PBLQ

voor een sterke
publieke sector

Rapport

Onderzoek naar de beveiliging van patiëntgegevens

PBLQ

Onderzoek naar de beveiliging van patiëntgegevens

[Eindrapport]

Alles moet zo simpel mogelijk gehouden worden, maar ook niet simpeler”
Albert Einstein

“Never let a good crisis go to waste”
Winston S. Churchill

“Zwarte markt voor medische gegevens groeit”
Health Warning-rapport (26 oktober 2016)

auteurs	T. Hooghiemstra, J. Oud, M. Radema, M. Spruit, P. Wielaard
project	5519
versie	1.0
datum	1 december 2016

PBLQ

Managementsamenvatting

Naar aanleiding van een aantal incidenten met patiëntgegevens in zorginstellingen heeft de minister van VWS 16 maart jl. aan de Tweede Kamer toegezegd dat zij onafhankelijk onderzoek zal laten uitvoeren naar:

1) De wijze waarop zorginstellingen in de dagelijkse praktijk omgaan met de beveiliging van hun patiëntgegevens.
2) Hoe hierin verbetering kan worden aangebracht.

Het hier beschreven, door PBLQ uitgevoerde onderzoek (juli-november 2016), is kwalitatief en indicatief van aard. Het is gebaseerd op (groeps)interviews met betrokkenen uit het werkveld, alsmede een enquête en een bespreking van de resultaten uit het onderzoek met betrokkenen. Onder zorginstellingen worden in dit onderzoek conform de aanvraag verstaan: ziekenhuizen (inclusief privéklinieken, zelfstandige behandelcentra en revalidatiecentra) en GGZ-instellingen.

Op welke wijze gaan zorginstellingen in de dagelijkse praktijk om met de beveiliging van hun patiëntgegevens?

Ten opzichte van het onderzoek ‘Toegang tot digitale patiëntendossiers binnen zorginstellingen’ van de Autoriteit Persoonsgegevens uit 2013 (toen CBP) krijgt informatiebeveiliging en privacybescherming in de meeste instellingen meer aandacht en er zijn veel (nieuwe) good practices.

De externe omgeving van zorginstellingen wordt door de vergevorderde digitalisering van patiëntendossiers, de vlucht van eHealth, gezondheidsapps, big data en de toename van cyberdreigingen steeds complexer, alsook door wijzigingen in het zorgdomein zelf, zoals de decentralisaties. Steeds meer (digitale) patiëntgegevens worden verwerkt en steeds meer daarvan worden c.q. moeten worden verwerkt buiten de kring van rechtstreeks bij de behandeling betrokkenen, als gevolg waarvan de risico’s op incidenten met patiëntgegevens toenemen. Informatiebeveiliging en privacybescherming vergen constante aandacht. In die zin is er sprake van een continue toename van risico’s en verbeterpotentieel.

De wil en het besef dat patiëntgegevens moeten worden beschermd is er bij zorginstellingen; het is zelfs de basis onder het medisch beroepsgeheim. Bovendien wordt de aandacht voor de beveiliging van patiëntgegevens extra gestimuleerd door onder andere de meldplicht datalekken (artikel 34a Wbp) en de toename van cyberdreigingen. Uit de interviews, enquête en het Cybersecuritybeeld Nederland 2016 blijkt bijvoorbeeld dat ransomware voor veel zorginstellingen een groeiend probleem is. Er wordt hard gewerkt aan informatiebeveiliging en privacybescherming, onder meer door de opzet van een Zorg-CERT (Z-CERT) en het inzetten van specifieke functionarissen en het uitvoeren van bewustwordingscampagnes.

In de praktijk staan de vertrouwelijkheid en de beschikbaarheid van gegevens soms op gespannen voet met elkaar. Het is in meer situaties (technisch en organisatorisch) mogelijk dan nu het geval is om maatregelen ten behoeve van privacybescherming te treffen die ook een positief effect hebben op de zorgverlening. Veelal zijn de kosten daarvan echter relatief hoog. Een voorbeeld is het gebruik van authenticatie met behulp van een toegangspas die tevens uitlogt als de werkplek wordt verlaten en automatisch inlogt in iedere volgende werkplek.

Er is behoefte aan eenduidige en goed hanteerbare handvatten voor informatiebeveiliging en privacybescherming in de dagelijkse praktijk, voor bewerkersovereenkomsten, de omgang met incidenten, de

bescherming van patiëntgegevens in de onderzoekspraktijk en bij landelijke kwaliteitsregisters. Incidenten zijn niet te voorkomen omdat waterdichte beveiliging feitelijk niet mogelijk is, maar het gaat erom dat er wordt geleerd en dat de informatiebeveiliging en privacybescherming continu worden verbeterd.

Over het algemeen is er voldoende wet- en regelgeving ten aanzien van het werken met patiëntgegevens, maar is die wetgeving vooral (te) complex en daardoor soms onduidelijk in de zorgpraktijk. Uit het onderzoek komt geen indicatie naar voren dat verdere aanvulling van wet- en regelgeving voor informatiebeveiliging en privacybescherming in zorginstellingen noodzakelijk is, mede gelet op komende wet- en regelgeving, bestaande normen en (professionele) standaarden. Uit de interviews en enquête blijkt wel dat er vooral behoefte is aan het begrijpelijker maken van wet- en regelgeving en het vertalen ervan naar basisprincipes en concrete handvatten voor de praktijk.

Hoe kan hierin verbetering worden aangebracht?
Informatiebeveiliging en privacybescherming kunnen worden verbeterd door goed gedrag te bevorderen, good practices te delen, krachten te bundelen en handvatten voor wet- en regelgeving te bieden. Het anticiperen op de komst van de Algemene Verordening Gegevensbescherming (AVG) kan aangegrepen worden om tegelijk de nu al benodigde verbeteringen te realiseren.

1. *Goed gedrag bevorderen*

   Begin top-down met het goede voorbeeld door het management en verwijder drempels op de werkvloer die informatiebeveiliging en privacybescherming belemmeren. Voorbeelden:

   - Beleg de feitelijke eindverantwoordelijkheid voor de naleving van de informatiebeveiliging en privacybescherming bij de leiding van de zorginstelling en bespreek dit met de Raad van Toezicht.
   - Laat de leiding ervoor zorgen dat er voldoende mensen en middelen beschikbaar zijn voor het continu monitoren en verbeteren van informatiebeveiliging en privacybescherming. Dit omvat het aanwijzen (rol of functie) van een functionaris gegevensbescherming (FG) en een Information Security Officer (ISO).
   - Laat de leiding er voor zorgen dat de belangrijkste uitgangspunten, richtlijnen en standaarden voor informatiebeveiliging en privacybescherming zijn vastgelegd in een voor ieder toegankelijk beleid en dat de naleving daarvan wordt geborgd.
   - Laat de FG's of ISO's erop toezien dat alleen medewerkers die rechtstreeks bij de behandeling betrokken zijn, toegang hebben tot de patiëntinformatie, bijvoorbeeld door het monitoren van logging.
   - Neem in de jaarrapportage van de instelling een paragraaf op over de stand van zaken op het gebied van informatiebeveiliging.
   - Maak informatiebeveiliging en privacybescherming onderdeel van bestaande audits voor zover dit nog niet gebeurt.
   - Zorg dat medewerkers weten wat een datalek is en hoe daarmee omgegaan dient te worden.
   - Laat de FG of de ISO vanuit diens coördinerende rol voor relevante groepen medewerkers uitzoeken welke tekortkomingen er zijn op het gebied van kennis, vaardigheden en houding met betrekking tot informatieveiligheid en privacybescherming en op basis daarvan bepalen welke doelgroepgerichte opleiding en training nodig is.
   - Laat VWS onderzoeken of het niveau van informatiebeveiliging en privacybescherming bij landelijke registraties voldoende is.
   - Laat VWS agenderen dat thema's als informatiebeveiliging en privacybescherming voldoende in (medische) opleidingen aan bod komen, opdat het digibewustzijn wordt vergroot.

- Laat de koepels samen met VWS landelijke campagnes opzetten, gericht op alle meer dan 1.1 miljoen medewerkers werkzaam in de zorg en op alle gebruikers (patiënten), waarin de basisprincipes van (informatie)veilig werken en privacybescherming op duidelijke wijze wordt uitgelegd. Dit zal de komende jaren continue aandacht vragen.

2. *Good practices*

Belangrijke good practices die in het onderzoek naar voren zijn gekomen en die zowel volgens de geïnterviewden als PBLQ brede navolging verdienen, zijn:

- Het NFU-normenkader: dit geeft een beeld en handvatten over hoe informatiebeveiliging en wet- en regelgeving geïntegreerd aangepakt kunnen worden.
- Het handboek NEN 7510: voorbeelden hieruit kunnen worden gebruikt om informatiebeveiliging en privacybescherming relatief eenvoudig te handhaven door het nemen van technische en procedurele maatregelen die de zorgprocessen niet hinderen.
- Een geïntegreerd systeem en proces voor het registreren en afhandelen van datalekken en andere cyberincidenten in de bestaande systematiek voor de afhandeling van (andere) veiligheidsincidenten (veiligheidsincidentmelding- (VIM) / veiligheidsmanagementsysteem (VMS)), zoals diverse zorginstellingen al doen.
- Het toetsen op de aanwezigheid van goede (sub)bewerkersovereenkomsten en het naleven van de afspraken meenemen in audits, zoals diverse zorginstellingen al doen.
- Campagnes, zoals de NVZ-campagne ZEKER, die de bewustwording en eigen verantwoordelijkheid stimuleren bij het omgaan met gevoelige informatie.
- Informatiebeveiliging en privacybescherming (bijvoorbeeld voldoen aan de NEN 7510 en het hebben van een bewerkersovereenkomst) als onderdeel van de ICT-paragraaf van inkoopvoorwaarden, zoals al in sommige zorginstellingen gebeurt.

