Handvatten Informatieveiligheid

voor het leveren van betrouwbare zorg;
een BBMCare document

februari 2017

Inhoud

Bijlagen

1 Introductie

1.1 Aanleiding

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 ervaren velen informatieveiligheid als een apart en ingewikkeld vakgebied 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 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. Een toenemende inzet en vooral afhankelijkheid van internetdiensten maakt organisaties steeds kwetsbaarder.

Organisaties besteden hun automatiseringsdiensten vaak uit en er wordt steeds meer gebruik gemaakt van clouddiensten. Maar zijn hierover de juiste afspraken gemaakt? Want, als er zaken fout gaan is de opdrachtgever verantwoordelijk! In veel gevallen gaat het gelukkig (nog) goed, maar de kans dat het een keer fout gaat, wordt wel steeds groter.

En zijn ook medewerkers zich voldoende bewust van de beveiligingsrisico's die hun organisatie loopt? Zijn zij op de hoogte hoe te handelen bij het vermoeden van een datalekken en weten ze wat de consequenties kunnen zijn als een datalek niet wordt gemeld? Het is belangrijk dat organisaties kunnen aantonen dat het voldoende heeft gedaan om medewerkers te informeren om dit soort beveiligingsrisico's te minimaliseren.

Om organisaties effectiever te ondersteunen bij het werken aan informatieveiligheid zijn de ***Handvatten Informatieveiligheid*** opgesteld.
Uitgangspunten zijn:
- de vraagstelling *wat heeft een medewerker nodig om goede zorg te verlenen?* (op basis van hetgeen de cliënt, en namens de cliënt de organisatie, hiervan verwacht!);
- een praktische uitwerking van de belangrijkste beveiligingsmaatregelen;
- een laagdrempelige start.

In § 1.2 wordt ingegaan op belang en vooral op de betrokkenheid van de medewerker bij het leveren van zorg en wordt de relatie gelegd naar beveiligingsmaatregelen. De Handvatten Informatieveiligheid maken deel uit van het pakket BBMCare; de afzonderlijke handvatten hebben betrekking op de normelementen uit de NEN 7510. Daarover in § 1.3 meer. In Hoofdstuk 2 worden de 12 handvatten uitgewerkt.

1.2 Betrokkenheid medewerker

Bij 'het leveren 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 of het melden van beveiligingsincidenten.

Bewustwordingsaspecten worden in dit document 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 de 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 beveiligingsincidenten 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?*

In bijlage A is een overzicht opgenomen vanuit de vraag: *wat heeft een medewerker in de zorg nodig om goede zorg te leveren?* Antwoorden worden gevonden door het stellen van de vervolgvragen:
- *wat moet een organisatie daar voor regelen?*
- *wat moeten zorgmedewerkers weten en*
- *hoe kunnen zorgmedewerkers bijdragen aan een betere dienstverlening?*

1.3 BBMCare en beveiligingsniveau Laag

De Handvatten Informatieveiligheid zijn opgenomen in het pakket BBMCare-documenten. BBMCare staat voor BasisBeveiligingsModel voor de Caresector. Het BBMCare is een instap- én beheermodel voor het inrichten én onderhouden van informatieveiligheid in de caresector.

De overige BBMCare-documenten zijn:
- de Handleiding,
- het Stappenplan,
- het Inventarisatie- en Classificatiedocument informatieveiligheid,
- het Werkdocument NEN 7510 en
- het Presentatiedocument.

De Handvatten Informatieveiligheid richten zich op het beveiligingsniveau Laag. In het BBMCare wordt gesproken over de beveiligingsniveau's Laag en Gemiddeld; zie de Handleiding § 6.1. Het beveiligingsniveau Laag verwijst naar de 'twaalf belangrijkste maatregelen' uit het Praktijkboek NEN 7510 § 1 *Waar te beginnen?* (Zie ook bijlage D2).

In de praktijk zullen een aantal van deze maatregelen reeds zijn getroffen. Wat meestal nog aandacht nodig heeft zijn de formele en procedurele zaken zoals een beveiligingsbeleid, de organisatie van informatieveiligheid en vooral de bewustwordingsactiviteiten. Ga daarmee aan de slag door gebruik te maken van de informatie uit hoofdstuk 2 van dit document. Dit leidt tot een beveiligingsniveau Laag. 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 het commitment van de directie.

Door je te richten op het beveiligingsniveau Laag heb je een overzichtelijk begin 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 het beveiligingsniveau Laag wellicht al voldoende. De focus komt dan vooral te liggen op de afspraken (contracten en bewerkersovereenkomsten) met de dienstverleners om de verantwoordelijkheid voor informatieveiligheid te borgen.

2 Handvatten beveiligingsniveau Laag

Bij de uitwerking van de twaalf handvatten zijn hier en daar inleidende teksten overgenomen uit het Praktijkboek NEN 7510 H1 *Waar te beginnen*, aangevuld met praktische informatie en aanbevelingen gericht op de organisatie en vooral ook op de medewerkers. Uitgebreide informatie is uiteraard te vinden bij de betreffende normelementen / paragraaf in de Norm- en Praktijkboeken NEN 7510.

Vooral de aanbevelingen die medewerker-gerelateerd zijn hebben te maken met bewustwordings-activiteiten en zijn hier en daar overgenomen uit de e-learningcursus *Veilig omgaan met vertrouwelijke informatie*.

Elk handvat wordt afgesloten met de z.g. toetsingscriteria ZZ3 (zie bijlage D7). Deze toetsingscriteria zijn ook terug te vinden in het zogenaamde Policy Framework waaraan wordt gerefereerd in sommige bewerkersovereenkomsten, bijvoorbeeld die van Nedap. Beschouw de toetsingscriteria vooral niet als een verplichting maar als *richtinggeven*d voor het uitwerken van de betreffende normelementen. Het is handig zich bewust te zijn van de toetsingscriteria die auditors *kunnen* hanteren.

In veel organisaties hebben vrijwilligers, daar waar dat mogelijk is, dezelfde rechten als medewerkers met een arbeidscontract. Als in dit document wordt gesproken over medewerkers kan dat in veel gevallen ook van toepassing op vrijwilligers.

2.1 Stel informatiebeveiligingsbeleid op (paragraaf 5.1.1)

Praktijkboek NEN 7510

> *Hoe eenvoudig zo'n eerste versie van informatiebeveiligingsbeleid ook mag zijn: zonder plan (beleid) zijn alle acties zonder st(ruct)uur. Dat kan variëren van het najagen van de verkeerde prioriteiten tot het handelen naar de waan van de dag.*
>
> *Gaandeweg zal het beleid verbeteren: het is een iteratief proces. De vijand van het goede is het beste: accepteer dat de beginversie onvolkomen is. Wijs je leiding hier ook op en eis van hen ook steun als tegenstanders het argument van 'niet goed genoeg' te berde brengen in de hoop niets te hoeven doen.*

Via het Praktijkboek NEN 7510 is een voorbeeld van een informatiebeveiligingsbeleid (IBbeleid) te vinden, document 511-1. In dit voorbeeld worden nagenoeg alle aspecten benoemd die van belang kunnen zijn. Neem daaruit over wat je aanspreekt en laat vooral weg wat (nog) niet relevant lijkt.

In de volgende paragraaf wordt ingegaan op de organisatie van informatieveiligheid, hoofdstuk 4 van het voorbeelddocument.

Betrokkenheid medewerkers

Laat medewerkers weten dat het IBbeleid beschikbaar is; geef een samenvatting in een nieuwsbrief of plaats een bericht op een discussiepagina.
Reserveer een directory Informatieveiligheid die voor iedereen toegankelijk is en plaats daar alle relevante documenten.
Zie ook de aanbevelingen in § 2.11 Leef beveiligingsbeleid na.

Toetsingscriteria ZZ3

> *a. De directie stelt het beleidsdocument vast om kaders mee te geven bij de uitwerking en uitvoering van de informatiebeveiliging.*
> *b. De directie communiceert het beleid naar alle medewerkers en alle relevante externe partijen.*
> *c. De directie legt de besluitvorming en datering van het beleidsdocument aantoonbaar vast.*

2.2 Stel vast wie waarvoor verantwoordelijk is (paragraaf 6.1.3)

Praktijkboek NEN 7510

> *Als het al niet in het informatiebeveiligingsbeleid duidelijk is geworden, moet alsnog voor een ieder duidelijk zijn wie waarvoor verantwoordelijk is. Als niemand verantwoordelijk is voor onderwerp X, dan is ook niemand op onderwerp X aanspreekbaar. Vertrouw er niet op dat 'iedereen' zich wel verantwoordelijk voelt. Om te beginnen is dat inefficiënt (dubbel werk bijvoorbeeld) en bovendien zullen weinigen zich ook echt verantwoordelijk voelen als er iets fout gaat!*

Rollen en functies van de verantwoordelijken voor informatieveiligheid en de belangrijkste beveiligingsfuncties worden meestal opgenomen in het IBbeleid. In bijlage B van dit document als voorbeeld een beschrijving van de portefeuillehouder IB, een Functionaris IB (in plaats van de modenaam Security Officer), Functionaris Gegevensbescherming, Coordinator calamiteitenteam ICT, kwaliteitscoordinator en auditor.Maak vooral ook gebruik van een Contactgroep Informatieveiligheid (IB). De groepsleden ondersteunen elkaar bij de uitvoering van beveiligingsvraagstukken. Voor kleine organisaties kunnen dit 2 personen zijn met overlappende functies en rollen, bijvoorbeeld de bestuurssecretaris en de medewerker kwaliteit.

