Informatiebeveiliging Synchroon

Versie juni 2017

Door de toenemende digitalisering, samenwerking en daarmee gepaard gaande gegevensuitwisseling is informatiebeveiliging de laatste jaren al steeds meer een issue. Door de nieuwe wet- en regelgeving (bijvoorbeeld Meldplicht datalekken, Cliëntenrechten bij elektronische verwerking van gegevens, Algemene verordening gegevensbescherming (AVG), herziening NEN-normen) en door incidenten in het veld, is binnen Synchroon een toenemend besef van urgentie ontstaan om dit op orde te brengen. De impact van het niet op orde hebben van de informatiebeveiliging kan groot zijn, zowel qua imago (je staat zo op de voorpagina van de krant) als bedrijfsmatig (herstelacties, boetes).

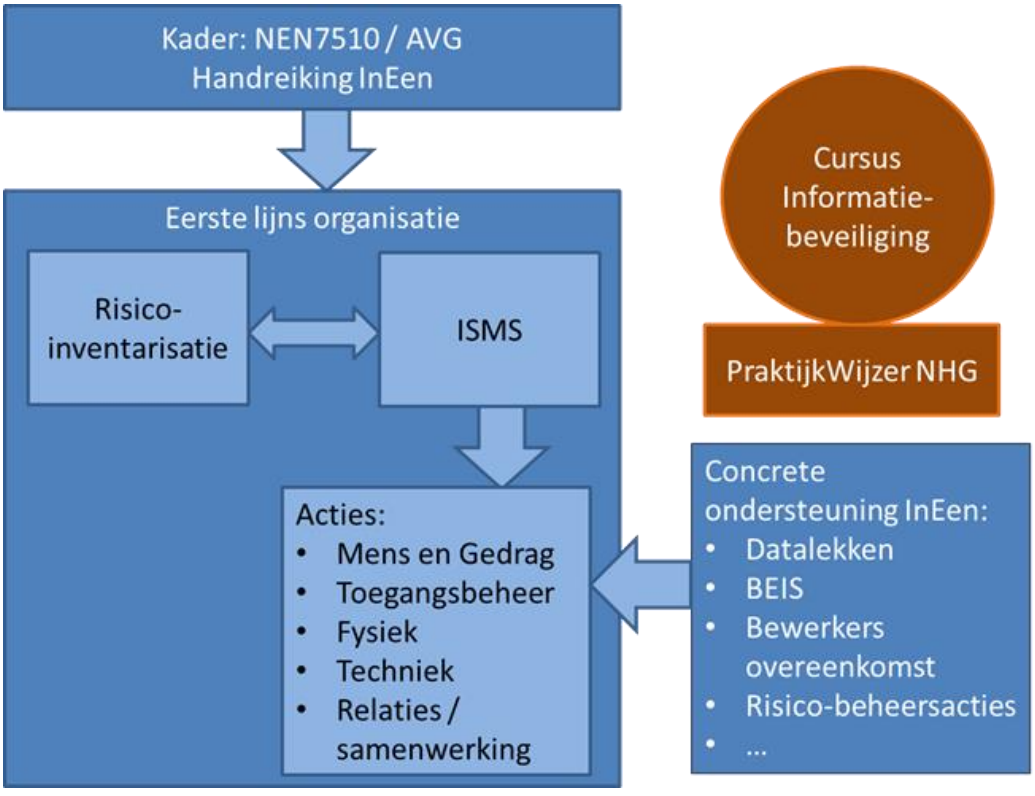
De basis voor informatiebeveiliging in de zorg is de NEN-norm 7510 met de aanvullingen 7512 en 7513. Daarnaast hebben we te maken met regels vanuit verschillende juridische kaders (bijvoorbeeld WGBO, Wbp / AVG, Wet cliëntenrechten, meldplicht datalekken, gedragscode EGiZ).

Samenhangend pakket activiteiten

InEen ondersteunt eerstelijns organisaties, zoals Synchroon, op het terrein van informatiebeveiliging. Synchroon sluit aan bij de bijeenkomsten over dit thema die door InEen worden georganiseerd om haar kennis actueel te houden. Informatiebeveiliging gaat daarbij zeker niet alleen over privacy-aspecten, maar over drie samenhangende onderdelen:

1. Beschikbaarheid van informatie
2. Integriteit (correctheid) van informatie
3. Toegankelijkheid van informatie (privacy)

In schema:



Activiteiten Synchroon

Synchroon heeft in 2016 een IPM (Integraal Privacy Management) beheercontract binnen Stichting Privacyzorg afgesloten. Om de huidige situatie van Synchroon in kaart te brengen is door Stichting Privacyzorg eind 2016 een audit uitgevoerd. Er is gekeken naar de bedrijfsdoelstellingen en de wettelijke eisen die worden gesteld aan de zorgprocessen binnen Synchroon. Vervolgens is advies afgegeven voor de inrichting van de benodigde veranderingen die vereist zijn om compliant te kunnen gaan worden aan de privacywetgeving. Hierna volgen de ondernomen en nog op te pakken acties naar aanleiding van de audit.

