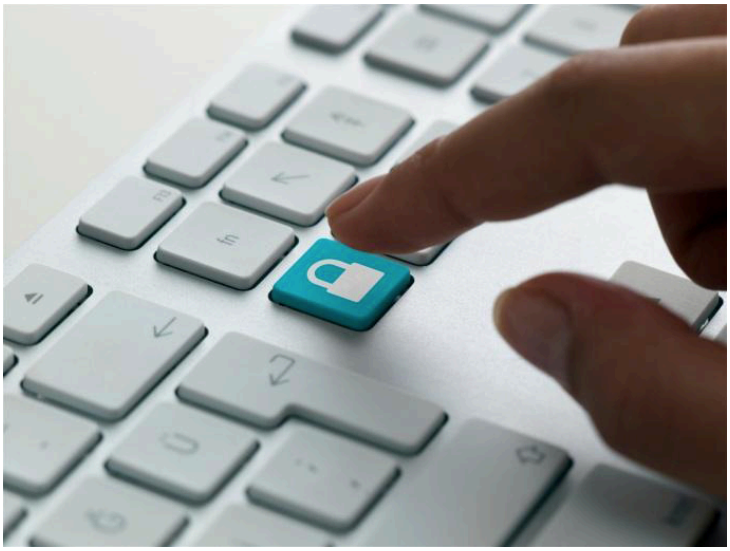
NEN 7510: Een kwestie van goede zorg

Menig zorginstelling geeft aan nog niet te voldoen aan de NEN 7510 omdat deze (nog) niet verplicht is. Wettelijk is dit wellicht het geval, maar wat nu als men dit bekijkt vanuit het perspectief van het verlenen van de best mogelijke zorg aan patiënten? Zou een zorginstelling vanuit dat oogpunt het niet als een verplichting moeten zien? Als je als zorginstelling aangeeft dat je de klant centraal stelt, hoe rijmt dit dan met een bewuste keuze om het borgen van de informatiebeveiliging voor je uit te schuiven ?

In deze whitepaper wordt een duidelijk beeld gegeven waarom het invoeren van de NEN 7510 ook voor zorginstellingen wenselijk is. Vervolgens wordt aangegeven met welke stappen dit te realiseren is.

1. Wat is de NEN 7510 en waarom is deze norm geïntroduceerd?
2. 7 redenen om de NEN 7510 in te voeren
3. Aanpak invoering NEN 7510
4. Oplossing voor het vastleggen en inzichtelijk houden van het invoerproces



Wat is de NEN 7510 en waarom is deze norm geïntroduceerd?

Wat is de NEN 7510?

De NEN 7510 is een door het Nederlands Normalisatie-instituut ontwikkelde norm voor informatiebeveiliging voor de zorgsector in Nederland. De norm is gebaseerd op de Code voor Informatiebeveiliging. De NEN 7510 biedt zorginstellingen een leidraad voor het formuleren, vastleggen en controleren van de interne informatiebeveiliging.

Onder informatiebeveiliging in de zorgsector wordt verstaan: “het waarborgen van de **beschikbaarheid**, **integriteit** en **vertrouwelijkheid** van alle informatie die benodigd is om patiënten verantwoorde zorg te kunnen bieden.”

Feitelijk is de NEN 7510 een bundeling van ongeveer 150 paragrafen (verdeeld over 11 hoofdstukken) waarin allerlei zaken die informatiebeveiliging raken, worden beschreven. Daarbij wordt aangegeven waarom men aan deze paragraaf moet voldoen en er wordt een richtlijn gegeven hoe men dit zou moeten bewerkstelligen.

Achtergrond bij de invoer van de NEN 7510

Patiënten worden steeds mondiger en eisen steeds meer van een zorgverlener. Ze willen meer weten over hun behandeltraject. Was vroeger de wil van de arts wet. Tegenwoordig willen patiënten weten waarom iets gebeurt en zijn ze eerder geneigd een second opinion aan te vragen. Als gevolg hiervan moet informatie die vroeger alleen beschikbaar was voor de zorginstelling zelf, nu gedeeld worden met vele belanghebbenden. Hierdoor is de noodzaak van informatiebeveiliging sterk toegenomen.