Betrokkenheid medewerkers

In nagenoeg alle organisaties wordt er met nadruk op gewezen dat *alle* medewerkers, dus ook vrijwilligers en extern personeel, verantwoordelijk zijn voor informatieveiligheid. Daarmee wordt het belang duidelijk van de volgende paragraaf: zorg voor bewustwording, kennis en informatie over informatieveiligheid.

Toetsingscriteria ZZ3

> *a. De organisatie heeft taken, verantwoordelijkheden en bevoegdheden met betrekking tot de informatiebeveiliging vastgesteld en toegewezen met als doel de beschikbaarheid, integriteit en vertrouwelijkheid van de persoonsgegevens en overige informatie in de bedrijfsprocessen binnen en buiten de organisatie te waarborgen.*
>
> *b. De organisatie heeft met betrekking tot bedrijfsprocessen of administraties of registraties waarin persoonsgegevens worden bewerkt, een lijnmanager als proceseigenaar en, in de zin van de Wbp, als houder van de registratie aangewezen en heeft de registratie aangemeld bij de Autoriteit Persoonsgegevens of bij een eigen Functionaris Gegevensbescherming.*

2.3 Zorg voor bewustwording, opleiding en training (paragraaf 8.2.2)

Praktijkboek NEN 7510

> *Beveiligen is mensenwerk. Niet alleen voor het opstellen en bewaken van allerlei beveiligingsmaatregelen, maar ook in de alledaagse naleving. Besef dat meer dan de helft van de informatiebeveiligingsincidenten wordt veroorzaakt door eigen medewerkers, meestal niet met kwade bedoelingen maar uit onkunde of onbenul. Informatiebeveiliging is voor tachtig procent mensenwerk en voor twintig procent techniek.*

In het Normboek NEN 7510 is het normelement *Bewustwording, opleiding en training ten aanzien van informatiebeveiliging* als volgt verwoord:

> *Een organisatie die patiëntgegevens verwerkt behoort ervoor te zorgen dat opleiding en training inzake informatiebeveiliging zijn geregeld voor alle medewerkers bij aanvang van het dienstverband en dat regelmatig in opfrissing van die kennis is voorzien.*

Er zijn vele manieren om medewerkers bewust te maken van informatiebeveiliging. Bijvoorbeeld prikkelende slogans op muismatjes, flyers, informatiebrieven, flitsberichten op je beeldscherm, etc. Wat van belang is dat een organisatie in alle redelijkheid kan faciliteren dat medewerkers niet alleen de aangeboden informatie hebben gezien of gelezen maar ook daadwerkelijk tot zich hebben opgenomen. Daarvoor wordt steeds meer gebruik gemaakt van e-learning. Een e-learningcursus is laagdrempelig; nagenoeg alle medewerkers hebben ict-faciliteiten en/of internet thuis en kunnen de e-learningcursus volgen wanneer hun dat uitkomt. e-Learning is ook educatief. Door het aandragen van informatie en het laten beantwoorden van vragen moeten medewerkers wel informatie ‘verwerken’ en tot zich laten doordringen.

Het volgen van een e-learningcursus, inclusief cursusresulaten kun je koppelen aan het HRMsysteem. Heeft een organisatie een eigen Leermanagementomgeving dan gaat dat vanzelf, wordt de cursus gevolgd via een webportaal dan moeten cursusresultaten veelal handmatig via excelsheets gekoppeld aan een HRMsysteem.

Bewustwording levert nagenoeg aan elk onderwerp uit dit hoofdstuk een bijdrage; zie de tabel in bijlage A. Daarbij wordt uitgegaan van twee invalshoeken:

- verplicht; zaken die medewerkers moeten weten middels cursussen en protocollen (4e kolom)
- stimulerend; wat hebben medewerkers nodig om een bijdrage te kunnen leveren aan een betere dienstverlening (5e kolom).

Toetsingscriteria ZZ3

> *a. De organisatie heeft de uitvoering van de werkprocessen en de informatieverwerking geborgd in richtlijnen, procedures, protocollen, standard operating procedures (SOP’s) en ondersteunende techniek.*
> *b. Richtlijnen, procedures, protocollen en instructies zijn voor bevoegde en bekwame medewerkers beschikbaar en worden periodiek geactualiseerd.*
> *c. De organisatie heeft voor gebruikers werkinstructies voor apparatuur en systemen opgesteld om een juist gebruik te bevorderen en om fouten te voorkomen (voor beheerders zie 10.1.1).*
> *d. De leiding ziet er op toe dat medewerkers in het gebruik worden getraind (bekwaam zijn).*
> *e. De organisatie besteedt in het werkoverleg of anderszins periodiek aandacht aan informatieveiligheid, informatiebeveiliging en privacybescherming op de werkplek (uitwerking van 4.4.3)*

2.4 Neem maatregelen tegen kwaadaardige programmatuur (paragraaf 10.4.1)

Praktijkboek NEN 7510

> *Gebeurt meer dan de helft van de informatiebeveiligingsincidenten door toedoen van eigen medewerkers, de rest gebeurt door 'derden'. Inmiddels is er een heuse 'industrie' ontstaan om met kwade bedoelingen informatiebeveiliging te omzeilen. Gezondheidszorg is in toenemende mate een aantrekkelijke prooi. Vaak – en wellicht steeds vaker – wordt hierbij gebruikgemaakt van kwaadaardige programmatuur: virussen, wormen, spyware, Trojaanse paarden en vele andere vormen van 'malware'.*

Veel ellende is te voorkomen met maatregelen die kant-en-klaar te koop zijn. Voer ze vandaag nog in en zorg – net zo belangrijk – dat alle instrumenten om je te beschermen tegen kwaadaardige programmatuur ook up-to-date zijn en blijven.

Gericht op medewerkers

Wanneer is een site betrouwbaar?

> Voor het verzenden van gevoelige informatie, zoals je creditcardgegevens, is het belangrijk dat je gebruik maakt van een beveiligde internetverbinding. Dan staat er https:// in de adresbalk van je browser in plaats van het normale http://. Bij de meeste browsers zie je ook een slotje in de adresbalk of onderin in het browserscherm.
> Kijk voor meer informatie op www.alertonline.nl

Risico's internet

- Het gebruik van internet brengt altijd risico's met zich mee; denk aan:
- Het onbewust binnenhalen van ongewenste software die de prestatie van je PC of het netwerk kan beïnvloeden of zelfs het hele internetverkeer kan platleggen.
- Het onbewust binnenhalen van software die zich als een 'spion' gedraagt en kan meekijken met wat je doet of hebt opgeslagen.

Surf op safe!

- Laat nooit vertrouwelijke of gevoelige informatie achter op internet.
- Laat websites waarvan je de betrouwbaarheid in twijfel trekt links liggen.
- Download geen (illegale) software; er kunnen virussen in zitten en het kan je werkgever juridisch in problemen brengen.

Toetsingscriteria ZZ3:

> *a. De organisatie heeft beschermingsmaatregelen getroffen om kwaadaardige software (waaronder virus, spyware en andere malware) te detecteren en de gevolgen hiervan te mitigeren.*
> *b. De organisatie heeft beschermingsmaatregelen getroffen tegen andere inbreuken die de informatieveiligheid kunnen aantasten zoals: hacken, phishing, social engineering enz.*
> *c. De organisatie houdt de beschermingsmaatregelen up to date conform de nieuwste definities en inzichten en logt detectie en verwijdering van kwaadaardige software.*
> *d. De organisatie controleert periodiek de werking van de beschermingsmaatregelen en herstelt waar nodig de negatieve gevolgen van kwaadaardige software en andere inbreuken.*
> *e. De organisatie informeert de gebruikers over schadelijke software en mogelijke risico's (aansluitend op 8.2.2.).*

2.5 Sluit overeenkomsten af voor dienstverlening en communiceer veilig

Praktijkboek NEN 7510

In veel gevallen is de organisatie de 'houder' van gevoelige gegevens (bijvoorbeeld patiënt gegevens). Daarvoor geldt een hele reeks aan voorwaarden en maatregelen. In de communicatie van diezelfde gevoelige gegevens met anderen, gelden voor de houder dezelfde voorwaarden en maatregelen nog steeds: ze houden echt niet op bij de voordeur. Het dragen van verantwoordelijkheden die uit informatiebeveiliging voortvloeien, is alleen mogelijk op basis van heldere afspraken met de communicatiepartners. Als er geen afspraken met therapeut X bestaan, is niets te zeggen over hoe betrouwbaar hij met 'uw verantwoordelijkheden' omgaat.

2.5a Sluit overeenkomsten af voor dienstverlening (6.2, 10.2 en 10.8)

Als gebruik wordt gemaakt van diensten van een externe partij zal er een overeenkomst zijn afgesloten met een service level agreement (sla) voor bijvoorbeeld afspraken over de gewenste beschikbaarheid van de dienstverlening.

Als de dienstverlenende partij persoonsgegevens bewaart of kan bewerker is vanaf januari 2016 een bewerkersovereenkomst (bwo) verplicht. In de bwo worden afspraken gemaakt tussen de 'Verantwoordelijke' (zorginstelling) en de 'Bewerker' (dienstverlener) van de persoonsgegevens. Daarbij ligt het accent op de vertrouwelijkheid, de privacyaspecten. Meestal zijn het aparte overeenkomsten, soms is het een aanvulling op een bestaand contract. Naast bwo's van leveranciers kan ook worden uitgegaan van modellen. De NVZ- en ActiZmodellen kunnen ook worden gebruikt door niet-leden.

