KNMP-richtlijn

Informatiebeveiliging

Geautoriseerd 1 januari 2013

KNMP

1 Inleiding

Bij het verlenen van zorg aan patiënten en het uitwisselen van informatie met andere zorgverleners werkt men in de apotheek met privacygevoelige persoonsgegevens. Deze gegevens vallen onder de reikwijdte van de Wet bescherming persoonsgegevens (WBP). De WBP eist in artikel 13 dat de apotheek passende technische en organisatorische maatregelen uitvoert om deze patiëntgegevens te beschermen. Om die wettelijke zorgvuldigheid te borgen is er een landelijke norm voor informatiebeveiliging in de zorg vastgesteld: de NEN7510. De Inspectie voor de Gezondheidszorg beschouwt de NEN7510 als de norm waarop getoetst kan worden. Ook de wet BSN-z en het Programma van eisen voor een Goed Beheerd Zorgsysteem (NICTIZ) stellen informatiebeveiliging conform de NEN7510 verplicht. Het Programma van eisen voor een Goed Beheerd Zorgsysteem (GBZ) stelt daarnaast nog een aantal aanvullende eisen aan de informatiebeveiliging.

Het totaal aan maatregelen in de NEN7510 is groot en complex. Daarnaast geldt de norm voor grootschalige organisaties (ziekenhuizen), voor samenwerkingsverbanden en voor de kleinschalige praktijk van bijvoorbeeld een apotheker of een fysiotherapeut. Daarom is met deze richtlijn voor de beroepsgroep van openbaar apothekers de NEN7510 'vertaald' naar de apotheeksituatie. De Nederlandse Apotheek Norm (NAN) beschrijft wat onder verantwoorde zorg in de openbare apotheek wordt verstaan. Informatiebeveiliging raakt zeer veel normen in de NAN zowel met betrekking tot de zorgprocessen als de randvoorwaarden daarvoor. Deze richtlijn is opgesteld als een thematische richtlijn aanvullend op de algemene richtlijnen van de NAN.

De aanbevelingen in de richtlijn zijn direct afgeleid uit de NEN 7510. De GBZ-eisen zijn gebaseerd op het Programma van Eisen voor een Goed Beheerd Zorgsysteem (GBZ) van het NICTIZ (versie 2.0 2007). Voldoen aan de NEN 7510 en de GBZ-eisen behoren tot de voorwaarden voor aansluiting van de apotheek op het Landelijk Schakelpunt (LSP). Aangezien het LSP en het aansluiten op het LSP nog in ontwikkeling is zijn deze eisen te beschouwen als suggestie en daarom separaat in een aanhangsel opgenomen. In dit aanhangsel zijn alleen die GBZ-eisen beschreven welke de informatiebeveiliging raken en dan alleen voor zover ze niet in de NEN 7510 zijn beschreven. Ze zijn letterlijk overgenomen uit het Programma van Eisen.

Deze richtlijn informatiehuishouding – beveiliging bevat analoog aan de NEN 7510 de volgende hoofdstukken:

1. Beleid
2. Organisatie
3. Beheer
4. Personeel
5. Fysieke beveiliging
6. Operationeel beheer van informatiesystemen en van informatie-uitwisseling
7. Toegangsbeveiliging
8. Aanschaf, ontwikkeling en onderhoud van informatiesystemen
9. Continuïteitsbeheer
10. Naleving
11. Incidenten

Hoofdstuk 1 Beleid

1.1 Principe
De apotheek heeft een vastgelegd beleid op het gebied van informatiebeveiliging.

Aanbevelingen
1. De apotheek heeft een beleidsplan op het gebied van informatiebeveiliging.

   Toelichting
   Het beleidsplan informatiebeveiliging bevat:
   - doelstellingen van informatiebeveiliging
   - organisatie van informatiebeveiliging (taken, bevoegdheden en verantwoordelijkheden)
   - interne controle, review en audit van processen en procedures
   - risicoanalyses van informatiesystemen (computers, servers, netwerk, programmatuur) en processen (menselijk handelen)

   De apotheek beoordeelt en evalueert jaarlijks het beveiligingsbeleid op vragen als:
   - voldoet het beleid nog?
   - zijn in de organisatie of in de ICT-omgeving zaken veranderd die een invloed hebben op het beleid?.

   De resultaten van deze evaluatie worden vastgelegd en zo nodig gecommuniceerd naar het apotheekteam. Informatiebeveiliging kan in de algemene beleidscyclus worden opgenomen. Hiervoor kunnen verbeteractiviteiten worden opgenomen in het kwaliteitsjaarplan en verantwoord worden in het kwaliteitsjaarverslag van de apotheek.

Hoofdstuk 2 Organisatie

2.1 Principe
In de apotheekorganisatie zijn de verantwoordelijkheden op het gebied van informatiebeveiliging belegd en vastgelegd

Aanbevelingen
1. Binnen de apotheekorganisatie zijn taken, bevoegdheden en verantwoordelijkheden op het gebied van informatiebeveiliging toegewezen.

   Toelichting
   In de apotheekorganisatie hebben alle medewerkers een rol binnen de organisatie van informatiebeveiliging. Aan de hand van het beleid worden de taken, bevoegdheden en verantwoordelijkheden voor informatiebeveiliging toegewezen binnen de organisatie. Dit wordt naar het apotheekteam gecommuniceerd. De rol van leden van het apotheekteam kan wordenbeschreven in het kwaliteitshandboek in een taakomschrijving. Zie hiervoor ook artikel 13 van de Wet Bescherming Persoonsgegevens. Deze verplicht de verwerker van persoonsgegevens om technische en organisatorische maatregelen te treffen die een “passend beschermingsniveau” garanderen.

