Bijlage 11

Taakomschrijving rollen NEN informatiebeveiliging

1. Doel

In dit document leggen we vast hoe de taken en bevoegdheden ten aanzien van informatiebeveiliging verdeeld zijn over de diverse medewerkers. Tevens wordt aangegeven welke taken op regelmatige basis per medewerker terugkeren.
Uiteraard dient het document aangepast worden aan de functies binnen uw organisatie. Voordeel van deze vorm is dat het een duidelijk inzicht geeft van de taakverdeling per functionaris. De functiebeschrijvingen hoeven dan ook in principe niet meer aan worden gepast.

2. Doelgroep

Alle betrokkenen bij informatiebeveiliging.

3. Afkortingen

EPD	Elektronisch Patiënten Dossier
AIOS	Arts In Opleiding tot Specialist
DA	Doktersassistente
CODA	Coördinerend doktersassistente
ANW	Avond-, nacht- en weekendzorg
RBS	Relatie Beheer Systeem
BSN	Burger Service Nummer

4. Werkwijze

4.1 Toewijzing van taken en bevoegdheden

4.1.1 Bestuurlijke verankering

- De formele goedkeuring en herziening van het informatiebeveiligingsbeleid van de CIHN vindt plaats door het bestuur. Het informatiebeveiligingsbeleid is van toepassing op de CHN B.V., CIHN en OCE B.V..
- Het bestuur delegeert de verantwoordelijkheid voor het opstellen, implementeren en handhaven van het beveiligingsbeleid aan de directeur CIHN. Deze heeft voor uitvoering en toezicht de taak gedelegeerd aan de kwaliteitsfunctionaris.
- Uitvoering, implementatie en controle op naleving van het beveiligingsbeleid worden uitgevoerd door de leidinggevenden binnen de CIHN. Zij communiceren de resultaten aan de kwaliteitsfunctionaris. Minimaal één maal per jaar vindt aan de hand van steekproeven een controle op naleving van het beveiligingsbeleid plaats. De resultaten hiervan worden door de directeur gecommuniceerd aan het bestuur, middels de directiebeoordeling.

4.1.2 Toewijzing en vastlegging van verantwoordelijkheid van informatiebeveiliging

- Iedere locatiemanager of leidinggevende is zelf verantwoordelijk voor een adequate beveiliging van de informatie binnen de locatie/afdeling. Hiertoe dienen de managers de maatregelen, zoals beschreven in dit

informatiebeveiligingsbeleid, te implementeren en controle uit te oefenen op naleving, onder andere door te rapporteren aan de kwaliteitsfunctionaris.
- De systeemeigenaren van patiëntregistratiesysteem en telefonie hebben de gedelegeerde verantwoordelijkheid om zorg te dragen voor de praktische implementatie van de beveiligingsmaatregelen ten aanzien van ICT-systemen. Tevens treden zij op als contactpersonen voor de kwaliteitsfunctionaris, daar waar het gaat om afstemming over beveiligingsmaatregelen.
- De leidinggevenden dragen zorg voor uitvoering van de beveiligingsmaatregelen ten aanzien van personeel, onder meer bij de aanname, uitdiensttreding en functiewijzigingen van personeelsleden. Zij worden hierin ondersteund door de P&O-adviseur.
- Iedere medewerker binnen de organisatie is verantwoordelijk voor alle aspecten van informatiebeveiliging binnen de eigen invloedssfeer.

4.2 Te onderscheiden functies en rollen binnen de CIHN

Veel medewerkers binnen de CIHN werken met gevoelige informatie, zoals personeels- en patiëntgegevens. Daarnaast zijn veel beleidszaken en data op de financiële afdeling confidentieel.
We onderscheiden het volgende type medewerkers in het secundaire proces:

