SpotOnMedics
All-In-One Platform

Informatiebulletin:

NEN 7510 norm, informatiebeveiliging in de zorg

Juli 2016

Inhoudsopgave

Informatiebulletin:
NEN7510, informatiebeveiliging in de zorg

SpotOnMedics en NEN-normen

Informatiebeveiliging voor zorg in Nederland

Informatiebeveiliging wordt steeds belangrijker en is ook in de zorg een breed gespreksonderwerp geworden. De NEN7510 wordt hierbij als norm gebruikt. In dit verband zal ook uw praktijk een antwoord moeten geven op vragen zoals in de vragenlijst van KNGF plusprogramma en Keurmerk Fysiotherapie worden genoemd.

In dit informatiebulletin informeren we u over de stand van zaken bij SpotOnMedics op het gebied van informatiebeveiliging en de Normbladen die op dit punt relevant zijn.

Welke NEN-normen zijn relevant?

In de communicatie wordt voornamelijk gesproken over de NEN7510. Deze basisnorm geeft kaders aan het werken met geautomatiseerde processen, servers, internettoegang, programmatuur en veel andere aspecten zoals toegangbeveiliging, backup en de beschikbaarheid van de informatiessystemen. Naast de NEN7510 zijn er aanvullende normen voor de zorgsector geformuleerd.

In dit informatiedocument wordt er verder ingegaan op de volgende normen:

- NEN7510; basis normering
- NEN7512; als aanvulling op de NEN7510
- NEN7513; als aanvulling op de NEN7510

SpotOnMedics en de NEN-normen

SpotOnMedics is op de hoogte van de genoemde NEN-normen en heeft maatregelen getroffen om ervoor te zorgen dat haar informatie- en serversystemen voldoen aan de gestelde eisen en normen.

SpotOnMedics heeft verschillende stappen genomen om te komen tot een adequate informatiebeveiliging. Zo zijn de SpotOnMedics FysioOne serversystemen geplaatst in Nederlandse rekencentra die goed beveiligd zijn en de noodzakelijke voorzieningen

hebben om de continuïteit van het functioneren van de programmatuur en opgeslagen gegevens te waarborgen. De rekencentra voldoen hierbij aan de eisen in de NEN7510 / ISO 27001 normeringen.

Dit jaar heeft VECOZO gemeld een aanscherping van de informatiebeveiliging door te willen voeren. SpotOnMedics is hierover met VECOZO in gesprek en zal binnen de hieraan gestelde termijn (voor eind 2016) aan voldoen. In dit kader is het belangrijk om expliciet te melden dat FysioOne van de zogenaamde 2-laags authenticatie voorzien gaat worden. Deze 2-laags authenticatie kunt u zien als aanvulling op het huidige inlog mechanisme (van gebruikersnaam en wachtwoord) en zal versterkt worden met een aanvullende unieke toegangssleutel per inlogsessie. De SpotOnMedics technische staf werkt momenteel aan de realisatie van deze extra toegangsbeveiliging. Met betrekking tot de hiervoor benodigde extra functionaliteit en gebruiksinstructies kunnen we u bevestigen dat deze ruimschoots voor eind december 2016 gereed is.

In de komende maanden zullen we u informeren over de stand van zaken op dit gebied van informatiebeveiliging middels periodieke nieuwsbrieven.

Omdat we merken dat het onderwerp informatiebeveiliging veel vragen oproept, zijn in dit informatiebulletin de verschillende normen beknopt toegelicht en informeren we u over maatregelen die u als praktijk zelf kunt en dient te nemen.
Voor een goede en doeltreffende informatiebeveiliging moeten we immers gezamenlijk stappen ondernemen en heeft u als praktijk daar ook een belangrijke rol in.

NEN7510: informatiebeveiliging in de zorg

Als basis normering geldt in de zorg de NEN7510, Informatiebeveiliging in de zorg.

SpotOnMedics heeft haar programmatuur, serversystemen, internettoegang, stroomvoorziening, fysieke toegangsbeveiliging en backup-processen e.d. ondergebracht in een extern rekencentrum dat voldoet aan de NEN7510 / ISO 27001 normeringen.