2. De apotheek voert een risicoanalyse uit gericht op informatiebeveiliging en definieert maatregelen om onverantwoorde risico’s tegen te gaan.

   Toelichting
   Het uitvoeren van een risicoanalyse heeft tot doel de gevolgen van bedreigingen, waaraan een bedrijfsproces, een informatiesysteem (computers, servers, netwerk, programmatuur) of informatie van de apotheek blootstaat te analyseren en op grond hiervan een passend beveiligingsniveau te bepalen. Eens per jaar maar ook bij invoering of wijziging van een kritisch systeem voert de apotheek een risicoanalyse uit op de processen binnen de apotheek en de onderliggende informatiesystemen (computers, servers, netwerk, programmatuur). De apotheekorganisatie besteedt specifieke aandacht aan systemen die door externen worden beheerd en onderhouden.

Hoofdstuk 3 Beheer

3.1 Principe

Binnen de apotheek wordt op een gestructureerde manier omgegaan met het beheer van informatie en informatieverwerkende middelen om risico's zoveel mogelijk terug te dringen

Aanbevelingen

1. Binnen de apotheek is een overzicht beschikbaar van de bedrijfsmiddelen (in de apotheek en extern) die een rol spelen in de dagelijkse informatieprocessen van de apotheek.

   Toelichting
   Om een beeld te krijgen van de invloed van bedrijfsmiddelen (zie definities) en er zeker van te zijn dat deze allemaal onder toezicht zijn, moeten deze geïnventariseerd worden. Bij deze inventarisatie wordt vastgelegd waar deze zich bevinden en wie er verantwoordelijk voor is.

2. Gegevens binnen de apotheek zijn beoordeeld en ingedeeld in risicocategorieën volgens een vaste classificatieprocedure.

   Toelichting
   Hierbij wordt gekeken naar hoe kritisch gegevens voor de apotheek zijn. Aan deze classificatie zijn beveiligingsniveaus en daarmee maatregelen gekoppeld.
   Een manier waarop men gegevens kan classificeren is door beoordeling op de volgende drie onderwerpen:
   - Beschikbaarheid (hoe groot kunnen de gevolgen zijn als de gegevens niet beschikbaar zijn)
   - Integriteit: Hoe groot kunnen de gevolgen zijn als de gegevens niet correct zijn
   - Vertrouwelijkheid: Hoe groot kunnen de gevolgen zijn als de gegevens 'lekken'. (privacy)

   Door gegevens per categorie in te delen in lage, middelhoge of hoge impact indien er een incident plaat vindt kunt u snel inzicht krijgen in de meest gevoelige gegevens binnen uw organisatie.
   Patiëntgegevens behoren altijd tot de hoogste categorie bijvoorbeeld vanwege privacywetgeving en patiëntveiligheid (medicatiebewaking, overdracht van medicatiegegevens).

3. De apotheek hanteert een goedkeuringsproces voor de installatie en het in gebruik nemen van nieuwe systemen (AIS maar ook, computers, servers, netwerksystemen en andere programmatuur).

   Toelichting
   Om ook op de lange termijn de informatiebeveiliging op orde te houden is het van belang dat bij de installatie van nieuwe systemen de risico's die hieraan verbonden zijn geïnventariseerd en geanalyseerd. Hierbij is het belangrijk dat in de apotheek alleen met geldige licenties gewerkt wordt aangezien de risico's bij illegale software vele malen groten zijn. Daarnaast worden alleen diensten afgenomen bij betrouwbare leveranciers waarvan u bijvoorbeeld garantie en service ontvangt.

   Definieer voor de installatie en het in gebruik nemen van nieuwe informatieverwerkende middelen een goedkeuringsprocedure. Leg daarin tenminste de volgende elementen vast.
   - Inschatting van de risico's voor in gebruik neming.
   - Taken, bevoegdheden en verantwoordelijkheden voor de verschillende stappen in het proces.

4. Voordat apparatuur en media uit de apotheek worden afgevoerd (indien ze defect zijn of vervangen worden) dienen programmatuur en gegevens verwijderd of overschreven te worden.

   Toelichting
   Systemen (computers, servers, netwerksystemen en programmatuur) en verwijderbare media (CD's, DVD, USB-stick) dienen dusdanig leeggemaakt te zijn zodat programmatuur en gegevens niet te achterhalen zijn door derden. Indien u deze meegeeft aan een derde partij moet leegmaken, achterhalen en vernietigen contractueel geregeld zijn.

Hoofdstuk 4 Personeel

4.1 Principe

Het personeel binnen de apotheek kent zijn verantwoordelijkheden op het gebied van informatiebeveiliging en is betrouwbaar in het hanteren van vertrouwelijke apotheekgegevens.

Aanbevelingen

1. Voor aanvang van en tijdens werkzaamheden in de apotheek wordt voor vast en tijdelijk personeel een beveiligingsonderzoek (screening) uitgevoerd.

   Toelichting
   Voorbeelden van beveiligingsonderzoeken kunnen zijn:
   - het laten opvragen van een verklaring omtrent het gedrag
   - het natrekken van referenties (met instemming van werknemer)
   - het raadplegen van het BIG-register
   - het bespreken van het onderwerp in het functionerings- of beoordelingsgesprek

   De aard van de functie bepaalt de mate van “screening”. Het is van belang dat het personeel zich ervan bewust is hoe de informatiebeveiliging is geregeld in de praktijk. Ook voor tijdelijke medewerkers is het belangrijk dat ze hun rol kennen in de informatiebeveiliging en daarop aangesproken kunnen worden.

2. In het arbeidscontract of de taakomschrijving in het kwaliteitssysteem is opgenomen dat de medewerker een verantwoordelijkheid heeft betreffende informatiebeveiliging. Het niet naleven hiervan kan disciplinaire maatregelen ten gevolge hebben.

