Bijlage 13

Personeelsbeleid in kader van informatiebeveiliging

1. Inleiding

Doel van dit document is het verzamelen van alle aspecten die relevant zijn in het kader van personeelsbeleid en NEN 7510, en deze op gestructureerde wijze presenteren. NEN 7510 betreft het brede terrein van informatiebeveiliging, volgens wettelijke normen. Het gaat hier om het beschermen van de privacy van de patiënt in alle aspecten, maar ook die van de medewerkers.

Mensen maken fouten, bewust of onbewust. Daardoor kan de goede afloop van informatieprocessen negatief worden beïnvloed. Om de kans op bewuste fouten te verkleinen wordt de betrouwbaarheid van personeel bij aanname al getoetst, worden bepalingen in de arbeidscontracten opgenomen en wordt het vertrek van personeel zorgvuldig begeleid. Om medewerkers te helpen onbewuste fouten zoveel mogelijk te voorkomen, of de schade die hieruit volgt te beperken, worden zij getraind in de beveiligingsmaatregelen en is een duidelijke procedure nodig om beveiligingsincidenten te kunnen melden.

Dit document sluit aan op het informatiebeveiligingsbeleid. Bij de voorbereidingen voor de certificering in 2009 zijn de eisen in het beleid opnieuw besproken en zijn keuzes gemaakt voor de wijze waarop binnen de CIHN een en ander georganiseerd is (hoofdstuk 2). In hoofdstuk 3 zal beschreven worden hoe we dit momenteel vormgeven, of op korte termijn willen gaan uitvoeren.

2. Beveiligingseisen ten aanzien van personeel

2.1 Functies en verantwoordelijkheden

- Bij iedere functie binnen de CIHN moet worden vastgesteld of het noodzakelijk is – naast de reguliere richtlijnen en gedragscodes – een specifieke beschrijving van de bijbehorende taken ten aanzien van informatiebeveiliging op te nemen. In de toekomst zullen deze aanvullende beveiligingstaken opgenomen worden in de functieomschrijving. Gekozen is dit te uit te voeren bij iedere functieherziening waarbij de functiebeschrijving moet worden aangepast. Voor bestaande functies wordt volstaan met het opstellen van een nieuwe gedragscode ten aanzien van vertrouwelijke informatie en het vastleggen van de toegang die de medewerkers nu uit hoofde van hun functie hebben tot gevoelige informatie.
- De leidinggevenden hebben de verantwoordelijkheid om de werkzaamheden van individuele personeelsleden op het vlak van informatiebeveiliging periodiek te beoordelen. Dit zal plaatsvinden tijdens het functionerings- of het praktijkgesprek.
- Bij nieuw of onervaren personeel dient de leidinggevende na te gaan of extra toezicht op het naleven van de beveiligingsmaatregelen noodzakelijk is.

2.2 Screening bij het aannemen van personeel

- Van iedereen die bij de instelling komt werken, wordt instemming met de geldende gedragscodes gevraagd en bekendheid met de beveiligingsrichtlijnen verondersteld. Het arbeidsvoorwaardenreglement maakt deel uit van het arbeidscontract. De gedragscodes zullen deel gaan uitmaken van het arbeidsvoorwaardenreglement en zitten in de inwerkmap.
- Bij de aanname van personeel wordt de betrouwbaarheid van de persoon in kwestie en zijn of haar geschiktheid voor de functie getoetst. Dit proces wordt in beveiligingstermen screening genoemd. De screening zal minimaal de volgende punten omvatten:
  - Controle van het curriculum vitae van de sollicitant.
  - Bevestiging van beweerde professionele kwalificaties, middels opvragen van diploma's; deze worden in het personeelsdossier bewaard.
  - Onafhankelijke identiteitscontrole (paspoort).
- Voor werknemers die binnen de instelling een bijzondere functie gaan vervullen ten aanzien van toegang tot gevoelige systemen, kan een antecedentenonderzoek of integriteitonderzoek onderdeel uitmaken van de selectieprocedure. Dit onderzoek kan onder andere bestaan uit navraag bij referenten, een verklaring van goed gedrag, et cetera.
- Informatiebeveiliging moet voor personeel en tijdelijke externe medewerkers:
  - bij het aannemen worden besproken.
  - in de functieomschrijvingen en contracten worden geregistreerd.
  - tijdens het dienstverband op naleving worden gecontroleerd.
  - in het personeelsbeleid worden gewaarborgd.