- Directeur: toegang tot personeelsdossiers en financiële zaken.
- Medisch adviseur: toegang tot medische dossiers door middel van een persoonlijke UZI-pas. Ook toegang tot klachten en bandopnames die met toestemming zijn opgevraagd (geen rechtstreekse toegang).
- Financiële administratie: toegang tot financiële zaken, beperkte toegang tot patiëntenregistratie in verband met facturatie, toegang tot salarisgegevens van personeel.
- P&O-adviseur: toegang tot personeelsdossiers en personeelssysteem, toegang tot Arbo-site in verband met verzuimmeldingen.
- Beleidsmedewerker: betrokken bij beleid, geen toegang tot personeels- of patiëntgegevens.
- Kwaliteits- en klachtenfunctionaris: geen rechtstreekse toegang tot patiëntgegevens en bandgesprekken; alleen toegang via bevoegde medewerkers met UZI-pas tot vooraf aangevraagde en goedgekeurde bandgesprekken en tot inzien van patiëntcontacten uit Protopics met betrekking tot klachtenafhandeling of interne meldingen.
- Programmacoördinator OCE b.v.: alleen in het kader van de zorg van de OCE toegang tot patiëntgegevens die gedeeltelijk geanonimiseerd zijn in het kader van de DBC-zorg.
- Secretariaat: toegang tot diverse confidentiële zaken in het kader van ondersteuning van de directeur. Toegang tot patiëntregistratiesysteem met eigen UZI-pas in het kader van ICT-problemen, faxen van contacten, onderzoek bij klachten, verzoeken, et cetera.
- ICT-adviseur: toegang tot Protopics middels eigen UZI-pas op naam ten behoeve van controle van het systeem middels testpatiënten. Ook beheer van hard- en software van het systeem voor opname van bandgesprekken. Hiermee heeft de ICT-adviseur indirect de mogelijkheid gesprekken te beluisteren of patiëntencontacten in te zien. De UZI-pas blijft op de post op een beveiligde locatie.

- ICT-medewerker: toegang tot Protopics in het kader van oplossen en testen technische applicatieproblemen, versturen van contacten, et cetera, middels UZI-pas op naam.
- Locatiemanagers: toegang tot Protopics en het voor hen relevante deel van het personeelssysteem. Toegang tot Arbo-site voor verzuimbeheer eigen medewerkers. Mogelijkheid tot het opnemen van bandgesprekken in het kader van toetsing; voor klachten en interne meldingen alleen na aanvraag door kwaliteitsfunctionaris of medisch adviseur met goedkeuring van directeur.
- CODA's: toegang tot Protopics in het kader van ANW-zorg (persoonlijke UZI-pas), en tevens tot vooraf geselecteerde bandgesprekken van doktersassistenten ten aanzien van toetsing.
- Alle kantoormedewerkers: toegang tot RBS, met daarin contactgegevens, adresgegevens, BSN en verjaardagen van huisartsen, medewerkers, et cetera.

In het primaire proces:

- Doktersassistenten: toegang tot patiëntregistratiesysteem inclusief EPD. Ze zijn hiertoe gemandateerd door de huisarts (collectief) met een persoonlijke UZI-pas.
- Baliemedewerkers: toegang tot patiëntregistratiesysteem exclusief EPD, met persoonlijke UZI-pas.
- AIOS, waarnemers, startende DA zonder persoonlijke UZI-pas: toegang tot patiëntregistratiesysteem exclusief EPD.
- Huisartsen, AIOS en waarnemers met persoonlijke UZI-pas: toegang tot patiëntregistratiesysteem inclusief EPD.

4.3 Functies die een uitvoerende rol spelen in NEN 7510

Iedereen binnen de CIHN heeft te maken met informatiebeveiliging. Via instructies, reglementen, gedragscodes en informatiebijeenkomsten wordt men hier ook van bewust gemaakt. Echter, de verantwoordelijkheid voor de borging van het informatiebeveiligingsbeleid ligt bij een aantal medewerkers in het secundaire proces.

Degenen die taken uitvoeren die van belang zijn in het kader van de certificering van de organisatie voor NEN 7510 zijn:

- kwaliteitsfunctionaris
- leidinggevenden (locatiemanagers, controller, directeur)
- P&O-adviseur
- ICT-adviseur
- systeemeigenaren van Protopics en Telefonie
- ICT-medewerker

In de volgende paragrafen worden de taken en bevoegdheden per functie beschreven. Per functie zal in de bijlage een overzicht gegeven worden van de reguliere zaken die uitgevoerd moeten worden (per kwartaal, jaar, et cetera).

4.3.1 Kwaliteitsfunctionaris

Evaluatie en actualisering

- De gedelegeerde verantwoordelijkheid voor het periodiek evalueren en actualiseren van het informatiebeveiligingsbeleid is toegekend aan de kwaliteitsfunctionaris van de CIHN.
- De organisatie zal tenminste eens per jaar - onder verantwoordelijkheid van de kwaliteitsfunctionaris - een globale risicoanalyse uitvoeren om vast te stellen of voor specifieke gegevens of (nieuwe) informatiesystemen aanvullende maatregelen noodzakelijk zijn.
- De organisatie zal - onder verantwoordelijkheid van de kwaliteitsfunctionaris - het beleid tenminste eens per drie jaar evalueren en indien nodig actualiseren. De evaluatie zal zich richten op:
  - Effectiviteit van het beveiligingsbeleid, gebaseerd op de geregistreerde beveiligingsincidenten;
  - De kosten en het effect van de genomen beveiligingsmaatregelen;
  - Het effect van veranderingen in de technologie.

