Kraamzorg Mama

Informatiebeveiliging in de zorg

Naam:	Imran Chaudhry
Studentnummer:	08057001
Opleiding:	Bedrijfseconomie
Klas:	BE 4C
Plaats:	Den Haag
Onderwijsinstelling:	De Haagse Hogeschool
Datum:	1 juli 2014
Stage bedrijf:	Kraamzorg Mama
Bedrijfsmentor:	Nasser Rashidi
Adres:	Zinkwerf 12C
Postcode en plaats:	2544 EE Den Haag
Docentbegeleider:	C. van Eck
Vrijgegeven voor publicatie door:	Nasser Rashidi
Handtekening:	

Samenvatting

Aanleiding

Kraamzorg Mama is een kraamzorgbureau dat al jaren goed staat aangeschreven bij cliënten, verloskundigen en alle zorgverzekeraars. Kraamzorg Mama levert haar diensten in Zuid-Holland en Midden Nederland. Kraamzorg Mama heeft in haar dagelijkse processen te maken met verschillende normen die opgesteld zijn door de overheid.

Kraamzorg Mama wil gebruik gaan maken van een applicatie om het hele proces vanaf de inschrijving van een cliënt tot aan de declaratie te beheren. De processen die gerelateerd zijn aan het gebruik van deze applicatie moeten voldoen aan de wettelijke normen en richtlijnen voor informatiebeveiliging in de zorg. Naast het gebruik van de applicatie en informatiesystemen is ook de verwerking van informatie op niet digitale wijze onderhevig aan wettelijke normen en richtlijnen. Op dit moment is het nog niet inzichtelijk in hoeverre Kraamzorg Mama voldoet aan deze normen.

De hoofdvraag waarop in dit rapport antwoord wordt gegeven luidt als volgt:

Wat zijn de belangrijkste risico's van de informatiebeveiliging binnen Kraamzorg Mama en op welke wijze kan Kraamzorg Mama deze risico's afdekken?

Uitvoering

De huidige situatie van de informatiebeveiliging is in kaart gebracht door de primaire processen van Kraamzorg Mama te beschrijven en het houden van een interview met de IT manager. Aan de hand van de uitkomsten en bevindingen zijn de risico's bepaald. Bij het bepalen van de risico's is de bescherming van persoonsgegevens leidend. Aan de hand van de risico's zijn de maatregelen bepaald per beveiligingscategorie. Deze categorieën zijn afgeleid uit de Code voor Informatiebeveiliging. Voor het bepalen van de status van de beveiligingen en de mogelijke maatregelen is de NEN 7510 gebruikt als richtlijn. De risico's zijn bepaald aan de hand van een QuickScan en beoordeeld aan de hand van de stoplichtmethode.

De belangrijkste risico's liggen in de volgende categorieën:

- Beveiligingsbeleid
- Organisatie van de beveiliging
- Personeel
- Toezicht

De resultaten van de risicoanalyse tonen aan dat de categorieën die hierboven zijn beschreven te maken hebben met beleid en structuur. Dit betekent dat een groot deel van de risico's afgedekt kan worden door het invoeren van een informatiebeveiligingsbeleid en het effectief uitvoeren van dit beleid. Het controleren van het beleid moet een continu proces zijn en geaccepteerd en uitgedragen worden door de gehele organisatie.

De controle op naleving van het beleid moet geschieden volgens de PDCA-cyclus. In een optimale situatie zou de controle zowel intern als extern worden uitgevoerd. Dit betekent dat onafhankelijke specialisten op het gebied van audit en informatiebeveiliging toetsen of het beleid wel voldoet aan de gestelde eisen.

Conclusies

- De primaire processen en de technische beveiliging van Kraamzorg Mama zijn goed ingericht. Het management investeert veel tijd en middelen in het verbeteren van deze aspecten.
- De organisatie heeft geen beleid geformuleerd met betrekking tot de informatiebeveiliging en het beschermen van persoonsgegevens. De focus van het management ligt sterk op de technische beveiliging.
- De IT manager is verantwoordelijk voor de informatiebeveiliging en bezit geen expertise op het gebied van ontwikkelen van beleid en het uitdragen van dit beleid naar de medewerkers van de organisatie toe.
- Voor het aannemen en ontslaan van personeel zijn geen speciale maatregelen genomen om preventief de bescherming van persoonsgegevens en andere gevoelige informatie te realiseren.
- Er vinden binnen de organisatie geen externe controles plaats door onafhankelijke specialisten.

Aanbevelingen

- Het management van Kraamzorg Mama moet investeren in de organisatorische zijde van de informatiebeveiliging. Dit kan men doen door beleid te formuleren en dit beleid actief uit te dragen naar alle medewerkers van de organisatie toe. De informatiebeveiliging moet een bredere implicatie krijgen dan alleen de technische zijde van de beveiliging.
- De verantwoordelijkheden voor het beleid moeten gedragen worden door managers en medewerkers gezamenlijk. Dit kan men realiseren door verantwoordelijkheden te geven aan medewerkers en hen bewust te maken van het belang van goede bescherming van gevoelige informatie.
- Kraamzorg Mama moet bij het aantrekken van nieuw personeel controles doorvoeren om potentiële medewerkers te controleren op hun betrouwbaarheid met de omgang van persoonsgegevens en andere gevoelige informatie. Hiernaast moet de organisatie regelmatig trainingen en cursussen aanbieden aan de medewerkers om het kennisniveau en de bewustwording te verhogen.
- De organisatie dient naast het interne beleid en het controle protocol een externe IT auditor in te schakelen om een onafhankelijk beoordeling te geven van het beleid en de uitvoering hiervan. De controles van de uitvoering van het beleid moeten structureel zijn en volgens de PDCA-cyclus uitgevoerd worden.

Inhoudsopgave

1. Inleiding

Dit afstudeeronderzoek is tot stand gekomen op basis van mijn afstudeeropdracht bij Kraamzorg Mama. De afstudeeropdracht is een verplicht onderdeel van de hoofdfase van de opleiding Bedrijfseconomie. De duur van de opdracht bedraagt zeventien weken.

Tijdens mijn opdracht zal ik onderzoeken wat de status is van de informatiebeveiliging bij Kraamzorg Mama. Hierbij wordt gekeken naar de bescherming van persoonsgegevens met behulp van normen en richtlijnen voor informatieveiligheid.

Het verslag zal beginnen met een introductie van de organisatie. Dit geeft een beeld van de organisatie en de wijze waarop de leiding wordt gevoerd. Hiernaast is een korte beschrijving gegeven van de verschillende afdelingen.

Vervolgens wordt de aanleiding en structuur van de opdracht toegelicht. Daaropvolgend wordt het theoretisch kader behandeld welke de basis is voor het beantwoorden van de deelvragen.

Aansluitend hierop worden de deelvragen van het onderzoek uitgewerkt en beantwoord.

Tenslotte kunt u in het laatste gedeelte de conclusies en aanbevelingen lezen die zijn gebaseerd op de resultaten uit de deelvragen.

2. Organisatie

Organisatieomschrijving

Kraamzorg Mama is een kraamzorgbureau dat al jaren goed staat aangeschreven bij cliënten, verloskundigen en alle zorgverzekeraars. Kraamzorg Mama werkt met mensen die de kraamzorg en de kraamvrouw begrijpen (ervaren kraamverzorgsters). Kraamzorg Mama levert haar diensten in Zuid-Holland en Midden Nederland. Kraamzorg Mama levert kwalitatieve zorg en blijft streven naar zorgverbeteringen. Naast de gekwalificeerde kraamverzorgende wordt er intern gewaakt over de kwaliteit van de zorg door de zorgcoördinatoren en de kwaliteitsmanager.

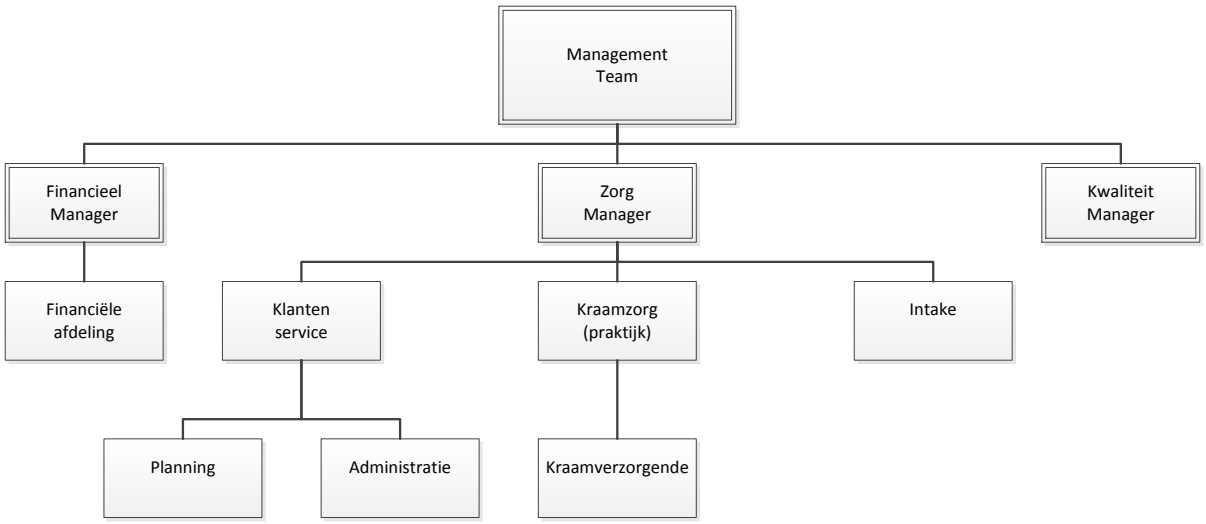
Kraamzorg Mama bestaat uit drie hoofdafdelingen, namelijk de afdelingen Financiën, Zorg en Kwaliteit. De afdelingen ondersteunen gezamenlijk het doel van Kraamzorg Mama namelijk het leveren van kwalitatieve kraamzorg.

Missie

De missie van Kraamzorg Mama is het organiseren van geboortezorg waarbij ieder gezin volledig met zelfvertrouwen, gezondheid en geluk kan wennen aan de nieuwe gezinssituatie.

Organisatiestructuur

Hieronder is een organogram opgenomen van de organisatiestructuur binnen Kraamzorg Mama.



Figuur 1 organogram

Om een goed beeld te krijgen van de organisatie zijn hieronder de hoofdafdelingen kort toegelicht.

Financiën

De afdeling Financiën is verantwoordelijk voor het declareren van de kosten van de zorg bij de zorgverzekeraar. Hiernaast houdt de afdeling een registratie van de gewerkte uren van de medewerkers bij in de Zorgapplicatie. Deze uren worden gecontroleerd alvorens ze worden

gedeclareerd. De declaratie wordt verstuurd via het verzekeringsportaal Vecozo. Tevens stelt de financiële afdeling een factuur op voor de cliënt in verband met de wettelijke eigen bijdrage.