   Toelichting
   Apotheekmedewerkers hebben toegang tot die informatie die noodzakelijk is voor het goed uitoefenen van zijn of haar functie. Iedereen heeft daarmee een rol in de informatiebeveiliging.
   Neem in het arbeidscontract of de taakomschrijving op dat de medewerker een verantwoordelijkheid heeft betreffende informatiebeveiliging. Nadere omschrijving daarvan kan daarbij in een protocol worden vastgelegd. Stel bij het niet naleven hiervan disciplinaire maatregelen op die gehandhaafd worden. Leg hierbij, indien van toepassing, vast dat deze verantwoordelijkheden zich ook uitstrekken buiten de praktijk en gelden buiten de normale werktijden. Dit hangt samen met het geheimhoudingsbeding van de werknemers.

3. Medewerkers van de apotheek die gebruik maken van informatiesystemen en die geen wettelijke geheimhoudingsplicht hebben, moeten bij het begin van hun dienstverband een geheimhoudingsverklaring ondertekenen als onderdeel van het arbeidscontract.

   Toelichting
   Apothekers en apothekersassistenten hebben vanuit de wet BIG (artikel 88) een wettelijke geheimhoudingsplicht. Voor de apotheekmedewerkers die deze wettelijke geheimhoudingsplicht niet hebben moet het arbeidsrechtelijk duidelijk zijn dat ook zij een (afgeleide) geheimhoudingsplicht hebben. Voor deze medewerkers (administratief personeel, bezorgers, apotheekhulpen, schoonmakers) is het daarom raadzaam een geheimhoudingsbeding op te nemen in hun arbeidscontract, ook voor apothekersassistenten is het wenselijke een dergelijk beding op te nemen in het contract. Een aantal zaken is opgenomen in de model arbeidsovereenkomsten van de CAO Apotheken. Dit is van belang bij het aannemen van tijdelijk personeel en ook bij bijvoorbeeld stagiaires of vakantiewerkers.

4. Alle gebruikers van de informatiesystemen zijn op passende wijze ingewerkt op het gebied van informatiebeveiliging en de bijbehorende procedures en bij nieuw personeel wordt extra op de naleving hiervan toegezien.

Toelichting
Het informatiebeveiligingsbeleid wordt in de apotheek door het apotheekteam gedragen. Iedereen is op de hoogte van zijn of haar verantwoordelijkheid. Alle nieuwe gebruikers van informatiesystemen (AIS, maar ook computers, servers, netwerk en andere programmatuur) worden op een passende wijze ingewerkt volgens een procedure. Daarnaast is het advies om dit onderwerp regelmatig terug te laten komen tijdens werkoverleggen. Het bewustzijn en kennisniveau kan steekproefsgewijs via een enquête getest worden.

5. Binnen de apotheek is gewaarborgd dat de toegangsrechten tot informatiesystemen en fysieke ruimtes van medewerkers en externe partijen worden ingetrokken bij het beëindigen van hun (arbeids)contract.

   Toelichting
   De apotheek hanteert een uitdiensttredingsprocedure. Hierin staat ook dat bij uitdiensttreding/einde contract alle toegangsrechten tot de informatiesystemen (computers, servers, netwerk, programmatuur) en tot de fysieke ruimtes van de apotheek worden ontnomen. Dit is ook van belang bij tijdelijk personeel. Denk daarbij ook aan het inleveren van bijvoorbeeld de UZI-pas.

6. De apotheek kent de risico's van werken op afstand en heeft over werken op afstand beleid geformuleerd (bv. toegang tot de informatiesystemen van de apotheek vanaf thuis). Thuiswerken met privacygevoelige informatie dient zoveel mogelijk te worden vermeden.

   Toelichting
   Thuiswerken zorgt voor extra risico's omdat dit externe toegang moet toestaan op de informatiesystemen van de apotheek en gegevens over een extern netwerk gaan.
   In het informatiebeveiligingsbeleid zijn regels opgenomen over het verlenen van toegang tot de informatiesystemen op afstand. De apotheek hanteert een procedure de volgende elementen zijn opgenomen:
   - Aanvragen van toegang
   - Goedkeuring aanvraag
   - Aanmaken account op Virtual Private Network voorziening.

Hoofdstuk 5 Fysieke beveiliging

5.1 Principe

Fysieke toegang van derden tot informatie en informatiesystemen (computers, servers, netwerk, programmatuur) is zoveel mogelijk beperkt en gereguleerd.

Aanbevelingen

1. In de apotheek zijn de risico's beoordeeld van de werkzones waarin personeel, informatiesystemen en andere gegevens (recepten, kaartenbakken) worden beschermd. Naar aanleiding hiervan neemt de apotheek aanvullende maatregelen zodat alleen geautoriseerd personeel toegang kan krijgen tot informatie.

   Toelichting
   Patiënten hoeven geen toegang te hebben tot de gehele apotheek met haar medicijnen en privacygevoelige informatie. Afhankelijk van de locatie binnen de apotheek dienen dan ook specifieke maatregelen genomen te worden. Denk daarbij aan beveiliging van informatie en informatiesystemen bij de algemeen toegankelijke balie-eilanden, bij meenemen van de patiënt door de apotheek naar een achter in het gebouw gelegen spreekkamer, bij het meenemen van vertegenwoordigers naar het kantoor van de apotheker, etc.

2. In de apotheek zijn informatiesystemen zodanig geplaatst en beveiligd dat de risico's van schade en storing van buitenaf en de kans op ongeautoriseerde toegang, gebruik of meekijken beperkt is.

   Toelichting
   Informatiesystemen zijn kwetsbaar voor elektronische storingen en schade door bijvoorbeeld brand, wateroverlast etc. maar ook voor diefstal of oneigenlijk gebruik. Hiertegen moeten ze dan ook beschermd worden. Denk hierbij aan het plaatsen van servers in een afsluitbare kast. Besteed aandacht aan de computers die op de balie staan en makkelijk gestolen kunnen worden.