Overzicht van de middelen

- Inzicht in het overzicht van de relevante bedrijfsmiddelen (databestanden, programmatuur, apparatuur, diensten).
- De toegepaste methode voor risicoclassificatie zal bij de periodieke evaluatie en eventuele bijstelling van het informatiebeveiligingsbeleid (eens per drie jaar) worden geëvalueerd.

Verantwoordelijkheden van de leiding

- Locatiemanagers, ICT-adviseur, P&O-adviseur en overige leidinggevenden binnen de organisatie zullen door de kwaliteitsfunctionaris worden ingelicht over: het informatiebeveiligingsbeleid, de hierbij behorende richtlijnen en gedragscodes en specifieke maatregelen of procedures die gelden voor informatiesystemen. De leidinggevende is vervolgens verantwoordelijk voor het kenbaar maken en uitdragen van deze informatie aan de (interne en externe) medewerkers.
- Het actualiseren en tijdig kenbaar maken van beveiligingsmaatregelen, richtlijnen, gedragscodes en procedures is een verantwoordelijkheid van de kwaliteitsfunctionaris. Voor de leidinggevenden moet duidelijk zijn waar de laatste versies van deze documenten zijn terug te vinden. Bij publicatie van deze documenten dient rekening gehouden te worden met de vertrouwelijkheid van bepaalde beveiligingsinformatie.

Beleid ten aanzien van toegangsbeveiliging

- De kwaliteitsfunctionaris is in hoofdlijnen verantwoordelijk voor de inrichting van en controle op toegangsbeveiliging van de systemen die de organisatie gebruikt. Uitvoering hiervan is gedelegeerd aan de ICT-adviseur in samenwerking met de locatiemanagers.

Controle op toegangsrechten

- Binnen de organisatie is sprake van twee systemen waar toegangsrechten aan kunnen worden toegekend, te weten:
  - Toekennen van toegangsrechten met betrekking tot het patiëntregistratiesysteem is de verantwoordelijkheid van de locatiemanager.
  - Toekennen van toegangsrechten met betrekking tot de archivering is de verantwoordelijkheid voor de directeur, die hierbij wordt ondersteund door de P&O-adviseur. Hiervoor wordt een formulier gebruikt t.a.v. het

toekennen van rechten tot de verschillende hoofdstukken van de archivering. Controle op de toegekende toegangsrechten vindt eenmaal per jaar steekproefsgewijs plaatst door de kwaliteitsfunctionaris.

Controle op naleving van technische normen

- Er dient een jaarlijkse controle plaats te vinden op naleving van de technische beveiligingsnormen binnen operationele systemen en netwerken. Dit is in de contracten met de leveranciers aangepast en geborgd.
- De controles worden uitgevoerd door de kwaliteitsfunctionaris i.s.m. een inhoudelijk deskundige.

Het rapporteren van beveiligingsincidenten en zwakke plekken in programmatuur

- Ieder beveiligingsincident in programmatuur wordt gemeld bij de locatiemanager. Die neemt dit op met de systeemeigenaar.
- De systeemeigenaar heeft regulier overleg met de systeemleverancier om meldingen te rapporteren.
- De systeemeigenaar brengt rapportage uit aan de kwaliteitsfunctionaris, waarbij acties bepaald worden.
- Incidenten worden besproken in het MT-overleg, waar ook de acties gekoppeld worden aan verantwoordelijken voor afhandeling. Ook dient terugkoppeling naar de melder verzorgd te worden.
- De kwaliteitsfunctionaris verzamelt gegevens over beveiligingsincidenten zodat de aard, omvang en de kosten van incidenten en storingen worden gekwantificeerd en bewaakt. Deze informatie wordt gebruikt om terugkerende of zeer ingrijpende incidenten of storingen vast te stellen.

4.3.2 Locatiemanagers

Organisatie

- Iedere locatiemanager is zelf verantwoordelijk voor een adequate beveiliging van de informatie binnen haar locatie. Hiertoe dient zij de maatregelen zoals die beschreven zijn in het informatiebeveiligingsbeleid te implementeren en te controleren op naleving.
- Jaarlijkse controle op naleving van beleid (steekproeven, controle).
- Goedkeuring nieuwe ICT-middelen/wijzigingen (indien verantwoordelijk hiervoor; gebruik acceptatieprocedure, i.s.m. ICT-adviseur).