De overheid heeft het initiatief genomen om tot een eenduidige normering van de informatiebeveiliging in de zorg te komen. Hieruit vloeide in 2005 de NEN 7510 voort.

De doelstelling was dat de gehele zorg in 2008 verplicht aan deze norm zou moeten voldoen. Om zo na de toen geplande koppeling van zorggegevens aan de BSN-nummers te kunnen garanderen dat de BSN-nummers optimaal beveiligd zouden zijn. Toen zowel de introductie van BSN-nummers in de zorg en de introductie van het EPD vertraging opliepen, heeft het IGZ de druk op het voldoen aan de NEN 7510 normering verminderd.

Op dit moment is de verwachting dat het IGZ de norm verplicht zal gaan stellen, zodra er voldoende organisaties adequate zorg kunnen bieden en aan de normering voldoen. Instellingen die op dat moment niet aan de norm voldoen, zullen vanaf dat moment de werkzaamheden moeten staken.

7 Redenen om de NEN 7510 in te voeren

1. **Wet Bescherming Persoonsgegevens**
   Hoewel de NEN 7510 formeel niet in de wet is opgenomen, is iedere instelling die te maken heeft met de verwerking van persoonsgegevens verplicht zich te houden aan de Wet Bescherming Persoonsgegevens. In Artikel 13 van deze wet staat onder meer vermeld dat instellingen passende technische en organisatorische maatregelen dienen te nemen om persoonsgegevens te beveiligen tegen verlies of onrechtmatige verwerking.

2. **Onderdeel van de factor 'Kwaliteit leveren'**
   Het IGZ toetst zorginstellingen op het leveren van kwaliteit. Informatiebeveiliging is een integraal onderdeel van het leveren van kwaliteit. Zorgdragen dat informatie vertrouwelijk en integer behandeld wordt, is net zo belangrijk als het verzorgen van een wond.

3. **Verwachting samenleving**
   De samenleving verwacht van zorgorganisaties dat zij niet alleen het beste met onze gezondheid voor hebben, maar dat zij ook zorgen voor adequate informatiebeveiliging. Het gaat in dit geval om zaken als:
   a. Beschikbaarheid: Toegang hebben tot de juiste informatie op het juiste moment
   b. Integriteit: Beschikken over correcte informatie
   c. Vertrouwelijkheid: de informatie vertrouwelijk behandelen. Patiënten hechten veel waarde aan het feit dat informatie alleen gedeeld wordt met mensen die het echt dienen te weten.

4. **Regelgeving gebruik BSN-nummers**
   Alle zorgaanbieders, indicatieorganen en zorgverzekeraars moeten sinds 1 juni 2009 het BSN gebruiken bij het uitwisselen van gegevens over patiënten of cliënten. In de regelgeving over het gebruik van BSN-nummers staat expliciet aangegeven dat instanties die toegang hebben tot de BSN-nummers hun informatiebeveiliging op orde moeten hebben.

5. **Conformeren wordt verplicht**
   De gezondheidsinspectie doet haar best om de NEN 7510 verplicht te stellen. Op dit moment kunnen zij dit nog niet hardmaken, aangezien er nu nog te weinig instellingen aan de NEN 7510 voldoen. Nu verplicht stellen zou tot gevolg hebben dat onvoldoende instellingen in formele zin zorg mogen leveren. Echter op het moment dat er voldoende instellingen voldoen aan de NEN 7510, of IGZ een middel vindt om de NEN 7510 wel verplicht te stellen, zullen ze dat zeker doen. Voldoe je op dat moment dan niet, dan loop je het risico dat je je werkzaamheden zal moeten staken.

6. **Belang bij incidenten**
   Veel organisaties denken dat zij de informatiebeveiliging goed op orde hebben, maar komen er bij incidenten achter dat dit niet het geval blijkt te zijn. Vindt er een incident plaats dan wil je aan kunnen tonen:
   a. hoe de informatiebeveiliging geregeld is,
   b. of welke stappen je aan het ondernemen bent om de informatiebeveiliging op orde te brengen.