Zorg

De afdeling Zorg is verantwoordelijk voor het afnemen van indicaties aan de hand van het Landelijk Indicatie Protocol. Hiernaast is de afdeling verantwoordelijk voor de intake van cliënten. Deze indicatie en intakes worden geregistreerd in de Zorgapplicatie. De afdeling is ook verantwoordelijk voor de overige processen die gerelateerd zijn aan het leveren van zorg zoals het inroosteren van medewerkers.

Kwaliteit

De afdeling Kwaliteit heeft een controlerende en toezichthoudende rol binnen de organisatie. De afdeling is verantwoordelijk voor het afhandelen van klachten en het afnemen van klanttevredenheidsonderzoeken. Aan de hand van eventuele klachten en resultaten van de onderzoeken kan de afdeling verbeterpunten signaleren en maatregelen doorvoeren. Hierom monitort de afdeling Kwaliteit in hoofdlijnen de belangrijkste processen van de organisatie.

3. Afstudeeropdracht

Aanleiding

Kraamzorg Mama heeft in haar dagelijkse processen te maken met verschillende normen die opgesteld zijn door de overheid. Tegenwoordig wordt steeds meer informatie van en over patiënten digitaal bewaard in verschillende systemen. Deze verschillende informatiesystemen worden weer gekoppeld aan andere informatiesystemen. Een toename van cybercrime incidenten en maatschappelijke bewustwording rondom privacy kwesties heeft gezorgd voor een toegenomen bewustwording van de risico's.

Kraamzorg Mama wil gebruik gaan maken van een applicatie om het hele proces vanaf de inschrijving van een cliënt tot aan de declaratie te beheren. De processen die gerelateerd zijn aan het gebruik van deze applicatie moeten voldoen aan de wettelijke normen en richtlijnen voor informatiebeveiliging in de zorg. Naast het gebruik van de applicatie en informatiesystemen is ook de verwerking van informatie op niet digitale wijze onderhevig aan wettelijke normen en richtlijnen. Op dit moment is het nog niet inzichtelijk in hoeverre Kraamzorg Mama voldoet aan deze normen.

Probleemanalyse

De hoofdvraag waarop in dit rapport antwoord wordt gegeven luidt als volgt:

Wat zijn de belangrijkste risico's van de informatiebeveiliging binnen Kraamzorg Mama en op welke wijze kan Kraamzorg Mama deze risico's afdekken?

Om een antwoord te kunnen geven op de bovengenoemde hoofdvraag, moeten er eerst een aantal deelvragen beantwoord worden. De deelvragen luiden als volgt:

1. Hoe zien de huidige processen er binnen de organisatie uit?
2. Wat is de huidige situatie van de informatiebeveiliging?
3. Wat zijn de belangrijkste risico's voor de informatiebeveiliging?
4. Wat zijn de mogelijke maatregelen voor de risico's?
5. Op welke wijze kan naleving van de maatregelen worden gecontroleerd?
6. Hoe kan Kraamzorg Mama nieuwe ontwikkelingen op het gebied van informatiebeveiliging monitoren?

Het doel van de opdracht is het inzichtelijk maken van de naleving van de wettelijke normen voor informatiebeveiliging in de zorg, waarbij de belangrijkste risico's in kaart gebracht worden met maatregelen om risico's af te dekken.

Om tot een onderbouwd antwoord op de hoofdvraag te komen zal er voor de eerste deelvraag inzichtelijk gemaakt worden wat de belangrijkste primaire processen zijn en wat de relatie van deze processen is met het onderwerp informatiebeveiliging. Dit zal gebeuren aan de hand van bestaande werkbeschrijvingen van Kraamzorg Mama.

De tweede deelvraag zal beantwoord worden aan de hand van een afgenomen interview met de IT Manager. Op basis van de bevindingen van de reeds beantwoorde deelvragen worden

de risico's voor deelvraag drie bepaald en toegelicht. Vervolgens wordt de ernst van deze risico's bepaald aan de hand van de stoplichtmethode. Voor de vierde deelvraag worden de maatregelen voor de belangrijkste risico's bepaald aan de hand van richtlijnen van de NEN 7510 en de Code voor Informatiebeveiliging. Op de vijfde en zesde deelvragen wordt antwoord gegeven op basis van de PDCA-cyclus en bestaande methodieken uit de literatuur.

4. Theoretisch kader

In dit hoofdstuk zijn de basisbegrippen en definities gegeven met betrekking tot het onderwerp informatiebeveiliging om een duidelijk beeld te krijgen over het onderwerp. Door deze definities en begrippen te bepalen kan vanuit een gedefinieerde basis gekeken worden naar de informatiebeveiliging binnen Kraamzorg Mama.

Informatiebeveiliging

Informatiebeveiliging en privacybescherming zijn twee begrippen die nauw met elkaar verweven zijn. Door de vele overlappingen tussen de twee termen is het vanuit praktisch oogpunt gewenst om de bescherming van persoonsgegevens te zien als een onderdeel van de informatiebeveiliging.

In de NEN 7510 bundel wordt informatie als volgt beschreven:

> Informatie kan in veel verschillende vormen voorkomen. De informatie kan onder meer zijn afgedrukt of geschreven op papier, elektronisch zijn opgeslagen, per post of via elektronische media worden verzonden, op film worden getoond of mondeling worden uitgewisseld. Informatie behoort altijd op geschikte wijze te worden beschermd, rekening houdend met de vorm of de wijze waarop deze wordt gedeeld of opgeslagen (p. 6).

Het begrip goede informatiebeveiliging staat niet gelijk aan veel beveiligingsmaatregelen, een strikte naleving van wet- en regelgeving en opgestelde normen. Als er sprake is van een onderlinge samenhang van de verschillende maatregelen, waarbij maatregelen zijn gestandaardiseerd, dan kan men spreken over goede informatiebeveiliging.

Van der Wel (2006) beschrijft informatiebeveiliging als volgt: “Informatiebeveiliging houdt zich bezig met de eisen die de organisatie stelt aan de beschikbaarheid, integriteit en vertrouwelijkheid van de informatievoorziening” (p. 9). Het object van de informatiebeveiliging is de informatievoorziening. De drie genoemde aspecten zijn hieronder toegelicht.

- *Beschikbaarheid:* Het zekerstellen dat gegevens en informatiediensten op de gewenste momenten beschikbaar zijn voor gebruikers.
- *Integriteit:* Het waarborgen dat gegevens niet ongecontroleerd worden gewijzigd of verloren gaan.
- *Vertrouwelijkheid:* Het beschermen van gegevens tegen onbevoegde kennisname.

Kort gezegd is informatiebeveiliging het treffen en onderhouden van een samenhangend pakket maatregelen om de betrouwbaarheid van de informatievoorziening te waarborgen.

Wet bescherming persoonsgegevens

Van der Wel (2006) beschrijft de Wet bescherming persoonsgegevens als volgt: “Volgens de Wet bescherming persoonsgegevens (Wbp) is degene die het doel en de middelen vaststelt voor de verwerking van persoonsgegevens, de ‘verantwoordelijke’. De verantwoordelijke kan een natuurlijk persoon, een rechtspersoon of een samenwerkingsverband zijn. Bij het doel en

middelen voor de verwerking van de persoonsgegevens moet men denken aan de manier van dossiervoering en –archivering, instandhouding van informatievoorziening en geautomatiseerde gegevensopslag. Op de 'verantwoordelijke' berusten alle verplichtingen van de wet" (p. 114).

Een persoonsgegeven is in de Wbp artikel 1 als volgt geformuleerd: elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon.

De verwerking van persoonsgegevens is al volgt geformuleerd: elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens[1].

De definitie bevat een aantal elementen die expliciet aandacht vragen. Allereerst moet het gaan om informatie 'betreffende' een natuurlijke persoon. Voorts moet deze persoon zijn geïdentificeerd of althans identificeerbaar zijn. Als er aan één van beide elementen niet is voldaan, dan is er geen sprake van persoonsgegevens en is de wet niet van toepassing. Hoewel het gaat om twee onderscheiden beoordelingsmomenten, staan zij niet los van elkaar[2].

Verband tussen gegeven en persoon

Niet elk technisch of toevallig verband tussen een gegeven en een persoon is dus voldoende om dat gegeven een persoonsgegeven te doen zijn. Is deze mogelijkheid weliswaar theoretisch aanwezig maar is ondenkbaar dat dit ook daadwerkelijk gebeurt, dan kan ervan worden uitgegaan dat de gegevens niet als persoonsgegevens worden aangemerkt[3].

De Europese privacyrichtlijn 95/46/EG waarop de Wbp is gebaseerd, geeft een iets uitgebreidere omschrijving.

De Richtlijn geeft in artikel 2 onder a als definitie van persoonsgegevens:

Iedere informatie betreffende een geïdentificeerde of identificeerbare natuurlijke persoon, hierna 'betrokkene' te noemen; als identificeerbaar wordt beschouwd een persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificatienummer of van een of meer specifieke elementen die kenmerkend zijn voor zijn of haar fysieke, fysiologische, psychische, economische, culturele of sociale identiteit[4].

Risicoanalyse

Een risicoanalyse is niet het wegnemen van risico's maar wel het beheersen van risico's tot een aanvaardbaar niveau. Wat aanvaardbaar is, is afhankelijk van de organisatie en wet- en regelgeving (Wemmenhove, Schreij & Arends, 2008).

[1] http://wetten.overheid.nl/BWBR0011468/geldigheidsdatum_18-04-2014 Opgehaald 18 april 2014
[2] http://www.cbpweb.nl/wbpnaslag/1/Paginas/wbp-artikel-1-a.aspx Opgehaald 18 april 2014
[3] http://www.cbpweb.nl/wbpnaslag/1/Paginas/wbp-artikel-1-a.aspx Opgehaald 18 april 2014
[4] https://www.cbpweb.nl/downloads_rs/rs_conc_actieve_openbaarmaking.pdf Opgehaald 18 april 2014

Alvorens de risico's worden geanalyseerd moeten deze eerst in kaart worden gebracht. Aangezien de bescherming van persoonsgegevens de primaire zorg is, van de organisatie ten opzichte van hun cliënt, wordt het bepalen van risico's hierop afgestemd. Omdat er sprake is van een eerste inventarisatie van de risico's binnen de organisatie volstaat het om een QuickScan uit te voeren om de risico's te bepalen. Overbeek, Lindgreen en Spruit (2003) omschrijven een QuickScan als volgt: "Een QuickScan is een vorm van risico-inschatting die uitgaat van 'good business practices', ofwel van zeer algemene, maar breed aanvaarde normen". Een QuickScan brengt twee voordelen met zich mee. Het eerste voordeel is het verkrijgen van inzicht in het huidige informatiebeveiligingsbeleid. Het tweede voordeel van de QuickScan is dat het zorgt voor bewustzijn en aandacht voor de informatiebeveiliging. Een uitgebreidere inventarisatie kan te veel tijd kosten en is om een eerste indruk te krijgen van de huidige situatie ongewenst. In dit onderzoek wordt voornamelijk gekeken naar de hoofdlijnen van de informatiebeveiliging in combinatie met de bescherming van persoonsgegevens. De organisatie kan indien men dit nodig acht in de toekomst een meer gedetailleerd onderzoek verrichten.