3. *Krachten bundelen*

De effectiviteit van informatiebeveiliging en privacybescherming kan worden vergroot door onderling en met andere betrokken organisaties samen te werken. Mogelijkheden voor verdere krachtenbundeling die in de interviews en de enquête genoemd zijn:

- Laat koepels in overleg met VWS en toezichthouders (AP en IGZ) meer sectorale afspraken maken en richtlijnen, modeldocumenten en gedragscodes opzetten en beschikbaar stellen:
  - Laat de IGZ en de AP op bestuurlijk niveau hun toezichtstaken ten aanzien van beschikbaarheid van patiëntgegevens (patiëntveiligheid) en vertrouwelijkheid (bescherming van persoonsgegevens) meer op elkaar afstemmen en hun informatieverstrekking en richtsnoeren meer baseren op door de koepels geventileerde behoeften uit de praktijk.
  - Laat de koepels en VWS gezamenlijk, op basis van de behoeften van de zorginstellingen, komen tot aanvullende sectorale afspraken, richtlijnen, modeldocumenten, standaardbewerkersovereenkomsten en gedragscodes op het gebied van informatiebeveiliging en privacybescherming, en zorgen dat hoogwaardige privacybeschermende technologie en bijbehorende protocollen worden ontwikkeld.
- Laat VWS faciliteren dat de verdere uitbouw van Z-CERT versneld en verbreed kan worden.

4. *Het bieden van handvatten voor wet- en regelgeving*

VWS, koepels en toezichthouders dienen te faciliteren dat wet- en regelgeving goed begrepen kan worden door zorgmedewerkers via praktische handvatten voor de praktijk, bijvoorbeeld:

- Maak vigerende wet- en regelgeving voor zorgmedewerkers behapbaar in sectorale en beroepsgerichte gedragscodes en thematische richtsnoeren.

- Maak informatiebeveiliging en privacybescherming onderdeel van de subsidievoorwaarden (bijvoorbeeld aangesloten zijn op Z-CERT en voldoen aan de NEN 7510).
- Laat de koepels en VWS er gezamenlijk voor zorgen dat de relevante normen en standaarden, voor zover dit nog niet het geval is, drempelvrij beschikbaar komen voor zorginstellingen.
- Bevorder dat authenticatiemiddelen met een hoog betrouwbaarheidsniveau landelijk worden toegepast binnen de zorg. Mede door het bij wet aangenomen digitale inzagerecht en de komst van patiëntportalen en persoonlijke gezondheidsomgevingen worden authenticatiemiddelen met een hoog betrouwbaarheidsniveau noodzakelijk.
- Geef aan zorginstellingen en gemeenten duidelijke handvatten over hoe zij om dienen te gaan met het medisch beroepsgeheim en het verwerken van patiëntgegevens, bijvoorbeeld in de jeugd-GGZ vanwege de uitvoering van de decentralisatiewetten. Overweeg pas aanvullende wet- of regelgeving als de handvatten onvoldoende blijken.

5. *Het anticiperen op de komst van de AVG*
   De AVG legt de lat voor informatiebeveiliging en privacybescherming hoger dan de vigerende wet- en regelgeving. Ten opzichte van de Wet bescherming persoonsgegevens (Wbp) komt de AVG met een aantal veranderingen:
   1) Accountability (documenteren en implementeren: kunnen laten zien dat AVG wordt nageleefd).
   2) Extra rechten (vergeetrecht, dataportabiliteit).
   3) Privacy by design.
   4) Privacy Impact Assessments.
   5) Hogere boetes.
   6) Strengere regels voor bewerkers / verwerkers.

   De voorbereiding op het kunnen voldoen aan de AVG en het verbeteren met de compliance van de huidige wetgeving, waaronder de Wbp, kan gecombineerd worden tot één verbeterslag. Met name vermeldenswaardig zijn:
   - Inventariseer welke externe partijen patiëntgegevens verwerken en in hoeverre daarbij gebruik wordt gemaakt van diensten van subbewerkers. Benoem verantwoordelijken voor het bijhouden van de lijst met subbewerkers. Sluit met de bewerkers bewerkersovereenkomsten af die voldoen aan de eisen die de AP daaraan stelt (waaronder het inventariseren en melden van subbewerkers, alsmede het borgen van de afspraken met de subbewerkers).
   - Laat zorginstellingen in hun contracten met bewerkers opnemen dat:
     - De zorginstelling precies wil weten welke patiëntgegevens door welke subbewerkers worden bewerkt.
     - Bewerkers en subbewerkerscontracten voldoen aan de voorwaarden die de AP daaraan stelt. Op deze wijze is geen verdere aanvulling van wetgeving nodig en kan door middel van de bewerkingsovereenkomst een incident als de bewerking van patiëntdossiers door gevangenen worden voorkomen.
   - Pas '*privacy by design'* toe. Zorg bijvoorbeeld dat in nieuwe systemen een goed autorisatiesysteem zit en dat er gebruik wordt gemaakt van voldoende sterke authenticatiemiddelen.
   - Zorg als beveiligingsmaatregel dat gegevens minimaal gepseudonimiseerd worden voordat zij voor wetenschappelijk onderzoek verstrekt worden aan andere (onderzoeks)organisaties (bijvoorbeeld landelijke kwaliteitsregisters) en zet een procedure op om de pseudonimiseringssleutel goed te beschermen. De FG van een zorginstelling kan dan controleren of de pseudoniemen voldoende beschermd zijn en de regels hieromtrent voldoende nageleefd worden. Dit kan onder meer worden meegenomen in een privacy impact assessment (PIA).

- Geef - na overleg tussen VWS en de AP - in de nationale uitvoeringswet behorende bij de AVG een duidelijk antwoord op de vraag of en in hoeverre en onder welke voorwaarden gepseudonimiseerde patiëntgegevens gebruikt mogen worden bij (wetenschappelijk) onderzoek en kwaliteitsregisters.

PBLQ

Inhoudsopgave

PBLQ

1. Inleiding

Het voorliggende rapport beschrijft de resultaten van het onderzoek naar de beveiliging van patiëntgegevens in zorginstellingen. Onder het begrip ‘zorginstellingen’ wordt in dit onderzoek conform de aanvraag verstaan: ziekenhuizen (inclusief privéklinieken, zelfstandige behandelcentra en revalidatiecentra) en GGZ-instellingen. Het onderzoek is gestart op 21 juli en afgerond op 28 november 2016.

1.1 Aanleiding

In de brief van 16 maart 2016 heeft de minister van VWS aan de Tweede Kamer toegezegd dat VWS onafhankelijk onderzoek zal laten doen naar de vraag op welke wijze zorginstellingen in de dagelijkse praktijk omgaan met de beveiliging van hun patiëntgegevens en hoe hierin verbetering kan worden aangebracht.

Daarbij is het volgens de minister vooral de kunst om het belang van de bescherming van patiëntgegevens verankerd te krijgen in de praktijk van de zorginstelling, in het gedrag van leidinggevenden en medewerkers én in de (aanspreek)cultuur in de zorginstellingen.

Het op te zetten onderzoek moet antwoord geven op de onderzoeksvragen zoals toegezegd in de brief van 16 maart 2016. Daarnaast heeft de minister nog een drietal vragen aan PBLQ voorgelegd die de Tweede Kamer tijdens het Algemeen Overleg op 29 juni jl. aan de minister stelde.

De onderzoeksvragen sluiten aan op de resultaten uit de campagne van de Nederlandse Vereniging van Ziekenhuizen (NVZ) die liep van 26 oktober tot 6 november 2015. De NVZ-campagne met de naam ZEKER stimuleerde bewustwording en eigen verantwoordelijkheid bij het omgaan met gevoelige informatie. In het onderzoek wordt specifiek aandacht besteed aan de wijze van omgaan met incidenten van schending van de bescherming van patiëntgegevens, die zich nu eenmaal altijd onverhoopt voor kunnen doen. In dit verband kan ook de meldplicht datalekken genoemd worden die sinds 1 januari jl. van kracht is. Ook wordt aandacht geschonken aan situaties waarin wordt gewerkt met bewerkers in de zin van de Wet bescherming persoonsgegevens (Wbp), bijvoorbeeld voor het digitaliseren van patiëntgegevens, en aan de bescherming van gegevens die worden gebruikt ten bate van wetenschappelijk onderzoek. Bovendien gaat het onderzoek op verzoek van de minister in op de vraag hoe op de beste wijze voorkomen kan worden dat medische dossiers door gevangenen worden bewerkt.

1.2 Onderzoeksvragen

De **onderzoeksvragen** zijn:

1. Hoe is de bescherming van patiëntgegevens verankerd in de praktijk van de zorginstellingen, het gedrag van leidinggevenden en medewerkers én in de (aanspreek)cultuur in de zorginstellingen?
2. Hoe is de bescherming van patiëntgegevens geborgd in situaties waarin wordt gewerkt met subbewerkers, waarbij gebruik moet worden gemaakt van een bewerkersovereenkomst?
3. Hoe wordt in zorginstellingen omgegaan met incidenten van schending van de bescherming van patiëntgegevens?

4. Hoe is de bescherming van patiëntgegevens voor wetenschappelijk onderzoek geborgd?
5. Behoeft de regelgeving met betrekking tot de bescherming van patiëntgegevens in zorginstellingen en bij subbewerkers aanscherping?

In aanvulling hierop heeft de minister van VWS naar aanleiding van vragen tijdens het Algemeen Overleg in de Tweede Kamer op 29 juni jl. nog de volgende drie vragen aan PBLQ gesteld:

6. Hoe is het gesteld met de verantwoordelijkheidsverdeling in de praktijk (wie hebben er in de praktijk toegang tot het dossier en hoe is dit formeel geregeld) ?
7. Wat is de stand van zaken met betrekking tot het digitaliseren van papieren dossiers?
8. Worden er opleidingen/ trainingen over informatiebeveiliging gegeven? Zo ja; aan wie?