Bescherming persoonsgegevens
Synchroon is verplicht om de bescherming van persoonsgegevens (aantoonbaar) te borgen. Met het afsluiten van een IPM- contract bij Stichting Privacyzorg zal er een correcte administratie bijgehouden gaan worden waarin de volgende zaken worden vastgelegd:

- *Welke persoonsgegevens worden vastgelegd*
- *Wie de ontvangers zijn*
- *Wat de Doelbinding is*
- *Gehanteerde Informatiebeveiliging*
- *Rechtmatige grondslag*
- *Geldende Procedures*
- *Afgenomen Evaluaties/PIA's*
- *De Risico's en Wijzigingen die hebben plaatsgevonden*

Autorisatiebeleid
Synchroon heeft (nog) geen volledig beschreven autorisatiebeleid welke bepaald hoe autorisaties binnen Synchroon toegekend worden. De autorisaties, dus welke rol in het KIS mag welke data zien, is vastgelegd. De rechtmatigheid hiervan is vastgesteld door PrivacyZorg. Bij een aanvraag voor een inlog in het KIS wordt er door PrivacyZorg een geheimhoudingsverklaring naar de gebruiker gestuurd. Indien deze getekend retour ontvangen is maakt Synchroon een inlog aan door deze aan te vragen bij VitalHealth.

Alle autorisaties en wijzigingen moeten bijgehouden worden, dit zal gebeuren binnen de PMDB (Privacy Management Data Base) van Stichting Privacyzorg waarbij aangeven wordt hoe de borging plaatsvindt. Hierbij wordt het onderwerp "Ontvangers" beschreven waar de borging uit bestaat, zoals bijvoorbeeld een geheimhouding-, bewerkers- of samenwerkingsovereenkomst.

Functionaris voor de Gegevensbescherming
Synchroon is wettelijk verplicht om een officiële door de Autoriteit Persoonsgegevens geregistreerde "Functionaris voor de Gegevensbescherming" (FG) te benoemen welke een administratie voert (privacy register) over alle verwerkingen van persoonsgegevens. Een medewerker van Stichting Privacyzorg, de heer P.W.A. SChell, is bij de Autoriteit Persoonsgegevens aangemeld als FG voor Synchroon. De FG is onder meer verantwoordelijk voor het managen van datalekken binnen Synchroon en de bij Synchroon aangelsoten huisartspraktijken.

Datalekken
Voor de uitvoering van dienstverlening door Synchroon is het noodzakelijk dat de organisatie (veelal) bijzondere persoonsgegevens verwerkt. In het kader van de huidige en toekomstige regelgeving, vereist de verwerking van bijzondere persoonsgegevens extra waarborgen. Synchroon zal in 2017 een plan uitwerken voor een systematische en organisatie brede methode voor de borging van privacy.

Synchroon werkt, samen met PrivacyZorg, aan een aantal procedures zoals:

I. Privacyreglement

Dit reglement beschrijft wat de wet aangeeft hoe Synchroon om dient te gaan met privacy Wet- en regelgeving.

II. Informatiebeveiligingsplan

Het informatiebeveiligingsplan geeft aan hoe de wettelijk verplichte NENnormen worden nageleefd.

III. Autorisatiematrix (autorisatiebeleid)

Binnen Synchroon is onvoldoende beschreven welke eisen en maatregelen gelden op het gebied van de toegang tot en het gebruik van ICT-objecten in het algemeen, en persoons- en bijzondere persoonsgegevens binnen de informatiesystemen in het bijzonder. Er zal worden beschreven op welke wijze er met gegevens en informatiesystemen binnen de organisatie omgegaan moet worden, welke controles op het juist toepassen van het beleid er uitgevoerd worden en op welke wijze het beheer van de autorisaties binnen Synchroon is geregeld.

Collectief abonnement huisartspraktijken Synchroon

Via Zorgconnect Noord-Oost Brabant heeft Synchroon voor de bij haar aangelsoten huisarts praktijken een collectief abonnement afgesloten. Via dit abonnement krijgen de praktijken:

- Hulp bij vragen over privacy en informatiebeveiliging
- Een kennisdatabase met alle van toepassing zijnde wet en regelgeving, gedragscodes, en richtlijnen, NEN hulpmiddelen e.d.
- Collectief beheer; eigen Functionaris Gegevensbescherming
- Beschikking over talloze actuele templates
- Jaarlijkse Privacy Audits en privacy rapportages
- 7 x 2 4 Quickresponse Team bij datalekken en incidenten