2.3 Arbeidscontract

- In het arbeidscontract van werknemers en in de overeenkomst met externen dienen de verantwoordelijkheden op het gebied van informatiebeveiliging te zijn vastgelegd. Het gaat hierbij om:
  - geheimhoudingsverklaring;
  - zwijgplicht;
  - eventuele sancties.
- In contracten met externe bedrijven wordt een clausule opgenomen waarin geheimhoudingsplicht wordt benoemd en afspraken hierover worden gemaakt.

2.4 Zwijgplicht en geheimhoudingsplicht

- Medewerkers dienen een geheimhoudingsverklaring te tekenen; dit is een artikel in de arbeidsovereenkomst. Deze geheimhoudingsverklaring is voorzien van een boetebeding en daarmee uitgebreider dan de standaard geheimhoudingsplicht zoals opgenomen in de CAO.
- Voor externen dient een geheimhoudingsverklaring in het contract te zijn opgenomen.
- Externe bezoekers dienen een geheimhoudingsverklaring te tekenen op het moment dat zij de HAP in ANW-tijd bezoeken (bijvoorbeeld op de belcentrale).
- De geheimhoudingsverklaring wordt actueel gehouden door de P&O-adviseur en is in lijn met het informatiebeveiligingsbeleid.

2.5 Taakuitvoering

2.5.1 Verantwoordelijkheden van de leiding

- Leidinggevenden binnen de CIHN 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 medewerkers.
- Het actualiseren en tijdig kenbaar maken van beveiligingsmaatregelen, richtlijnen, gedragscodes en procedures is een verantwoordelijkheid van de kwaliteitsfunctionaris. Voor de leidinggevende 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.

2.5.2 Bewustwording, opleiding en training voor informatiebeveiliging

- In introductieprogramma's van nieuw personeel wordt informatiebeveiliging als vast onderdeel meegenomen.
- Bij opleidingen in het gebruik van informatiesystemen dient expliciet aandacht te worden besteed aan de beveiligingsmaatregelen die specifiek bij het informatiesysteem horen. Indien deze opleidingen door derden worden gegeven, dan moeten informatiebeveiliging en de eigen procedures onderdeel zijn van het opleidingsprogramma. De functioneel beheerder ziet toe op naleving van deze afspraak bij opleidingen.
- Bij nieuwe versies van programmatuur of apparatuur dient de functioneel beheerder te beoordelen of aanvullende training op het gebied van informatiebeveiliging aan de medewerkers noodzakelijk is.
- Regelmatig worden activiteiten uitgevoerd die het beveiligingsbewustzijn bevorderen en op peil houden. In de jaarplannen wordt daar aandacht aan besteed.
- Bekendheid met gedragsregels (omgaan met papier, wachtwoorden, USB-sticks, gebruik internet voor andere doeleinden en dergelijke)
- Controleren op naleving van de regels en controle op het gedrag van de doktersassistenten in de medische dossiers (logging).

2.5.3 Disciplinaire maatregelen

- In het geval van bewust doorbreken van beveiligingsmaatregelen door een interne of externe medewerker wordt melding gemaakt aan de direct leidinggevende. Op basis van de ernst van de beveiligingsovertreding wordt bepaald welke disciplinaire maatregel wordt gehanteerd. Deze maatregelen variëren van een waarschuwing tot onmiddellijk ontslag en eventuele juridische stappen.

2.6 Einde en wijziging van de aanstelling

- Bij uitdiensttreding of functiewijziging van een medewerker zal door de leidinggevende worden nagegaan of de rechten van toegang tot gebouw, apparatuur en informatie op de juiste wijze zijn ingetrokken of gewijzigd.
- De vertrekkende medewerker zal bij uitdiensttreding worden gewezen op eventuele resterende verplichtingen op het gebied van informatiebeveiliging, zoals een blijvende verplichting tot geheimhouding.

3. Vormgeven van de beveiligingseisen bij de CIHN

In dit hoofdstuk wordt aangegeven in welke mate bovenstaande eisen (hoofdstuk 2) en maatregelen binnen de CIHN zijn vormgegeven, en welke maatregelen op termijn nog zullen worden genomen.