Ten behoeve van het onderzoek zijn met 42 personen van ruim 20 organisaties diepte-interviews gevoerd. Deze personen hebben inzicht in of spelen een rol bij de beveiliging van patiëntgegevens in ziekenhuizen en de geestelijke gezondheidszorg. Bijlage A bevat de lijst van geïnterviewde personen. Daarnaast zijn op de geanonimiseerde enquête 25 reacties ontvangen.

Bovendien is relevante documentatie bestudeerd. Bijlage B bevat de lijst hiervan.

Het onderzoek is uitgevoerd als indicatief onderzoek. Dit betekent dat een beperkte hoeveelheid personen en documentatie is geraadpleegd en in beperkte mate bewijsmateriaal is gezocht om de bevindingen te staven. De onderzoekers hebben de indruk dat alle betrokkenen open en actief mee hebben gewerkt aan het onderzoek.

1.3 Werkwijze

De werkwijze bestaat uit drie hoofdfasen:

In de eerste fase is allerlei relevante documentatie verzameld voor het opstellen van een referentiekader. Daartoe is allereerst uitgebreide deskresearch verricht naar relevante casuïstiek en praktijkvoorbeelden uit nieuws- en tijdschriften. De opbrengst is gebruikt tijdens de diepte-interviews en de inrichting van de digitale enquête in fase 2. Vervolgens is allerlei relevante wet- en regelgeving in kaart gebracht met betrekking tot informatiebeveiliging en privacybescherming in de zorg. Tenslotte zijn bestaande goede praktijken uit zowel de (wetenschappelijke) literatuur als uit de praktijk verzameld. Hierbij is niet alleen gebruik gemaakt van desktopresearch, maar hebben de onderzoekers ook hun netwerk bij de instellingen geraadpleegd. Tevens zijn de koepels gevraagd om relevante informatie aan te leveren. De opbrengst is gebruikt tijdens de diepte interviews en de inrichting van de anonieme digitale enquête.
De eerste fase heeft geleid tot een referentiekader. De tweede fase bestaat uit diepte-interviews met de koepels en de IGZ, enkele ziekenhuizen, GGZ-instellingen en ICT-leveranciers. Een overzicht van de geïnterviewde personen is bijgevoegd in bijlage A. De geraadpleegde documentatie staat in bijlage B.
Voor de interviews met de koepels zijn tevens de aspecten van de “Zeker campagne”, de Toetsingscriteria van ZKN keurmerk consument, de open brief van de AP van 15 februari 2016, de door de AP gepubliceerde constatering 17 mei jl. - dat drie ziekenhuizen geen goede afspraken hadden gemaakt met een bedrijf dat namens het ziekenhuis digitaal patiëntgegevens verwerkte - en de open brief van de IGZ van 17 maart 2016 meegenomen.

Voor de diepte-interviews met de instellingen is gesproken met functionarissen betrokken in een keten, met leden van de Raad van Bestuur, medische professionals (van geneesheer-directeur tot internist tot ziekenhuisapotheker tot verpleegkundige), privacy officers / functionarissen gegevensbescherming, informatiebeveiligingsfunctionarissen, ICT medewerkers, bewerkers tot en met ICT leveranciers. De geselecteerde functionarissen hebben aansluiting met “wat er al is” en de praktijkvoorbeelden. Zij zijn zo goed als mogelijk geselecteerd op basis van het netwerk van de onderzoekers en de opdrachtgever waarbij enerzijds gestreefd is naar een spreiding van zorginstellingen (academisch, perifeer, GGZ), maar waarbij nadrukkelijk ook gepoogd is om binnen een zorginstelling meerdere functionarissen te spreken om zo de situatie in de instelling vanuit meerdere perspectieven te belichten.

Van de interviews zijn verslagen gemaakt. De verslagen zijn gebruikt voor de analyse van de onderzoekers in fase 3. Deze informatie is niet herleidbaar verwerkt in het rapport.

In fase 2 is tevens een anonieme digitale enquête opgezet. De enquête is kwalitatief van aard en heeft een indicatief karakter. Dit ter ondersteuning van de diepte-interviews en de verrijking van het onderzoek: representativiteit van de uitkomsten is met de enquête noch beoogd noch nagestreefd. Om de responsiviteit te vergroten zijn twee varianten opgesteld: een uitgebreide enquête voor experts uit het veld en een beperkte voor mensen uit de praktijk en op de werkvloer. In lijn met de opdracht is in de enquêtes voornamelijk gevraagd naar verbetermogelijkheden. In totaal zijn vijfentwintig reacties op beide enquêtes binnengekomen.

De derde fase bestaat uit analyse en toetsing. Het onderzoeksteam heeft in interne werksessies de verzamelde informatie en bevindingen - op basis van de interviews, beschrijvingen en de enquête – geanalyseerd op grond van het referentiekader. Dit heeft geleid tot conclusies en aanbevelingen, die tijdens de EffectenArena[1] met een selectie van vooraanstaande geïnterviewden zijn besproken.

1.4 Leeswijzer

Voorafgaand aan de beantwoording van de onderzoeksvragen behandelen we in hoofdstuk 2 eerst het referentiekader van dit onderzoek. Daarna volgt een hoofdstuk per beantwoorde vraag.

Hoofdstuk 3: Bescherming patiëntgegevens in de praktijk, gedrag én in cultuur

Hoofdstuk 4: (Sub)bewerkers

Hoofdstuk 5: Incidenten

Hoofdstuk 6: Bescherming van patiëntgegevens in wetenschappelijk onderzoek

Hoofdstuk 7: Wet – en regelgeving

In hoofdstuk 8 beantwoorden we de aanvullende vragen en we eindigen met onze conclusies en aanbevelingen in hoofdstuk 9.

[1] De deelnemers aan de EffectenArena staan in Bijlage A.

PBLQ

2. Referentiekader

Dit referentiekader bestaat uit twee delen: ten eerste een referentiekader voor informatiebeveiliging en privacybescherming in het algemeen.[2] Ten tweede de relevante wet- en regelgeving, inclusief (beroeps)normen.[3]

2.1 Informatiebeveiliging en privacybescherming

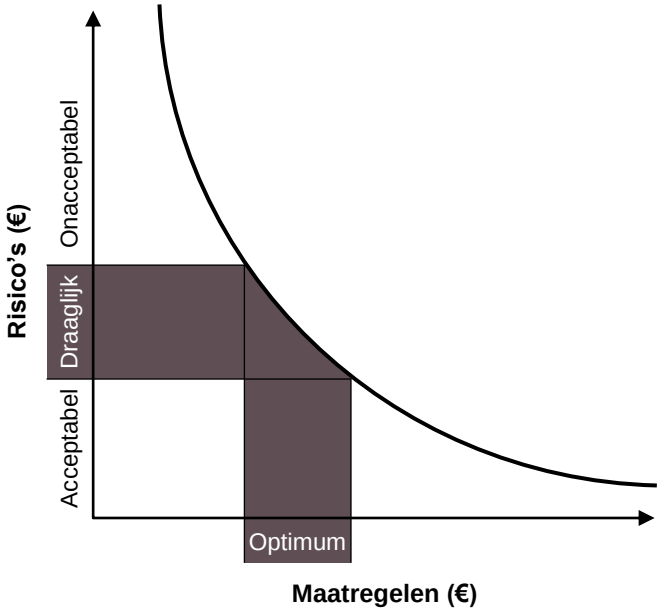
Zorginstellingen verwerken als onderdeel van hun zorgverlenende taken veel gegevens, ook privacygevoelige gegevens. Deze gegevens zijn noodzakelijk voor het verlenen van goede zorg. Niet beschikbare of onjuiste gegevens kunnen verstrekkende gevolgen hebben voor het succes van de zorg en daarmee de gezondheid van patiënten. Maar ook het ongeautoriseerd gebruik of het uitlekken van privacygevoelige gegevens kan vervelende gevolgen hebben. Dit vraagt om goede beveiliging van de gegevens, oftewel goede informatiebeveiliging en privacybescherming.

Informatiebeveiliging is het treffen en onderhouden van een samenhangend pakket maatregelen om de beschikbaarheid, integriteit (juistheid) en vertrouwelijkheid van de gegevens in de organisatie te waarborgen. Het beschermen van privacygevoelige gegevens zoals patiëntgegevens maakt hier deel van uit, evenals het voorkomen en aanpakken van ongeautoriseerd gebruik van (privacygevoelige) gegevens.

Informatiebeveiliging is geen eenmalige actie, maar een zaak die continu aandacht vraagt van alle betrokkenen. Het vraagt om een procesmatige aanpak waarbij tijdig bijstelling plaats kan vinden op basis van nieuwe of gewijzigde risico's.

De risico's waar informatiebeveiliging zich op richt, ontstaan door bedreigingen voor de informatievoorziening. Het betreft een grote verscheidenheid aan bedreigingen, variërend van menselijke fouten tot hackers en computervirussen, en van storingen in de ICT tot blikseminslag en overstroming. De risico's kunnen worden beperkt door het nemen van beveiligingsmaatregelen. Te weinig maatregelen is niet goed, maar te veel is ook niet goed. Te veel maatregelen is niet alleen te duur, maar het werpt ook teveel hindernissen op voor de degenen die met de gegevens moeten werken. De uitdaging is dan ook om het optimum te vinden (zie figuur).

[2] P. van Houten, M. Spruit & K. Wolters, *Informatiebeveiliging onder controle*, Pearson, Amsterdam, 2015; M. Spruit, *Volwassenheid informatiebeveiliging, RAAK-project Veilig Water*, Haagse Hogeschool, 2016; M. Spruit & M. de Graaf, Een twee-sporenaanpak voor informatiebeveiliging, *Management Executive*, nr. 1, 2004, pag. 34-37.
[3] De relevante wet- en regelgeving, relevante NEN-normen, T.F.M. Hooghiemstra en S. Nouwt, *SDU Commentaar, Wet bescherming persoonsgegevens*, editie 2016; J. Krabben (PrivacyCare) en T.F.M. Hooghiemstra (PBLQ), *Patiëntauthenticatie*, advies in opdracht van minister van VWS van augustus 2016; *Handreiking Betrouwbaarheidsniveaus* (Versie 4) (Forum Standaardisatie, november 2016).