Om de risico's en maatregelen te bepalen volstaat het volgens Overbeek en Sipman (1999) om het goed boerenverstand, oftewel professional judgement, te gebruiken. Voor de meer ingrijpendere risico's en maatregelen is het noodzakelijk om een uitgebreidere risicoanalyse te verrichten. Volgens Overbeek, Lindgreen en Spruit (2003) zijn veel van de maatregelen een kwestie van ervaring en gezond verstand.

De risico's kunnen een intern en extern karakter hebben. Tijdens dit onderzoek ligt de focus voornamelijk op de interne organisatorische risico's. Relevante externe risico's zijn uiteraard ook aandachtsgebieden voor dit onderzoek.

Om de risico's te analyseren is het essentieel om volgens een vastgestelde methodiek te werk te gaan. Om dit te kunnen bewerkstelligen is ervoor gekozen om gebruik te maken van een bestaand risicoanalysemodel. Een kwantitatieve risicoanalyse is voor de huidige situatie te uitgebreid, aangezien dit de eerste inventarisatie is van de status van het informatiebeveiligingsbeleid. Hiernaast is een kwantitatieve risicoanalyse tijdrovend en complex die een hoge mate van expertise vergt. Tevens kan een uitgebreide risicoanalyse leiden tot teveel informatie, waardoor het nemen van beslissingen moeilijker wordt.

In dit onderzoek wordt gebruik gemaakt van de QuickScan methode. Dit houdt in dat de risico's geschat worden. Om de risico's te bepalen wordt een QuickScan uitgevoerd aan de hand van een interview en een kritische blik op de primaire processen van de organisatie. De risico's die bepaald zijn aan de hand van de QuickScan worden vervolgens beoordeeld aan de hand van de stoplichtmethode. De stoplichtmethode is een middel om de status van een risico te beoordelen door gebruik te maken van drie kleuren namelijk rood, oranje en groen. Deze kleuren worden gebruikt om te bepalen of het risico al dan wel of niet gemitigeerd moet worden.

Voor het onderzoek zal er een inventarisatie van de risico's worden verricht. Van deze risico's zal, aan de hand van de stoplichtmethode, bepaald worden welke van de risico's de meeste aandacht behoren te krijgen. Om de lijst met risico's op een acceptabel niveau te houden

zullen alleen de belangrijkste risico's (key risks) worden geselecteerd, waarvoor vervolgens de belangrijkste maatregelen (key controls) zullen worden voorgesteld.

5. Hoe zien de huidige processen binnen de organisatie eruit

Kraamzorg Mama heeft in haar dagelijkse bedrijfsvoering te maken met verschillende processen. Om zicht te krijgen op de huidige situatie van de informatiebeveiliging is het van belang om de processen van het primaire proces te beschrijven.

In het primaire proces van Kraamzorg Mama wordt de Zorgapplicatie en het Vecozo portaal gebruikt voor het verwerken, controleren en opvragen van verschillende klantgegevens. Tevens worden er via de mailadressen van medewerkers klantgegevens verstuurd. Naast de processen die te maken hebben met het gebruik van de Zorgapplicatie en inzage in het Vecozo portaal zijn er uiteraard ook andere mogelijke aandachtspunten voor de informatieveiligheid die niet gerelateerd zijn aan het primaire proces. Om een goed zicht te hebben op de processen die direct een relatie hebben met toegang tot gevoelige informatie zijn de belangrijkste stappen van het primaire proces beschreven.

Hieronder zijn de stappen van het primaire proces beschreven die betrekking hebben op het gebruik van de Zorgapplicatie, het Vecozo portaal en andere gerelateerde processen die te maken hebben met privacy gevoelige informatie.

Deelprocessen Inschrijving:

In dit deel van het proces wordt de inschrijving van de cliënt bevestigd. De zorgconsulent heeft hiervoor telefonisch contact met de cliënt en vraagt aanvullende gegevens op. In het onderstaande schema zijn de deelprocessen schematisch weergegeven.

Figuur 2 processen Inschrijving

De belangrijkste deelprocessen voor het onderzoek zijn hieronder toegelicht.

1. Input: Kraamzorg Mama ontvangt een aanvraag voor het verlenen van kraamzorg. Deze aanvraag kan via het online formulier, schriftelijke aanmeldingsformulier, telefonische klantenservice of via de zorgverzekeraar aangevraagd worden.
   Procesuitvoerende: Afdeling Klantenservice.

2. Vervolgens wordt het BSN nummer, verzekeringsnummer, de ingangsdatum verzekering en de naam van de verzekering opgevraagd en gecontroleerd in Vecozo (verzekeringsportaal).
   Procesuitvoerende: Afdeling Klantenservice.

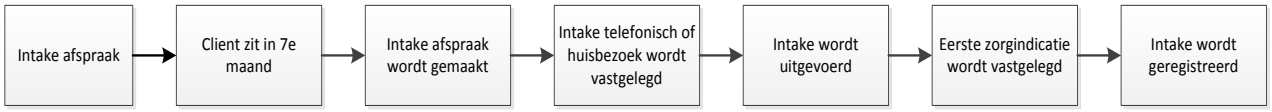
3. Het registreren van de gegevens, die verkregen zijn via het Vecozo portaal, in het cliëntdossier in de Zorgapplicatie, waarbij het BSN nummer als kenmerk wordt gebruikt.
   Procesuitvoerende: Afdeling Klantenservice.

4. Na de aanmelding wordt telefonisch contact opgenomen met de cliënt om de aanvraag te bevestigen. Hierbij worden telefonisch aanvullende gegevens opgevraagd ten bate van de zorgverlening. Deze gegevens worden na afloop van het gesprek ook ingevoerd in de Zorgapplicatie.
   Procesuitvoerende: Afdeling Klantenservice.

5. Voor de bevestiging van de zorg wordt er een bevestigingsbrief opgemaakt vanuit de Zorgapplicatie. Hierna is de cliënt ingeschreven.
   Procesuitvoerende: Afdeling Klantenservice.

Deelproces Intake:

In dit deelproces wordt het uitvoeren van intakes ingepland en geregistreerd. In het onderstaande schema zijn de deelprocessen schematisch weergegeven.



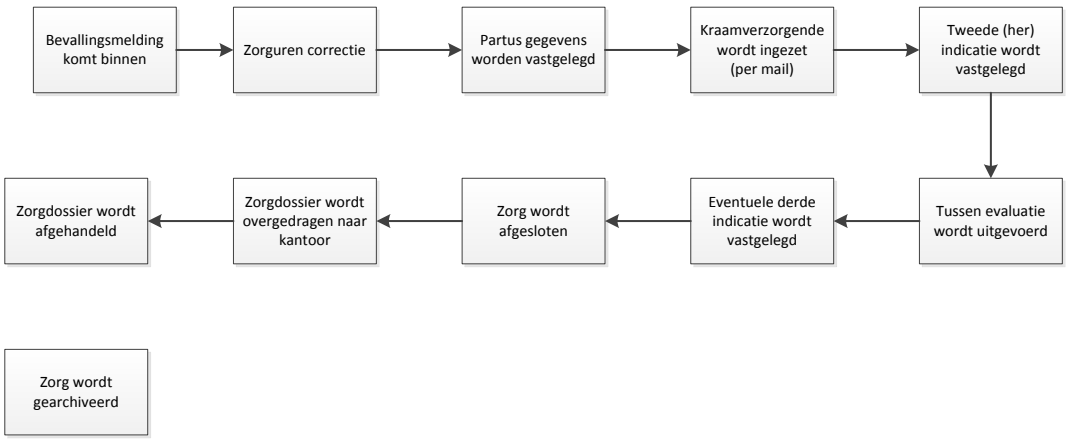
Figuur 3 processen Intake

Het belangrijkste deelproces voor het onderzoek is hieronder toegelicht.

6. Na een intakegesprek met de cliënt worden aanvullende gegevens bijgewerkt in het digitale cliëntdossier in de Zorgapplicatie.
   Procesuitvoerende: Intaker.

Deelproces Zorg:

In dit deelproces wordt de zorg ingezet, wordt het zorgplan bijgehouden en wordt de cliënt overgedragen (via de mail) naar de kraamverzorgende. In het onderstaande schema zijn de deelprocessen schematisch weergegeven.



Figuur 4 processen Zorg

De belangrijkste deelprocessen voor het onderzoek zijn hieronder toegelicht.

7. De bevallingsgegevens worden geregistreerd wanneer de cliënt op het punt staat om te bevallen. De gegevens worden geregistreerd in de Zorgapplicatie.
   Procesuitvoerende: Planning.

8. Eventuele correcties op de te verlenen uren kraamzorg worden geregistreerd in de Zorgapplicatie.
   Procesuitvoerende: Planning.

9. Afwijkingen bij geen beschikbaarheid kraamverzorgende wordt contact opgenomen met de ketenpartner. Gegevens uitwisseling gebeurd via de mail.
   Procesuitvoerende: Planning.

6. Wat is de huidige situatie van de informatiebeveiliging

Om de risico's te bepalen is het van belang om de huidige situatie van de informatiebeveiliging in kaart te brengen. Hiervoor is een interview afgenomen met de IT manager van Kraamzorg Mama. Het interview is opgenomen in de bijlage van het verslag. Het interview en de beschrijving van de processen zullen vervolgens geanalyseerd worden om de risico's te bepalen. De uitkomst van het interview is hieronder beschreven en toegelicht.

Toegangsbeveiliging

Kraamzorg Mama maakt voor het toegang krijgen tot de computers, het portaal en de Zorgapplicatie gebruik van toegangswachtwoorden. De eisen die zijn gesteld aan de wachtwoorden zijn dat de wachtwoorden hoofdletters, kleine letters, nummers en leestekens moeten bevatten. Bij het kiezen van een wachtwoord controleert het systeem automatisch of een gekozen wachtwoord voldoet aan de eisen. De wachtwoorden moeten per kwartaal gewijzigd worden en dit wordt automatisch door het systeem aangegeven.

Gebruikersrechten

De beveiliging van de bestanden geschiedt aan de hand van de machtigingen en beperkingen die zijn opgelegd aan de personeelsleden, dit zorgt ervoor dat niet iedereen toegang heeft tot persoonsgegevens. Hiernaast heeft het personeel met een machtiging in de meeste gevallen alleen toegang tot de informatie die voor hen relevant is voor het uitvoeren van hun werkzaamheden. Voor de applicatie heeft men gebruikersrechten waarvoor gebruikers van de applicatie persoonlijke inlogcodes hebben. Alle computers zijn gekoppeld aan afdelingen en elke afdeling heeft vaste users. De Zorgapplicatie is niet toegankelijk zonder een wachtwoord. Alle zorgconsulenten kunnen in de applicatie de zorgverlening benaderen die aan hen is toegekend. De afdeling financiën heeft inzicht in het zorgdossier, met betrekking tot de zaken die relevant zijn voor de financiële afwikkeling, van de cliënt in verband met de afwikkeling van de declaratie bij de zorgverzekeraar en de inning van de wettelijke eigen bijdrage. Naast bestaande beveiligingsmaatregelen werkt Kraamzorg Mama met een eigen ontwikkelde applicatie om de veiligheid en betrouwbaarheid te verbeteren en meer grip te krijgen op de informatietoegankelijkheid.