In de bwo's is onder anderen opgenomen hoe de Bewerker de beveiligingsaspecten heeft geregeld en hoe de Verantwoordelijke dat kan controleren om aan zijn wettelijke verplichting te voldoen. In de bwo's die sommige cloudleveranciers aanbieden is sprake van een wederkerige verantwoordelijkheid: ook de Bewerker krijgt de mogelijkheid om na te gaan of de Verantwoordelijke zijn beveiligingszaken op orde heeft. In het gunstigste geval wordt die beoordeling overgelaten aan een onafhankelijk partij, een z.g. Trusted Third Part (TTP). Dit soort bwo's is opgesteld op basis van samenwerking en partnerschap; wederkerigheid in de betekenis van elkaar vertrouwen. Het is te verwachten dat dit in de toekomst steeds belangrijker wordt maar de huidige realiteit is dat het beveiligingsniveau van de doorsnee care-instelling niet in verhouding staat tot die van de cloudleveranciers en daarom wederkerigheid met betrekking tot informatieveiligheid in veel gevallen niet reëel is. Zeker niet in het juridische deel van het contract. Een alternatief zou kunnen zijn om in een appendix een aantal beveiligingsmaatregelen te benoemen waaraan de verantwoordelijke stelt zich te houden; zie bijvoorbeeld de beveiligingseisen die een leverancier stelt aan haar onderaannemers.

Aandachtspunten

a. Bepaal in overleg met de leverancier van welke overeenkomst gebruik wordt gemaakt, van een basismodel of van het leveranciersmodel; in beide gevallen wellicht aangevuld met specifieke wensen.

b. Zorgt dat de overeenkomsten in lijn zijn met de mate van beveiliging die de organisatie wenst in termen van beschikbaarheid, integriteit en vertrouwelijkheid / privacy.

Het volgende geldt voor bwo's:

c. Vermeld expliciet wanneer en vooral hoe Verantwoordelijke en Bewerker elkaar informeren over mogelijke datalekken.

d. Verantwoordelijke heeft de wettelijke taak toe te zien op de naleving van privacyaspecten van haar cliënten (10.2). Dus ook toezien op hoe de Bewerker dit heeft geregeld. Neem dit op in de overeenkomst en maak hier ook gebruik van!

e. Mei 2018 wordt de Europese Privacyverordening van kracht (AVG). Daarin onderstaande punten die moeten voorkomen in een bwo. Omdat bwo's vaak een langere looptijd hebben die punten nu al opnemen. Zie ook de factsheet *Impact van de Europese Privacyverordening* van ICT&Recht:
   de doeleinden ven de gegevensverwerking;
   het soort persoonsgegevens die verwerkt worden;
   de categorieën van betrokkenen op wie de gegevens zien;
   het passend beveiligen van de gegevens;
   het uitvoeren van audits bij de Bewerker (en beschikbaar stellen aan de Verantwoordelijke)
   het na afloop vernietigen of terugleveren van de gegevens aan de Verantwoordelijke.

f. Stem de aansprakelijkheidsparagraaf af met de aansprakelijkheidsverzekeraar van de organisatie.

g. Laat de bedrijfsjurist altijd een laatste blik werpen op de overeenkomst.

2.5b Maak afspraken over gegevensuitwisseling (10.8)

De NEN 7512, *de vertrouwensbasis voor gegevensuitwisseling*, levert een nadere invulling voor een aantal normelementen van de NEN 7510 waarvan de belangrijkste de 10.8.

De NEN 7512 is vooral van belang als een zorgorganisatie samen met een externe partij een verbinding opzet voor het uitwisselen van zorggegevens. De norm geeft in detail aan, op basis van de classificatie van de te communiceren gegevens, welke vooral technische maatregelen nodig zijn voor een veilige communicatie. Als gebruik wordt gemaakt van bestaande dienstverlening zoals Vecozo zal zijn voldaan aan deze norm.

Organisaties moeten alert zijn op het uitwisselen van zorginformatie via *onveilige* kanalen zoals via email medische gegevens van een cliënt uitwisselen met een huisarts. Als geen gebruik wordt gemaakt van een veilige emaildienst zoals Zorgmail kan dit een potentieel datalek zijn.

<u>Aandachtspunten</u>

a. Inventariseer met welke partijen en vooral met welke personen buiten de organisatie zorginformatie wordt uitgewisseld en op welke manier. Denk ook aan het sociaal domein en aan familie of mantelzorgers van de cliënt.

b. Verbied het *versturen* van zorginformatie via email, fax of post; mits voorzien van beschermende maatregelen zoals encryptie van het emailbericht en een aangetekend poststuk.

c. Maak afspraken hoe om te gaan met het 'onveilig' *ontvangen* van zorginformatie; verwerk de informatie maar verwijder de bron en neem contact op met de afzender om herhaling te voorkomen.
   Alternatieven zijn bijvoorbeeld:
   - De Vecozo Berichtenbox (een gratis dienst, niet te verwarren met het Berichtenverkeer)
   - Zorgmail of een vergelijkbare regionale dienstverlener (commercieel)
   - eGPO; het elektronisch Gestructureerd Patiënten Overlegis een webapplicatie, bedoeld voor zorgverleners om de communicatie tussen zorgverleners onderling én tussen zorgverleners en patiënten te vereenvoudigen
   - Cliëntportalen

   NB wees alert op nieuwe ontwikkelingen; zie rapport RZCC.
   https://www.zivver.com/201607_RZCC_Veilig-mailen-in-de-zorg.pdf

d. Maak protocollen hoe om te gaan in bijzondere situaties. Bijvoorbeeld in geval van een spoedopname dossiergegevens van de cliënt meegeven aan de begeleider of ambulancemedewerker.

e. WhatsApp versleutelt alle berichten! Toch wordt WhatsApp niet als 100% veilig beschouwd. Maak gebruik van een messenger app zoals Signal of een messenger app die speciaal is ontwikkeld voor gebruik in de gezondheidszorg zoals Siilo, Kanta Messenger of MD Linking.

f. Informeer alle betrokkenen bij de organisatie over het veilig communiceren van zorggegevens; wijs op de gevaren (niet voldoen aan de Wgbo en Wbp) en reik alternatieven aan. Maak gebruik van de mogelijkheden zoals opgesomd bij het normelement Bewustwording (8.2.2). Met name de e-learningcursus *Veilig omgaan met vertrouwelijke informatie* gaat vanuit verschillende invalshoeken in op veilige communicatie.

Opmerking
Ook de NEN 7512 is, evenals de NEN 7513 (logging), gratis verkrijgbaar via de websites van NEN en VWS.

Toetsingscriteria ZZ3

6.2.3
a. De organisatie contracteert diensten in het kader van informatievoorziening volgens een vaste procedure waarbij eisen en afspraken met meetbare criteria worden vastgelegd in een onderliggende service level agreement (SLA) (zie ook 10.2.1 t/m 10.2.3).
b. De organisatie volgt voor wijzigingen in de overeenkomsten met betrekking tot dienstverlening, criteria en rapportering een wijzigingsprocedure die waarborgt dat deze niet eenzijdig worden doorgevoerd.
c. De organisatie legt afspraken met betrekking tot gepland onderhoud en de gevolgen voor beschikbaarheid van systemen in overeenkomsten schriftelijk vast.

10.2.1
a. De organisatie heeft (aansluitend op 6.2.3) het belang en het niveau van beveiliging alsmede de uitvoering daarvan met de externe partij besproken en vastgelegd in de schriftelijke overeenkomst inclusief bijlagen.

10.2.2
a. De organisatie controleert en beoordeelt de dienstverlening door externe partijen periodiek en daar waar nodig tussentijds.

10.8.1
a. De organisatie heeft beleid voor het beschikbaar stellen en/of het uitwisselen van gegevens binnen de organisatie en met derden.
b. Het beleid geeft aan welke soorten gegevens in aanmerking komen voor uitwisseling, met welke partijen (zorginstellingen, leveranciers en andere externen) en voor welk doel gegevens worden uitgewisseld en welke voorwaarden gelden bij welke soorten gegevens.
c. De organisatie heeft overzicht welk (medisch of niet medisch) apparaat of installatie welke informatie ontsluit en op welke wijze deze informatie wordt uitgewisseld (ondermeer via koppelingen, verbindingen, protocollen, portals, in the cloud).

10.8.2
a. De organisatie heeft de verantwoordelijkheden en bevoegdheden voor het beschikbaar stellen en veilig uitwisselen van gegevens (en programmatuur) vanuit de verschillende registraties / verwerkingen met derden belegd.
b. De organisatie legt de afspraken vast in een overeenkomst met de derde partij waarin de verantwoordelijkheden, rechten en plichten van beide partijen eenduidig beschreven zijn en waarin is opgenomen hoe gegevensuitwisseling veilig tot stand komt en hoe inzage en bewerking van de gegevens door bevoegden is geregeld.

c. Beide partijen controleren de integriteit van de uit te wisselen gegevens en hebben procedures om niet integere gegevens te herstellen.

10.8.4
a. De organisatie beveiligt uitwisseling van elektronische berichten om kwaliteit en vertrouwelijkheid te beschermen (zie 10.8.1 en 10.8.2).

2.6 Beveilig de toegang tot systemen (paragrafen 11.3.1, 11.5.2 en 11.5.3)

Praktijkboek NEN 7510

Elke geregistreerde gebruiker dient een unieke gebruikersidentificatie te krijgen, die slechts persoonsgebonden is of persoonlijk mag worden gebruikt. Groepsaccounts en dergelijke zijn dus verboden!