De benodigde beveiligingsmaatregelen worden in het algemeen onderverdeeld in twee groepen:

- De organisatiebrede basisbeveiliging.
- De aanvullende beveiligingsmaatregelen voor de kritische processen en systemen.

Systemen waarin patiëntgegevens worden verwerkt zijn kritische systemen. Voor deze systemen mag men er niet zonder meer vanuit gaan dat de maatregelen van de basisbeveiliging alle risico's voldoende reduceren. Met behulp van risicoanalyse kan bepaald worden of, en zo ja, welke maatregelen aanvullend nodig zijn.

Binnen de procesmatige aanpak van informatiebeveiliging worden verscheidene activiteiten uitgevoerd, waaronder:

- Het opstellen van informatiebeveiligingsbeleid.
- Het organiseren van informatiebeveiliging in de organisatie.
- Het identificeren en analyseren van risico's ten aanzien van de informatie(voorziening).
- Het selecteren, invoeren en onderhouden van beveiligingsmaatregelen.
- Het borgen van de naleving van de getroffen beveiligingsmaatregelen.
- Het maken en controleren van beveiligingsafspraken met leveranciers en ketenpartijen.
- Het accepteren van de restrisico's.
- Het detecteren, registreren en analyseren van informatiebeveiligingsincidenten.
- Het geven van opvolging aan opgetreden incidenten, bijvoorbeeld het melden van een datalek aan de toezichthouder of betrokkenen.
- Het meten en verbeteren van de awareness ten aanzien van informatiebeveiliging.
- Het controleren van de informatiebeveiliging.

Informatiebeveiliging staat niet op zichzelf, maar behoort een natuurlijk onderdeel te zijn van de processen in de zorginstelling. Hierdoor zien mensen de beveiligingsaspecten als logisch en zijn eerder geneigd de beveiligingsmaatregelen te accepteren in hun werk. Bij het selecteren van beveiligingsmaatregelen en de

daarvoor benodigde hulpmiddelen dient er op gelet te worden dat de maatregelen en hulpmiddelen zo min mogelijk impact hebben op de inrichting van het dagelijkse werk.

We kunnen de volgende succesfactoren voor de informatiebeveiliging in zorginstellingen formuleren:

1) De directie heeft een beleid voor informatiebeveiliging opgesteld, heeft hierover goed gecommuniceerd en bewaakt zichtbaar de navolging ervan.
2) Er is een sluitende inrichting van de informatiebeveiligingsorganisatie, met voldoende ervaren mensen en alle benodigde bevoegdheden.
3) Het eigenaarschap van kritische processen en systemen is adequaat ingevuld en geborgd.
4) Awareness ten aanzien van informatieveiligheid wordt geborgd door goede informatieverstrekking, actieve participatie en voorbeeldwerking.
5) Met alle relevante leveranciers en ketenpartijen zijn afspraken met betrekking tot informatiebeveiliging gemaakt en die worden gecontroleerd.
6) Er is een baseline voor informatiebeveiliging ingevoerd en de actualiteit en naleving van de maatregelen wordt geborgd.
7) Voor alle kritische processen en systemen is een actuele risicoanalyse beschikbaar en de follow up ervan wordt geborgd.
8) Alle kritische componenten van de informatievoorziening worden gemonitord op potentieel schadelijke bedreigingen.
9) De betrouwbaarheid van alle kritische componenten van de informatievoorziening wordt regelmatig getoetst.
10) Alle incidenten met betrekking tot de informatievoorziening worden adequaat gemeld, geregistreerd en gerapporteerd.
11) De organisatie en processen voor de informatiebeveiliging worden regelmatig geaudit door ervaren auditors.

2.2 Wet en regelgeving, inclusief (beroeps)normen

Er is veel wet- en regelgeving en er zijn ook al veel (beroeps)normen inzake informatiebeveiliging en privacybescherming. Bovendien neemt de wet- en regelgeving verder toe, zoals het op 4 oktober jl. door de Eerste Kamer aangenomen Wetsvoorstel cliëntenrechten elektronische gegevensuitwisseling, waardoor de patiënt straks zelf kan bepalen wie zijn medisch dossier mag inzien. Artikel 25 van die wet[4] geeft aan dat deze wet aangehaald dient te worden als Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg. Daarnaast worden steeds hogere niveaus van informatiebeveiliging en privacybescherming voorgeschreven op grond van diverse Europese verordeningen en richtlijnen, zoals de Algemene Verordening Gegevensbescherming (AVG) die vanaf 25 mei 2018 van toepassing zal zijn, de eIDAS-verordening voor elektronische identiteiten over betrouwbaarheidsniveau's en authenticatie die 1 juli 2016 in werking is getreden en de 8 augustus jl. in werking getreden EU-richtlijn Netwerk en Informatiebeveiliging (NIB). Hieronder volgt een overzicht van de meest relevante wetten, regels en (beroeps)normen. In de documentatielijst is waar mogelijk een digitale link opgenomen naar de betreffende tekst van deze wet- en regelgeving.

[4] www.eerstekamer.nl/behandeling/20161019/publicatie_wet/document3/f=/vk8f2rahsksv.pdf. Staatsblad 2016, nr. 373.

1) Archiefwet
2) Auteurswet
3) Grondwet (in het bijzonder artikel 10 en 13)
4) Wet kwaliteit, klachten en geschillen zorg
5) Richtlijnen Centrale Commissie Mensgebonden Onderzoek (CCMO)
6) Richtlijnen van de International Conference on Harmonisation of technical requirements for registration of pharmaceutical for human use. Good Clinical Practice.
7) Telecommunicatiewet
8) Wet beroepen in de individuele gezondheidszorg (Wet BIG)
9) Wet bescherming persoonsgegevens (Wbp), inclusief meldplicht datalekken (artikel 34a Wbp)
10) Wetsvoorstel Computercriminaliteit III
11) Wet gebruik Burgerservicenummer in de zorg (Wbsn-z)
12) Wet geneeskundige behandelingsovereenkomst (WGBO), eigenlijk boek 7 BW artikel 7:446 e.v.
13) Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg
14) Wet medisch-wetenschappelijk onderzoek met mensen (WMO, niet te verwarren met de andere Wmo voor maatschappelijk ondersteuning)
15) Wet maatschappelijke ondersteuning (Wmo)
16) Jeugdwet
17) Wet langdurige zorg
18) Wet op het hoger onderwijs en wetenschappelijk onderzoek

19) Algemene Verordening Gegevensbescherming (AVG)
20) eIDAS-Verordening
21) EU-Richtlijn Netwerk en Informatiebeveiliging (NIB)
22) Europese richtlijn medische apps
23) Zorgbrede govenancecode 2017
24) Richtlijn omgaan met medische gegevens, KNMG
25) (herziene) Convenant medische technologie (IGZ)

26) NEN 7510 (informatiebeveiliging in de zorg)
27) NEN 7512 (Vertrouwensbasis voor gegevensuitwisseling)
28) NEN 7513 (Logging)
29) Richtsnoeren beveiliging persoonsgegevens van de Autoriteit Persoonsgegevens
30) Handreiking betrouwbaarheidsniveau's. Versie 4, Forum Standaardisatie.

2.3 Vertrouwen, bescherming en beveiliging

Verwerken van persoonsgegevens: de Wbp en de AVG

Bescherming van persoonsgegevens is onderdeel van het recht op privéleven (artikel 8 EVRM) en is verder als grondrecht erkend in artikel 16 VWEU en in artikel 10 Grondwet. De wet vereist dat het verwerken van persoonsgegevens goed beveiligd plaatsvindt. Deze eis is vastgelegd in artikel 13 Wbp. Deze wet stelt de algemene eisen aan het verwerken van persoonsgegevens.

De tekst van de AVG staat sinds 25 mei 2016 vast en wordt 25 mei 2018 van toepassing. Het is dan de belangrijkste wetgeving op het gebied van de bescherming van persoonsgegevens in de EU. De verordening vervangt de Wbp. Tot 25 mei 2018 dient hierop te worden voorbereid.

De AVG omvat aangescherpte regels voor bescherming van (bijzondere) persoonsgegevens en hoge boetes voor niet naleving daarvan. Een verschil met de huidige Nederlandse privacywetgeving uit de Wbp is dat de verplichtingen in de AVG op veel punten gedetailleerder zijn uitgewerkt. Daarbij komt ook aan de orde op welke wijze aan de norm moet zijn voldaan. Er wordt een accent gelegd op accountability. Dat betekent dat organisaties die persoonsgegevens verwerken, verplicht worden hun verwerkingsprocessen te beschrijven en zodanig in te richten dat ze in staat zijn aan te tonen dat ze voldoen aan de wet.
Naast het algemene vereiste dat iedere organisatie moet zorgdragen voor een adequate beveiliging verplicht de AVG organisaties om *"privacy impact assessments"* te verrichten, om *"privacy by design"* toe te passen en dit alles vast te leggen. Daarnaast zullen organisaties veel meer aandacht moeten gaan besteden aan de wijze van informeren van betrokkenen over de verwerking van hun persoonsgegevens. Ook om te voldoen aan het inzage- en correctierecht zal een organisatie processen moeten inrichten.
In de AVG staat een verplichting aan de lidstaten tot het vaststellen van nadere regels binnen de grenzen van de verordening bij de verwerking van gegevens betreffende de gezondheid. Dat komt in een nationale uitvoeringswet te staan.
Kortom: de Wbp wordt in de komende jaren vervangen door de AVG met aangescherpte voorwaarden voor (het) proces van de verwerking van (bijzondere) persoonsgegevens (in de zorg). De precieze uitwerking volgt. In het navolgende hanteren we de Wbp als geldend recht.