Organisatorisch

Naast het gebruik van toegangswachtwoorden en gebruikersrechten heeft Kraamzorg Mama ook een aantal organisatorische maatregelen getroffen. Deze maatregelen zijn gerelateerd aan de toegang tot het Vecozo portaal en bedrijfsgegevens. Het Vecozo portaal is alleen toegankelijk voor leden van het Management Team, de manager van de afdeling Financiën en de leidinggevende van de afdeling Planning. De communicatie tussen de Zorgapplicatie en de Vecozo server gebeurt over een Hyper Text Transfer Protocol Safe verbinding. Deze verbinding wordt gebruikt bij informatie uitwisseling waar sprake is van verzenden van gevoelige informatie. Het Vecozo portaal werkt met een systeemcertificaat en houdt loggegevens bij van de gebruikers. Deze loggegevens worden gebruikt om te controleren of men niet zomaar onterechte en irrelevante gegevens opvragen van personen. De zorggegevens worden opgeslagen op de centrale server. Deze server is toegankelijk via een extern

bureaublad. Het bureaublad is weer beveiligd met een toegangswachtwoord. De server staat op het hoofdkantoor in een aparte ruimte.

Gegevensbescherming

Voor de verzending van gegevens via de mail zijn momenteel geen instructies en protocollen opgesteld. Het gebruik van email voor de verzending van persoonsgegevens is beperkt tot het moment van het inzetten van de zorg, waarbij de kraamverzorgster via de mail gegevens ontvangt over de cliënt om vervolgens de dienstverlening te kunnen uitvoeren. Tevens zijn er geen afspraken gemaakt met ketenpartners over de omgang met persoonsgegevens die zijn uitgewisseld met de ketenpartners, met betrekking tot het verlenen van de zorg.

Voor het opslaan van gegevens en documenten wordt gebruik gemaakt van de server en dropbox. Door het gebruik van dropbox kunnen medewerkers documenten van verschillende locaties benaderen. In dropbox worden voornamelijk bestanden met procedures en format bestanden opgeslagen voor gemeenschappelijk gebruik. Dit betekent dat er geen persoonsgegevens worden opgeslagen in dropbox. De PC voorzieningen van Kraamzorg zijn voorzien van USB poorten en men kan dus informatie opslaan op USB sticks. Er zijn geen protocollen of maatregelen voor het gebruik van USB sticks. De medewerkers zijn er wel van bewust dat het niet toegestaan is om bestanden en andere informatie van de computers op een USB stick te zetten.

Control

Informatiebeveiligingsincidenten of vermoedens hiervan kunnen getraceerd worden door de logbestanden te raadplegen. Deze logbestanden worden automatisch bijgehouden en kunnen op elk gewenst moment worden opgehaald. De logbestanden worden momenteel niet periodiek gecontroleerd op indicaties van onrechtmatige toegang of onrechtmatig gebruik van de persoonsgegevens. Er zijn geen vastgelegde procedures voor het tijdig en doeltreffend behandelen van informatiebeveiligingsincidenten en zwakke plekken in de beveiliging, zodra deze zijn ontdekt en gerapporteerd. Momenteel is er geen verantwoordelijke aangewezen die regelmatig beoordeeld of de beveiligingsmaatregelen binnen de organisatie daadwerkelijk worden nageleefd. Tevens wordt er buiten kantooruren niet door een verantwoordelijke gecontroleerd of er documenten met gevoelige persoonsgegevens aanwezig zijn op werkplekken, in vergaderruimtes, bij printers/kopieerapparaten of in niet-afgesloten papierbakken. Hierdoor kan een verantwoordelijke niet vaststellen of de gedragsregels voor de omgang met documenten met gevoelige persoonsgegevens effectief zijn en de medewerkers voldoende bewust zijn van het beleid van organisatie. Hiernaast worden er geen sociale engineering tests uitgevoerd. In deze tests proberen experts per telefoon of per e-mail onder valse voorwendselen, persoonsgegevens te achterhalen. Hiermee kan de verantwoordelijke vaststellen in hoeverre gedragsregels voor het verstrekken van persoonsgegevens daadwerkelijk worden nageleefd.

De werking van de technische informatiebeveiliging wordt zowel intern als extern gecontroleerd. De interne controle wordt uitgevoerd door middel van een audit door de IT manager. Hiervoor worden de beveiligingsindicatoren die zijn opgesteld door de IT manager

getoetst. Er is op strategisch niveau besloten samen te werken met twee partijen, namelijk Vallence voor hosting en Netinvestement voor de applicatie beveiliging, de samenwerking is nauw en wordt per kwartaal getoetst. Deze partijen rapporteren over de werking van de server en of er beveiligingsincidenten zijn voorgevallen.

Kraamzorg Mama heeft geen overzicht van alle informatie verwerkende bedrijfsmiddelen. Voor de vervanging van bedrijfsmiddelen of het gebruiken van de bedrijfsmiddelen voor andere doeleinden is op dit moment geen procedure voor het verzekeren van de verwijdering van gevoelige bedrijfs- en persoonsgegevens. Tevens is er geen sprake van een officieel expliciet gecommuniceerde clear desk/screen beleid.

Personeel

Kraamzorg Mama beschikt over een beknopt privacy protocol en een handboek voor kantoormedewerkers waarin het beleid is vastgelegd. Hier wordt niet actief naar verwezen bij het in dienst treden van de organisatie. Hiernaast zijn er geen verantwoordelijkheden toegewezen op zowel sturend als uitvoerend niveau. De medewerkers krijgen geen training en regelmatige bijscholing over het informatiebeveiligingsbeleid en de informatiebeveiligingsprocedures van de organisatie, voor zover relevant voor hun functie, waarbij expliciet aandacht wordt besteed aan de omgang met persoonsgegevens.

Documentatie

De hardcopy documenten van cliënten en andere belangrijke bedrijfsgegevens worden gesorteerd en gearchiveerd in kasten die zijn voorzien van sloten. Hiernaast is het pand voorzien van een inbraakalarm. Managers van de hoofdafdelingen hebben toegang tot deze documenten en kunnen deze op aanvraag verstrekken aan belanghebbenden. Binnen de organisatie is een papierversnipperaar aanwezig om gevoelige documenten te kunnen vernietigen. Kraamzorg Mama heeft te maken met een bewaarplicht van zeven jaar van de klantgegevens. De persoonsgegevens worden vernietigd na het verstrijken van deze periode.

7. Wat zijn de belangrijkste risico's voor de informatiebeveiliging

In dit hoofdstuk zijn de risico's beschreven. De risico's zijn bepaald aan de hand van de QuickScan methode die is uitgevoerd op basis van de beschrijving van de huidige processen en het interview. De risico's zijn volgens de tien hoofdcategorieën, die vastgesteld zijn de door de Code voor Informatiebeveiliging, inzichtelijk gemaakt. Deze richtlijnen zijn tevens leidend in de NEN 7510. De hoofdcategorieën en hun doelstellingen zijn hieronder opgesomd en kort toegelicht.

1. Beveiligingsbeleid: Het bieden van ondersteuning en een duidelijke richting aan het management ten behoeve van de beveiliging.
2. Organisatie van de beveiliging: Het beheer van de informatiebeveiliging voor structuur en het toekennen van verantwoordelijkheden.
3. Classificatie en beheer van de bedrijfsmiddelen: Bescherming van de bedrijfsmiddelen.
4. Personeel: Het verminderen van risico's van menselijk handelen.
5. Fysieke beveiliging en omgeving: Het voorkomen van onbevoegde fysieke toegang tot informatie en informatiesystemen.
6. Computer- en netwerkbeheer: Zorgdragen voor veilig gebruik van IT- middelen.
7. Toegangsbeveiliging: Voorkomen van ongeautoriseerde toegang tot informatie en informatiesystemen.
8. Ontwikkeling en onderhoud van systemen: Vereiste beveiliging van de levenscyclus van de systemen waarborgen.
9. Continuïteitsplanning: Voorbereiding van alternatieve wijzen om de bedrijfsprocessen voort te zetten bij omvangrijke calamiteiten.
10. Toezicht: Controleren van de naleving van het beveiligingsbeleid.

Voor het bepalen en beoordelen van de risico's zijn de risico's in een tabel beschreven. De risico's zijn per categorie beschreven en beoordeeld aan de hand van de stoplichtmethode, waarbij de kleuren rood, oranje en groen de risicobeoordeling aangeven. Bij het beoordelen van de risico's is de bescherming van de persoonsgegevens leidend. Dit betekent dat er bepaalde verhoogde risico's kunnen zijn binnen de organisatie die niet een verhoogd risico status krijgen bij de beoordeling hiervan, omdat deze risico's niet direct gerelateerd zijn aan de bescherming van persoonsgegevens. De betekenissen van de kleuren van de stoplichtmethode zijn hieronder kort toegelicht:

- ***Rood:*** Er is sprake van een verhoogd risico, waarvoor maatregelen vereist zijn.
- ***Oranje:*** Er is sprake van een gemiddeld risico met de potentie om een verhoogd risicostatus te krijgen.
- ***Groen:*** Er is sprake van een incidenteel risico, welke men kan afhandelen volgens de bestaande procedures.

In de onderstaande tabellen zijn de hoofdcategorieën aangeven met de risico's die zijn gerelateerd aan de betreffende hoofdcategorie.