3.1 Algemeen

Bij het aannemen van personeel wordt gekeken naar de gebleken geschiktheid van de kandidaat. Cv en diploma's worden gecontroleerd; de diploma wordt bij het personeelsdossier gevoegd.

Medewerkers op kantoor krijgen een tijdelijke arbeidsovereenkomst met bijbehorende proeftijd; deze wordt na de proefperiode omgezet in een vast dienstverband mits er geen contra-indicaties zijn. Ieder jaar vindt minimaal éé functioneringsgesprek plaats met de direct leidinggevende.

Medewerkers in de ANW-dienst doorlopen een inwerktraject van minimaal zeven bijeenkomsten en scholing. Tijdens dit inwerktraject worden alle regels (zowel medisch-inhoudelijk als organisatorisch) uitgelegd.

Onderstaand worden de belangrijkste onderdelen besproken: de arbeidsovereenkomst, de functiebeschrijvingen, de inwerkmap en de functioneringsgesprekken (voor DA ook wel praktijkgesprekken genoemd).

3.1.1 De arbeidsovereenkomst

- De arbeidsovereenkomst bevat een geheimhoudingsverklaring met boetebeding.
- Eisen ten aanzien van informatiebeveiliging zijn nog niet in de functiebeschrijving opgenomen. Wel zijn de systemen met gevoelige informatie beschreven en zijn de rollen en taken voor wat betreft informatiebeveiliging vastgelegd. De diverse functies worden beschreven, inclusief de gevoelige informatie waartoe men toegang heeft.
- Het arbeidsvoorwaardenregelement maakt deel uit van het arbeidscontract. Hierin zullen in de toekomst extra eisen ten aanzien van beveiliging worden opgenomen.

3.1.2 Functieomschrijvingen

- Voor alle functies moet gekeken worden of voldoende beschreven staat wat de rechten en plichten zijn van de medewerker ten aanzien van informatiebeveiliging. In 'Taakomschrijving rollen NEN 7510 informatiebeveiliging' (bijlage 11) staan de diverse functies beschreven, inclusief de systemen en gevoelige informatie waartoe men toegang toe heeft uit hoofde van de functie.
- In de toekomst zullen functiebeschrijvingen van functies die worden herzien ook meteen aangepast worden aan de eisen. Tot die tijd volstaan wij met een extra artikel voor het arbeidsvoorwaardenreglement en met het vastleggen van de diverse rollen en het daarmee vastleggen tot welke informatie eenieder gelegitimeerd toegang heeft.

3.1.3 De inwerkmap voor doktersassistenten

In de inwerkmap zijn nu regels opgenomen voor het internetgebruik. Hieraan is een instructie toegevoegd met betrekking tot het omgaan met privacygevoelige informatie, werken met UZI-passen, omgaan met papieren gegevens, het gebruik van wachtwoorden

en het gebruik van USB-sticks en dergelijke. Deze regels worden ook mondeling door de leidinggevende toegelicht in het inwerktraject.

3.1.4 Functioneringsgesprekken/praktijkgesprekken

De direct leidinggevende houdt jaarlijks functioneringsgesprekken met de kantoormedewerkers. Bij alle doktersassistenten worden praktijkgesprekken gevoerd, minimaal één keer per jaar. Voor nieuwe doktersassistenten zijn afwijkende afspraken gemaakt.
Een vast onderdeel van deze functioneringsgesprekken is het omgaan met privacygevoelige informatie en informatiebeveiliging. Dit item is toegevoegd aan het format formulier 'functioneringsgesprekken'. Bij nieuw en onervaren personeel is van groot belang hier extra op toe te zien, in ieder geval ter bewustwording.

Voor kantoorpersoneel en bijvoorbeeld baliemedewerkers is nog niet beschreven hoe vaak en wanneer gesprekken plaatsvinden (bijvoorbeelde aan het einde van de proefperiode, of na zes maanden). Dit zal in het personeelsbeleid van 2010 worden opgenomen.

3.1.5 Derden

Externe bezoekers dienen een geheimhoudingsverklaring te tekenen wanneer zij bij hun bezoek zicht hebben op privacygevoelige informatie (bijvoorbeeld in ANW-uren op de belcentrale). Hierop wordt toegezien door de CODA's.
In contracten met externe bedrijven is een clausule opgenomen waarin geheimhoudingsplicht wordt benoemd en afspraken hierover worden gemaakt. Dit is gebeurd voor alle contracten met ICT-leveranciers en met Protopics.