De Wbp
Voor het goede begrip van dit rapport zullen we de kern van de Wbp en de begrippen toelichten. De Wbp is van toepassing voor zover het gaat om het verwerken van persoonsgegevens. Een persoonsgegeven is 'elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon'. Daarbij gaat het ook om gegevens die in hun onderlinge samenhang of op zich, indirect tot een persoon te herleiden zijn. Het 'verwerken' omvat elke handeling met betrekking tot de persoonsgegevens, zoals het inzien, opslaan en delen van de gegevens. Degene wiens persoonsgegevens worden verwerkt is de 'betrokkene' in de zin van de Wbp.

Verantwoordelijke
De normen van de Wbp richten zich grotendeels tot de 'verantwoordelijke' voor de gegevensverwerking. Dit is volgens de Wbp 'degene die het doel en de middelen voor de verwerking van persoonsgegevens vaststelt'. De partij die de gegevens van betrokkenen voor door hem vastgestelde doelstellingen vastlegt en bepaalt hoe de verwerking plaatsvindt, is verantwoordelijke voor die gegevensverwerking. Dat kunnen ook meerdere partijen samen zijn. Wanneer een partij de gegevens vastlegt in opdracht en voor doelstellingen van een ander treedt zij op als 'bewerker' van de gegevens in de zin van de Wbp.
Niet alleen is de verantwoordelijke degene die de verplichtingen uit de Wbp moet opvolgen, ook is hij het aanspreekpunt voor betrokkenen met betrekking tot de gegevensverwerking en het uitoefenen van zijn rechten.

Bewerker en bewerkerovereenkomst
De vraag naar de (sub)bewerkers is een belangrijke vraag in dit onderzoek. De bewerker verwerkt persoonsgegevens onder gezag van de verantwoordelijke. De eventuele subbewerker is daar weer een 'onderaannemer' van waar het gaat om het verwerken van persoonsgegevens.

De Autoriteit Persoonsgegevens (AP) heeft aangegeven aan welke eisen een bewerkersovereenkomst moet voldoen. Een bewerkersovereenkomst moet aan een aantal minimumeisen voldoen:
1) De overeenkomst moet specifiek gaan over de gegevensverwerking door de bewerker.

2) De verplichtingen moeten over en weer duidelijk zijn vastgelegd in de overeenkomst. Het soort gegevens, de doeleinden van de verwerking, de duur van de opslag en beveiligingsmaatregelen moeten er bijvoorbeeld gedetailleerd in zijn opgenomen.
3) In de overeenkomst moet staan hoe de verantwoordelijke kan toezien op de naleving van de waarborgen.
4) De overeenkomst moet een geheimhoudingsplicht bevatten voor de bewerker en zijn personeel.
5) Als er sprake is van subbewerkerschap, moeten ook daarover bepalingen in de overeenkomst worden opgenomen.

Het begrip ‘bewerker’ wordt in de komende AVG ‘verwerker’ genoemd.

Voor de verwerker in de AVG gelden ten opzichte van de bewerker in de Wbp de volgende aanvullende specifieke verplichtingen:

- Bewerkers worden verplicht een overzicht bij te houden van alle categorieën persoonsgegevens die zij verwerken in opdracht van een verantwoordelijke;
- Bewerkers mogen niet langer nieuwe sub-bewerkers inschakelen zonder toestemming van de verantwoordelijke;
- In bepaalde gevallen moet de bewerker, voorafgaand aan de verwerking van persoonsgegevens, de AP consulteren omtrent de effectieve bescherming van de rechten en vrijheden van betrokkenen of een Privacy Impact Assessment uitvoeren;
- Bewerkers dienen in bepaalde gevallen zelf een privacy officer (of data officer) aan te stellen. Dit is bijvoorbeeld het geval wanneer de bewerker een publieke organisatie is, bij de verwerking sprake is van op grote schaal reguliere en systematische monitoring van betrokkenen of wanneer de primaire activiteiten van de verwerking bestaan uit het op grote schaal verwerken van bijzondere persoonsgegevens.

Grondslag
De Wbp vereist een grondslag voor de gegevensverwerking op grond van artikel 8 Wbp. Daarin wordt aangegeven voor welke doeleinden persoonsgegevens verwerkt mogen worden. De verantwoordelijke dient de doeleinden vast te stellen.
Als daarbij ook ‘bijzondere’ gegevens worden verwerkt zoals bedoeld in artikel 16 Wbp, is een grondslag uit artikel 8 Wbp alleen niet voldoende. Het verwerken van bijzondere persoonsgegevens is verboden, tenzij sprake is van een van de uitzonderingen in de Wbp (artt. 17 t/m 23 Wbp). Bijzondere persoonsgegevens zijn bijvoorbeeld strafrechtelijke gegevens of gezondheidsgegevens. Bij zorginstellingen zal het verwerken van bijzondere gegevens bijna altijd aan de orde zijn. Een grondslag voor het verwerken van patiëntgegevens kan bijvoorbeeld zijn een wettelijke verplichting, de goede uitvoering van de behandelingsovereenkomst of toestemming van een patiënt.

Gezondheidsgegevens
Onder gezondheidsgegevens worden blijkens de Memorie van Toelichting bij de Wbp alle gegevens verstaan die de geestelijke of lichamelijke gezondheid van een persoon betreffen. Een afspraak in de agenda bij de longarts wordt ook als een gezondheidsgegeven beschouwd.
De Wbp geeft een ontheffing voor het verwerken van ‘gegevens betreffende de gezondheid’ aan hulpverleners en instellingen wanneer dat noodzakelijk is voor de goede zorgverlening aan de betrokkene (artikel 21 lid 1 onder a Wbp). Ook kan de ontheffing voortvloeien uit de uitdrukkelijke toestemming van de betrokkene (artikel

23 Wbp). Uitdrukkelijke toestemming dient aan bepaalde voorwaarden te voldoen om een geldige ontheffing en grondslag te bieden.
Gegevens betreffende de gezondheid mogen alleen worden verwerkt door personen op wie een geheimhoudingsplicht rust, dan wel aan wie deze contractueel is opgelegd. Ook de verantwoordelijke zelf is op grond van de wet gehouden tot geheimhouding, behoudens het geval de wet hem tot mededeling van bepaalde gegevens verplicht.
Ook andere bijzondere gegevens kunnen worden verwerkt door hulpverleners en instellingen als dat in aanvulling op de gezondheidsgegevens noodzakelijk is voor de goede behandeling of verzorging van betrokkenen. (Artikel 21 lid 3 Wbp)

Verder verwerken van gegevens
De Wbp regelt in artikel 9 dat verzamelde gegevens niet verder mogen worden verwerkt voor andere doeleinden die niet verenigbaar zijn met het doeleinde van verkrijging. Daarboven geldt op grond van artikel 9 lid 4 Wbp dat een verwerking achterwege moet blijven wanneer een geheimhoudingsplicht aan het (verder) verwerken in de weg staat. Dat kan aan de orde zijn bij vertrouwelijke gegevens die onder toepassing van een geheimhoudingsplicht worden verwerkt. Deze bepaling correspondeert met het medisch beroepsgeheim van zorgverleners zoals uit de WGBO (7:457 BW) volgt. Verder geldt voor BIG-geregistreerde professionals artikel 88 van de Wet BIG. Op grond van dit artikel is eenieder die zorg verleent op het gebied van de individuele gezondheidszorg verplicht tot geheimhouding van datgene wat hem in de uitvoering van het beroep is toevertrouwd.

Beveiligingseisen
Op grond van artikel 13 Wbp dient de verantwoordelijke passende technische en organisatorische maatregelen te treffen om persoonsgegevens te beveiligen tegen verlies of enige vorm van onrechtmatige verwerking. ‘Passend’ betekent in dit verband dat de beveiliging in overeenstemming is met het risico van de gegevensverwerking (in verband met onder andere de aard van de gegevens en het gebruik) de stand van de techniek en de kosten van de tenuitvoerlegging. Het begrip ‘passend’ duidt op proportionaliteit tussen de beveiligingsmaatregelen en de te beschermen gegevens. Naarmate bijvoorbeeld de gegevens een gevoeliger karakter hebben, of de context waarin deze wordt gebruikt een grotere bedreiging voor de persoonlijke levenssfeer betekent, worden zwaardere eisen gesteld aan de beveiliging van de gegevens. Er is geen verplichting om altijd de hoogste mate van beveiliging te realiseren. Daarom duidt ook het feit dat inbreuken zijn gemaakt op het beveiligingsniveau niet noodzakelijkerwijs op nalatigheid in de beveiliging. Er moet sprake zijn van een adequate beveiliging.
Er kunnen geen algemene uitspraken worden gedaan over wat als een ‘passende beveiligingsmaatregel’ kan worden beschouwd. Dit criterium moet in het licht van de concrete omstandigheden worden ingevuld en is voor een deel dynamisch. Het vereiste niveau van bescherming is hoger naarmate er meer maatregelen voorhanden zijn om dat niveau te waarborgen. "In het algemeen kan worden gesteld dat indien met naar verhouding geringe extra kosten meer beveiliging kan worden bewerkstelligd deze als ‘passend’ moeten worden beschouwd, terwijl kosten die disproportioneel zijn aan de extra beveiliging die daardoor zou worden verkregen, niet worden vereist. Met zich ontwikkelende techniek zal periodiek een nieuwe afweging moeten worden gemaakt", stelt de wetgever vast.
Technische en organisatorische maatregelen dienen cumulatief te worden getroffen. Software is een belangrijk instrument tot beveiliging.
De AP, voorheen het CBP, toezichthouder op de Wbp, heeft in de Richtsnoeren Beveiliging van persoonsgegevens de eisen omtrent beveiliging nader uitgewerkt.