Personeel (i.s.m. P&O)

- Uitvoeren beleid bij nieuw personeel (onderdeel inwerktraject).
- Werkwijze bij uitdiensttreding; men blijft verplicht tot geheimhouding.
- Jaarlijkse controle middels steekproef op toegangsrechten en laten vervallen van rechten van ex-medewerkers.

Fysieke en omgevingsbeveiliging

- Calamiteitenplan opstellen en implementeren, inclusief regelmatig testen van de procedure (1x per jaar).
- Clear desk/clear screen policy: opstellen van beleid en regelmatig controle hierop.
- Controle door locatiemanagers op gedrag op de werkvloer.

4.3.3 ICT-adviseur

Overzicht van de middelen

- Actueel houden van overzicht van de relevante bedrijfsmiddelen (databestanden, programmatuur, apparatuur, diensten).

Volgen en bewaken contracten met derden

- De ICT-adviseur dient de contracten aan te passen in samenspraak met locatiemanagers (indien voor hen van toepassing). Ook moet hij ervoor zorgen dat de CHN in staat gesteld wordt de maatregelen te controleren.
- Deze controles zullen periodiek moeten worden uitgevoerd, middels leveranciersbeoordelingen.

Beleid ten aanzien van toegangsbeveiliging

- De kwaliteitsfunctionaris is in hoofdlijnen verantwoordelijk voor de inrichting van en controle op toegangsbeveiliging van de systemen die de CHN gebruikt. Uitvoering hiervan is gedelegeerd aan ICT-adviseur in samenwerking met de locatiemanagers.

4.3.4 Systeemeigenaren

Middelen

- Gegevens aanleveren voor middelenmatrix.

Beheer ICT-voorzieningen/aanschaf en onderhoud ICT-systemen/Toegangsbeveiliging

- Overzicht over contracten met betreffende leverancier; inclusief service level agreements.
- Uitvoeren van leveranciersbeoordeling, inclusief voorstellen tot wijziging van contracten.
- Toezien op vertrouwelijke verwerking van gegevens door leveranciers (middels contracten en toezicht op gedrag).
- Wijzigings- en acceptatieprocedure voor werkplekken opstellen per locatie (met behulp van ICT-adviseur)
- Goedkeuring nieuwe ICT-middelen/wijzigingen.
- Bij nieuwe versies nagaan en beoordelen of aanvullende training voor medewerkers op het gebied van informatiebeveiliging nodig is.
- In de wijzigingsprocedure zijn duidelijke richtlijnen opgenomen voor een formele goedkeuringsprocedure voor voorgestelde wijzigingen en communicatie over de wijzigingen aan alle betrokkenen. De applicatiebeheerder zorgt voor communicatie van wijzigingen op de werkvloer. Hiervoor stelt hij een procedure op.
- De autorisatie (functiescheiding) goed vastleggen (zie Protocol mandatering); autorisatietabel met regels vastleggen.

Bijlage

Periodieke taken per rol uitgezet in de tijd; daarnaast geldt voor alle functies een doorlopende aandacht voor informatiebeveiliging in allerlei opzichten. Onderstaand overzicht is gericht op activiteiten die periodiek terugkomen en opgenomen moeten worden in een jaarplanning.

Kwaliteitsfunctionaris		
	Uitvoeren globale risicoanalyse	1x per jaar
	Evalueren van beleid, desgewenst actualiseren	1x per 3 jaar
	Toetsen of overzicht bedrijfsmiddelen nog actueel is	1x per jaar
	Methode voor risicoclassificatie evalueren	1x per 3 jaar
	Informatiebeveiligingsbeleid evalueren	1x per 3 jaar
	Controle op uitvoering controles door locatiemanagers (bijv. toegangsrechten, uitvoeren leveranciersbeoordeling)	1x per jaar

Locatiemanagers		
	Controle op uitvoering beleid	1x per jaar
	Controle op toegangsrechten en het vervallen van rechten van uitdienst medewerkers	1x per jaar
	Toetsen, testen en evalueren van calamiteitenplan	1x per jaar

Systeemeigenaar		
	Bijdrage aan leveranciersbeoordeling	1 à 2 x per jaar of vaker indien nodig

ICT-adviseur		
	Volgen/bewaken contracten	1 à 2 x per jaar of vaker indien nodig