Met authenticatie kan een gebruiker 'bewijzen' dat hij degene is die hij claimt te zijn. Er bestaan sterkere en zwakkere vormen van authenticatie. De norm vereist ten minste een wachtwoordsysteem als authenticatie. Zwakkere vormen zijn dus niet toegestaan, sterkere verdienen de voorkeur. Wanneer gekozen wordt voor een wachtwoordsysteem, dan wordt aangeraden om de norm NEN-EN 12251 toe te passen voor verdere uitwerking.

In het proces van identificeren en authenticeren worden uiteraard systemen gebruikt die op hun beurt zeer goed, misschien wel bijzonder goed moeten worden beheerd en beveiligd. Het gaat om de sleutel van het sleutelkastje, zogezegd: als je die sleutel te pakken krijgt, krijg je de beschikking over alle sleutels!

De organisatie dient ervoor te zorgen dat 'passende' gewoontes worden gebruikt bij het kiezen en gebruiken van wachtwoorden, dat gebruikers niet elkaars identificatie- en authenticatiemiddelen gebruiken en dat gebruikers niet hun identificatie- en authenticatiemiddelen overdragen aan anderen.

Het Praktijkboek stelt in de eerste alinea dat groepsaccounts niet zijn toegestaan. De toelichting in het Normboek is iets genuanceerder; zie *Aandachtspunten en aanbevelingen voor implementatie* in § 11.5.2. Het verbod geldt voor informatiesystemen die patiëntgegevens verwerken. En ook dan zijn er uitzonderingsgevallen mogelijk; óf omdat unieke traceerbaarheid niet nodig is (bijvoorbeeld alleen leestoegang) óf aanvullende beheersmaatregelen zijn getroffen met uiteindelijk het gewenste effect.

Gericht op medewerkers

- Ga zorgvuldig om met je bevoegdheden; wees je bewust van je verantwoordelijkheid.
- Geef iemand die dat formeel niet mag geen toegang tot jouw gegevens en bestanden. Als dat wel nodig is dan kan dat via de beheerder geregeld worden.
- Als je weet dat er een kans bestaat op misbruik van je wachtwoord, bijvoorbeeld omdat iemand heeft meegekeken, verander dan je wachtwoord.
- Bedenk dat het veilig omgaan met wachtwoorden óók betekent dat jij geen oneigenlijk gebruik maakt van het wachtwoord van iemand anders. Ook niet om te kijken hoe het gaat met een cliënt van een collega waarbij je je betrokken voelt.

Toetsingscriteria ZZ3

11.3.1
a. Lijnmanagement wijst de medewerkers op het belang van het gebruik van adequate wachtwoorden en bijbehorend gedrag.
b. De organisatie dwingt waar mogelijk technisch het gebruik van sterke wachtwoorden af en van periodieke vernieuwing.
c. Lijnmanagement ziet toe op de naleving van adequate wachtwoorden.
11.5.2

a. Elke gebruiker binnen de organisatie logt in, op het netwerk en op de mailaccount en de gedeelde documenten in de kantooromgeving, met een persoonlijke gebruikersnaam en een sterk wachtwoord.
b. De organisatie maakt elke medewerker / gebruiker bevoegd voor die verwerkingen en/of applicaties die noodzakelijk zijn ter ondersteuning van de werkzaamheden (zie ook 11.6.1).
c. Afhankelijk van de verwerking en/of de applicatie wordt bij het inloggen aanvullende authenticatie (in de zorg b.v. BIG-registratie) gevraagd.
11.5.3
a. De organisatie zorgt dat vereiste wachtwoordconventies waar mogelijk door systeeminstellingen worden ondersteund en afgedwongen.

2.7 Zorg voor continuïteitsvoorzieningen (paragraaf 14.1.3)

Praktijkboek NEN 7510

> *Informatiebeveiliging is niet alleen beveiligen tegen inbreuk van buitenaf, maar ook zorg dragen dat informatievoorziening zo veel mogelijk ongestoord kan verlopen. Een van de aspecten die hiertoe worden gerekend, is continuïteit. Hierbij speelt een scala aan activiteiten zoals back-ups, noodstroom, uitwijkcentrum en redundantie.*

De eerste en belangrijkste aanzet voor continuïteitsbeheer is ervoor te zorgen dat medewerkers weten waar ze bij hun werkzaamheden afhankelijk van zijn en dat ze bekend zijn met alternatieven.

Bijvoorbeeld:
- Papieren nooddossier als back-up voor het digitale dossier; per lokatie in een afgesloten kast
- Extramuraal: looplijsten met toegang- en zorginformatie dagelijks beschikbaar bij recepties
- Intramuraal: medicatielijsten dagelijks beschikbaar per locatie in een afgesloten kast.

Opmerking

Voor het formeel inrichten van continuïteitsbeheer in een latere fase kan worden uitgegaan van tabel 1 van het BBMCare Inventarisatie & Classificatiedocument Informatieveiligheid. Daarin zijn vanuit de processen de bijbehorende informatieobjecten (zowel applicaties als informatie) benoemd, mét de gewenste betrouwbaarheidsvereisten. De objecten met beschikbaarheidseis Hoog en Zeer Hoog komen in aanmerking voor continuïteitsmaatregelen.

Gericht op medewerkers

Communiceer naar betrokkenen de continuïteitsmaatregelen die de organisatie reeds getroffen heeft.

Faciliteer discussies over de continuïteit van de dienstverlening, over het omgaan met onverwachte situaties. Benadruk de eigen verantwoordelijkheid.

> "*Meestal ben juist jij degene die goed kan inschatten wat in de gegeven situatie het beste is; vertrouw op je onderbuikgevoel. Als je om welke reden dan ook besluit later terug te komen of als je vindt dat de politie moet worden gebeld, koppel dat altijd terug binnen je team of organisatie".*

Toetsingscriteria ZZ3

> *a. De organisatie heeft als onderdeel van de continuïteitsplannen (zie 14.1.1a) (nood)procedures en workarounds ontwikkeld en geïmplementeerd om in geval van ICT-verstoring en/of andere verstoringen de continuïteit van de (kritische) bedrijfsprocessen zo ver als mogelijk te handhaven en de oorza(a)k(en) van verstoring zo snel mogelijk weg te nemen.*
> *b. De organisatie heeft voorzieningen om de bereikbaarheid van en communicatie met medewerkers die over specifieke kennis beschikken zeker te stellen.*
> *c. Medewerkers met kennis van vitaal belang zorgen er ten aller tijde voor bereikbaar te zijn.*

2.8 Houd rekening met intellectueel eigendom (paragraaf 15.1.2)

Praktijkboek NEN 7510

Er zijn twee levensgrote bezwaren tegen het gebruik van 'gepiratiseerde' software. Ten eerste is de herkomst veelal schimmig, waardoor eenvoudig kwaadaardige programmatuur kan binnensluipen. Ten tweede kunnen rechthebbenden bij vermoeden van inbreuk op intellectuele rechten, onmiddellijke inbeslagname vorderen van de apparatuur waarop de gepiratiseerde software zich bevindt (de continuïteit is dan ver te zoeken). Verder spelen andere risico's, zoals strafrechtelijke vervolging en reputatieschade.

Toetsingscriteria

a. De organisatie heeft beleid ten aanzien van verwerving en gebruik van materiaal en programmatuur waarop intellectuele eigendomsrechten van derden berusten, waaronder software en licenties (zie ook 12.5.5).
b. De organisatie legt de daaruit voortvloeiende verplichtingen vast, toetst het rechtmatig gebruik en komt de verplichtingen na.
c. De organisatie heeft afgedwongen dat contractpartners de verplichtingen met betrekking tot intellectuele eigendomsrechten van andere partijen nakomen en de organisatie vrijwaart voor eventuele aanspraken van de rechthebbende.
d. De organisatie maakt bij in- en uitdiensttreding met medewerkers zo nodig afspraken over intellectuele eigendomsrechten.

2.9 Beveilig bedrijfsdocumenten (paragraaf 15.1.3)

Praktijkboek NEN 7510:

Belangrijke bedrijfsdocumenten moeten worden beveiligd tegen verlies, vernietiging en vervalsing (denk hierbij aan accountingbestanden, declaraties, medische dossiers, dag lijsten, transactielogbestanden, auditlogbestanden en operationele procedures). Elektronisch opgeslagen gegevens moeten 'digitaal duurzaam' zijn, eventuele encryptiesleutels moeten ook worden bewaard en gegevens kunnen worden opgevraagd op een wijze die geschikt is voor juridische procedures.

Medische dossiers dienen 15 jaar bewaard te worden vanuit het oogpunt van de WGBO. Voor toedienlijsten is de bewaartermijn minimaal 2 jaar. Vanuit de WBP is er geen wettelijke termijn voor het bewaren van persoonsgegevens. Organisaties kunnen hier zelf invulling aangeven mits er vanuit andere wetten en richtlijnen geen verplichte termijnen zijn. Denk bijvoorbeeld aan de archiefwet of de fiscale bewaarplicht. Vanuit de fiscale bewaarplicht moeten loongegevens 7 jaar worden bewaard. Daar bovenop geldt dat gegevens niet langer mogen worden bewaard dan noodzakelijk. Zo moeten medische dossiers na 15 jaar worden vernietigd en heeft een cliënt het recht om een dossier eerder te laten vernietigen.