   Hoe meer organisaties voldoen aan de norm, hoe hoger de verwachtingen vanuit de maatschappij. Nu wordt er nog geaccepteerd dat 'eraan gewerkt wordt', maar op een gegeven moment verwacht men dat je hiervoor de procedures hebt vastliggen.
7. **Voorkomen incidenten**
   Een goede informatiebeveiliging kan bepaalde incidenten (zoals verkeerde medicatie, te laat handelen etc.) voorkomen.

Conclusie: Informatiebeveiliging is Goede Zorg
Het bieden van goede zorg staat centraal in iedere zorgorganisatie. Daarbij zou het zorgdragen voor een goede omgang en beveiliging van de informatie een integraal onderdeel moeten zijn van het bieden van goede zorg.

De juiste aanpak leidt tot het gewenste resultaat!

Nu er genoeg redenen zijn gegeven om met de NEN 7510 invoering aan de slag te gaan, kan het dikke juridisch opgestelde handboek een obstakel vormen. Daarbij is het voor menig zorginstelling niet duidelijk wie er nou verantwoordelijk is voor de invoer van de NEN 7510. Naast het bepalen van de eindverantwoordelijkheid van de invoer van de NEN 7510, wordt u ook geholpen met vragen als:
Hoe kunt u overzicht over het hele proces houden en toch, indien nodig, precies zien hoever de status van een maatregel is?
Hoe kunt u de implementatie van de NEN 7510 het beste aanpakken?

Verantwoordelijkheid invoer NEN 7510

Informatiebeveiliging heeft impact op de hele organisatie. Het heeft niet alleen betrekking op het beveiligen van computers en software, maar het betreft ook over andere informatie zoals folders, boeken, dossiers, handelingen bij een klant en de interne en externe communicatie. Informatiebeveiliging heeft te maken met facetten als verantwoordelijkheden, afspraken met leveranciers, de positie ten opzichte van andere zorgverleners, de positie ten opzichte van patiënten en hoe je beleid en procedures in je organisatie hebt geregeld en geborgd.

Het feit dat informatiebeveiliging de hele organisatie raakt, maakt de invoer van de NEN 7510 de verantwoordelijkheid van het hoogste niveau van de organisatie. Indien aanwezig zal dit de Raad van Toezicht zijn, waardoor wij in het vervolg van deze whitepaper spreken over de Raad van Toezicht (RvT).

Hoe houdt de Raad van Toezicht overzicht en inzicht?

Als een Raad van Toezicht geconfronteerd wordt met een incident of een controle, willen ze kunnen laten zien dat er aan een oplossing wordt gewerkt.

- Welke actie is er al ondernomen?
- Waar wordt aan gewerkt?
- Wat is de status van de diverse maatregelen?

Hoe overzichtelijker en duidelijker dit getoond kan worden, hoe beter het is.
Maar hoe krijgt een organisatie dit voor alle 150 onderdelen van de NEN 7510 voor elkaar en is de Raad van Toezicht tevens in staat het grote geheel te overzien?

In eerste instantie moet er per onderdeel een vertaalslag gemaakt worden van het handboek naar de eigen organisatie. Elk van de 11 hoofdstukken dient hiervoor in kleinere stukken verdeeld te worden. Per onderdeel moet vervolgens bepaald worden wie met dit onderdeel aan de slag gaat en welke vraag deze persoon precies moet beantwoorden.