3. In de apotheek is een 'clean desk' en 'clear screen' beleid ingesteld.

   Toelichting
   Omdat de apotheek open staat voor haar klanten is het belangrijk dat bijvoorbeeld gegevens van andere klanten niet op de balie liggen ('clear desk') en dat als een computer onbeheerd achterblijft op het scherm geen gegevens blijven staan ('clear screen'). Ook in andere ruimtes moet bewust en integer met gegevens omgegaan worden. In het kwaliteitshandboek kan opgenomen worden dat medewerkers bij het verlaten van de balie of werkplek alle papieren etc. opruimen en bij het verlaten van een computerwerkplek een screensaver aangezet wordt of het systeem afgesloten wordt.

Hoofdstuk 6 Operationeel beheer van informatiesystemen en van informatie-uitwisseling

6.1 Principe

Het apotheekteam beschikt over duidelijke instructies over hoe om te gaan met informatiesystemen en media die gegevens dragen.

Aanbevelingen

1. De apotheek heeft elektronische of schriftelijke procedures opgesteld voor de bediening van alle informatiesystemen.

   Toelichting
   Gebruikershandleidingen (bijvoorbeeld aangeleverd door de leveranciers van de informatiesystemen) dienen altijd ter beschikking te staan aan het apotheekteam. Deze kunnen voor de belangrijkste processen ook vertaald worden naar stappenplannen voor het uitvoeren van de processen zoals beschreven in het kwaliteitshandboek.

2. De apotheek heeft procedures opgesteld voor de behandeling en opslag en verwijdering van media (tapes, CD's, DVD's, memorysticks, laptops, etc.maar ook papier) om de erop opgeslagen gegevens te beschermen tegen ongeoorloofde openbaarmaking of misbruik.

   Toelichting
   Onder media worden tapes, CD's, DVD's, memorysticks, laptops, etc. maar ook papier verstaan. Hier moet zorgvuldig mee omgegaan worden aangezien deze makkelijk verloren of meegenomen kunnen worden. Hiervoor is een procedure opgesteld waarin is beschreven welke media mogen worden gebruikt voor (versleutelde) opslag, hoe hiermee omgegaan moet worden en hoe deze uiteindelijk afgevoerd moeten worden. Denk hierbij ook aan het gebruik maken van deze informatie buiten de apotheek zoals FTO, patiëntbespreking met de voorschrijver etc.

6.2 Principe

De apotheek heeft informatiebeveiliging gewaarborgd wanneer informatie wordt uitgewisseld (zowel binnenkomend als uitgaand) met andere partijen zoals andere zorgverleners, zorggroepen, verzekeraars.

Aanbevelingen

3. De apotheek beschikt over een lijst, waarin is opgenomen welke gegevens in aanmerking komen voor uitwisseling, zowel intern als extern, inclusief de daarbij geldende voorwaarden.

   Toelichting
   Om vertrouwelijke gegevens te beschermen moet de uitwisseling hiervan beperkt worden tot alleen de minimaal noodzakelijke. Beleid dient opgesteld te worden voor het uitwisselen van gegevens samen met geldende voorwaarden afhankelijk van de classificatie van deze gegevens. Een voorbeeld hiervan kan een procedure zijn om de identiteit van een zorgverlener vast te stellen bij spoedverzoeken.

4. De apotheek beschikt over een overzicht van de organisaties waarmee gegevens worden uitgewisseld, hierbij is ook opgenomen om welke gegevens het gaat en op welke manier die uitgewisseld worden.

5. Voor informatie op publiek toegankelijke systemen (bijvoorbeeld een website) wordt een screening uitgevoerd.

   Toelichting
   De apotheek communiceert informatie naar het algemene publiek schriftelijk (folders, bladen) maar ook elektronisch (website, E-mails). Deze informatie zal geen privacygevoelige informatie mogen zijn, maar mogelijk dat het openbaar maken van bepaalde gegevens toch wetgeving kan schenden, bijvoorbeeld bij het online plaatsten van een gesprekverslag. Daarom moet informatie die publiek gemaakt wordt eerst hierop worden getoetst. Dit kan via een goedkeuringsprocedure.

6.3 Principe
De apotheek heeft maatregelen getroffen om gegevens tijdens elektronische gegevensuitwisseling te beveiligen tegen beschadiging, verlies, ongeautoriseerde toegang, misbruik en manipulatie

Aanbevelingen
6. De apotheek past maatregelen toe voor de bescherming van gegevens tijdens geautomatiseerde uitwisseling of elektronische communicatie, passend bij de gebruikte informatiesystemen en gegevens naar aanleiding van de classificatie hiervan.

   Toelichting
   Bij de AIS leverancier kan nagegaan worden hoe dit voor een specifiek AIS geregeld is. Daarnaast moet er ook gekeken worden hoe dit is geregeld voor andere vormen van informatie-uitwisseling (bijvoorbeeld e-mail). Ook dient gebruik te worden gemaakt van een beveiligd netwerk (bijvoorbeeld eZorg of eHealthNet).

7. De apotheek maakt met zorgverleners waarmee informatie uitgewisseld wordt afspraken over informatiebeveiliging en heeft deze afspraken vastgelegd.

   Toelichting
   Een voorbeeld van een dergelijke afspraak is een OZIS-gebruikersovereenkomst waarin de afspraken over informatiebeveiliging zijn vastgelegd.

6.4 Principe
De apotheek verhindert dat kwaadaardige programmatuur informatie en informatiesystemen beschadigt of vernietigt.