	Risicocategorie	**Risico omschrijving**	**Beoordeling**
1.	Beveiligingsbeleid	Er is geen beleid geformuleerd met betrekking tot de omgang met persoonsgegevens	
		Er zijn geen procedures voor het melden van informatiebeveiligingsincidenten	
		Er is geen verplichting voor het melden van informatiebeveiligingsincidenten	
		Er is geen beleid m.b.t. het gebruik van mobiele apparaten	
		Er is geen officieel beleid m.b.t. het gebruik van social media	
2.	Organisatie van de beveiliging	Er zijn geen verantwoordelijkheden toegewezen aan de medewerkers voor de informatiebeveiliging	
		Geen afspraken met ketenpartners over de omgang met persoonsgegevens bij uitwisseling van persoonsgegevens	
3.	Classificatie en beheer van de bedrijfsmiddelen	Het verdwijnen of kwijtraken van bedrijfsmiddelen, doordat er geen overzicht van de beschikbare bedrijfsmiddelen en de gebruikers hiervan is	
4.	Personeel	Er is geen officieel aanname/ ontslag beleid waar gericht wordt gekeken naar de bescherming van persoonsgegevens	
		Er zijn geen trainingen of cursussen om het personeel bewust te maken m.b.t. de omgang met persoonsgegevens en wettelijke verplichtingen	
		Beveiligingsincidenten worden mogelijk niet gemeld door medewerkers	
		Het downloaden van ongewenste programmatuur door medewerkers	
		Medewerkers vatbaar voor social engineering	
		Tijdelijke medewerkers/ stagiaires die gebruik maken van de bedrijfsmiddelen	
5.	Fysieke beveiliging en omgeving	Er is geen officiële clear desk/ screen policy	
		Het pand is beveiligd met een alarm	
		Alleen medewerkers hebben toegang tot de bedrijfsmiddelen	
		Hardcopy documenten zoals zorgdossiers worden in het archief opgeborgen	

Tabel 1

	Risicocategorie	Risico omschrijving	Beoordeling
6.	Computer- en netwerkbeheer	Aanvallen van hackers en virussen	
		Verwijdering van gegevens van bedrijfsmiddelen bij vervanging	
		Vernietigen van persoonsgegevens na de wettelijke bewaarplicht	
7.	Toegangsbeveiliging	Er wordt gebruik gemaakt van toegangswachtwoorden	
		Medewerkers werken met gebruikersrechten	
		Medewerkers worden niet verplicht hun wachtwoord geheim te houden	
		Medewerkers weten waar de gebruikersrechten voor dienen en wat de eventuele consequenties bij het niet naleven van de regels zijn	
8.	Ontwikkeling en onderhoud van systemen	Er wordt gebruik gemaakt van encryptie voor de uitwisseling van gegevens tussen de organisatie en Vecozo portaal	
		Het verzenden van persoonsgegevens via de mail	
9.	Continuïteitsplanning	Er is geen continuïteitsplan aanwezig	
10.	Toezicht	Er is geen bijsturing mogelijk door onvoldoende toezicht en evaluatie	
		Er is geen periodieke controle van de logbestanden	
		Er wordt niet periodiek gecontroleerd op naleving van wet- en regelgeving	

Tabel 2

In de bovenstaande tabellen is te zien dat de belangrijkste risico's voornamelijk liggen in de volgende categorieën:

- Beveiligingsbeleid
- Organisatie van de beveiliging
- Personeel
- Toezicht

De maatregelen voor deze categorieën en de overige met rood beoordeelde risico's worden in het volgende hoofdstuk behandeld.

8. Wat zijn de mogelijke maatregelen voor de risico's

In dit hoofdstuk zijn een aantal voorstellen van maatregelen gedaan om de informatiebeveiliging naar een hoger niveau te brengen. De essentiële maatregelen die in dit hoofdstuk worden voorgesteld zijn preventief en moeten zorgen voor de basis van de informatieveiligheid. Deze basis wordt ook wel de baseline genoemd. De baseline is een set van maatregelen die door de gehele organisatie wordt doorgevoerd. Deze baseline vormt de ondergrens van de beveiliging waaraan de organisatie minimaal moet voldoen. Bij het voorstellen van de maatregelen is er bewust voor gekozen om de hoofdlijnen van de maatregelen te beschrijven. Dit omdat er momenteel geen officieel beleid is met betrekking tot de informatiebeveiliging. Om te beginnen is het van belang om structuur en richting te geven aan de informatiebeveiliging. Als de organisatie structuur en richting heeft gegeven aan de informatiebeveiliging, dan kan er op een gedetailleerder niveau gekeken worden naar additionele maatregelen.

Zoals in het voorgaande hoofdstuk benoemd zijn de risicocategorieën beveiligingsbeleid, organisatie van de beveiliging, personeel en toezicht de belangrijkste aandachtspunten voor de voorgestelde maatregelen. Naast de voorgenoemde categorieën zullen de overige risico's die met rood zijn beoordeeld ook behandeld worden. Bij het aandragen van de maatregelen zijn de richtlijnen van de NEN 7510 leidend. Naast de NEN 7510 zijn ook andere bronnen zoals de richtlijnen van het College Bescherming Persoonsgegevens (CBP) en de Code voor Informatiebeveiliging in acht genomen. Deze verschillende richtlijnen vertonen overigens in grote mate overlappingen en zijn op enkele aspecten complementair aan elkaar. Voor Kraamzorg Mama is werken naar het voldoen aan de NEN 7510 een doelstelling en daarom is de NEN 7510 dus ook de basis voor het bepalen van de maatregelen. De achterliggende gedachte van het voldoen aan de NEN 7510 is het beschermen van de persoonsgegevens van de cliënten en het voldoen aan wet- en regelgeving betreffende persoonsgegevens.

De maatregelen worden hieronder per categorie toegelicht.

Beveiligingsbeleid

Volgens Overbeek en Sipman (1999) komt beveiliging voort uit een algeheel bedrijfsbeleid. Dit beleid moet door het management worden uitgedragen. "Structureel werken aan beveiliging kan alleen wanneer dit door de gehele organisatie wordt gedragen, te beginnen bij de top" (Overbeek & Sipman, 1999, p.80).

Om tot een goed beveiligingsbeleid te komen is het noodzakelijk om te weten wat de huidige situatie is van de informatiebeveiliging. Aan de hand van de huidige situatie kunnen in een beleidsdocument zaken opgenomen worden die niet goed functioneren of niet expliciet gecommuniceerd zijn naar de belanghebbenden binnen de organisatie. Bij het verrichten van de QuickScan zijn de volgende punten naar voren gekomen met betrekking tot de categorie beveiligingsbeleid:

- Er is geen beleid geformuleerd met betrekking tot de omgang met persoonsgegevens.
- Er zijn geen procedures voor het melden van informatiebeveiligingsincidenten.

- Er is geen verplichting voor het melden van informatiebeveiligingsincidenten.

Om de voorgenoemde punten te kunnen afdekken is het van belang dat de organisatie een beleidsdocument uitbrengt. Door een beleidsdocument te publiceren toont het management zich betrokken bij de informatiebeveiliging. In dit beleid moeten de doelstelling van het beleid worden opgenomen om de belanghebbenden binnen de organisatie het nut en belang van de informatiebeveiliging in te laten zien. In het beleid worden ook de verwachtingen en de verantwoordelijkheden van het management ten opzichte van de medewerkers beschreven. In de huidige situatie is het van belang dat met het beleidsdocument informatie wordt verschaft over het doel en het belang van de informatiebeveiliging, de wettelijke verplichtingen ten opzichte van de cliënten en de procedures voor het melden van incidenten. In ditzelfde document worden tevens de verplichtingen en verantwoordelijkheden van de medewerkers ten opzichte van het management benoemd. Eventuele consequenties voor niet naleving van het beleid dienen ook opgenomen te worden en expliciet benadrukt te worden. Bij het niet naleven van de in het beleidsdocument opgenomen bepalingen kunnen de medewerkers van de organisatie gewezen worden op het beleid. In het document dient tevens opgenomen te worden dat naleving periodiek wordt gecontroleerd en geëvalueerd. Het management dient het beleid te handhaven om ervoor te zorgen dat de bepalingen van het document worden nageleefd. Het beleidsdocument moet te allen tijde beschikbaar zijn voor belanghebbenden. Het informatiebeveiligingsbeleid dient kenbaar gemaakt te worden aan (mede)verantwoordelijken in de organisatie.

De minimaal vereiste aspecten die opgenomen dienen te worden in het beleidsdocument zijn hieronder opgesomd.

- De doelstelling.
- Een definitie van informatiebeveiliging en persoonsgegevens.
- Toelichting van het belang van de informatiebeveiliging.
- De verantwoordelijkheden van het management en medewerkers.
- Verplichting en procedures van het melden van beveiligingsincidenten.
- Consequenties van niet naleving van het beleid met betrekking tot wet- en regelgeving.
- Maatregelen die getroffen zijn voor de bescherming van persoonsgegevens worden expliciet vermeld.
- Beleid ten opzichte van bewustwording en training in omgang met privacygevoelige informatie.

Naast de reeds genoemde punten is het aan te raden om ook richtlijnen in het document op te nemen voor een clear desk en clear screen beleid.

Organisatie van de beveiliging

Om het beleid ook daadwerkelijk te kunnen uitvoeren is het van belang dat de bescherming van de informatie wordt georganiseerd. Dit kan men verwezenlijken door verantwoordelijkheden en taken toe te wijzen aan medewerkers van de organisatie. Hiermee kan de beveiliging van de informatie structuur aannemen. Dit betekent dat de rollen en

verantwoordelijkheden verdeeld moeten worden over verschillende functies van de organisatie en dus niet een taak is die volledig aan de IT manager wordt toegewezen. De IT manager alleen is dus niet voldoende om de organisatie van de beveiliging te organiseren. De directie is verantwoordelijk voor het coördineren en beoordelen van de organisatie van de beveiliging en het toewijzen van rollen. De directie zal de rollen moeten verdelen over verschillende lagen van de organisatie bij managers, beheerders, gebruikers of auditors. Om te bepalen wat de meest relevante stappen zijn voor de organisatie, zijn de punten die aan de hand van de QuickScan aan het licht zijn gekomen hieronder opgesomd:

- Er zijn geen verantwoordelijkheden toegewezen aan de medewerkers voor de informatiebeveiliging.
- Geen afspraken met ketenpartners over de omgang met persoonsgegevens bij uitwisseling van persoonsgegevens.

Om de voorgaande aspecten te kunnen afdekken moet de directie de organisatie van de beveiliging specificeren en duidelijk gaan inrichten. Dit betekent dat de directie ervoor moet zorgen dat de structuur van het beleid en de organisatie uitvoerbaar gemaakt wordt en dat men kan starten met het implementeren van het beleid. De belangrijkste stappen die ondernomen moeten worden om de organisatie van de beveiliging te structuren zijn hieronder toegelicht.

- Het toekennen van taken en verantwoordelijkheden aan verschillende functies en medewerkers.
- Verantwoordelijkheden voor bescherming persoonsgegevens moeten expliciet worden vermeld.
- Zorgen voor de benodigde middelen om het beleid te kunnen implementeren.
- Afspraken maken over de samenwerking tussen verschillende functies binnen de organisatie.
- Zorgen voor specialistisch advies van externen voor onafhankelijk oordeel.
- Afspraken maken met ketenpartners over de omgang met persoonsgegevens.
- Zorgen voor structuur en het werken volgens een cyclus om continu te kunnen evalueren en verbeteren.
- Wettelijke kaders en richtlijnen aangeven.
- Consequenties voor niet uitvoeren van de taken communiceren.
- Het aanbieden en stimuleren van trainingen en opleiding met betrekking tot informatiebeveiliging.
- Contacten leggen en onderhouden met belangengroepen om deskundig advies te kunnen inwinnen.