Meer informatie via onderstaande links.
Autoriteit Persoonsgegevens:
https://autoriteitpersoonsgegevens.nl/nl/over-privacy/persoonsgegevens/bewaren-van-persoonsgegevens

Inspectie gezondheidszorg:
http://www.igz.nl/actueel/veelgestelde-vragen/bewaartermijn-toedienlijsten-en-nullijsten/

WGBO:
https://www.knmg.nl/advies-richtlijnen./praktijkdilemmas/praktijkdilemma/hoe-lang-moet-ik-medische-dossiers-van-patienten-bewaren.htm

Belastingdienst:
http://www.belastingdienst.nl/wps/wcm/connect/bldcontentnl/belastingdienst/zakelijk/ondernemen/administratie/administratie_opzetten/hoe_lang_moet_u_uw_administratie_bewaren

Toetsingscriteria ZZ3

a. De organisatie hanteert richtlijnen en procedures voor de totstandkoming, identificering en archivering van (al dan niet formele) documenten en voor de fysieke en logische beveiliging daarvan (zie ook 7.2.1 en 2).
b. De organisatie hanteert richtlijnen en procedures voor de totstandkoming, archivering en naslag van beleid, richtlijnen, procedures en protocollen die noodzakelijk zijn voor adequate en veilige uitvoering van de bedrijfsprocessen.
c. De organisatie evalueert en reviseert richtlijnen, procedures en protocollen periodiek.
d. De organisatie hanteert relevante bewaartermijnen voor formele bedrijfsdocumenten.

2.10 Bescherm persoonsgegevens (paragraaf 15.1.4)

Praktijkboek NEN 7510

> *In het algemeen volgt de plicht tot bescherming van persoonsgegevens uit de Wet bescherming persoonsgegevens (Wbp), in het bijzonder uit de Wet geneeskundige behandelingsovereenkomst (Wgbo). Hoewel beoefenaren van individuele beroepen in de gezondheidszorg de verwerking van persoonsgegevens van hun patiënten niet hoeven te melden, zijn zij wel verplicht om de persoonsgegevens van hun patiënten adequaat te beschermen. Het Autoriteit Persoonsgegevens (AP) heeft hiervoor materiaal beschikbaar*

Stel Privacyreglementen op voor persoonsgegevens cliënten en medewerkers, eventueel ook van vrijwilligers.
Maar ook procedures voor toegang, inzage, overdracht en afschrift cliëntdossiers.
Via internet zijn diverse voorbeelddocumenten te vinden; raadpleeg ook de website van de AP.

Betrokkenheid medewerkers
Neem in het privacybeleid een hoofdstuk FAQ's op; vul dit naar aanleiding van problemen en vragen vanaf het zorgveld. Medewerkers zullen eerder de FAQ's inkijken dan een formeel reglement, zeker als ze er zelf aan hebben bijgedragen!

Mogelijke onderwerpen:
Het Zorgdossier

- Welke gegevens horen in het zorgdossier?
- Hoe moet ik de zorgdossiers bewaren?
- Dossierplicht?
- Overdragen van het zorgdossier?
- Wanneer mag je iemand wel informeren en wanneer niet?
- Van wie is het Zorgdossier?
- Wie mag lezen in / heeft toegang tot het dossier?
- Mag je familie informatie geven over hoe het met de cliënt gaat?

Eerste contactpersoon

- Wie kan 1e contactpersoon zijn?
- Wat zijn de taken van een 1e contactpersoon?
- Wat wordt er met de toestemming of adviezen van de 1e contactpersoon gedaan?
- Verwachtingen van de 1e contactpersoon naar jou?
- Wat mag jij verwachten van een 1e contactpersoon?

Zie ook de eerste 4 casussen e-learningcursus IB en de Nedap bewustwordingsfilmpjes op YouTube:
https://www.youtube.com/results?search_query=nedap+privacy

Inspirerend is het een VNG initiatief dat 22 juni 2016 tijdens de Bestuurlijke conferentie '*In goed vertrouwen. De privacy van de jeugd geborgd*' van start is gegaan.
https://vng.azavista.com/event_website_pages/view/5719f8c5-09f0-4580-91d5-357eac110004/5719f839-64f4-4646-9abe-357eac110004/598fae3d46

Toetsingscriteria ZZ3

> *a. De organisatie heeft maatregelen getroffen ter bescherming van vertrouwelijke persoonsgegevens en overige vertrouwelijke informatie (zie ook 8.1.2, 8.1.3, 8.2.1, 8.2.2, 9.1.1 en 9.2.1).*
> *b. De organisatie hanteert richtlijnen en procedures waarin is vastgelegd onder welke omstandigheden toestemming wordt verleend voor het uitwisselen van persoonsgegevens.*
> *c. De organisatie heeft een regeling voor het melden en opvolgen van privacy-incidenten.*

2.11 Leef beveiligingsbeleid na (paragraaf 15.2.1)

Praktijkboek NEN 7510

Tachtig procent van de beveiligingsincidenten wordt veroorzaakt door mensen. Zonder het organiseren van een vorm van controle zal men zich minder goed aan de regels houden. Verantwoordelijken voor de verschillende beveiligingsprocedures moeten ten eerste hun zaakjes goed voor elkaar hebben. En ten tweede moeten deze verantwoordelijken periodiek op een objectieve en onpartijdige wijze worden beoordeeld.

Betrokkenheid medewerkers

Maak informatieveiligheid bespreekbaar; draag bij aan een werkomgeving waarin het vanzelfsprekend is om beveiligingsincidenten te melden én te bespreken. Informatieveiligheid kan een vast agendapunt zijn bij werkoverleg. Of breng informatieveiligheid zo nu en dan ter sprake tijdens de koffiepauze. Bijvoorbeeld naar aanleiding van een bewustwordingscursus.

Gespreksonderwerpen kunnen zijn:

- Houd geen eigen administratie over cliënten bij.
- Neem geen vertrouwelijke informatie over cliënten mee naar huis.
- Print niet onnodig vertrouwelijke cliëntinformatie.
- Laat vertrouwelijke cliëntdocumenten niet onbeheerd achter; dit geldt zowel op de werkplek als bij print-, kopieer- en faxapparatuur.
- Gooi vertrouwelijke cliëntdocumenten alleen weg in een afgesloten bak of papierversnipperaar.
- Vind je vertrouwelijke cliëntgegevens daar waar je deze niet verwacht? Meld dit!

Toetsingscriteria ZZ3

a. De organisatie heeft een ISMS ingericht (zie 4.1 t/m 4.7.3).
b. De organisatie beschikt over informatiebeveiligingsbeleid dat mede is afgestemd op relevante wet- en regelgeving en normen (zie 5.1.1 en 5.1.2).
c. De organisatie heeft mede op basis van risicoanalyse passende beheersmaatregelen getroffen (zie 6.1.1 t/m 15.3.2).
d. De organisatie voert een auditprogramma uit dat, aansluitend op het ISMS, de werking en doeltreffendheid van de beheersmaatregelen toetst.
e. De organisatie ziet op deze wijze toe op de naleving van het informatieveiligheidsbeleid.

2.12 Rapporteer beveiligingsincidenten (paragraaf 13.1.1)

Praktijkboek NEN 7510

> *Zonder rapportage van incidenten zal er niets kunnen worden geleerd en aangepast binnen de organisatie. Het rapporteren van (bijna)ongelukken behoort tot het reguliere professionele handelen.*

Het rapporteren van beveiligingsincidenten heeft als doel om gebreken en zwakheden die verband houden met de informatievoorziening zodanig kenbaar te maken dat corrigerende maatregelen kunnen worden genomen. Het acteren op incidentmeldingen is een belangrijke motor voor het verbeteren van de informatiebeveiliging.

Als gevolg van de uitbreiding van de Wbp met de meldplicht datalekken is extra aandacht nodig voor incidenten waarbij het vermoeden bestaat dat het er sprake kan zijn van een datalek. De wet spreekt van een datalek wanneer *persoonsgegevens* verloren raken of onrechtmatig worden verwerkt; ook wanneer niet met zekerheid gesteld kan worden dat hiervan geen sprake is. Onder onrechtmatige verwerking valt onder andere het aanpassen en/of veranderen van persoonsgegevens en onbevoegde toegang tot, of afgifte van deze gegevens.

Met deze brede omschrijving valt dus veel onder de definitie datalek. Denk hierbij aan verlies van mobieltjes van medewerkers, gestolen laptops met gegevens van cliënten, verlies van een USB-stick in de trein, of het sturen van een mail waarin de adressen van anderen zichtbaar zijn. Ook een calamiteit binnen de organisatie zoals een brand waarbij persoonsgegevens verloren zijn gegaan en er geen back-up beschikbaar is, ziet de wet als een datalek.

De Wbp gaat mei 2018 plaatsmaken voor een Europese privacyverordening, de Algemene Verordening Gegevensbescherming (AVG). De AVG geeft een iets andere invulling aan de meldplicht. Als een laptop, beveiligd met toegangscode en password, wordt gestolen en het is niet duidelijk of de beveiliging is doorbroken, moet dit onder de Wbp worden gemeld als datalek. Als de AGV van kracht wordt moet de melding wel intern als een datalek worden geregistreerd maar pas als een lek manifest wordt, melden aan de Autoriteit Persoonsgegevens.