Aanbevelingen
8. In de apotheek zijn maatregelen ingevoerd voor de preventie en detectie van kwaadaardige programmatuur

   Toelichting
   Om informatiesystemen te beschermen tegen kwaadaardige programmatuur moeten hiervoor maatregelen genomen worden. (bijvoorbeeld een actuele virusscanner en firewall) en moeten medewerkers op de hoogte zijn van deze maatregelen.

6.5 Principe
De apotheek maakt met leveranciers en externe beheerders van informatie en informatiesystemen contractuele afspraken over de kwaliteit van de dienstverlening en de informatiebeveiliging.

Aanbevelingen
9. Voor de informatiesystemen van de apotheek die fysiek op een externe locatie staan of door een externe partij worden beheerd gelden beveiligingsprocedures en beveiligingsmaatregelen.

   Toelichting
   Om de informatiebeveiliging onder controle te houden is het van belang dat iedereen die toegang heeft tot de informatiesystemen dezelfde procedures volgt. Dit geldt dus ook voor informatiesystemen die fysiek op een externe locatie staan en voor externe beheerders die toegang hebben tot de systemen van de apotheek. Hiervoor moeten afspraken gemaakt worden en contracten opgesteld worden met externe beheerders van informatiesystemen waarin vastgelegd wordt dat van hen verwacht wordt dat zij zich ook conformeren aan het geldende informatiebeveiligingsbeleid en daaraan gerelateerd procedures en maatregelen.

10. Bij het uitbesteden van het beheer van informatiesystemen door de apotheek aan derden dienen met de contractant beveiligingsmaatregelen overeengekomen te zijn en te worden opgenomen in het contract.

    Toelichting
    Doordat het beheer bij een andere partij ligt heeft de medewerkers van deze partij ook toegang tot de systemen en informatie. Beveiligingsmaatregelen die gelden voor de medewerkers van de apotheek dienen dan ook te gelden voor deze beherende partij.
    Denk hierbij aan maatregelen in de medewerker van de beheerder in de apotheek werkt maar ook indien de dienstverlening op afstand plaatsvindt. Een belangrijke aspect hierbij is een geheimhoudingsverklaring bijvoorbeeld in het privacyreglement van de beheerder.

11. In het contract is opgenomen dat de apotheek door de beheerder in staat wordt gesteld de overeengekomen beveiligingsmaatregelen bij de beheerder te kunnen controleren (het gaat hierbij om de contractuele afspraak, niet om daadwerkelijk uitvoeren van deze controle).

    Toelichting
    Om te waarborgen dat beveiligingsmaatregelen ook doorgevoerd zijn door de externe partij moet dit getoetst kunnen worden door bijvoorbeeld een audit of een enquête. In het contract dient opgenomen te zijn dat de externe partij dient te rapporteren over ingevoerde informatiebeveiligingsmaatregelen en dat de apotheek het recht heeft periodiek een toets uit te (laten) voeren op de werking van de ingevoerde maatregelen.

12. In het contract met derden die toegang hebben tot fysieke ruimten, informatie en informatiesystemen van de apotheek zijn beveiligingsvoorwaarden en bijbehorende sancties opgenomen.

    Toelichting
    Om risico's voor de apotheek door ongewenst gedrag van derden, waaronder leveranciers, enigszins te beperken en deze partijen te stimuleren bewust om te gaan met de gevoelige gegevens waar ze toegang toe krijgen, moeten hierover afspraken en verantwoordelijkheden worden vastgelegd en maatregelen genomen kunnen worden indien de partij zich hier niet aan houdt.

6.6 Principe

In de apotheek wordt bij het in gebruik nemen van nieuwe systemen of het wijzigen en testen van bestaande systemen zodanig gewerkt dat de informatievoorziening en informatiebeveiliging intact blijft.

Aanbevelingen

13. In de apotheek zijn procedures over in gebruik nemen en testen en controle op wijzigingen in informatiesystemen.

    Toelichting
    Een belangrijk aspect hierin is het toewijzen van een duidelijke verantwoordelijke voor het toelaten, checken en testen van wijzigingen in systemen. Om ongeautoriseerde wijzigingen of opzettelijk misbruik van gegevens en diensten te verkleinen moeten wijzigingen via een vast proces verlopen waarin onder andere autorisaties van de verschillende medewerkers en (interne en externe) beheerders zijn vastgelegd.

Hoofdstuk 7 Toegangsbeveiliging

7.1 Principe

In de apotheek is toegang van personen tot informatie en informatiesystemen zoveel mogelijk beperkt en gereguleerd.

Aanbevelingen

1. De apotheek hanteert procedures voor het toekennen/registreren van toegangsrechten voor apotheekmedewerkers en voor het afmelden van het gebruik van apotheekmedewerkers.

   Toelichting
   Alleen bevoegden hebben toegang tot de (onderdelen van) de informatiesystemen van de apotheek. De apotheek hanteert daarom een procedure, in lijn met het informatiebeveiligingsbeleid, waarin het toekennen, aanpassen en intrekken van autorisaties en rechten is beschreven per rol, functie of groep gebruikers op basis van een gebruikersidentificatie. Denk daarbij aan rollen als apotheker, apothekersassistenten en administratief medewerker. Hierin is opgenomen dat iedere gebruiker een unieke gebruikersidentificatie voor persoonlijk gebruik heeft op basis van zijn of haar functie. Let op bij het verlenen van 'speciale' toegangsrechten welke een vergroot risico zijn. Temeer omdat deze meer mogelijk maken op het systeem.

2. De apotheek hanteert procedures voor het instellen, wijzigen en intrekken van wachtwoorden en toegangspassen

   Toelichting
   Om toegang te controleren is het belangrijk dat gebruikers en beheerders kunnen worden geïdentificeerd en deze met een wachtwoord of toegangspas inloggen wat alleen bij hen bekend is en voldoende sterk is (niet snel te raden, voldoende lengte en speciale tekens gebruiken). Het intrekken van wachtwoorden en toegangspassen dient een onderdeel te zijn van de procedure uitdiensttreding.