Naast de afspraken die gemaakt moeten worden met de ketenpartner is er een aanvullend risico met betrekking tot de bescherming van persoonsgegevens. De uitwisseling van de persoonsgegevens tussen Kraamzorg Mama en haar medewerkers en ketenpartners verloopt nu via reguliere mailaccounts. De uitwisseling van gegevens zou in een beveiligde omgeving moeten plaatsvinden om de bescherming van persoonsgegevens te verbeteren. De diensten van een aanbieder zoals Zorgmail voldoet aan deze eisen. Zorgmail is een dienst die voldoet

aan onder meer de volgende eisen van de bescherming van de gegevens van de organisatie en cliënt met betrekking tot de uitwisseling van persoonsgegevens:

- Vertrouwelijkheid
- Authenticatie
- Integriteit
- Onweerlegbaarheid
- Betrouwbaarheid
- SPAM-vrije omgeving
- Constante virusscanning

Personeel

De maatregelen op het gebied van personeel behoren tot de belangrijkste aandachtspunten voor de beveiliging van gegevens. Dit omdat het menselijk handelen gezien wordt als de zwakste schakel in de informatiebeveiliging. De technische afdekking van risico's is namelijk tot op een bepaalde hoogte goed te realiseren. Bij menselijk handelen spelen echter vele factoren een rol en is de beveiliging van dit aspect een complexere kwestie. Het verminderen van het risico van het personele aspect begint al bij het aannemen van personeel. Dit kan te maken hebben met een bepaalde gevoelige functie die een medewerker vervult. Hiernaast zijn medewerkers zich vaak niet bewust van risico's, doordat men vaak dezelfde handelingen verrichten en het management geen bewustzijn programma's initieert. Medewerkers werken vaak op een soort van automatische piloot en zijn hierdoor niet alert op mogelijke risico's. Tevens zijn medewerkers gevoelig voor social engineering waarbij kwaadwillende, medewerkers die niet op hun hoede zijn, doelbewust manipuleren om toegang te krijgen tot gevoelige informatie. Naast voorgenoemde zaken kunnen onzorgvuldigheid en laksheid ook leiden tot tekortkomingen in de informatiebeveiliging. Het investeren in bewustzijn bij personeel is een stap voor zijn voor het plaatsvinden van incidenten. Hierbij geldt het gezegde voorkomen is beter dan genezen.

Uit de QuickScan zijn de volgende aandachtspunten naar voren gekomen:

- Er is geen officieel aanname/ontslag beleid waar gericht wordt gekeken naar de bescherming van persoonsgegevens.
- Er zijn geen trainingen of cursussen om het personeel bewust te maken m.b.t. de omgang met persoonsgegevens en wettelijke verplichtingen.
- Beveiligingsincidenten worden mogelijk niet gemeld door medewerkers.
- Medewerkers vatbaar voor social engineering.
- Tijdelijke medewerkers/ stagiaires die gebruik maken van de bedrijfsmiddelen.

Om de bovengenoemde punten te kunnen beheersen dient de organisatie een aantal stappen te ondernemen. De belangrijkste aandachtspunten zijn hieronder opgesomd.

- Medewerkers bewust maken van hun verantwoordelijkheden.
- Het opgestelde beleid implementeren.
- Medewerkers bewust maken over mogelijke gevolgen van hun handelen.

- Medewerkers verplichten (potentiele) beveiligingsincidenten te rapporteren.
- Beveiligingstaken en verantwoordelijkheden bij het aannemen van personeel vastleggen in functiebeschrijving.
- Het screenen van sollicitanten door middel van controle op referenties of verklaring van goed gedrag.
- Personeel dient een geheimhoudingsverklaring te ondertekenen bij indiensttreding.
- De wettelijke kaders communiceren naar de medewerkers.
- Bewustzijn creëren bij medewerkers door regelmatige training en opleiding, waarbij expliciet aandacht wordt besteed aan de bescherming van persoonsgegevens.
- Personeel informeren over beveiligingsprocedures.
- Disciplinaire maatregelen bij herhaaldelijk verwijtbaar nalatigheid met betrekking tot de informatiebeveiliging.
- Blokkeren van toegangsrechten tot bedrijfsmiddelen bij uitdiensttreding.
- Personeel bewust maken van social engineering.
- Tijdelijke medewerkers voorzien van aparte bedrijfsmiddelen die geen gevoelige informatie bevatten of toegang bieden tot gevoelige informatie via een netwerk.
- Beleid met betrekking tot het gebruik van social media opstellen.

Toezicht

De laatste categorie voor de informatiebeveiliging is het toezicht. Onder toezicht wordt verstaan het controleren van de naleving van de regels en procedures die opgenomen zijn in de behandelde beveiligingscategorieën. Met het toezicht kan de organisatie controleren of de beveiligingsmaatregelen en relevante wetgevingen worden nageleefd. Hiernaast verzamelt de organisatie informatie over de werking van het beleid en mogelijke tekortkomingen van het beleid waarop de organisatie maatregelen kan nemen en kan bijsturen. Zonder toezicht kan het beveiligingsbeleid niet goed functioneren en bestaat het risico dat de medewerkers het beleid niet serieus nemen. Hiernaast zal de organisatie ook geen zicht hebben op de status van de informatiebeveiliging. Door regelmatige controles in te voeren kan de organisatie voorkomen dat het tegen onverwachte incidenten aanloopt.

De belangrijkste aandachtspunten voor de categorie toezicht zijn:

- Er is geen bijsturing mogelijk doordat er geen toezicht en evaluatie is.
- Er wordt niet periodiek gecontroleerd op naleving van wet- en regelgeving.

Om het toezicht vorm te geven moeten een aantal stappen ondernomen worden. De belangrijkste stappen zijn hieronder opgesomd.

- Er moet periodiek gecontroleerd worden of de omgang met persoonsgegevens voldoet aan wet- en regelgeving.
- Er moet periodiek gecontroleerd worden op de naleving van het beveiligingsbeleid.
- Er moeten periodiek zowel intern als extern audits uitgevoerd worden.
- Er moeten periodiek social engineering tests uitgevoerd worden.
- Bij niet naleving van het beleid worden treffende maatregelen genomen.

- Er moeten periodiek werkplek controles worden uitgevoerd.
- Er moet gecontroleerd worden of beveiligingsmaatregelen daadwerkelijk geïmplementeerd worden.

9. Op welke wijze kan naleving van de maatregelen worden gecontroleerd

Eén van de belangrijkste zaken om een goed informatiebeveiligingsbeleid in stand te houden is het controleren van de uitvoering van het beleid. Controle is er om te kunnen vaststellen dat het beleid wordt geïmplementeerd en of dit effectief is. Hiernaast is controle van belang omdat er na verloop van tijd nieuwe risico's kunnen ontstaan of dat er nieuwe aanvullende wet- en regelgeving is ontwikkeld waaraan de organisatie zich dient te houden. Het alleen invoeren van maatregelen is niet voldoende. Er moet gecontroleerd worden of de risico's zijn afgenomen. Om een goede controle uit te kunnen voeren is het van belang om een auditplan op te stellen. Bij het opstellen van het auditplan kunnen checklists geïntegreerd worden voor het uitvoeren van de audits. Het Nederlands Normalisatie-Instituut biedt verschillende checklists aan om stapsgewijs de status van het informatiebeveiligingsbeleid te kunnen monitoren volgens de richtlijnen van NEN 7510 norm. Hiermee kan inzicht verkregen worden in de werking van de processen. Aan de hand van de checklists kan bepaald worden of alles goed functioneert of dat er zaken verbeterd moeten worden. Bij het uitvoeren van een interne controle is het van belang dat de interne auditor onafhankelijk is van de processen die gecontroleerd worden. Dit betekent dat men geen controles behoort uit te voeren met betrekking tot de eigen werkzaamheden of eigen afdeling. De controle van het beleid dient structureel van aard te zijn om constante verbetering en optimalisatie van het informatiebeveiligingsbeleid te realiseren. Hiervoor dient men te werken volgens een cyclus. Een methode hiervoor is de Plan, Do, Check, Act-cyclus (PDCA-cyclus). In de onderstaande afbeelding zijn de stappen van de PDCA-cyclus weergegeven.

Afbeelding 1 PDCA-cyclus

Naast de interne controle is het aangeraden om ook een externe controle uit te laten voeren. Deze controle kan uitgevoerd worden door de accountant of andere specialisten op het gebied van informatiebeveiliging. Een voordeel van de externe controle is dat er met een frisse en onafhankelijke blik gekeken wordt naar het beleid en de uitvoering hiervan. Het uitvoeren van controles heeft als bijkomend voordeel dat het een preventieve werking heeft op de

uitvoerders van het beleid. De medewerkers blijven hierdoor bewust van het feit dat de zij gecontroleerd worden op de uitvoering van hun taken en verantwoordelijkheden. De naleving van het beleid controleren houdt ook in dat er in het geval van een incident wordt gekeken of verbeteringen zijn doorgevoerd. Om het beleid up-to-date te houden is het noodzakelijk dat er een baseline is geformuleerd waarop de organisatie de controle kan baseren. Hiernaast is het van belang dat er periodiek een QuickScan wordt uitgevoerd om te kijken wat de status is van bepaalde risico's en of er nieuwe risico's zijn die aandacht verdienen.

10. Nieuwe ontwikkelingen op het gebied van informatiebeveiliging monitoren

Het is voor een organisatie van belang om, naast alle maatregelen die een organisatie treft, up-to-date te blijven over de ontwikkelingen in hun vakgebied. Door op de hoogte te blijven van nieuwe wet- en regelgeving en ontwikkelingen op het gebied van het managen van de informatiebeveiliging, zorgt de organisatie ervoor dat het beleid constant voldoet aan de eisen van het laatste moment.

Het monitoren van ontwikkelingen op het gebied van informatiebeveiliging kan op verschillende manieren plaatsvinden. De meest voor de hand liggende manier is het volgen van de ontwikkelingen en mededelingen van certificeringsorganisaties zoals het Nederlands Normalisatie-Instituut. Voor Kraamzorg Mama is het raadplegen van de website van NEN 7510 een goed manier om op de hoogte te blijven van de ontwikkelingen die in lijn zijn met de NEN 7510 norm. Op de website van NEN 7510 kan men informatie en nieuws vinden over nieuwe ontwikkelingen op het gebied van informatiebeveiliging in de zorg. Hiernaast doet het CBP regelmatig mededelingen en geeft het regelmatig adviezen met betrekking tot informatiebeveiliging en het beschermen van persoonsgegevens. Op de website van het CBP zijn geregeld nieuwsberichten te vinden die gerelateerd zijn aan de bescherming van persoonsgegevens. Het CBP biedt ook de mogelijkheid om maandelijks per e-mail informatie te ontvangen over nieuwe publicaties, activiteiten en andere relevante informatie.

Kraamzorg Mama kan tevens regelmatig contact onderhouden met andere kraamzorg organisatie en ketenpartners in de branche over hun aanpak, vernieuwingen en ontwikkelingen op het gebied van informatiebeveiligingsbeleid.