Ten aanzien van de systeembeschikbaarheid van de SpotOnMedics programmatuur geldt dat deze is vastgelegd en voor de fysiotherapiepraktijken is geborgd, in een formele SpotOnMedics SLA (Service level Agreement). Dit "document" is vast onderdeel van een te sluiten SpotOnMedics software gebruik- en licentieovereenkomst.

Naast de SLA heeft SpotOnMedics ter waarborging van de gegevens van haar klanten (fysiotherapiepraktijken) en de door de klanten vastgelegde patiëntgegevens een zogenaamde SpotOnMedics CoC (Code Of Conduct) opgesteld waarin beschreven is op welke wijze SpotOnMedics met de opgeslagen gegevens omgaat. Met de CoC belooft SpotOnMedics aan haar relaties vertrouwelijkheid en geheimhouding. De afspraken m.b.t. geheimhouding zijn door SpotOnMedics conform de NEN7510 integraal verankerd in de arbeidsovereenkomsten van haar werknemers en eventueel ingehuurde externe relaties.

Praktijken die besluiten om SpotOnMedics een gegevensconversie te laten uitvoeren als onderdeel van een te maken overstap besluit, ondertekenen met SpotOnMedics een aanvullende geheimhoudingsverklaring ter expliciete borging van de geheimhouding van de te ontvangen en technisch te converteren patiëntgegevens.

NEN7512: aanvullende eisen en maatregelen t.o.v. 7510

Ten aanzien van de besproken NEN7512 geldt dat deze norm aanvullende eisen en maatregelen beschrijft t.o.v. de NEN7510. De NEN7512 handelt over gegevensuitwisseling waarbij de zorgverlener één van de partijen in een te maken gegevensuitwisseling is.
In de norm zijn naast de te hanteren eisen en spelregels verschillende scenario's voor gegevensuitwisseling beschreven. Bij al deze scenario's is het van cruciaal belangrijk dat de partijen die in een dergelijke gegevensuitwisseling betrokken zijn, ook daadwerkelijk zijn wie ze claimen te zijn en dat bovendien de op te zetten communicatie geoorloofd is.

SpotOnMedics voldoet aan deze normering en geeft daarbij de volgende toelichting:

1) Identificatie van gebruikers in het SpotOnMedics platform is van oorsprong conform de type 1-factoridentificatie (gebruikersnaam, wachtwoord). De hogere vereisten die bij een 2-factoridentificatie nodig zijn wordt momenteel geïmplementeerd in de SpotOnMedics infrastructuur. Bij een 2-factoridentificatie niveau wordt de combinatie van juiste gebruikersnaam en juiste wachtwoord uitgebreid met een unieke activeringscode per inlogsessie.

2) In de NEN7512 zijn verschillende communicatiescenario's uitgewerkt.
   Ten aanzien van de SpotOnMedics infrastructuur kunnen we het volgende melden:

   - alle communicatie tussen SpotOnMedics serversystemen, praktijken en gebruikers verloopt via https: een versleuteld protocol (encryptie) zodat de verstuurde gegevens niet lees- of herkenbaar zijn.

   - de SpotOnMedics serverplatforms staan in beveiligde ISO- en NEN gecertificeerde rekencentra die onder Nederlands recht en grondgebied vallen.

   - het SpotOnMedics platform wordt dagelijks getoetst op "server- en programmatuur veiligheid". Het resultaat van deze dagelijkse toetsing is via de inlogpagina voor platform gebruikers raadpleegbaar.

   - in FysioOne opgemaakte rapportages die aan huisarts/verwijzers verzonden worden verloopt via een beveiligd Zorgmail netwerk.
     De toegang tot dit netwerk wordt door de praktijk zelf gecontracteerd. Voor het

activeren van deze koppeling hanteert Zorgmail een gecontroleerd protocol waarbij de praktijk zelf direct betrokken is in het proces van het activeren van de Zorgmail koppeling in FysioOne.