3. Aan bepaalde apotheekmedewerkers of beheerders kan in onvoorziene noodsituaties de bevoegdheid worden toegekend om de normale toegangsafscherming te doorbreken.

   Toelichting
   In noodgevallen kan het nodig zijn dat tijdelijk speciale bevoegdheden aan een gebruiker of beheerder worden toegekend om problemen te verhelpen. Denk aan noodsituaties als ziekte of plotseling overlijden van de apotheker of de persoon die de hoogste toegangsrechten heeft.

   Stel bijvoorbeeld een enveloppe procedure op die aangeeft wie de enveloppe met het wachtwoord voor speciale bevoegdheden uit de kluis mag halen en onder welke voorwaarden. Deze enveloppe kan bijvoorbeeld ook alle informatie bevatten die normaal op een overdrachtsformulier vermeldt wordt.

   Zorg ervoor dat de hiervoor geautoriseerde medewerkers op de hoogte zijn van de noodprocedure. En dat ook de voorwaarden waaronder de beheerder van het informatiesysteem in noodgevallen toegang kan krijgen zijn vastgelegd.

4. In de apotheek zijn toepassingen, systemen en netwerkvoorzieningen zodanig ingericht dat toegang alleen mogelijk is in overeenstemming met geldige bevoegdheden en een wachtwoord.

   Toelichting
   Informatiesystemen dienen zo ingericht te zijn dat alleen geautoriseerde gebruikers en beheerders toegang kunnen krijgen.

5. In de apotheek zijn onbeheerde computers voldoende beveiligd en zodanig ingesteld dat inactieve computers op plaatsen met verhoogd risico een time-out voorziening hebben.

   Toelichting
   Om de toegang tot computers te beperken tot geautoriseerde gebruikers die op dat moment zijn ingelogd moeten deze uitloggen of een screenlock activeren (Bij het gebruik van microsoft Windows kan dit door middel van: Windows-toets + L) als zij het systeem onbeheerd achterhalen.
   Daarnaast is een time-out ingesteld die dit uitschakelen automatisch doet na een bepaalde tijd voor het geval het handmatig inschakelen een keer vergeten wordt. Dit is van groot belang voor computers die zich op of bij de balie bevinden maar ook relevant voor andere computers die in de apotheek staan.

6. In de apotheek is een scheiding aangebracht tussen het interne en het externe netwerk van de apotheek.

   Toelichting
   Indien er een onbeveiligde internet verbinding aanwezig is in de apotheek (anders dan bijvoorbeeld E-HealthNet of E-Zorg) is het belangrijk dat de computer waarop deze is aangesloten niet aan het normale netwerk van de apotheek is aangesloten.

Hoofdstuk 8 Aanschaf, ontwikkeling en onderhoud van informatiesystemen

8.1 Principe
In de apotheek zijn de risico's voor informatieveiligheid van het in gebruik nemen van nieuwe informatiesystemen bekend.

Aanbevelingen
1. De apotheek heeft de risico's in kaart gebracht aangaande de beveiligingseisen bij het aanschaffen, wijzigen en onderhouden van een informatiesysteem.

   Toelichting
   Uitgangspunt voor nieuwe of aangepaste informatiesystemen is dat ze moeten voldoen aan wettelijke eisen en geldende regelgeving. Deze eisen moeten aan de leverancier meegegeven worden. Daarvoor wordt een risicoanalyse uitgevoerd aangaande de NEN7510 en wet- en regelgeving voor het aanschaffen, wijzigen en onderhouden van een informatiesysteem.

   Daarnaast heeft de apotheker als zorgverlener de verantwoordelijkheid om zich te verzekeren dat de gebruikte systemen het zorgproces zoals hij dat uitvoert voldoende ondersteund.

8.2 Principe
Indien de apotheek betrokken is bij het ontwikkelen en testen van informatiesystemen wordt hierbij op verantwoorde wijze met 'productie'-gegevens omgegaan.

Aanbevelingen
2. Indien de apotheek betrokken is bij het testen van zijn AIS zijn er gescheiden ontwikkel-, test- en productieomgevingen en procedures aanwezig voor het overdragen van programmatuur van het ontwikkel- en teststadium naar het productiestadium

   Toelichting
   Om tijdens het ontwikkelen en testen van programmatuur niet per ongeluk informatie te wijzigen of verwijderen of gaten in de beveiliging te maken moet dit in een gescheiden omgeving plaatsvinden en na goedkeuring pas geïmplementeerd worden op operationele systemen. Ontwikkeling en initieel testen vindt niet op productiesystemen of met productiedata plaats.

3. Indien de apotheek betrokken is bij het testen van systemen worden strenge beveiligingsmaatregelen in acht genomen in het geval patiëntengegevens bij systeem- en acceptatietesten worden gebruikt

   Toelichting
   Soms is het noodzakelijk om informatiesystemen te testen met de werkelijke gegevens zoals deze in de dagelijkse activiteiten van apotheek worden gebruikt. Het is dan belangrijk dat deze gegevens niet uitlekken, ongewild aangepast worden, enz. Indien er gebruik wordt gemaakt van privacygevoelige gegevens moet een set van gepseudonymiseerde of geanonimiseerde gegevens worden gebruiken. Maak bij privacygevoelige gegevens en/of databases een kopie van de (geanonimiseerde) gegevens om te testen zodat de integriteit en beschikbaarheid van deze gegevens niet aangetast kan worden door deze testen.