Om een goed beeld te geven van de status van ieder van de 150 onderdelen, zou van ieder onderdeel een dossier aangelegd moeten worden. Per onderdeel moet vervolgens vastgelegd worden, of er al aan dat onderdeel voldaan wordt en indien dit niet het geval is, in welke fase van het proces men zit om hier wel aan te voldoen. Daarbij dienen ter controle de benodigde documenten, procedures, risico-inventarisaties etc. aan dat dossier gekoppeld te worden.
Een goede ICT oplossing is hierbij essentieel.
Door dit hele proces te automatiseren, wordt het mogelijk om in helicopterview te zien wat de status van de NEN 7510 implementatie is. Daarnaast kunt u tot in detail zien welke afdeling zijn taken al heeft afgerond of waar het nodig is om een project te starten om de maatregel tijdig door te voeren. Door het prioriteren van door te voeren maatregelen en een inschatting van de daaruit voortvloeiende kosten, is de RvT in staat een integraal werkplan of meerjarenplan op te stellen.

Stappenplan voor een succesvolle implementatie van de NEN 7510

Stap 0: Risicoanalyse
Voordat u het NEN 7510 handboek erbij pakt, is het goed om getriggerd vanuit de NEN 7510 onderwerpen een Business Impact Analyse (BIA) te maken. Een BIA heeft als doel: “Het inventariseren van de risico’s en de impact van deze risico’s op de organisatie.” De BIA geeft zowel inzicht in de financiële als de niet financiële impact.
Aan de hand van de uitkomsten van de BIA kan er prioriteit gegeven worden aan bepaalde onderdelen uit de NEN 7510.

Stap 1: Signaleren van knelpunten
Per onderdeel moet bepaald worden wat de vraag vanuit de NEN 7510 is en of de organisatie hier wel/niet aan voldoet. Zodra u de vraag met JA kunt beantwoorden en u het bewijs hiervoor kunt leveren, is dit onderdeel afgerond.

Stap 2: Welke maatregel moet genomen worden en is het noodzakelijk dat die genomen wordt?

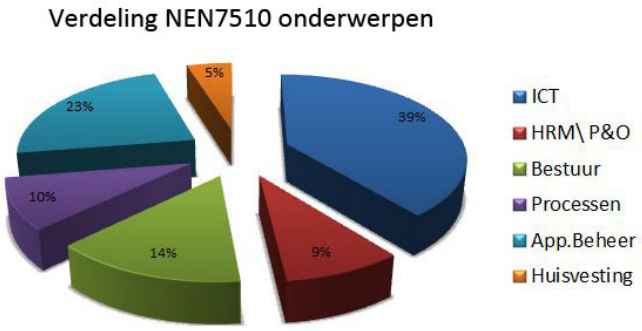
Indien u niet voldoet aan de norm dient u te bepalen welke maatregel er genomen moet worden om wel op dit onderdeel te kunnen voldoen.

Vervolgens dient u te beslissen of het voor de organisatie van belang is om aan deze norm te conformeren. U moet bepalen of de risico's van een incident (imagoschade, kosten, productieverlies etc.) zich verhouden tot de kosten die het invoeren van de maatregel met zich meebrengt. Alleen als een maatregel wettelijk verplicht is, moet u voldoen en zijn kosten geen afweging.

Mocht besloten worden om een maatregel niet door te voeren, dient dit wel onderbouwd (inclusief risicoanalyse) bij de maatregel aangegeven te worden en dit moet in de NEN rapportage worden aangegeven.

Stap 3: Verantwoordelijkheid bepalen

Informatiebeveiliging is niet uitsluitend een technische aangelegenheid. Alle organisatieonderdelen hebben met informatie te maken, en dus ook met de risico's en daarbij behorende maatregelen. Vanuit de NEN 7510 kunnen de vragen toegewezen worden aan verschillende afdelingen binnen de organisatie, zoals ICT, HRM\P&O, Bestuur, Processen, Applicatiebeheer en Huisvesting.



Bepaal nu per maatregel wie deze maatregel gaat uitwerken en leg de eindverantwoordelijkheid bij deze persoon/afdeling neer.

Stap 4: Plan van aanpak & planning

De eindverantwoordelijke ontwikkelt een plan van aanpak en werkt de stappen die er genomen moeten worden om als organisatie te voldoen aan de maatregel uit. Dit dient zo gedetailleerd mogelijk te gebeuren zodat er tevens bepaald kan worden wat de bijbehorende kosten zijn. Mede op basis hiervan kan de Raad van Toezicht een meerjarenplan opstellen waarbij er op basis van prioriteit en budget bepaald wordt, welke maatregelen er op welk moment uitgevoerd wordt.