3.2 Screening bij het aannemen van personeel

Dit wordt uitgevoerd als beschreven in paragraaf 2.2.

3.3 Taakuitvoering

3.3.1 Verantwoordelijkheden van de leiding

- De kwaliteitsfunctionaris licht de leidinggevenden binnen de CIHN in over het informatiebeveiligingsbeleid, de hierbij behorende richtlijnen en gedragscodes en specifieke maatregelen of procedures die gelden voor informatiesystemen. Dit gebeurt in speciale werkoverleggen of tijdens MT-vergaderingen.
- De leidinggevende is vervolgens verantwoordelijk voor het kenbaar maken en uitdragen van deze informatie aan de (interne en externe) medewerkers. Zij gebruiken hiervoor de reguliere werkoverlegmomenten en zetten informatiebeveiliging als vast punt op de agenda.
- De kwaliteitsfunctionaris zorgt voor het documentbeheer.

3.3.2 Bewustwording, opleiding en training voor informatiebeveiliging, controle tijdens werkzaamheden

- In introductieprogramma's van nieuw personeel wordt informatiebeveiliging als vast onderdeel meegenomen (zie inwerkprocedure/inwerkmap).
- Bij opleidingen in het gebruik van informatiesystemen of bij nieuwe functionaliteiten dient expliciet aandacht te worden besteed aan de beveiligingsmaatregelen die bij het informatiesysteem horen (bijvoorbeeld introductie UZI-pas). Indien derden deze opleidingen geven (bijvoorbeeld

Protopics), dan moeten informatiebeveiliging en de eigen procedures onderdeel te zijn van het opleidingsprogramma. De ICT-adviseur ziet toe op naleving van deze afspraak bij opleidingen.

- Middels een acceptatieprocedure voor nieuwe versies van programmatuur of apparatuur, zal als vast onderwerp worden opgenomen dat de ICT-adviseur dient te beoordelen of aanvullende training op het gebied van informatiebeveiliging aan de medewerkers noodzakelijk is.
- Regelmatig worden activiteiten uitgevoerd die het beveiligingsbewustzijn bevorderen en op peil houden. In de jaarplannen en werkoverleggen wordt daar aandacht aan besteed. Eén maal per jaar zal een externe spreker tijdens het werkoverleg extra aandacht geven aan dit onderwerp (denk dan aan de kwaliteitsfunctionaris of ICT-adviseur).
- Controle op de naleving door de medewerkers wordt gewaarborgd, onder andere door structurele logging van inloggegevens. Minimaal één maal per jaar (voorafgaand aan de praktijkgesprekken) zal een steekproef voor alle doktersassistenten/baliemedewerkers worden gehouden, om naleving van de gedragsregels ten aanzien van logging te beoordelen. Hierbij wordt onder andere gekeken naar het ongeautoriseerd inzien van contacten (‘afgebroken contacten’).

3.3.3. Disciplinaire maatregelen

Deze worden uitgevoerd als beschreven in paragraaf 2.5.3.

3.4 Einde en wijziging van de aanstelling

Bij uitdiensttreding of functiewijziging van een medewerker zal door de leidinggevende worden nagegaan of de rechten van toegang tot gebouw, apparatuur en informatie op de juiste wijze zijn ingetrokken of gewijzigd.
De vertrekkende medewerker zal bij uitdiensttreding worden gewezen op eventuele resterende verplichtingen op het gebied van informatiebeveiliging, zoals een blijvende verplichting tot geheimhouding.
Een checklist ‘personeel uit dienst’ helpt bij het controleren van deze punten.

3.5 Melden van beveiligingsincidenten

Om lering te kunnen trekken uit incidenten, is het van het grootste belang dat deze ook gemeld worden aan de coördinerend doktersassistente of locatiemanager. Zoals gezegd gebeuren sommige fouten onbewust, of is men zich niet bewust van mogelijke gevolgen of risico’s.
Door een beveiligingsincident te melden en vervolgens te analyseren, is te beoordelen of procedures aangepast moeten worden, of scholing verbeterd moet worden. Of misschien dat er technische oplossingen bedacht kunnen worden om dergelijke situaties te voorkomen.