Hoofdstuk 9 Continuïteitsbeheer

9.1 Principe
De apotheek dient de gevolgen van calamiteiten op informatiesystemen zoveel mogelijk te beperken

Aanbevelingen
1. De apotheek beschikt over een calamiteitenplan om de verstoring van informatiesystemen als gevolg van calamiteiten en beveiligingsincidenten tot een aanvaardbaar minimum te beperken

   Toelichting
   Om de continuïteit van de informatiesystemen en daardoor de zorgverlening aan de patiënt in de apotheek te garanderen is het belangrijk om een gestructureerd afhandelingproces te volgen in het geval van een beveiligingsincident of calamiteit. Hierbij kan gebruik worden gemaakt van een checklist of calamiteitenplan.
   Incidenten of calamiteiten waarmee rekening gehouden dient te worden zijn onder andere :
   - Storingen van het AIS
   - Wegvallen van de netwerkverbinding
   - Stroomstoringen
   - Waterschade, blikseminslag of brand

2. Het calamiteitenplan wordt in de apotheek periodiek, evenals na een incident of calamiteit, getest, geëvalueerd en onderhouden.

   Toelichting
   In het geval van een calamiteit moet worden vastgelegd welke specifieke acties die genomen zijn. Hiermee kan het calamiteitenplan geëvalueerd en zo nodig bijgesteld worden. Plannen dienen jaarlijks geëvalueerd te worden zo nodig aangepast te worden. Dit kan ook uitbesteed worden aan een externe partij.

9.2 Principe
De beschikbaarheid van informatie binnen de apotheek is gewaarborgd.

Aanbevelingen
3. Regelmatig worden regelmatig reservekopieën gemaakt van essentiële gegevens en programmatuur en het terugzetten hiervan wordt getest.

   Toelichting
   In geval van een incident moet snel een kopie teruggezet kunnen worden om de dagelijkse activiteiten van de apotheek weer lopend te krijgen. Het gaat hierbij niet alleen om het AIS maar ook andere informatiesystemen binnen de apotheek.

4. De apotheek heeft maatregelen getroffen om te garanderen dat patiëntengegevens beschikbaar blijven zolang de geldende wettelijke bewaartermijn dit vereist.

   Toelichting
   Er bestaat een wettelijke bewaartermijn voor medische documenten (WGBO). Er moet een procedure worden opgesteld voor elektronische opslag van gegevens, waarbij rekening moet worden gehouden dat elektronische opslagmedia een beperkte economische levensduur hebben. De elektronische opslagmedia moeten regelmatig op betrouwbaarheid en houdbaarheid worden herzien, opdat toegankelijkheid tot gearchiveerde gegevens wordt gewaarborgd. Elektronische opslag vergt planning.

Hoofdstuk 10 Naleving

10.1 Principe

De implementatie van informatiebeveiliging binnen de apotheek wordt periodiek door een onafhankelijke partij beoordeeld

Aanbevelingen

1. Het informatiebeveiligingsbeleid en de geïmplementeerde informatiebeveiligingsmaatregelen van de apotheek worden periodiek en bij belangrijke wijzigingen, intern en onafhankelijk beoordeeld.

   Toelichting
   Om er zeker van te zijn dat de informatiebeveiliging goed op orde is en er geen onnodige en ongewenste risico's worden gelopen zal een externe partij regelmatig moeten controleren of de geïmplementeerde maatregelen uit het informatiebeveiligingsbeleid voldoen in de praktijk.
   De apotheek laat minimaal jaarlijks en bij belangrijke wijzigingen de implementatie van de informatiebeveiliging door een onafhankelijke partij beoordelen (bv. door kwaliteitskring of overkoepelende organisatie) en evalueert periodiek intern de implementatie van informatiebeveiliging.

   Het onafhankelijk beoordelen kan op verschillende manieren plaatsvinden, bijvoorbeeld: collegiale toets, visitatie of een externe toets of certificering of het opnemen van een paragraaf in het kwaliteitsjaarverslag.

Hoofdstuk 11 Incidenten

11.1 Principe

De apotheek registreert incidenten op het gebied van informatiebeveiliging om achteraf de oorzaak vast te kunnen stellen.

Aanbevelingen

1. De apotheek hanteert procedures voor het bewaken en vastleggen van het informatiesysteemgebruik

   Toelichting
   Om na een incident de oorzaak en/of veroorzaker te achterhalen is het belangrijk om het inloggen/ gebruik maken van informatiesystemen (AIS maar ook computers, servers, netwerk en andere programmatuur) te registreren. Alle aanlogpogingen op kritische systemen met alle activiteiten die daarop plaatsvinden worden daarvoor geautomatiseerd geregistreerd in een logboek. Een juiste instelling van de systeemklokken is van wezenlijk belang om de nauwkeurigheid van auditlogboeken te waarborgen.

2. De apotheek hanteert procedures voor het melden en afhandelen van informatiebeveiligingsincidenten of storingen die hier van invloed kunnen zijn.

   Toelichting
   Stel een incident managementprocedure op waarin informatiebeveiligingsincidenten en storingen die een invloed hierop hebben worden meegenomen. Wijs hierin ook verantwoordelijkheden toe aan leidinggevenden, gebruikers, beheerders, etc. Storingen die door gebruikers worden gerapporteerd en die betrekking hebben op problemen met een computer of een informatiesysteem kunnen in een logboek worden bijgehouden.

Totstandkoming

Deze richtlijn is in 2009-2010 opgesteld door ATOS-Consultancy in opdracht van het Kwaliteitsprogramma ICT van de KNMP. Concepten van de richtlijn zijn in 4 bijeenkomsten beoordeeld door een werkgroep van openbaar apothekers en ziekenhuisapotheker. De concept richtlijn is op implementeerbaarheid getoetst in 10 openbare apotheken en voorgelegd aan 3 apotheekketens.