Aandachtspunten

a) Leg beveiligingsincidenten vast op een centrale plek in de organisatie.
Wijs een persoon of dienst (bijv. helpdesk, receptie) aan waar beveiligingsincidenten kunnen worden gemeld. Het is handig vooraf op basis van de meest voorkomende meldingen enkele categoriën te benoemen; bijvoorbeeld besmetting van spyware of virussen, verlies of diefstal van ITmiddelen, etc. Zie ook de voorbeelden in het Normboek NEN 7510. Sluit eventueel aan op een bestaand meldingensysteem zoals Topdesk; meldingen kunnen ook eenvoudig worden opgenomen in een Excelsheet.

b) Beoordeel beveiligingsincidenten periodiek. Neem in het regulier overleg van bijvoorbeeld de Contactgroep IB als vast agendapunt ‘Evaluatie incidenten’ op.

c) Bereid je voor op het melden van een datalek aan de AP.
Als zich een datalek voordoet moet je binnen enkele dagen actie ondernemen en als er een weekend tussen zit misschien nog dezelfde dag. Wijs een medewerker aan als Functionaris Gegevens-bescherming en maak een protocol voor de afhandeling. Uitgebreide informatie is te vinden via https://ictrecht.nl/factsheets/impact-van-de-meldplicht-datalekken/.

Onderstaande link verwijst naar een praktisch document met aansprekende voorbeelden.
https://www.lhv.nl/service/handreiking-meldplicht-datalekken-de-eerstelijnszorg

Nog enkele opmerkingen over datalekken en de acties binnen de organisatie wanneer zich een voorval of situatie voordoet die *mogelijk* een datalek kan blijken te zijn.

- Omdat je niets wilt missen moeten de meldingen laagdrempelig zijn (bij twijfel melden!); maak een emailadres mogelijkdatalek@organisatienaam.nl aan en laat dit binnenkomen bij de leden van de Contactgroep IB.
- Instrueer medewerkers in de melding transparant te zijn over het voorval. Meldingen moeten vooral feitelijk zijn en geen conclusies bevatten over oorzaken of schuldigen. Die laatste aspecten kunnen pas na onderzoek door FG of Contactgroep IB worden getrokken op basis van onderzoek van het gehele feitencomplex.
- De FG beoordeelt, eventueel samen met leden van de Contactgroep IB, of het ook werkelijk om een datalek gaat, gemeld moet worden aan de AP en eventueel aan betrokkenen.
- Het laatste wat je wilt is onnodig de benadeelde personen informeren; neem de tijd voor die afweging, het hoeft niet meteen.
- Als bij het datalek ook een Bewerker is betrokken zal in de betreffende Bewerkersovereenkomst zijn opgenomen hoe je elkaar kunt informeren, welke informatie de bewerker aan de organisatie moet verstrekken zodat de organisatie op correcte wijze kan melden bij de AP.
- Archiveren; afhankelijk van de aard van de melding is de bewaartermijn 1 tot 3 jaar.

d) Communiceer ook voorbeelden van datalekken die NIET gemeld hoeven te worden; bijvoorbeeld:
- Een brief met daarin persoonsgegevens wordt naar een foutief adres gestuurd, en wordt duidelijk ongeopend, retour gezonden.
- Iemand laat een koffer met daarin persoonsgegevens achter in de trein. De koffer is voorzien van een deugdelijk slot en komt via 'gevonden voorwerpen' ongeopend terug bij de rechtmatige eigenaar.
- Als een zorgmedewerker gebruik maakt van het wachtwoord van een behandelaar om toegang te krijgen tot medische persoonsgegevens, dan is er niet zo zeer sprake van een datalek, als van schending van interne voorschriften. In eerste instantie liggen dan disciplinaire maatregelen voor de hand.

Betrokkenheid medewerkers

e) Informeer alle medewerkers, vrijwilligers en extern personeel over de meldingsprocedure voor beveiligingsincidenten; benadruk de gezamenlijke verantwoordelijkheid.

f) Informeer alle medewerkers, vrijwilligers en extern personeel apart over de meldplicht datalekken. Benadruk de wettelijke verplichting en het spoedeisende karakter. Maak aansprekende voorbeelden van mogelijke datalekken. Geef als motto mee: *bij twijfel melden*!

g) Organiseer discussies, bijvoorbeeld middels een eenvoudige enquête: ‘Ben je een datalek?
Vragen kunnen zijn:
- Heb je het afgelopen jaar wel eens in een privéomgeving je cliënten besproken? (nooit, 1x, vaker)
- Laat je wel eens privacy-gevoelig documenten slingeren bij de copyeermachine? (nooit, 1x, vaker)

Afhankelijk van de score een luchtige tekst met als kern : Gefeliciteerd. . . , prima maar wees alert. . . . . , tja, verander je gewoonten . . .

h) Vast agendapunt team- of werkoverleg; maak gebruik van de periodieke evaluatie intern maar vooral van voorbeelden van beveiligingsincidenten uit de pers.

Toetsingscriteria ZZ3

a. De organisatie hanteert definities voor informatie-incidenten (zie ook normtekst NEN 7510 hoofdstuk 2; extern document).
b. De organisatie heeft procedures voor het melden van informatie-incidenten en het organiseren van opvolging; extra aandacht voor mogelijke datalekken..
c. Medewerkers melden informatie-incidenten volgens procedures via geëigende kanalen.
d. De organisatie legt informatie-incidenten afdelingsoverstijgend vast.
e. De organisatie hanteert een disclosureprocedure in het geval een informatie-incident negatieve gevolgen heeft voor de behandeling en/of schade toebrengt aan de patiënt.

Bijlage A

Overzicht Handvatten & betrokkenheid medewerker & NEN 7510

In de 3e kolom is de verwijzing opgenomen naar de paragraaf cq handvat dat hierop betrekking heeft.
Tussen haakjes is het normelement uit de NEN 7510 dat hierop van toepassing is.
In de laatste kolom is aangegeven welk casus uit de bewustwordingscursus
Veilig omgaan met vertrouwelijke informatie dit onderwerp ondersteunt; zie ook bijlage B.

Wat heeft een zorgmedewerker nodig om goede zorg te leveren?	***Wat moet de organisatie daarvoor regelen?***	***Verwijzing Handvat en § NEN 7510***	***Wat moeten zorg-medewerkers weten? 3 (8.2.2)***	***Hoe kunnen zorgmedewerkers bijdragen aan een betere dienstverlening? 3 (8.2.2)***	***Verwijzing e-learning cursus***
Ik wil kunnen vertrouwen op de kantoorautomatisering; ik wil me niet druk hoeven maken over phising-mails; daar hebben we toch de ITmedewerkers voor?	Firewall, antivirus sw,	4 (10.4.1)	Tips om malware te herkennen, regelmatig informeren over nieuwe phising-trucs, ...	Laat impact zien, bijv agv incident; maak melden laagdrempelig . .	Casus 9
Ik wil efficient kunnen communiceren ivm de zorg voor de cliënt; vooral met 1e lijns zorgprofessionals maar ook met familie en mantelzorgers, eventueel via sociale media	Veilig communicatie-protocol zoals Zorgmail regelen; tevens afspraken igv nood / spoedopnames.	5 (10.8) Wbp	Informeren over communicatieafspraken; uitgaande onversleutelde email, fax en post in normale situaties verbieden.	Ontvangen onveilige email, fax of post melden en in overleg met afzenders *en* organisatie alternatieven afspreken.	Casus 8
Ik wil kunnen zien wie een bepaalde actie heeft gedaan zodat, als dat nodig is, we het er over kunnen hebben; dus een unieke gebruikersidentificatie!	Regel toegangsbeheer tot ITdienst en applicaties in relatie tot de gewenste betrouwbaarheid; incl logging, rapportage en controle (monitoring)	6 (11.1-3)	Afspraken mbt inlogkodes, gebruik wachtwoorden, . . Technische ondersteuning .	Maak klachten bespreekbaar; een maatregel heeft pas effect als medewerkers er achter staan. Aanleiding kan zijn: *ik wil niet gehinderd worden door moeilijke en steeds veranderende wachtwoorden!*	Casus 6 en 7
Ik wil bij het dossier / toedienlijst kunnen wanneer ik dat nodig heb	Regel continuïteit ITmiddelen met een hoge beschikbaarheidseis	7 (14.1.3)	Alternatieven laten weten voor het geval dat . . . (nooddossier, dagelijkse medicatielijst, etc)	Zich voortdurend te realiseren waar je afhankelijk van bent en alternatieven kennen. Maar je kunt niet alles voorzien, vertrouw vooral op je onderbuikgevoel en koppel terug!	Casus 13

