Handvatten Informatieveiligheid

voor het leveren van betrouwbare zorg;
een BBMCare document

Waarom deze Handvatten?
Voor vele organisaties is er nog steeds een drempel om informatieveiligheid op de agenda te krijgen én te houden. Die drempel heeft wellicht te maken met het beeld dat informatieveiligheid niet wordt gezien als zorggerelateerd en dus minder relevant wordt gevonden. Daarnaast wordt informatieveiligheid als een apart en ingewikkeld vakgebied ervaren met een overdaad (133!) aan normelementen uit de NEN 7510.

Uit de praktijk blijkt echter dat maatregelen om misbruik van informatie en vooral van informatietechnologie te voorkomen, steeds meer nodig zijn. Vele organisaties hebben dit in het verleden ervaren; zoals een website die niet beschikbaar is door een aanval van hackers of bestanden die niet meer toegankelijk zijn als gevolg van kwaadaardige software. Ook maakt de toenemende inzet en vooral afhankelijkheid van internetdiensten organisaties steeds kwetsbaarder.

Om organisaties effectiever te ondersteunen bij het werken aan informatieveiligheid zijn de ***Handvatten Informatieveiligheid*** ontwikkeld.
Uitgangspunten zijn
- de vraagstelling *wat heeft een medewerker nodig om goede zorg te verlenen?*
- een praktische uitwerking van de belangrijkste beveiligingsmaatregelen;
- een laagdrempelige start.

Betrokkenheid medewerker
Bij 'het verlenen van goede zorg' staat de medewerker mét de cliënt centraal. *Wat heeft de medewerker daarvoor nodig?* Medewerkers zijn vooral afhankelijk van een betrouwbare informatievoorziening in termen van beschikbaarheid, integriteit en vertrouwelijkheid / privacy. Daarvoor heeft een organisatie beveiligingsmaatregelen getroffen. Medewerkers moeten zich daar niet alleen bewust van zijn maar vooral overtuigd zijn van het belang van die beveiligingsmaatregelen; pas dan kan worden verwacht dat de maatregelen effect hebben. Denk aan afspraken over het gebruik van wachtwoorden en het melden van beveiligingsincidenten.

Informatieveiligheid

Informatieveiligheid is een essentieel onderdeel van goede zorg en goed werkgeverschap. Informatieveiligheid gaat niet alleen om het afschermen van gegevens, maar ook over de beschikbaarheid en integriteit van gegevens. En bovenal, informatie-veiligheid moet werkbaar zijn voor de medewerkers.

Het is onmogelijk om informatie-veiligheid op orde te hebben wanneer medewerkers niet achter de richtlijnen en maatregelen staan. Informatieveiligheid moet daarom aan het primaire proces worden verbonden; middelen en maatregelen moeten bijdragen aan goede zorg en aan goed werkgeverschap.

Bewustwordingsaspecten worden in de Handvatten vanuit twee invalshoeken benaderd.
a) Medewerkers informeren over een aantal zaken die men behoort te weten en dient na te leven; bijvoorbeeld door een gedragscode te ondertekenen of het verplicht volgen van een bewustwordingsprogramma over informatieveiligheid. Maar bewustwordingsacties kunnen als hinderlijk worden ervaren: *ik heb hier helemaal geen tijd voor, ik moet mijn werk doen!* Daarom een tweede invalshoek.

b) Medewerkers actief betrekken bij nut en noodzaak van informatieveiligheid; laat medewerkers zelf ontdekken dat ze er uiteindelijk profijt van hebben. Integreer informatieveiligheid in hun werkprocessen. Maak daarbij gebruik van de nieuwe media zoals weblogs of richt een discussieforum in op het bedrijfsnetwerk. Ga bijvoorbeeld de discussie aan om smartphonetoepassingen zoals de camera en handige apps veilig voor het werk te gebruiken. Aanleiding voor discussies kunnen actuele beveiligings-incidenten zijn maar ook veel gestelde vragen zoals*: mag je met je mobiel een foto nemen van een huiduitslag bij je cliënt om te kunnen overleggen met je collega? mag je familie informatie geven over hoe het met de cliënt gaat?*

Twaalf Handvatten

Het document Handvatten Informatieveiligheid sluit aan op de 'twaalf belangrijkste normelementen' zoals beschreven in het Praktijkboek NEN 7510 § 1 *Waar te beginnen?* In de praktijk zullen een aantal van deze normelementen reeds zijn uitgewerkt in vooral technische beveiligingsmaatregelen. Wat meestal nog aandacht nodig heeft zijn de formele en procedurele zaken zoals een beveiligingsbeleid, de organisatie van informatieveiligheid en vooral de bewustwordingsactiviteiten. Richt daarop je aandacht. Daarmee wordt een stevige basis gelegd om informatieveiligheid als *business as usual* op de agenda te krijgen zowel door de betrokkenheid van de medewerkers als door het commitment van de directie.