De beveiligingsverplichting richt zich in de eerste plaats tot de verantwoordelijke. De verantwoordelijke moet in kaart brengen welk risico gemoeid is met de gegevensverwerkingen. Uit de Richtsnoeren Beveiliging van persoonsgegevens volgt dat het inrichten van een Plan Do Check Act (PDCA) cyclus in de organisatie daarvoor nodig is. Het verwerken van gezondheidsgegevens brengt bijzondere risico's met zich mee, mede in verband met de vertrouwelijkheid van de gegevens. De open norm van artikel 13 Wbp kan op passende wijze worden ingevuld, door te voldoen aan de bestaande (Nederlandse en internationale) normen voor informatiebeveiliging. Voor zorginstellingen betreft het onder andere de NEN 7510, 7512 en 7513. Er zal daarnaast moeten worden afgewogen welke aanvullende maatregelen eventueel nodig zijn in verband met de bijzonderheden en risico's van de verwerking.
De methode of het middel van toegang waarmee de gebruiker toegang krijgt vormt de authenticatie. Evenals identificatie van belang voor de beveiliging.
Onderdeel van beveiliging is ook het regelen van de (omvang van de) toegang tot gegevens (autorisaties) voor gerechtvaardigde gebruikers. Er dient een autorisatieprotocol te worden vastgesteld afhankelijk van de noodzaak bepaalde gegevens te verwerken, in overeenstemming met de grondslag voor de verwerking.

Rechten van betrokkenen
Een betrokkene heeft het recht inzage en een overzicht te verkrijgen van de verwerking van zijn persoonsgegevens van de verantwoordelijke. Ook heeft hij het recht op correctie, aanvulling, afscherming of verwijdering van gegevens wanneer deze feitelijk onjuist zijn of zonder rechtsgrond verwerkt worden. De bijzondere wetgeving geeft aanvullende rechten aan betrokkenen en patiënten. Zo heeft de betrokkene in beginsel recht op vernietiging van het dossier dat op grond van de WGBO door de zorg- of hulpverlener is vastgelegd. Dit onderscheid wordt in het onderzoek verder niet gemaakt. Uitgegaan wordt van de patiënt zoals bedoeld in de WGBO.

Wet op de geneeskundige behandelingsovereenkomst en wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (cliëntenrechten elektronische gegevensuitwisseling)
De WGBO is van toepassing op het verwerken van gegevens door de zorgverlener die hij in het kader van de behandeling van de patiënt heeft verkregen. Die wet verplicht hem de noodzakelijke gegevens vast te leggen in zijn dossier over de patiënt. Wanneer de zorgverlener gegevens over de patiënt wil delen heeft hij te maken met het beroepsgeheim dat in de WGBO verankerd is. Aan anderen dan de patiënt verstrekt de zorgverlener in beginsel slechts gegevens omtrent de patiënt met zijn toestemming. De toestemming van de patiënt verplicht de hulpverlener niet om te spreken. De hulpverlener dient immers ook het maatschappelijke en collectieve belang van het beroepsgeheim mee te wegen[5]. Overigens is er ook een andere grond voor doorbreking van het medisch beroepsgeheim, namelijk als er een wettelijke verplichting is om de gegevens aan een derde te verstrekken. De toestemming van de patiënt is niet nodig als het gaat om rechtstreeks bij de behandelingsovereenkomst betrokkenen en de betreffende informatie noodzakelijk is voor de behandeling.

Medisch beroepsgeheim belangrijke waarde bij beveiliging van patiëntgegevens
Van bijzondere waarde bij informatiebeveiliging en privacybescherming in de zorg is het medisch beroepsgeheim. Het medisch beroepsgeheim staat in toenemende mate onder druk. Het beroepsgeheim is er in de eerste plaats voor patiënten: zij moeten er altijd op kunnen vertrouwen dat wat zij met de arts bespreken

[5] Zie hiervoor factsheet medisch beroepsgeheim, https://www.rijksoverheid.nl/documenten/rapporten/2015/06/30/factsheet-medisch-beroepsgeheim bijlage bij Kamerstukken kst-34300-XVI-161

vertrouwelijk blijft. Zo blijft het ook een waarborg voor de toegankelijkheid van de zorg. Het beroepsgeheim is echter niet absoluut. Het gaat om een afweging wanneer artsen pal moeten staan voor het beroepsgeheim en wanneer zij dit mogen doorbreken.

Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg
Het wetsvoorstel cliëntenrechten bij elektronische gegevensuitwisseling in de zorg is 4 oktober jl. door de Eerste Kamer aangenomen en dient na de inwerkingtreding op 1 juli 2017 overeenkomstig artikel 25 van die wet[6] te worden aangehaald als Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg. Deze wet is een aanvulling op onder andere de Wbp/AVG, de Wgbo, de Wet gebruik burgerservicenummer in de zorg, de Wet marktordening gezondheidszorg en de Zorgverzekeringswet. Door deze wet kan de patiënt 3 jaar na de inwerkingtreding zelf bepalen wie zijn medisch dossier kan inzien. In het rapport Patiëntauthenticatie van PrivacyCare en PBLQ, dat voor de Minister van VWS onder andere ten behoeve van deze wet is geschreven, staat dat voor patiëntauthenticatie minimaal niveau ‘substantieel’ en voor veel situaties betrouwbaarheidsniveau ‘hoog’ (eIDAS) is vereist. Niveau ‘hoog’ is vereist indien er sprake is van een combinatie van het verwerken van gezondheidsgegevens, het BSN en het medisch beroepsgeheim. De minister en de Kamerleden hebben tijdens de behandeling van deze wet aangegeven dat het daarbij belangrijk is dat de burger beschikt over veilige authenticatiemiddelen op voldoende hoog betrouwbaarheidsniveau waarmee hij zijn gegevens in kan zien en opslaan. Daarom laat zij de bepalingen ten aanzien van elektronische inzage en elektronisch afschrift pas in werking treden op het moment dat een authenticatiemiddel op hoog niveau beschikbaar is voor veilige elektronische inzage en afschrift.

NEN en ISO-normen voor informatiebeveiliging
ISO/NEN 27001 en 27002, samen de Code voor informatiebeveiliging, vormen gezamenlijk de algemene norm voor de invulling van informatiebeveiliging. Voor gegevensbeveiliging in de zorg zijn de NEN 7510, 7512 en 7513 aanvullend van belang.

NEN 7510, NEN 7512, NEN 7513
De NEN-normen voor informatiebeveiliging in de zorg zijn ook richtinggevend voor de uitwerking van het identiteitsmanagement. Deze NEN-normen zijn opgenomen in de ‘Regeling gebruik Burgerservicenummer in de zorg’ als invulling van het vereiste van ‘passende technische en organisatorische beveiligingsmaatregelen in de zin van artikel 13 Wbp, en (op grond van de wet) van toepassing op gegevensverwerking waarbij het BSN wordt verwerkt.
De NEN 7510 is de norm voor het organiseren en borgen van informatiebeveiliging in de zorg. De norm richt zich op alle kleine en grote organisaties die hiermee te maken hebben. NEN 7510 is een algemene norm. De NEN 7512, NEN 7513 werken deze norm verder uit. De NEN 7510 geeft aanwijzingen over het organisatorisch en technisch inrichten van informatiebeveiliging in een zorginstelling. Het managementsysteem voor informatiebeveiliging en de risicoanalyse van informatiebeveiliging hebben een centrale plaats in de norm.
De Inspectie voor de Gezondheidszorg (IGZ) heeft aangegeven de NEN-normen te hanteren bij het toetsen van de vraag of zorginstellingen de juiste maatregelen treffen voor invoering en handhaving van adequate informatiebeveiliging.
Ook de AP hanteert de NEN 7510, 7512 en 7513 als uitgangspunt voor toetsen van passende beveiliging in de zorg, in het bijzonder ook voor toegangsbeveiliging.

[6] Staatsblad 2016, nr.373.

De NEN 7512 bevat een aanvulling voor een vertrouwensbasis voor gegevensuitwisseling in de zorg. In de NEN 7512 wordt de voor de gegevensuitwisseling vereiste zekerheid gekoppeld aan risicoklasse.
Als authenticatiemiddel kan gebruik worden gemaakt van *kennis* waarover de entiteit moet beschikken, van een fysiek authenticatiemiddel dat deze in *bezit* moet hebben, van een uniek *kenmerk* van de gebruiker of van een combinatie van deze authenticatiefactoren. De volgende authenticatiemiddelen worden onderscheiden: 1) Geheime kennis (wachtwoord, pincode); Fysiek kenmerk (biometrie; Fysiek bezit (token); Toetsbare verklaring (digitaal certificaat).
Benadrukt dient te worden dat de beveiliging van de toegang voor patiënten tot hun medische gegevens een continu managementproces vergt, waarbij risico's worden geïnventariseerd, beleid en plannen worden opgesteld, maatregelen worden geïmplementeerd en de effectiviteit van de genomen maatregelen wordt geëvalueerd waar vanaf het proces opnieuw begint.

eIDAS
De eiDAS-verordening van het Europees Parlement en de Raad is per 1 juli 2016 van toepassing. eIDAS legt criteria vast voor de betrouwbaarheidsniveaus van authenticatiemiddelen. Er zijn drie niveaus: laag, substantieel en hoog. Met deze verordening is er een wettelijk kader om betrouwbaarheidsniveaus te bepalen voor digitale overheidsdiensten.
Deze verordening gaat over de elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en leidt tot een wettelijk kader voor betrouwbaarheidsniveaus. De verordening regelt daartoe het grensoverschrijdend gebruik van elektronische identificatiemiddelen en vertrouwensdiensten tussen de lidstaten van de Europese Unie.
Om het stelsel in 2018 over de grens bruikbaar te laten zijn, zodat Nederlandse burgers de mogelijkheid hebben om met hun nationale middelen zich te authentiseren in andere landen, zal Nederland zijn eigen ETD-stelsel notificeren bij de Europese Commissie. Een lidstaat bepaalt zelf (of en) wanneer hij zijn stelsel wil notificeren. Notificatie is echter een voorwaarde om Nederlandse authenticatiemiddelen in andere EU-lidstaten te kunnen gebruiken. Nederland moet het in september 2018 mogelijk maken dat met genotificeerde middelen uit andere EU-lidstaten diensten afgenomen kunnen worden bij Nederlandse publieke instellingen en overheden.

eIDAS kent drie niveaus: laag, substantieel en hoog. Deze zijn nader uitgewerkt in een uitvoeringsverordening. Voor het vaststellen van de specificaties en procedures die in deze uitvoeringshandeling zijn opgenomen, is rekening gehouden met de internationale norm ISO/IEC 29115, de internationale norm op het gebied van betrouwbaarheidsniveaus voor elektronische identificatiemiddelen. eIDAS verschilt inhoudelijk van die internationale norm, met name wat betreft de vereisten voor het bewijs en de verificatie van de identiteit, alsmede wat betreft de wijze waarop de verschillen tussen de identiteitsregelingen van de lidstaten en de bestaande EU-instrumenten op dat gebied in aanmerking worden genomen.