Als ondersteuning op de bovengenoemde stappen kan Kraamzorg Mama zich tevens op verschillende websites aanmelden voor nieuwsbrieven die informatie geven over informatiebeveiliging in de zorg. Zijlstra Business Consultants geeft wekelijks een nieuwsbrief uit met uiteenlopende onderwerpen waaronder ook informatiebeveiliging en het managen hiervan. Het International Management Forum (IMF) geeft ook geregeld nieuwsbrieven uit en biedt cursussen en trainingen aan op het gebied van IT management.

Voor meer specialistische informatie over nieuwe ontwikkelingen is het aan te raden om gebruik te maken van diensten, advies en informatie van gespecialiseerde organisaties die bekend zijn met informatiebeveiligingsmanagement. Hiervoor kan men de accountant of kantoren inschakelen die gespecialiseerd zijn in het uitvoeren van IT audits. Dit soort organisaties zijn vanwege hun vakgebied goed op de hoogte van de nieuwste ontwikkelingen.

11. Conclusies en Aanbevelingen

Als afsluiting van het onderzoek is het van noodzakelijk belang om conclusies te trekken uit het verrichte onderzoek. Op basis van conclusies is het mogelijk om gedegen aanbevelingen te doen aan Kraamzorg Mama. De conclusies en aanbevelingen dienen antwoord te geven op de centrale onderzoeksvraag die als volgt luidt:

Wat zijn de belangrijkste risico's van de informatiebeveiliging binnen Kraamzorg Mama en op welke wijze kan Kraamzorg Mama deze risico's afdekken?

Conclusies

Om aanbevelingen te kunnen doen zijn de belangrijkste conclusies van de deelvragen opgesomd. De conclusies zijn hieronder per deelvraag beschreven.

Hoe zien de huidige processen er binnen de organisatie uit?

- De primaire processen van Kraamzorg Mama zijn goed ingericht. Kraamzorg Mama besteedt veel energie en aandacht aan de organisatie van de processen en een continu verbetering hiervan. Mede hierdoor heeft Kraamzorg Mama een Harmonisatie Kwaliteitsbeoordeling in de Zorgsector certificaat (HKZ-certificaat) behaald.

- De processen van Kraamzorg Mama zijn zodanig ingericht om onrechtmatige toegang van niet geautoriseerde personen binnen de organisatie tot de informatiesystemen uit te sluiten. De medewerkers van de afdeling Zorg onderhouden het contact met cliënten en hebben daardoor toegang tot de Zorgapplicatie en persoonsgegevens. De financiële afdeling heeft beperkte toegang tot persoonsgegevens.

- Kraamzorg Mama heeft nog geen duidelijke afspraken met ketenpartners omtrent de omgang met persoonsgegevens. Hiernaast verstuurt Kraamzorg Mama persoonsgegevens via reguliere mailaccounts naar interne zorgmedewerkers en ketenpartners voor het uitvoeren van de dienstverlening.

Wat is de huidige situatie van de informatiebeveiliging?

- Kraamzorg Mama maakt gebruik van toegangsbeveiliging en gebruikersrechten om de informatiebeveiliging te beheren. Dit betekent dat medewerkers alleen toegang hebben tot de bedrijfsmiddelen en applicaties middels een gebruikerswachtwoord. Naast het gebruik van een wachtwoord werkt Kraamzorg Mama met toegangsrechten voor het gebruik van de Zorgapplicatie.

- Kraamzorg Mama heeft een beperkt aantal medewerkers toegangsrechten gegeven tot het Vecozo portaal. Dit portaal is één van de belangrijkste toegangspoorten tot persoonsgegevens. Kraamzorg Mama en haar medewerkers zijn zeer alert op misbruik van het portaal. Hiernaast heeft Vecozo ook de nodige technische maatregelen genomen om misbruik te voorkomen.

- Het management van Kraamzorg Mama heeft geen officieel beleid opgesteld voor de bescherming van persoonsgegevens en de informatiebeveiliging. De informatiebeveiliging wordt vooral van de technische kant benaderd. De nadruk ligt op de bescherming van data en software en controle op inbreuk of ongeregeldheden in de informatiesystemen.

- Kraamzorg Mama werkt met een vaste kern medewerkers die toegang hebben tot gevoelige informatie. Voor het aantrekken van nieuw personeel, voor functies waarbij gevoelige informatie een rol speelt, is geen beleid of procedure opgesteld.

Wat zijn de belangrijkste risico's voor de informatiebeveiliging?

- De belangrijkste risico's liggen in de beveiligingscategorieën Beveiligingsbeleid, Organisatie van de beveiliging, Personeel en Toezicht.

- Kraamzorg Mama heeft geen officieel beleid en procedures ontwikkeld voor de informatiebeveiliging. Hiernaast zijn er geen verantwoordelijkheden toegewezen aan medewerkers over de omgang met informatie. Een belangrijk onderdeel van het controleren van de informatiebescherming, namelijk het toezicht en evaluatie, zijn niet een vast onderdeel van de informatiebeveiliging.

Wat zijn de mogelijke maatregelen voor de risico's?

- Het management van Kraamzorg Mama moet een informatiebeveiligingsbeleid formuleren om het beleid te kunnen communiceren en uitdragen naar de medewerkers. Het management moet de medewerkers actief wijzen op het beleid en bewust maken van de implementatie van het beleid.

- De verantwoordelijkheid van de organisatie moet door de hele organisatie heen gedragen worden door het toewijzen van verantwoordelijkheden aan medewerkers met verschillende functies.

- Kraamzorg Mama moet met betrekking tot het personeelsbeleid programma's initiëren om bewustzijn te creëren. Hiernaast moet er een screening plaatsvinden van medewerkers die nieuw worden aangenomen.

Op welke wijze kan naleving van de maatregelen worden gecontroleerd?

- Kraamzorg Mama dient een auditplan op te stellen, waarmee de werking van de maatregelen gecontroleerd kan worden. De controle kan intern en extern verricht worden. De controles moeten cyclisch verricht worden.

Hoe kan Kraamzorg Mama nieuwe ontwikkelingen op het gebied van informatiebeveiliging monitoren?

- Kraamzorg Mama kan bij verschillenede instanties zoals het Nederlands Normalisatie-Instituut, het CBP, IT auditors en verschillende consultantbureaus informatie inwinnen over nieuwe ontwikkelingen op het gebied van informatiebeveiliging en het beschermen van persoonsgegevens.

Aanbevelingen

Aan de hand van het onderzoek en de conclusies op basis van de deelvragen wordt bij het doen van de aanbevelingen antwoord gegeven op de centrale onderzoeksvraag.

Tijdens het onderzoek is gebleken dat de nadruk bij de informatiebeveiliging voornamelijk op de technische zijde van de informatiebeveiliging ligt. De informatiebeveiliging is hierdoor voornamelijk een verantwoordelijkheid van de IT manager. De technische zijde is daarom ook goed afgedekt en krijgt ook veel aandacht zoal het geval is met de zelfontwikkelde Zorgapplicatie.

De NEN 7510 en andere richtlijnen zoals de Code voor Informatiebeveiliging richten zich voor een groot deel op zaken die niets met de technische zijde van de beveiliging te maken hebben. Binnen Kraamzorg Mama bestaat er de misvatting dat de NEN 7510 betrekking heeft op het gebruik van een applicatie. Hierbij bestaat het idee dat een applicatie moet voldoen aan de NEN 7510. Dit is echter niet het geval. Het doel van de NEN 7510 is niet om een applicatie te beveiligen, maar de norm gaat over de omgang met informatiebeveiliging. Het gebruik van een applicatie is hier een onderdeel van. De zaken die in de richtlijnen zoals NEN 7510 en de Code voor Informatiebeveiliging naar voren komen hebben veelal te maken met juridische kaders, beleidsvorming, personele zaken, processen, toezicht en evaluatie. Dit komt mede doordat informatie in verschillende vormen in de organisatie is opgeslagen en uitgewisseld wordt, waardoor het niet beperkt is tot informatiesystemen. Het toepassen van de richtlijnen van de NEN 7510 betekent dat de verantwoordelijkheid voor de informatiebeveiliging gedragen wordt door de gehele organisatie beginnende bij de directie. Een succesvolle informatiebeveiliging is alleen mogelijk als de hele organisatie zich bewust is van het belang van informatiebeveiliging. De medewerkers zijn immers degenen die het beleid moeten uitvoeren.

De stappen die genomen moeten worden om de informatiebeveiliging te verbeteren kunnen niet geïnitieerd worden door de IT manager, omdat dit niet zijn taak en specialisatie is. De directie van Kraamzorg Mama is verantwoordelijk voor het ontwikkelen van een beleid, waarin de verschillende managers en medewerkers binnen de organisatie hun eigen verantwoordingen en taken voor de informatiebeveiliging nemen en uitvoeren.

Er bestaat binnen veel organisaties het idee dat het volgen of het hanteren van de maatregelen van de NEN 7510 een verplichting of een vereiste is om in aanmerking te komen voor een certificering. Dit is echter niet het geval. Dit is zelfs niet wenselijk omdat de norm een groot aantal maatregelen aandient, waarvan het praktisch onmogelijk is om deze allemaal te implementeren. De NEN 7510 is een goede basis om het informatiebeveiligingsbeleid vorm te

geven en in te richten. Elke organisatie is echter vrij om maatregelen en werkwijzen te hanteren die afwijken van de NEN 7510 mits men dit goed heeft onderbouwd. Het doel van de NEN 7510 is het initiëren van een proces om informatiebeveiliging structureel aan te pakken. Dit betekent dat men begint met een risicoanalyse. Aan de hand van geïdentificeerde risico's kiest en implementeert men passende maatregelen. Om de beveiliging continu te verbeteren is het noodzakelijk om naleving te controleren en evalueren om vervolgens volgens de PDCA-cyclus veranderingen door te voeren.

Om in aanmerking te komen voor een certificering zal in ieder geval een basis gelegd moeten worden. Met het onderzoek is een goede basis gelegd voor het opzetten van een informatiebeveiligingsbeleid. De methoden en aandachtspunten kunnen gebruikt worden om de belangrijkste zaken aan te pakken. De belangrijkste aandachtspunten zijn in het onderzoek bepaald aan de hand van hun relatie met de verwerking en bescherming van persoonsgegevens aangezien dit één van de belangrijkste aspecten bevat van de informatiebeveiliging in verband met wettelijke kaders. Als deze basis zaken in orde zijn gemaakt dan kan de organisatie kijken naar vervolgstappen om in aanmerking te komen voor de ISO/IEC 27001:2005 certificering.

De belangrijkste aanbevelingen worden hieronder opgesomd en kort toegelicht.

- Om richting en structuur te geven aan de informatiebeveiliging is het noodzakelijk dat Kraamzorg Mama een beleid voor de informatiebeveiliging formeel documenteert en dit beleid actief communiceert naar de huidige en nieuwe werknemers. Hiernaast moet de wettelijke verplichting met betrekking tot de omgang met persoonsgegevens opgenomen worden in het beleid. Tevens moet de verplichting om incidenten en privacy schendingen te melden opgenomen worden in het beleid.