Nadat het plan van aanpak is afgerond, wordt er een planning gemaakt waarin concrete taken worden toegewezen aan de personen die zorg gaan dragen voor de uitvoering.

Stap 5: Uitvoer taken
Nadat het budget beschikbaar is gesteld en er personen zijn vrijgemaakt om met een maatregel aan de slag te gaan, kan de uitvoering worden gestart. Vervolgens is het essentieel dat de voortgang gemonitord wordt en door voortgangsrapportages inzichtelijk gemaakt wordt.

Stap 6: Beleid borgen
De maatregelen zijn genomen. Nu is het van belang dat de organisatie deze gaat borgen in documenten en procedures waarin aangegeven wordt wat het beleid is, wat eventuele sancties zijn en hoe de maatregel gemonitord wordt etc.

Stap 7: Communicatie
Nadat een maatregel genomen is, dient de organisatie hierover geïnformeerd te worden. Zijn er zaken die voor het personeel veranderen, zorg er dan voor dat iedereen hiervan doordrongen is en dat het duidelijk voor hen is, waarom het van belang is dat deze zaken veranderen. Zo wordt er bewustwording en draagkracht gecreëerd.

Stap 8: (interne) Audit
Natuurlijk gaat een eindverantwoordelijke ervan uit dat bij het maken van het plan van aanpak en het opstellen van een takenlijst overal aan gedacht is. Toch is het goed om intern tussen afdelingen onderling, of door een kwaliteitsmedewerker te laten toetsen of er inderdaad op alle punten voldaan wordt aan het betreffende onderdeel van de NEN 7510.

ICT oplossing: Thysia Information Security Solution (TISS)

Wilt u graag hulp bij het invoeren van de NEN 7510? Hulp die verder gaat dan alleen een audit die laat zien op welke punten u nog niet voldoet aan de norm?
Dan biedt Thysia Information Management u hiervoor de oplossing.

Thysia helpt u bij een nulmeting waarbij de huidige situatie en risico's in kaart worden gebracht. Daarnaast krijgt u toegang tot de door Thysia ontwikkelde softwareoplossing TISS. In TISS worden u en uw medewerkers aan de hand van een duidelijk stappenplan door het implementatieproces heen geleidt.

De eigenschappen van TISS zijn:

- Er worden vragensets aangeboden, gebaseerd op de NEN 7510 normering. De vragensets zijn opgedeeld in categorieën waar verschillende personen in de zorginstelling verantwoordelijk voor zijn.
- Aan de hand van deze vragen kunt u een inventarisatie maken en een rapportage genereren met de risico's en knelpunten in uw informatiebeveiliging. Vervolgens zet u concrete acties uit ter verbetering van uw informatiebeveiliging. Deze acties bewaakt u eenvoudig via de applicatie.
- Binnen één omgeving heeft u realtime inzicht in de status rondom uw NEN 7510 conformiteit.
- TISS kan worden geïntegreerd met Microsoft SharePoint en Outlook of uw eigen documentbeheersysteem voor het beheren van documenten en taken.
- Aanpassingen en uitbreidingen in de norm worden toegevoegd aan de applicatie
- Snelle instap tegen lage kosten

Thysia Information Management

Thysia Information Management is expert op het gebied van SharePoint en informatiemanagement. De oplossingen van Thysia helpen organisaties eenvoudiger samenwerken en informatie delen. Specialisaties zijn SharePoint portals en document & workflow management oplossingen die naadloos geïntegreerd zijn met backoffice systemen. Speciaal voor de invoering van de NEN 7510 heeft Thysia de "Thysia Information Security Solution " applicatie ontwikkeld.

Thysia Information Management
Haagsemarkt 1, 4813 BA Breda, Nederland | Tel: +31 (0)76 521 88 46 | Fax: +31 (0)76 521 16 84
www.thysia.eu | info@thysia.eu