1. **Stel informatiebeveiligingsbeleid op**
2. **Stel vast wie daarvoor verantwoordelijk is**
3. **Zorg voor bewustwording, opleiding en training**
4. **Neem maatregelen tegen kwaadaardige programmatuur**
5. **Sluit overeenkomsten af over dienstverlening en communiceer veilig**
6. **Beveilig de toegang tot systemen**
7. **Zorg voor continuïteitsmaatregelen**
8. **Houd rekening met intellectueel eigendom**
9. **Beveilig bedrijfsdocumenten**
10. **Bescherm persoonsgegevens**
11. **Leef beveiligingsbeleid na**
12. **Rapporteer beveiligingsincidenten**

BBMcare producten

De Handvatten Informatieveiligheid zijn opgenomen in het pakket BBMCare-documenten. BBMCare staat voor BasisBeveiligingsModel in de Caresector. Het BBMCare is een instap- én beheermodel voor het inrichten én onderhouden van informatieveiligheid in de caresector. Het model is ontwikkeld in samenwerking met ActiZ en niet alleen beschikbaar voor de ouderenzorg, maar ook voor de geestelijke gezondheidszorg en de gehandicapten zorg.

Door uit te gaan van de 12 belangrijkste normelementen van de NEN 7510 is een praktische start gemaakt met het BBMCare; volg daarna het BBMCare Stappenplan en informatieveiligheid kan uitgroeien tot een beveiligingsniveau dat past bij de organisatie. Voor kleinschalige zorgorganisaties die nagenoeg alle automatiseringsactiviteiten hebben uitbesteed is deze start al bijna voldoende. De focus komt dan vooral te liggen op de afspraken (contracten en bewerkersovereenkomsten) met de dienstverleners om de verantwoordelijkheid voor informatieveiligheid te borgen.

Een nieuw uitgangspunt bij informatieveiligheid!

Bij het werken aan informatiebeveiliging wordt het traditionele denken vanuit wet- en regelgeving verlaten door uit te gaan van de vraag ***"Wat heeft een zorgmedewerker nodig voor het leveren van goede zorg?"*** Deze vraag is de basis voor elk informatieveiligheidstraject. Zie het voorbeeld hieronder hoe vanuit de behoefte van medewerkers de relatie wordt gelegd naar beveiligingsmaatregelen. De paragraafaanduiding staat voor een paragraafnummer van het bijbehorende normelement uit de NEN 7510.

Wat heeft een zorgmedewerker nodig om goede zorg te leveren?	***Wat moet de organisatie daarvoor regelen?***	***Verwijzing NEN 7510 e.a.***	***Wat moeten zorgmedewerkers weten? §8.2.2***	***Hoe kunnen zorgmedewerkers bijdragen aan een betere dienstverlening? NEN 7510 §8.2.2***
Ik wil niet dat mijn privegegevens op straat komen te liggen. Ik wil dat mijn client er op kan vertrouwen dat zijn of haar gegevens bij ons veilig zijn.	Privacyreglement medewerker- en clientgeg; bijbehorende protocollen zoals inzage dossier etc.	§15.1.4 **Handvat 10** Wgb Wbp	Reglementen en protocollen vertalen naar praktische FAQ's . . .	. . en FAQ's ter discussie stellen; bijwerken agv praktijkervaring. Discussies mbv sociale media
Ik wil bij het dossier / toedienlijst kunnen wanneer ik dat nodig heb	Regel continuïteit ITmiddelen met een hoge beschikbaarheidseis	§14.1.3 **Handvat 7**	Alternatieven laten weten voor het geval dat . . . (nooddossier, dagelijkse medicatielijst, etc)	Zich voortdurend realiseren waar ze afhankelijk van zijn en alternatieven kennen. Maar je kunt niet alles voorzien, volg je gevoel en koppel terug!

Belangstelling? Meer informatie is te verkrijgen via een van onderstaande emailadressen. De Handvatten worden gratis beschikbaar gesteld, voor de beveiligingsproducten BBMCare en de bewustwordingscursus *Veilig omgaan met vertrouwelijke informatie* moet worden betaald.

peter.vanderzwan@caresecure.nl - douwe@dejong-itadvies.nl