaart.

Als vuistregel geldt dat het managementsysteem voor informatiebeveiliging ten tijde van de fase 2-audit al enkele maanden geïmplementeerd moet zijn voordat tot certificatie overgegaan kan worden. Deze tijd heb je nodig om voldoende bewijsmateriaal te verzamelen, zodat de auditor vertrouwen krijgt dat je managementsysteem werkt.

In de meest gunstige situatie ziet de tijdlijn er als volgt uit:



Penetratietest

In **A.18.2.3** van het Normenkader Informatiebeveiliging lees je meer over de noodzaak van het uitvoeren van een zogenaamde penetratietest.

a Eisen aan de penetratietester

De penetratietest moet je laten uitvoeren door een externe én onafhankelijke partij. Het is dus niet toegestaan om dit zelf te doen.

Let bij de selectie van een partij op:

- Adequate expertise, let daarbij op certificeringen zoals CEH of OSCP en
- aantoonbare kennis/ervaring met de door jullie gebruikte technologieën.

b Greybox applicatiepenetratietest

De penetratietest die je als kandidaat-deelnemer moet laten uitvoeren is een zogenaamde greybox-test. Dit houdt in dat je de penetratietester beperkte inzicht geeft in je applicatie.

Dit kan onder meer inhouden:

- Toegang tot architectuur/ontwerpdocumentatie
- Inloggegevens voor verschillende rollen

Met deze achtergrondinformatie kan de penetratietester de test efficiënter uitvoeren. Er gaat geen tijd verloren aan het van buitenaf in kaart brengen van het achterliggende systeem/systemen.

c Scope

Het is niet nodig een penetratietest uit te voeren op de gehele architectuur en/of alle programmacode. Het gaat met name om de beveiliging van gegevens die over het MedMij-netwerk worden uitgewisseld. De focus moet dus liggen op de beveiliging van de externe koppelvlakken.

Let op! Een app of een web-portaal is ook een extern koppelvlak.

d Beoordeling

Veelal is het niet noodzakelijk het penetratietestrapport te delen met de MedMij-beheerorganisatie. De NEN 7510-auditor zal tijdens de fase 2-audit inzage willen hebben in het rapport van de penetratietest om vast te stellen dat deze voldoet aan de eisen die A.18.2.3 daaraan stelt.

Treed je toe in de rol van DVA (Dienstverlener Zorgaanbieder)?

Dan kun je de resultaten van een eventuele DigiD-audit deels hergebruiken.
We adviseren je voor je begint ook eerst contact op te nemen met:
leveranciersmanagement@medmij.nl.

Vragen

Heb je nog vragen?
Neem contact met ons op via het loket
op e-mailadres: **info@medmij.nl.**

oktober 2023