- De verantwoordelijkheden voor de informatiebeveiliging dienen te worden gedeeld binnen de organisatie. Dit betekent dat de medewerkers van verschillende afdelingen en functies actief moeten deelnemen in het uitvoeren van het beleid.

- Er moet beleid gevormd worden op het gebied van aannemen en ontslaan van personeel. Dit is een belangrijk punt omdat een belangrijke factor in het slagen van het beleid de uitvoering, alertheid en bewustzijn van de medewerkers is. Hierbij moet in het bijzonder aandacht besteedt worden aan de invulling van gevoelige functies en tijdelijke medewerkers.

- Het is voor Kraamzorg Mama noodzakelijk dat het informatiebeveiligingsbeleid wordt gecontroleerd en geëvalueerd, omdat de organisatie te maken heeft met constante veranderingen zoals nieuwe wettelijke eisen. Het werken volgens de PDCA-cyclus is hiervoor een gepaste methode.

- Er moeten afspraken gemaakt worden met ketenpartners over de omgang met persoonsgegevens.

Literatuurlijst

- Bulgurcu, B., Cavusoglu, H., Benbasat, I. (2010). Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. Mis Quarterly, 34, 523-544. Retrieved from http://misq.org/information-security-policy-compliance-an-empirical-study-of-rationality-based-beliefs-and-information-security-awareness.html?SID=g1roi1ir7cnu16bcrtsomfl4p5

- Oud, E.J. (2002). Praktijkgids Code voor Informatiebeveiliging. Schoonhoven, Nederland: Academic Service.

- Overbeek, P., Lindgreen, E.R., & Spruit, M. (2003). Informatiebeveiliging onder controle. Amsterdam, Nederland: Pearson Education.

- Overbeek, P., & Sipman, W. (1999). Informatiebeveiliging. 's-Hertogenbosch, Nederland: Tutein Nolthenius.

- Wel, J.A. van der. (2006). Informatiebeveiliging in de zorg. Den Haag, Nederland: Sdu.

- Wemmenhove, P., Schreij, J., & Arends, M. (2008). Information Risk Management in de praktijk. 's-Hertogenbosch, Nederland: Tutein Nolthenius.

Normen

- NEN Norm 7510:2007

- NEN-ISO/IEC 17799:2005

Bijlage
Interview

Interview huidige situatie van de informatiebeveiliging

1. **Wordt er binnen de organisatie gebruik gemaakt van toegangswachtwoorden?**

Ja, alle medewerkers die toegang nodig hebben tot de informatiesystemen gebruiken toegangswachtwoorden.

2. **Wat zijn de eisen die gesteld worden aan de wachtwoorden?**

De wachtwoorden moeten hoofdletters, klein letters, nummers en leestekens bevatten.

3. **Op welke manier worden bedrijfsbestanden en persoonsgegevens beveiligd?**

Via de applicatie heeft niemand toegang tot de bestanden, de gegevens intern zijn beveiligd in een server. De server wordt benaderd via een extern bureaublad. Deze is weer toegankelijk met een toegangswachtwoord.

4. **Maakt de organisatie gebruik van encryptie voor de uitwisseling van informatie?**

Ja, de communicatie tussen de Zorgapplicatie en het Vecozo portaal gebeurt over een https verbinding.

5. **Zijn er beperkingen in de applicatie met betrekking tot de toegang van bepaalde personen? Zo ja op welke manier is dit geregeld?**

De applicatie kent gebruikersrechten, personen die de applicatie gebruiken hebben een persoonlijke inlogcode. Alle zorgconsulenten kunnen onder hun eigen account de zorgen benaderen die aan hen zijn toegekend. De afdeling financiën kan ook relevante gegevens van het zorgdossier bekijken.

6. **Hoe is de applicatie beveiligd tegen toegang van derden?**

Gebruikersnaam en wachtwoord zijn vereist om toegang te krijgen tot de applicatie. Hiernaast is het pand fysiek beveiligd door middel van een inbraakalarm.

7. **Zijn er ook organisatorische maatregelen genomen met betrekking tot toegang tot de Applicatie en Vecozo?**

Het Vecozo portaal is alleen toegankelijk voor de hoofdplanning, hoofd financiën en het Management Team.

8. **Is er ook sprake van beveiligingsmaatregelen voor het verzenden van gevoelige informatie via de mail? Zo ja op welke manier?**

Nee, momenteel zij hier geen maatregelen voor genomen. Verzendingen van gegevens via de mail worden zoveel mogelijk beperkt.

9. **Kunnen gebruikers informatie op een USB zetten? Zo ja is dit op een beveiligde manier volgens protocollen?**

Ja, dit is wel mogelijk, maar het is algemeen bekend dat dit niet is toegestaan binnen de organisatie. Hiervoor zijn echter geen officiële protocollen en richtlijnen opgesteld.

10. **Op welke manier wordt de werking van de informatiebeveiliging gecontroleerd?**

Door middel van zowel interne als externe audit. Alle beveiligingsindicatoren worden dan getoetst.

11. **Worden er logbestanden gemaakt van de gebruikers? Zo ja hoe worden deze beheerd?**

Ja, dit proces is geautomatiseerd. Alle logs worden bijgehouden en kunnen op elke gewenst moment worden opgehaald.

12. **Is er sprake van sturing en ondersteuning vanuit de directie ten behoeve van de informatiebeveiliging? Zo ja waar blijkt dit uit?**

Ja, er is op strategisch niveau besloten samen te werken met twee partijen, namelijk Vallence voor hosting en Netinvestement voor applicatie beveiliging, de samenwerking is nauw en wordt per kwartaal getoetst.

13. **Is er een overzicht van alle informatie verwerkende bedrijfsmiddelen? Zo ja waar is dit overzicht opgenomen?**

Nee.

14. **Op welke manier is de fysieke beveiliging van de informatiemiddelen georganiseerd?**

Alle computers zijn gekoppeld aan afdelingen, en elke afdeling heeft vaste users. De toegang voor elke user is beperkt tot zijn functie. Hiernaast is het pand voorzien van een inbraakalarm.

15. **Is er sprake van een clear desk/screen beleid? Zo ja hoe wordt dit gecommuniceerd naar de werknemers toe en hoe wordt dit gehandhaafd?**

Nee, dit is niet officieel gecommuniceerd naar de medewerkers toe, hoewel de medewerkers er wel bewust van zijn dat documenten altijd opgeborgen moeten worden indien deze niet meer gebruikt worden.

16. **Wordt er rekening gehouden met nieuwe medewerkers en informatieveiligheid? Zo ja hoe worden zij ingelicht over het beleid en protocollen?**

Er is een privacy protocol opgesteld en beschikbaar binnen de organisatie die nieuwe medewerkers kunnen raadplegen. Hiernaast is er een handboek kantoormedewerkers waarin het beleid staat vastgelegd.

17. **Welke overige maatregelen zijn er genomen m.b.t. informatieveiligheid?**

De organisatie werkt momenteel met eigen op maat ontworpen software met admin panel.

18. **Zijn er maatregelen getroffen of beleid opgesteld voor het waarborgen van de informatieveiligheid van de hardcopy (papieren) documenten? Zo ja wat voor maatregelen en beleid?**

Ja, alle documenten zijn gesorteerd in mappen en opgeborgen in archiefkasten die voorzien zijn van sloten. De afdelingsmanager heeft toegang tot de hardcopy documenten en kan deze indien nodig verstrekken aan desbetreffende afdeling.

19. **Zijn er in het contract van personeelsleden bepalingen opgenomen die de omgang met persoonsgegevens toelichten en/of eventuele gevolgen van niet correct omgaan met persoonsgegevens aangeven?**

Nee.

20. **Is er binnen de organisatie een papierversnipperaar aanwezig om gevoelige documenten te kunnen vernietigen?**

Ja.

21. **Zijn er afspraken met ketenpartners over de omgang met uitgewisselde persoonsgegevens van cliënten? Zo ja wat zijn deze afspraken?**

Nee.

22. **Worden de hardcopy documenten vernietigd na de vastgestelde wettelijke bewaarplicht. Zo ja hoe wordt dit vernietigd?**

Ja. Met behulp van de papierversnipperaar.

23. **Wat is het beleid ten opzichte van bedrijfsmiddelen zoals computers die worden vervangen. Worden deze zomaar op straat gezet of is hier een beleid voor. Er staat namelijk mogelijk gevoelige informatie op de computers?**

Bedrijfsmiddelen worden niet zomaar vervangen of verwijderd. Hier is geen officieel beleid voor.

24. **Is er momenteel een beleidsdocument dat de maatregelen voor bescherming van de persoonsgegevens beschrijft?**

Nee.

25. **Zijn er verantwoordelijkheden, zowel op sturend als op uitvoerend niveau, toegewezen voor de informatiebeveiliging. Zo ja is dit ook vastgelegd?**

Momenteel is de IT manager verantwoordelijk voor de informatiebeveiliging op uitvoerend niveau. De verantwoordelijkheden zijn niet schriftelijk vastgelegd.

26. **Krijgen gebruikers training en regelmatige bijscholing over het informatiebeveiligingsbeleid en de informatiebeveiligingsprocedures van de organisatie, voor zover relevant voor hun functie. En wordt hierbij expliciet aandacht besteed aan de omgang met persoonsgegevens?**

Nee.

27. **Worden de logbestanden periodiek gecontroleerd op indicaties van onrechtmatige toegang of onrechtmatig gebruik van de persoonsgegevens en word er indien nodig actie ondernomen?**

De logbestanden worden niet periodiek gecontroleerd. Deze worden geraadpleegd bij een vermoeden van een incident.

28. **Zijn er procedures voor het tijdig en doeltreffend behandelen van informatiebeveiligingsincidenten en zwakke plekken in de beveiliging, zodra deze zijn gerapporteerd?**

Nee.

29. **Heeft de organisatie beleid ontwikkeld voor de bescherming en voor de geheimhouding van persoonsgegevens? Zo ja is dit beleid vastgelegd, geïmplementeerd en gecommuniceerd naar alle personen die betrokken zijn bij het verwerken van persoonsgegevens?**

Nee.

30. **Worden opslagmedia met gevoelige persoonsgegevens fysiek vernietigd of worden de persoonsgegevens vernietigd, verwijderd of overschreven met technieken die het onmogelijk maken om de oorspronkelijke persoonsgegevens terug te halen?**

Dit is tot op heden nog niet nodig geweest.

31. **Wordt er door een verantwoordelijke regelmatig beoordeeld of de beveiligingsmaatregelen binnen de organisatie daadwerkelijk worden nageleefd?**

Nee.

32. **Wordt er door een verantwoordelijke regelmatig beoordeeld of de beveiligingsmaatregelen binnen de technische systemen daadwerkelijk worden nageleefd?**

Ja.

33. **Wordt er buiten kantooruren door een verantwoordelijke gecontroleerd of er documenten met gevoelige persoonsgegevens aanwezig zijn op werkplekken, in vergaderruimtes, bij printers of kopieerapparaten of in niet-afgesloten papierbakken?**

Nee.

34. **Worden er sociale engineering tests uitgevoerd?**

Nee.