Ik wil niet dat mijn privégegevens op straat komen te liggen. Ik wil dat mijn cliënt er op kan vertrouwen dat zijn of haar gegevens bij ons veilig zijn.	Privacyreglement medewerker- en cliëntgeg;bijbehorende protocollen zoals inzage dossier etc.	10 (15.1.4) Wgbo, Wbp	Reglementen en protocollen vertalen naar praktische FAQ's . . .	. . en FAQ's ter discussie stellen; bijwerken agv praktijkervaring. Maak gebruik van sociale media	Casus 1-4, 10, 12
Er volgen enkele genuanceerdere uitlatingen. Het gaat hier vooral om maatregelen die een organisatie moet nemen a.g.v. de voorgaande.					
Ik wil weten hoe mijn organisatie omgaat met informatieveiligheid . .	Bev.beleid	1 (5.1.1)	Beleid communiceren	Team- / werkoverleg: IB vast agendapunt, discussie en terugkoppeling. Beleid verwoorden in FAQ's en publiceren ter info en om op te reageren.	Casus 17
	Bev.organisatie	2 (6.1.3)	IBtaken opnemen in functiebeschrijvingen		
	Naleven beleid	11 (15.2.1)	IB koppelen aan kwaliteitscyclus		
	Licentiebeheer	8 (15.1.2)	Protocol mbt omgaan ITmiddelen /illegale sw	Inspraak bij nwe ontwikkelingen!	-
	Beveiliging bedrijfs- en privacy-gevoelige doc's; van vernietiging tot digitale duurzaamheid	9 (15.1.3)	Herkennen vertr. doc's; opslag / bewaren e.d. Protocollen als bijlagen bij Privacybeleid	Privacyaspecten publiceren in FAQ's en a.h.v. discussie privacy-protocollen bijstellen	Casus 1-4, 10, 12
Ik wil dat ik ook op externe dienstverlening kan vertrouwen	Verantwoordelijkheid borgen middels afspraken met derden (SLA en Bwo)	5 (6.2, 10.2, 10.8)	-	-	-
Ik wil dat ook anderen van mijn 'fouten' leren; ik wil ook van anderen horen wat beter kan!	Incidentbeheer incl protocol datalekken; vastleggen en evalueren	12 (13.1.1) Wbp-datalekken	Meldingsprocedure incidenten inclusief herkennen mogelijke datalekken	Communiceer incidenten (ook a.h.v. persberichten), maak evaluaties bespreekbaar.	Casus 15

Bijlage B

Onderwerpen e-learning Informatiebeveiliging
Veilig omgaan met vertrouwelijke informatie

1,2 - Vertrouwelijke informatie; algemeen
3 - Vertrouwelijke cliëntgegevens
4 - Vertrouwelijke medewerkergegevens
5a - IT-middelen verliezen
5b - IT-middelen vinden
6 - Wachtwoord onthouden
7 - Wachtwoord vergeten
8a - E-mail op je werk
8b - E-mail privé en op je werk
9 - Betrouwbare website
10 - Sociale media en je werk
11a - Clear desk policy
11b - Flexwerkplek
12 – Thuiswerken
13 - Wat te doen bij calamiteiten?
14 - Veilig werken, ook onder stress
15 - Meld incidenten; ook datalekken!
16a,b,c - Controlevragen
17 Iedereen is verantwoordelijk voor IB!

e-learning IB; in te zetten als formele en toetsbare bewustwordingsactie.
De cursus is geaccrediteerd voor het kwaliteitsregister V&V; kan periodiek worden gebruikt en wordt dan ook regelmatig geactualiseerd.

Nieuwe onderwerpen begin 2017:

Werken op een tijdelijke werkplek; thuis of in een gezondheidscentrum
Gegevensuitwisseling, oa met sociale wijkteam; 2 casussen
Meld datalekken; uitgebreide informatie + casus

Bijlage C

Voorbeeld
organisatie informatiebeveiliging
(op te nemen in het IBbeleid)

Toelichting
In dit hoofdstuk wordt de organisatie van informatiebeveiliging binnen een instelling beschreven. Het is van groot belang dat de verantwoordelijkheden, taken en bevoegdheden met betrekking tot informatiebeveiliging op een eenduidige wijze zijn toegewezen. Deze toewijzing heeft tot doel te voorkomen dat zaken dubbel worden uitgevoerd of dat de uitvoering van beveiligingstaken achterwege blijft. Bovendien levert de toewijzing van taken en verantwoordelijkheden de mogelijkheid om decharge te verlenen voor de uitgevoerde werkzaamheden.

Rollen en functies van de informatiebeveiliging
Om informatiebeveiliging gestructureerd en gecoördineerd op te pakken worden bij de instelling een aantal rollen onderkend die aan functionarissen in de bestaande instelling zijn toegewezen. In de praktijk kunnen medewerkers verschillende rollen en functies hebben. Omdat de personele bezetting aan wijzigingen onderhevig is wordt die apart opgenomen in een bijlage en voorzien van een laatste wijzigingsdatum.

Bestuur
Het Bestuur is verantwoordelijk voor de informatiebeveiliging binnen de instelling en stelt het beleid vast. De Raad van Toezicht keurt het beleid goed. Informatiebeveiliging komt zo vaak als nodig op de agenda van het Directieteam. Het team wijst één van haar directeuren aan als *Portefeuillehouder informatiebeveiliging*.

De inhoudelijke verantwoordelijkheid voor informatiebeveiliging is door de Portefeuillehouder gemandateerd aan de Functionaris Informatiebeveiliging. Deze heeft de opdracht om op de informatiebeveiliging van de gehele instelling toe te zien.

Functionaris Informatiebeveiliging (FIB)
De FIB is een rol op strategisch en tactisch niveau. Hij adviseert het Bestuur. De FIB formuleert het beveiligingsbeleid, helpt bij een juiste vertaling daarvan naar instellingsonderdelen, ziet toe op de (uniforme) naleving ervan en rapporteert over lacunes, inconsistenties en onvolkomenheden. Hij heeft de bevoegdheid om onderzoek te doen of laten doen (audits) en informatie op te vragen en in principe ook te krijgen, tenzij privacy in het geding is; in alle bijzondere gevallen beslist het Bestuur. De FIB kan zowel gevraagd als ongevraagd van advies dienen. Idealiter valt de FIB daarom ook direct onder het Bestuur.

Op hoofdlijnen omvat deze functie de volgende verantwoordelijkheden:
- beleidsvorming, het beheren van het instellingsbrede informatiebeveiligingsbeleid en hieruit voortvloeiende richtlijnen en procedures;
- monitoring, controle en registratie, het bewaken van het niveau van informatiebeveiliging binnen de instelling;
- signaleren van tekortkomingen in de naleving van het informatiebeveiligingsbeleid en het geven van aanwijzingen voor aanvullende maatregelen aan het lijnmanagement;
- communicatie en voorlichting, het coördineren van de implementatie van het gewenste niveau van informatiebeveiliging en het stimuleren van het beveiligingsbewustzijn bij management, medewerkers en andere betrokkenen;
- evaluatie en advies, het adviseren van het directieteam en andere leidinggevenden over informatiebeveiliging en het rapporteren over de status van informatiebeveiliging binnen de instelling.

De FIB is een stafmanager en rapporteert functioneel direct aan de Portefeuillehouder binnen het Directieteam.

Functionaris gegevensbescherming (FG)[1]
De FG houdt binnen de instelling toezicht op de toepassing en naleving van de Wet bescherming persoonsgegevens. De wettelijke taken en bevoegdheden van de FG geven deze functionaris een onafhankelijke positie in de instelling.

De organisatie is wettelijk verplicht om de FG controlebevoegdheden te geven. Zo moet een FG bevoegd zijn om ruimtes te betreden, zaken te onderzoeken en inlichtingen en inzage te vragen. De FG moet in onafhankelijkheid zijn werkzaamheden kunnen verrichten binnen een organisatie. Een FG heeft dezelfde ontslagbescherming als leden van een ondernemingsraad. Dit betekent dat hij pas ontslagen kan worden na toestemming van de kantonrechter.

De werkzaamheden van een FG zijn onder meer:
- toezicht houden op de verwerking van persoonsgegevens;
- inventarisaties van gegevensverwerkingen maken en onderhouden;
- toezien op het melden en documenteren van inbreuken in verband met persoonsgegevens overeenkomstig artikelen 34a (meldplicht datalekken);zo nodig in overleg met derden op basis van een Bewerkersovereenkomst;
- vragen en klachten van mensen binnen en buiten de organisatie afhandelen;
- interne regelingen ontwikkelen;
- adviseren over technologie en beveiliging;
- input leveren bij het opstellen of aanpassen van een gedragscode.

Kwaliteitscoördinator
Er zijn relaties tussen kwaliteit en informatiebeveiliging. Beide onderwerpen richten zich namelijk op bepaalde aspecten van de bedrijfsvoering. Kwaliteitszorg richt zich op een continue verbetering van de bedrijfsprocessen teneinde de gewenste kwaliteit te kunnen leveren. Gewenste kwaliteit wordt bepaald door het management, de medewerkers, maar vooral ook door de cliënten van de organisatie en de maatschappelijke omgeving waar de organisatie zich in begeeft. Informatiebeveiliging richt zich op de beschikbaarheid, integriteit en de vertrouwelijkheid van de informatievoorziening. Hiermee kan informatiebeveiliging een bijdrage leveren aan de kwaliteit van de bedrijfsvoering.

Coördinator calamiteitenteam ICT
De Coördinator calamiteitenteam ICT bij de instelling wordt benoemd door het Bestuur op advies van de FIB. Hij is verantwoordelijk voor het incident- en calamiteitenbeheer ICTbinnen de instelling en is in dat kader ook bevoegd het tijdelijk isoleren van computersystemen of netwerksegmenten te gelasten.

Werkzaamheden zijn onder meer:
- het verzamelen van informatie over potentiële ICT-beveiligingsincidenten en beveiligingslekken;
- het centraal registreren van (potentiële) ICT-beveiligingsincidenten;
- het analyseren en beoordelen van de aard, omvang en oorzaak van het ICT-beveiligingsincident;
- het organiseren van de evaluatie van de afhandeling van ICT-beveiligingsincidenten;
- het adviseren van de staande organisatie over de te nemen preventieve en herstelacties bij ICT-beveiligingsincidenten van beperkte omvang;
- het adviseren van de calamiteitenorganisatie over de te nemen preventieve en herstelacties bij ICT-beveiligingsincidenten van grote omvang;
- het informeren en instrueren van de direct betrokkenen over de uit te voeren preventieve en herstelacties;

[1] Het Wetsvoorstel cliëntenrechtenzorg stelt een FG verplicht als bij een instelling meer dan 250 medewerkers in dienst zijn. Dit wetsvoorstel is najaar 2016 door de 1e Kamer aangenomen.
Ook de AVG stelt een FG verplicht; deze europese privacyverordening wordt omstreeks mei 2018 verplicht voor de lidstaten.