De eIDAS verordening dient op grond van overweging 11 van de verordening te worden toegepast in volledige overeenstemming met de beginselen inzake de bescherming van persoonsgegevens overeenkomstig Richtlijn 95/46/EG van het Europees Parlement en de Raad. Daarmee zijn de hiervoor behandelde Wbp en de eIDAS verordening met elkaar verbonden.

3. Bescherming patiëntgegevens in de praktijk, gedrag én in cultuur

AP vraagt extra aandacht voor bescherming patiëntgegevens (AP 15-02-2016)
(…) De Autoriteit Persoonsgegevens krijgt regelmatig vragen en signalen over patiëntendossiers die onder ogen zouden zijn gekomen van medewerkers van zorginstellingen die daar niets mee te maken hadden (…) Het voorkomen van incidenten en het daadwerkelijk goed regelen van gecontroleerde toegang tot patiëntgegevens bleek een complexe, maar niet onmogelijke opgave (…)

"Zwarte markt voor medische gegevens groeit" (Health Warning-rapport 26-10-2016)

Ziekenhuisapparatuur kwetsbaar door standaardwachtwoorden (Security.nl, 19-05-2016)
Apparatuur in ziekenhuizen is kwetsbaar voor aanvallen doordat er vaak van standaardwachtwoorden gebruik gemaakt wordt. Dat stelt Deloitte aan de hand van onderzoek onder 24 ziekenhuizen uit 9 verschillende landen. Meer dan de helft van de ziekenhuizen blijkt standaardwachtwoorden te gebruiken om apparatuur te beveiligen (…)

3.1 Bevindingen

De vertrouwelijkheid van patiëntgegevens is een kernwaarde voor zowel patiënten als zorgaanbieders en is ook de grond onder het medisch beroepsgeheim. Niemand wil de oorzaak zijn van een datalek. In beginsel is dat besef er bij iedereen in het primaire zorgproces.

Daarnaast is goede, veilige zorg een kernwaarde. Daarbij is informatie-uitwisseling tussen betrokken zorgverleners zowel een noodzaak als een risico. In de praktijk van zorgverlening leidt dit tot een belangenafweging tussen zorgkwaliteit en vertrouwelijkheid. De positie van vertrouwelijkheid kan worden versterkt, door enerzijds bewustwording en anderzijds het inzetten van ondersteunende technische en organisatorische maatregelen. Een voorbeeld is het gebruik van authenticatie met behulp van een toegangspas die tevens uitlogt als de werkplek wordt verlaten en automatisch inlogt in iedere volgende werkplek, alsook medische apparatuur.

Het delen van patiëntgegevens binnen de eigen organisatie onder voorwaarde van een behandelrelatie is een belangrijke pijler in de cultuur. Het formeel aanspreken, adviseren van privacyaspecten en informatieveiligheid gebeurt in de regel door de functionaris gegevensbescherming (FG) of de information security officer (ISO).

In de afgelopen jaren lijkt de positie van informatiebeveiliging en privacybescherming te zijn verbeterd. Veel instellingen hebben hiervoor meer capaciteit beschikbaar gesteld. Drivers hiervoor zijn onder andere de meldplicht datalekken (artikel 34a Wbp) en de toename van cyberdreigingen, zoals ransomware. Bewustwordingscampagnes hebben bij diverse zorginstellingen bijgedragen aan meer bewustwording. De NVZ campagne "Je bent zelf een datalek" van de tool "Zeker-Check" wordt positief gewaardeerd door zorginstellingen.

Men is zich steeds meer bewust geworden van het belang van informatiebeveiliging en privacybescherming. Zowel op managementniveau als op de werkvloer wordt het belang van informatiebeveiliging en privacybescherming onderkend. Op verschillende niveaus worden echter verschillende prioriteiten gesteld. Op de werkvloer bijvoorbeeld wordt de spanning tussen privacybescherming en medische gezondheid relatief sterk gevoeld. Gegevensbeschikbaarheid en integriteit worden sowieso belangrijk gevonden, al onderschatten veel zorgverleners de digitale dreigingen. Bewustwording vereist daarom constante aandacht.

Uit het onderzoek komt het beeld naar voren dat er veel gewerkt wordt met campagnes om bewustwording ten aanzien van informatiebeveiliging en privacybescherming te vergroten. Kortom, binnen veel zorginstellingen werkt men aan het verbeteren van de bewustwording. 'Lokale' bewustwordings-campagnes (door zorginstellingen binnen de eigen organisatie) oefenen doorgaans een positieve invloed uit op de bewustwording. Het beschikbaar stellen van campagnemateriaal door de overheid en de koepels kan dit effect versterken. Daarnaast is het van belang dat voldoende rekening wordt gehouden met de specifieke behoefte van bepaalde groepen medewerkers.

De externe omgeving van zorginstellingen wordt steeds complexer, niet alleen door de vergevorderde digitalisering van patiëntendossiers, big data en de toename van cyberdreigingen, maar ook door de digitalisering van complexe medische apparatuur, de vlucht van eHealth en gezondheidsapps en patiëntportalen en persoonlijke gezondheidsomgevingen, alsook door wijzigingen in het zorgdomein zelf, zoals de vernetwerking van de zorg en decentralisaties van jeugdzorg naar gemeenten.

Voorbeelden die bijdragen aan de complexe externe omgeving van zorginstellingen zijn onder andere:

Digitalisering van complexe medische apparatuur
Diverse geïnterviewden geven aan dat medische apparatuur, met veelal een eigen besturingssysteem, databasemanagementsysteem en applicatieprogrammatuur, in toenemende mate een gevaar vormt. Als oorzaken hiervoor worden genoemd dat deze systemen zelf meer patiëntgegevens verwerken en opslaan, zij steeds meer verbonden zijn met andere systemen van de zorginstellingen en steeds intensiever op afstand beheerd worden. Het gerealiseerde beveiligingsniveau loopt niet altijd in pas men het voor deze systemen benodigde beveiligingsniveau. Bovendien ontbreken veelal heldere richtlijnen en voorlichting.

eHealth en gezondheidsapps
Een van de geïnterviewde zorginstellingen heeft een onderzoek in voorbereiding naar de gevolgen van de inzet van eHealth. Daarbij wordt bijvoorbeeld gedacht aan de volgende casuïstiek rond een hartpatiënt in verschillende situaties zonder en met eHealth, waarbij de hartpatiënt:

1) in het ziekenhuis ligt met medische apparatuur van het ziekenhuis.
2) in behandeling is bij het ziekenhuis maar thuis gebruik maakt van apparatuur van het ziekenhuis.
3) in behandeling is bij het ziekenhuis maar thuis gebruik maakt van zijn eigen apparatuur.

Met name in de laatstgenoemde situatie is privacybescherming in relatief slecht beveiligde consumentenapparatuur moeilijk te realiseren. Bovendien is er een veelheid aan medische apps beschikbaar waarbij het niet altijd even helder is welke patiëntinformatie wordt verzameld en aan wie dit wordt doorgegeven. Het verstrekken aan andere organisaties van de persoonlijke gegevens is een

belangrijke pijler in diverse verdienmodellen. Overigens is een Europese richtlijn voor medische apps in de maak.

Patiëntportalen en persoonlijke gezondheidsomgevingen
Patiënten toegang geven tot hun eigen gegevens – onder andere op grond van de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg – vraagt om voldoende identificatie en authenticatie.
Ondanks de mogelijkheden om informatiebeveiliging en privacybescherming vanaf het begin goed in de patiëntportalen in te regelen, lijkt er vooralsnog weinig gebruikt te worden gemaakt van voldoende hoge betrouwbaarheidsniveaus van authenticatie, zoals beschreven in het rapport Patiëntauthenticatie van PrivacyCare en PBLQ.

Naast authenticatie is ook autorisatie bij de informatiebeveiliging en privacybescherming van systemen een zorgpunt. Dit zorgpunt wordt groter door bovengenoemde ontwikkelingen, zoals de vlucht van eHealth en gezondheidsapps, patiëntportalen en persoonlijke gezondheidsomgevingen en digitalisering van complexe medische apparatuur.

Vernetwerking van de zorg
Steeds meer patiëntgegevens worden in digitale vorm verwerkt en komen steeds vaker buiten de kring van rechtstreeks bij de behandeling betrokkenen terecht. Gemeenten en andere overheden ontvangen patiëntgegevens in het kader van de decentralisaties in de (jeugd)zorg. Diverse zorginstellingen en leveranciers geven aan dat de uitwisseling van patiëntgegevens in regionale netwerken, naast de evidente medische voordelen, ook risico's met zich brengen. Het 'DNA' van de gemeenten en andere overheden is niet altijd gelijk aan dat van de zorginstellingen en het opgebouwde 'DNA' van het medisch beroepsgeheim. De regels voor het delen van informatie van een persoon voor overheidsdoeleinden op basis van basisregistraties of van patiënten op basis van een medisch dossier waar geheimhouding op rust, is verschillend. Bovendien nemen de cyberdreigingen toe, zoals hacking, computervirussen, ransomware en phishing. Informatiebeveiliging en privacybescherming vergen constante aandacht. In die zin is er sprake van een continu verbeterpotentieel.

Informatiebeveiliging en privacybescherming landen alleen in een organisatie als dit van hoog naar laag door de organisatie gedragen wordt en op een realistische wijze kan worden uitgevoerd. Wat betreft leiderschap is het daarom van belang dat de leiding het belang van informatiebeveiliging en privacybescherming begrijpt, dit actief uitdraagt binnen en buiten de organisatie en de uitvoering ervan faciliteert, bijvoorbeeld door voldoende personeel en ondersteunende middelen hiervoor beschikbaar te stellen.