- Patiënt vult online vragenlijst in ter voorbereiding op bezoek aan de praktijk.
  De vragenlijst wordt gestuurd aan patiënten die ingeschreven en bekend zijn bij de praktijk en daarbij een persoonlijk e-mailadres aan de praktijk hebben opgegeven. De vragenlijst en de antwoorden van de patiënt op deze vragenlijst blijven altijd in het beveiligde rekencentrum van SpotOnMedics en worden niet via een e-mail verstuurd. Patiënten ontvangen voor het kunnen beantwoorden van dergelijke vragenlijsten van de praktijk een unieke gebruikersnaam en wachtwoord.

- Patiënt maakt online afspraak voor bezoek via de website van de praktijk.
  Deze functie is in FysioOne nog niet beschikbaar. Let op, een dergelijke functie heeft niet alléén impact op de FysioOne programmatuur maar ook op de website van de praktijk zelf.

- Zorgverlener stuurt declaratiegegevens van een patiënt via een geautomatiseerde koppeling aan zorgverzekeraar.
  Het verzenden van declaratiebestanden verloopt via het VECOZO portaal en een bijbehorend praktijk server-certificaat.

NEN7513: aanvullende eisen en maatregelen t.o.v. 7510

In de NEN7513 worden eisen en normen beschreven over het loggen van het systeemgebruik binnen de zorginstantie. De reikwijdte van de norm is zorgbreed, maar de voorbeeld scenario's handelen voornamelijk in de driehoek huisarts-ziekenhuis-apotheek. De paramedische sector wordt hierbij nog niet expliciet benoemd. SpotOnMedics beschouwd de NEN7513 als richtinggevend voor aansluiting op toekomstige landelijke zorginfrastructuur.

Status: in de SpotOnMedics serversystemen en programmatuur worden verschillende "gebeurtenissen" gemonitord en gelogged. Logging vindt met name plaats rond het het in- en uitloggen van gebruikers op het platform en inplannen en wijzigingen/verwijderen van agenda-afspraken.

Voor een zuivere logging is het van belang dat gebruikers over een persoonlijk account beschikken zodat in de log-bestanden ook terug te lezen is wie, wanneer welke toegang tot het informatiesysteem heeft gehad en welke functies heeft gebruikt c.q. gegevens heeft ingezien.

In FysioOne kan een praktijkhouder voor alle werknemers een eigen persoonlijk gebruikersaccount aanmaken en daarbij verschillende autorisatie niveaus toekennen. De functie gebruikersbeheer is alleen beschikbaar voor de medewerkers die beschikken over de functierol “manager” en “kwaliteitsmanager”.

Wat kunt u zelf doen?

Ten aanzien van de beveiliging van uw patiëntgegevens zijn onderstaande tips genoemd die u in uw praktijk kunt nemen ter verhoging van het beveiligingsniveau. Bespreek deze tips in uw praktijkoverleg en bepaal gezamenlijk hoe u dit in uw praktijk gaat toepassen.

1) Zorgt u ervoor dat uw therapeuten de beeldschermen / monitoren niet onbeheerd achterlaten

   Beheersmaatregel: wij adviseren om de PC's in op een slaapstand na 5 minuten met een wachtwoord beveiliging.

2) Verander regelmatig de wachtwoorden van de pc's en informatiesystemen in uw praktijk

   Beheersmaatregel: Het is raadzaam om de wachtwoorden (toegangscode) van alle gebruikers regelmatig te veranderen. Op deze wijze is het voor anderen moeilijker om het te weten te komen. Zo kunt u elk halfjaar uw therapeuten de opdracht geven om dit te wijzigen en maak gebruik van "sterke" wachtwoorden.

3) Verstuur geen patiëntberichten/informatie aan huisartsen en verwijzers via de 'normale' e-mail

   Beheersmaatregel: Wij adviseren u als u nog geen gebruik maakt van Zorgmail binnen uw praktijk om een beveiligde e-mailomgeving bij Zorgmail te activeren. In de software van FysioOne is het mogelijk om rapportages te versturen via het beveiligde netwerk van Zorgmail.

4) Bewaar kopie ID achter slot en grendel

   Beheersmaatregel: Indien u een kopie maakt van identificatiebewijzen van uw patiënten dan adviseren wij u deze op een beveiligde plek te archiveren. Ons advies is om deze direct te uploaden in de patiëntenkaart van FysioOne onder het tabblad 'Docs'.

Digitale perfectie: van patiëntendossier tot boekhouding

SpotOnMedics