Het definitieve concept werd door de KNMP-commissie informatievoorziening (CIV) beoordeeld en voorzien van een positief advies aan het Hoofdbestuur van de KNMP ter autorisatie. Het HB heeft de richtlijn op 14 juli 2010 als concept geautoriseerd met een overgangstermijn tot 1-1-13. Per 1-1-13 is de autorisatie van deze richtlijn definitief.

Aanhangsel

GBZ-eisen met betrekking tot informatiebeveiliging voor zover niet in de NEN 7510 beschreven. Alleen van toepassing bij aansluiting op het LSP.

Hoofdstuk 2 (principe 2.1)

1. Om aan de GBZ eisen te voldoen dient binnen de apotheek een GBZ verantwoordelijke aangewezen te zijn.

Hoofdstuk 6 (principe 6.3)

3. Een GBZ dient via een gekwalificeerde Zorgserviceprovider (ZSP) te communiceren met het Landelijk Schakel Punt (LSP).

Hoofdstuk 7 (principe 7.1)

4. Een GBZ moet zodanig zijn ingericht dat:
   a. alle UZI-paslezers gekoppeld zijn aan de werkplekken van de gebruikers,
   b. de PIN-code die ten behoeve van een UZI-pas wordt ingetoetst op een werkplek, exclusief wordt aangeboden aan de gekoppelde UZI-paslezer,

5. Van een GBZ dient het UZI-servercertificaat te zijn aangevraagd door de betreffende zorgaanbieder.

6. Een GBZ dient zijn UZI-servercertificaat te beveiligen tegen misbruik, en dient daartoe de van toepassing zijnde richtlijnen van het UZI-register na te volgen.

7. De zorgaanbieder verantwoordelijk voor het GBZ moet, conform de voorwaarden van het UZI-register, aanvragen respectievelijk tijdig vernieuwen:
   a. een UZI-servercertificaat voor het GBZ,
   b. UZI-passen voor de GBZ-gebruikers.

8. De GBZ-applicatiebeheerder moet op verzoek van de toezichthouder, binnen 24 uur, op basis van UZI-nummer een overzicht kunnen aanleveren van:
   a. alle zorgverleners die op dat moment gemandateerd zijn door of namens (één bepaalde) andere zorgverlener(s),
   b. indien de mandatering namens een zorgverlener is verleend, dient de mandaatbeheerder die het mandaat verstrekt heeft in het overzicht te staan, samen met de eventuele mandaatbeheerder(s) die het beheermandaat hebben doorgegeven.

9. De apotheek beschikt over procedures voor het veilig en verantwoord omgaan met een toegangspas zoals de UZI-pas.

Hoofdstuk 9 (principe 9.1)

10. Een GBZ dient 24 uur per dag en 7 dagen per week beschikbaar te zijn voor het afhandelen van berichten vanuit de Zorginformatiemakelaar (ZIM). uitgezonderd gepland onderhoud

Hoofdstuk 9 (principe 9.2)

11. Een GBZ dient dagelijks van zijn patiëntgegevens een back-up te maken en deze binnen 1 dag over te brengen naar een plaats die het beschermt tegen beschadiging en onbevoegde inzage.

Definities

Bedrijfsmiddel	Onder bedrijfsmiddel kan worden verstaan: • informatiebedrijfsmiddelen: gegevensbanken en gegevensbestanden, systeemdocumentatie, gebruikershandboeken, cursusmateriaal, bedieningsprocedures en ondersteunende procedures, continuïteitsplannen, uitwijkregelingen, gearchiveerde gegevens; • programmatuur: toepassingsprogrammatuur, systeemprogrammatuur, ontwikkelingshulp-bedrijfsmiddelen en hulpprogramma's; • fysieke bedrijfsmiddelen: computer- en communicatieapparatuur, gegevensdragers, medische en overige technische apparatuur, accommodatie; • diensten: computer- en communicatiediensten, algemene voorzieningen als verwarming, verlichting, energievoorziening, luchtbehandeling. Het begrip 'bedrijfsmiddelen' wordt in de NEN7510 ruim opgevat en omvat zowel gegevens en zaken die daaraan rechtstreeks zijn gerelateerd als overige voorzieningen die bij de informatievoorziening worden gebruikt.
Goed Beheerd Zorgsysteem (GBZ)	Omdat medische gegevens privacygevoelig zijn, staat veiligheid voorop bij gegevensuitwisseling. Daarom kunt u alleen deelnemen aan het EPD als u een goed beheerd zorgsysteem (GBZ) gebruikt. Dit betekent onder andere dat uw hard- en software geschikt is om gegevens te kunnen uitwisselen en dat u beschikt over een goede beveiliging.
Informatiesystemen	Het apotheek informatiesysteem (AIS), maar ook computers, servers, netwerk en andere programmatuur.
Landelijk Schakel Punt (LSP)	Het landelijk schakelpunt (LSP) is het centrale knooppunt voor de landelijke uitwisseling van patiëntgegevens tussen zorgaanbieders in Nederland.
Media	Tapes, CD's, DVD's, memorysticks, laptops, etc. maar ook papier.
Unieke Zorgverlener Identificatie (UZI)	Het Unieke Zorgverlener Identificatie Register (UZI-register) geeft een elektronisch paspoort (de UZI-pas) uit speciaal voor mensen die met zorggegevens werken.
Zorg Informatie Makelaar (ZIM)	Dit is een gemeenschappelijke ICT-voorziening die nodig is voor alle zorgaanbieders en andere zorgpartijen in Nederland om via hun goed beheerd zorgsystemen (GBZ'en) onderling patiëntgegevens te kunnen uitwisselen.
Zorg Service Provider (ZSP)	Leveranciers die zorgen voor de verbinding van zorgsystemen met het LSP worden zorgserviceproviders (ZSP's) genoemd