- het centraal informeren van gebruikers over (potentiële) ICT-beveiligingsincidenten;
- het coördineren van de uitvoering van preventieve en herstelacties.

Audit

Als de organisatie een eigen auditdienst heeft stemt de FIB zijn activiteiten daarmee af. Deze dienst voert onafhankelijk controleactiviteiten uit, veelal in overleg en in samenwerking met de externe accountant.

Contactgroep Informatiebeveiliging (Contactgroep IB)

De Contactgroep IB bestaat uit de FIB, FG, Kwaliteitscoördinator en Coördinator calamiteitenteam. De leden ondersteunen elkaar bij het uitvoeren van hun beveiligingstaken. Daarnaast vervult de Contactgroep een rol bij de vertaling van de strategie naar tactische en operationele plannen. Tevens adviseert de Contactgroep aan het directieteam over specifieke informatiebeveiligingsmaatregelen in projecten – variërend van allerhande staande projecten tot acquisities van bijvoorbeeld software of hardware.

Voorbeeld overzicht personele bezetting beveiligingsfuncties XXX

Rollen en samenwerkingsgroepen beveiligingsbeleid	**Overeenkomstige functies**	**Personele bezetting** dd xx-xx-xxxx
Portefeuillehouder informatiebeveiliging	Directeur	
Functionaris informatiebeveiliging(FIB)	Bestuurssecretaris	
Functionaris gegevensbescherming(FG)	Beleidsmedewerker	
Coördinator calamiteitenteam ICT	Manager ICT	
Kwaliteitscoördinator	Kwaliteitscoördinator	
Audit	Manager Afd X	
Contactgroep informatiebeveiliging (IB)	FIB FG Manager ICT Kwaliteitscoördinator	

Bijlage D – Te raadplegen documentatie

Opmerking vooraf over de NEN 7510, 7512 en 7513 (bijlagen D1, 2 en 4)
Het ministerie van VWS heeft een overeenkomst met NEN gesloten over de afkoop van deze drie NEN-normen. Vanaf 1 november 2014 zijn deze normen vrij beschikbaar via de NEN Normshop; http://www.nen.nl/NEN-Shop.htm.

D1 - NEN 7510:2011 *Normboek Informatiebeveiliging in de zorg*

In 2011 is dit normdocument vernieuwd. Bij het beschrijven van de normelementen wordt zoveel mogelijk de tekst van de ISO 27002 gevolgd. Aanpassingen daarop voor de gezondheidszorg zijn in de NEN7510 **vet** weergegeven.

D2 - NEN 7510:2011 *Praktijkboek Informatiebeveiliging in de zorg*

Het Praktijkboek is een initiatief van het NEN Cluster Gezondheidszorg. Het Praktijkboek volgt zoveel mogelijk de NEN 7510. Hoofdstuk 1 heeft als titel 'Hoe te beginnen?'. De hoofdstukken 3 en 4 geven aanvullende informatie over respectievelijk risicoanalyse en het managementsysteem informatiebeveiliging. Voor de normelementen worden in Hoofdstuk 5 t/m 15 handreikingen geboden in de vorm van toelichtingen op basis van 'best practice'.

Het Praktijkboek NEN 7510 is *niet* gratis beschikbaar maar te bestellen via www.nen.nl/NEN-Shop/Norm/UIT-632012-nl.htm. Daarnaast geeft een licentie op https://www.werkenmetnen7510.nl/ digitaal toegang tot het Praktijkboek met vele voorbeelddocumenten en een online werkboek. Voor een handreiking met voorbeelden ter ondersteuning van de auditfase zie bijlage 7 *Toetsingskader Informatieveiligheid in de zorg; ZZ3.*

D3 - NEN 7512:2015 *Een vertrouwensbasis voor gegevensuitwisseling in de zorg*

De norm is van belang voor elektronische gegevensuitwisseling van vertrouwelijke gegevens tussen Zorgpartijen waaronder ook cliënten en mantelzorgers.

Eerste alinea's Hoofdstuk 1 - Onderwerp en toepassingsgebied:

> *Deze norm beschrijft het classificeren van de gegevensuitwisseling en het bepalen van het risico hiervan voor de gezondheidszorg. Op basis van die classificatie worden voor de gegevensuitwisseling minimumeisen gesteld met betrekking tot de bron van de gegevens, het transportkanaal en de ontvanger van de gegevens. Bron en ontvanger kunnen personen zijn, maar ook organisaties of hun informatiesystemen. Als overkoepelend begrip wordt hiervoor in deze norm de term 'entiteiten' gebruikt.*
>
> *Deze norm heeft betrekking op de elektronische communicatie in de zorg, tussen zorgverleners en zorginstellingen onderling en met patiënten en cliënten, met zorgverzekeraars en andere partijen die bij de zorg zijn betrokken.*
>
> *Deze norm is in twee opzichten een aanvulling op de normelementen die NEN 7510 aan organisaties in de zorg geeft voor hun informatiebeveiliging. In de eerste plaats richt deze norm zich op de zekerheden die partijen elkaar moeten bieden als voorwaarde voor onderlinge gegevens-uitwisseling. Ten tweede levert deze norm een nadere invulling voor een aantal van de beheers-maatregelen van NEN 7510.*

D4 - NEN 7513:2010 ***Logging; het vastlegging van acties op elektronische patiëntdossiers***

De norm voorziet in eisen voor stelselmatige registratie van acties op elektronische patiëntdossiers. Deze registratie maakt het mogelijk de rechtmatigheid van de toegang tot het patiëntdossier te controleren. Daarnaast kan analyse van de logging ondersteuning bieden bij het verbeteren van het proces van de toegangscontrole tot patiëntgegevens.

D5 – Autoriteit Persoonsgegevens; ***Richtsnoeren en Beleidsregels***

De Autoriteit Persoonsgegevens (was tot 2016 het College Bescherming Persoonsgegevens) houdt toezicht op de naleving van de Wet bescherming persoonsgegevens (Wbp) en aanverwante wetten. De AP heeft in 2015 Richtsnoeren voor de beveiliging van persoonsgegevens opgesteld. Hoofdstuk 1 van deze Richtsnoeren geeft de eisen weer die de Wbp stelt aan het beveiligen van persoonsgegevens. Hoofdstuk 2, 3 en 4 geven aan hoe het CBP de beveiliging van persoonsgegevens beoordeelt en hoofdstuk 5 gaat nader in op het toezicht door het CBP. Deze Richtsnoeren dienen voor het CBP als uitgangspunt bij het onderzoeken en beoordelen van de beveiliging van persoonsgegevens en bij het toepassen van handhavende maatregelen.
In 2016 is de Wbp aangescherpt met o.a. de meldplicht datalekken. De AP heeft daarvoor Beleidsregels opgesteld. Zowel de Richtsnoeren als de beleidsregels zijn via de website van de AP te downloaden.

D6 - Nictiz; 2013 ***Wet &Regelgeving voor ICT en e-Health***

Citaat uit de Leeswijzer:

> *"De praktijk leert dat de vele wetten, normen en richtlijnen voor ICT in de zorg niet altijd goed leesbaar en te vinden zijn. Met dit boek biedt Nictiz zorgverleners, ICT'ers en andere mensen die in de zorgsector werkzaam zijn een overzicht van de wet- en regelgeving in de gezondheidszorg. De inhoud hiervan wordt zo toegankelijker. Het boek bestaat uit twee hoofdstukken: 'Wetten' en 'Veldnormen, richtlijnen en handreikingen'. Elk hoofdstuk bevat paragrafen met een korte samenvatting van een wet, veldnorm, richtlijn of handreiking. Waar nodig wordt gebruik gemaakt van voorbeelden om de wet of uitwerking van de wet te verduidelijken. Afhankelijk van de wet spreken we van patiënt, cliënt, zorgvrager, consument of burger. Hetzelfde geldt voor de termen zorgverlener, zorgaanbieder en hulpverlener."*

D7 - Toetsingskader ***Informatieveiligheid in de Zorg; ZZ3***

Het Nederlands Instituut voor Accreditatie in de Zorg (NIAZ) en de Nederlandse Orde van Register EDP-auditors (NOREA) hebben in december 2010 het initiatief genomen om toetsingscriteria voor de informatiebeveiliging in de zorg te ontwikkelen onder de projectnaam ZekereZorg3 (ZZ3). Dit '*om de invoering en naleving van de NEN7510 in de praktijk te ondersteunen, te kunnen toetsen en een instelling desgewenst te accrediteren of te certificeren*' (citaat uit de aanbiedingsbrief van september 2012).

De toetsingscriteria ZZ3 zijn gekoppeld aan de normelementen van de NEN 7510:2011. De criteria kunnen betrekking hebben op een verdieping ten aanzien van de patiëntveiligheid of aanvullend zijn voor medische technologie. Tevens zijn voorbeelden opgenomen van documentatie en bewijsmateriaal waarnaar bij een (interne of onafhankelijke) audit kan worden gevraagd.
De betaversie van dit toetsingskader kunt u vinden op de website van het NIAZ: http://www.niaz.nl/news/berichten-2012/uitrol-betaversie-van-het-toetsingskader-informatieveiligheid-in-de-zorg.