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 geldige 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 op aanwezigheid en volledigheid, 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 de organisatie en de complexiteit van de dienstverlening van de 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 specifieke 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).

NEN 7510 en MedMij

Voor MedMij gelden een aantal aanvullende eisen voor de NEN 7510-certificering

- De organisatienaam op het NEN 7510-certificaat is ook de organisatie die de MedMij Deelnemersovereenkomst sluit.
- De scope die op het NEN 7510-certificaat staat moet minstens de MedMij-dienstverlening beslaan. Als een deelnemer een NEN 7510-certificaat heeft maar de MedMij-dienstverlening nog niet in scope zit, dan kan deze bij de eerstvolgende NEN 7510-audit worden toegevoegd.
- Bij de selectie van de van toepassing zijnde NEN 7510-beheersmaatregelen moeten minimaal de maatregelen uit het MedMij Normenkader Informatiebeveiliging zijn opgenomen.

Normenkader Informatiebeveiliging MedMij

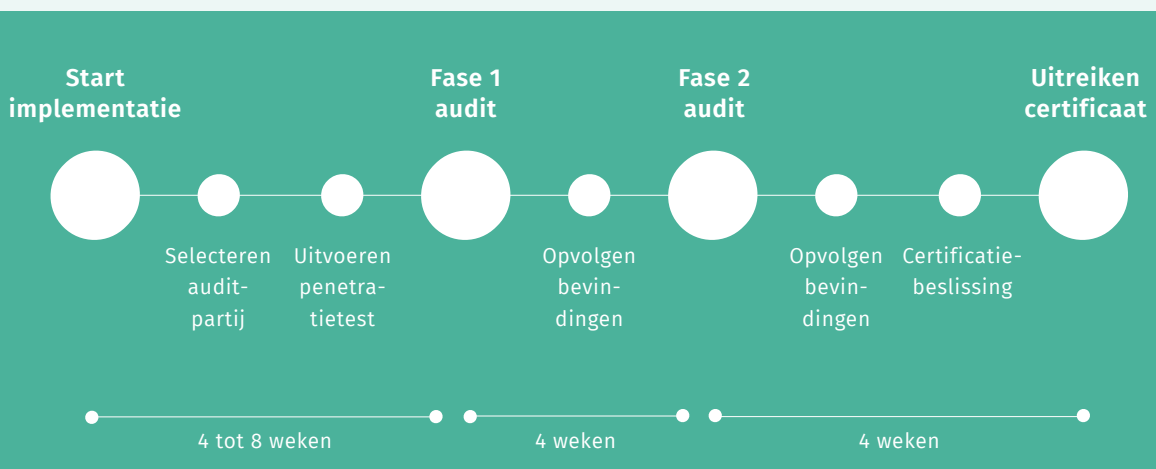
Bij de totstandkoming van het MedMij Afsprakenstelsel werd een risicoanalyse uitgevoerd en besloten om voor het beheersen van deze risico's de NEN 7510-beheersmaatregelen te hanteren. In het MedMij Afsprakenstelsel lees je meer over de aanvullende eisen in het **MedMij Normenkader Informatiebeveiliging**.

Doorlooptijd en tijdlijn

Allereerst moet je een managementsysteem opzetten. Je kunt hiervoor zelfstandig aan de slag gaan met de NEN 7510-documentatie. Om tijd te besparen kun je ook de hulp inroepen van gespecialiseerde adviseurs.

Het managementsysteem voor informatiebeveiliging moet op het moment dat je de fase 2-audit laat uitvoeren al enkele maanden geïmplementeerd zijn. Pas daarna kan tot certificatie overgegaan 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 norm **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
- Aantoonbare kennis/ervaring met de door jullie gebruikte technologieën
- Voor DVZA's: ervaringen met Logius DigiD technisch normenkader

b Whitebox en code review

De penetratietest die je als kandidaat-deelnemer moet laten uitvoeren is een zogenaamde whitebox-test. Dit houdt in dat je de penetratietester zoveel mogelijk inzicht geeft in je applicatie. Voor afsprakenstelsel release 1.5.0 is voorzien periodiek een greybox-test te laten plaatsvinden en initieel een whitebox-test of bij een grootschalige wijziging.

Een whitebox pentest houdt het volgende in:

- Toegang tot architectuur/ontwerpdocumentatie
- Toegang tot broncode
- Inloggegevens voor verschillende rollen

Met deze achtergrondinformatie kan de penetratietester de test efficiënter uitvoeren. Er gaat geen tijd verloren aan het in kaart brengen van de achterliggende 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 MedMij-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 DVZA (Dienstverlener Zorgaanbieder)?

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

Vragen

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

maart 2023