In 2013 constateerde het CBP in een onderzoek naar de toegang tot digitale patiëntendossiers in zorginstellingen dat thema's als informatiebeveiliging en privacybescherming op het bestuurlijke niveau van zorginstellingen onvoldoende 'leefden': uit dat onderzoek van het CBP bleek dat in geen van de toen onderzochte zorginstellingen het bestuur de toegang tot gedigitaliseerde patiëntendossiers zodanig had ingericht dat enkel medewerkers die een behandelrelatie met de betreffende patiënt hadden of als toegang voor de beheersmatige afwikkeling van de behandeling noodzakelijk was, toegang tot de patiëntgegevens hadden.
Uit voorliggend onderzoek komt het beeld naar voren dat dit inmiddels beter gaat dan ten tijde van het onderzoek door het CBP, maar niet overal in dezelfde mate.

De voorzitters van ActiZ, GGZ Nederland, NFU, NVZ en VGN hebben in het najaar van 2016 een geheel vernieuwde Zorgbrede Governancecode voor 2017 met een positief advies aan de besturen van de brancheorganisaties voorgelegd. De governancecode benoemt de vereiste kwaliteit. Over de boeg van kwaliteit wordt in de governance van veel zorginstellingen informatieveiligheid uitgewerkt. Slechts enkele zorginstellingen, met name UMC's, bespreken op dit moment met hun Raad van Toezicht en/of Raad van Bestuur vraagstukken van cybersecurity, hoewel cybersecurity onderdeel uitmaakt van informatiebeveiliging. Koepels en nationale instellingen kunnen een rol spelen in het faciliteren in de informatiebeveiliging in zorginstellingen. Een voorbeeld hiervan is een CERT voor de zorg (Z-CERT), gekoppeld aan de NCSC en andere CERT organisaties.

Een belangrijk onderdeel van de cultuur is dat de mensen op de werkvloer weten en accepteren dat als een product of systeem niet aan de beveiligingsnormen voldoet, dit niet wordt aangeschaft en dat deze gang van zaken/beleid actief door de leiding wordt gesteund, onder andere in de vorm van inkoopvoorwaarden.

In de meeste instellingen lijkt geen afrekencultuur te bestaan ten aanzien van datalekken, maar in interviews is aangegeven dat het toch kan gebeuren dat een ogenschijnlijke incidentveroorzaker onterecht de schuld van een datalek krijgt. Dit brengt enerzijds de kans met zich dat toekomstige potentiële incidenten niet of minder vaak worden gemeld, en anderzijds leidt dit ertoe dat er niet geleerd kan worden van reeds gemaakte fouten. Het is van belang dat blame-free gemeld kan worden.

Niet alle zorginstellingen geven in de interviews en enquêtes aan al volledig te voldoen aan de NEN 7510, terwijl deze baseline voor informatiebeveiliging en privacybescherming beschouwd kan worden als een minimum beveiligingsniveau. Er zijn verschillende methoden om vast te stellen in hoeverre en in welke mate de NEN 7510 is geïmplementeerd. UMC's benchmarken zich al meer dan 12 jaar iedere twee jaar tegen de norm en hebben daarvoor instrumenten ontwikkeld en beschikbaar gesteld aan de ziekenhuizen.

Daar waar informatiebeveiliging en privacybescherming lang werden beschouwd als op zichzelf staande, meer technische aangelegenheden die vaak belegd werden bij de ICT-afdeling, komt uit de interviews het beeld naar voren dat informatiebeveiliging bij een aantal instellingen als integraal onderdeel van goede zorg wordt gezien, en dan ook geïntegreerd wordt in bestaande processen en systemen rondom de dagelijkse zorg: voor het melden van beveiligingsincidenten wordt dan aansluiting gezocht bij bestaande processen rondom Veiligheids Incident Meldingen (VIM)-meldingen, omdat medewerkers daar reeds bekend mee zijn.

Voor medewerkers in zorg is de wet- en regelgeving voor informatiebeveiliging en privacybescherming vaak te abstract en onduidelijk voor hun specifieke werksituatie. Zo is het bijvoorbeeld niet altijd duidelijk wie rechtstreeks bij een behandeling betrokken is, en op grond daarvan bepaalde autorisaties zou moeten krijgen. Een ander voorbeeld is dat de NEN 7510 vaak als complex en moeilijk te begrijpen wordt beschouwd door medewerkers. Overigens is er wel een goed Handboek NEN 7510 met good practices, maar dat er zijn volgens sommige kleinere zorginstellingen teveel drempels (zoals kosten en administratieve handelingen) om dit aan te schaffen.

Zorginstellingen zijn zoekende waar het gaat om informatiebeveiliging en privacybescherming bij de uitwisseling van patiëntgegevens met onder meer gemeenten, bijvoorbeeld in het kader van de decentralisaties in de (jeugd)zorg. Recentelijk zijn in het i-Sociaal Domein convenanten, protocollen en vuistregels opgesteld. Meer duiding en voorlichting zijn wenselijk.

Binnen de brede groep van zorginstellingen en daarbuiten, bijvoorbeeld de gemeenten, wordt in wisselende mate samengewerkt en informatie uitgewisseld op het gebied van informatiebeveiliging en privacybescherming. Zo werken de UMC's bijvoorbeeld met elkaar samen op dit gebied en is structureel ingeregeld dat de NFU wordt gevoed door de groep van security officers en de groep van privacy officers.

3.2 Good practices

- **Managementrapportage**. Sommige zorginstellingen nemen informatiebeveiliging en privacybescherming mee in hun managementrapportage. De managementrapportage wordt vervolgens besproken in de lijnafdelingen.

- **Proces- en systeemeigenaarschap**. Een adequate invulling en borging van het eigenaarschap (verantwoordelijkheid) van kritische processen en systemen geldt als good practice voor informatiebeveiliging.

- **Aansluiten bij bestaande systematiek voor de afhandeling van (andere) veiligheidsincidenten.** Diverse zorginstellingen verankeren informatiebeveiliging en privacybescherming in het gedrag van medewerkers en de organisatiecultuur, door systemen en processen voor het registreren en afhandelen van datalekken en andere cyberincidenten te integreren in de bestaande systematiek voor de afhandeling van (andere) veiligheidsincidenten (veiligheidsincidentmelding- (VIM) / veiligheidsmanagementsysteem (VMS)). Door een categorie informatiebeveiliging aan deze systemen toe te voegen, kan voor het melden van beveiligingsincidenten worden aangesloten bij de bestaande systematiek voor de afhandeling van (andere) veiligheidsincidenten.

- **Protocollering.** Protocollering en het inrichten van processen voor het doen van meldingen van beveiligingsincidenten helpen bij het stimuleren van het doen van meldingen van incidenten. Door heel duidelijk en praktisch te maken wanneer en hoe gemeld moet worden, biedt een protocol handelingsperspectief voor medewerkers, zeker indien aansluiting wordt gezocht bij bestaande procedures voor het melden van andere incidenten.

- **Jaarlijkse Veiligheidsweek**. Een jaarlijkse Veiligheidsweek levert bij één van de geïnterviewde zorginstellingen een bijdrage aan het besef dat informatiebeveiliging en privacybescherming een natuurlijk onderdeel zijn van veiligheid in de zorg.

- **De NVZ-campagne ZEKER**. De NVZ-campagne ZEKER stimuleerde bewustwording en eigen verantwoordelijkheid bij de omgang met gevoelige informatie. In het bijzonder de NVZ-tool 'Doe de zeker-check' werd in meerdere interviews als positief ervaren, alsmede de persoonlijke aanpak en benadering. Treffend is daarbij de uitspraak: "Kijk uit Bert, je bent een datalek!". Tegelijkertijd biedt de tool bij elk thema concrete handvatten en tips, waarmee de tool direct van praktische waarde is voor op de werkvloer.

- **Smiley's en saddies**. Bij diverse instellingen worden inspectierondes gemaakt door het gebouw. Afdelingshoofden en medewerkers ontvangen feedback in de vorm van smiley's of een groene kaart met complimenten en toelichting. Ook worden saddies of rode kaarten neergelegd, met daarin de noodzakelijke verbeteracties. In sommige situaties worden foto's genomen om de situatie te bespreken, zonder 'blaming and shaming'. Na deze gesprekken zijn een goede follow up en regelmatige controles nodig.

- **Multifunctionele ID-kaart.** Er zijn zorginstellingen die een (ID)pas gebruiken voor niet alleen toegang tot fysieke locaties, maar ook voor het inloggen in een computersessie. Bij het niet-gebruiken van de pc wordt deze dan automatisch gelocked. Bij een van de instellingen is het zelfs mogelijk om met deze pas een computersessie ‘mee te nemen’ naar een ander systeem, doordat iedere andere pc waar de betreffende medewerker zich met de pas aanmeldt de lopende computersessie ‘overneemt’. Het is zelfs mogelijk om dit toe te passen bij het inloggen op complexe medische apparatuur.

- **‘Hello authenticatie’.** Tijdens een van de interviews werd ‘Hello authenticatie’ als voorbeeld genoemd. Deze gezichtherkenningsoftware signaleert wanneer iemand niet meer achter het scherm zit, en sluit de sessie vervolgens af. Bovendien is dit een voor de gebruiker erg makkelijke manier van authentiseren.

- **Follow-me printers**. Dit is een beveiligingsmaatregel tegen het vergeten van het afhalen van uitgeprinte (gevoelige) documenten, doordat documenten pas uitgeprint worden als de betreffende medewerker zich aanmeldt bij een printer. Dit ervaren gebruikers bovendien als een aantrekkelijke extra functionaliteit omdat ze op elke printer uit kunnen printen die op dat moment handig is, zonder dat ze daarvoor van tevoren een keuze voor plaats of tijd hebben moeten maken. Bij diverse zorginstellingen is dit al een geïmplementeerde maatregel.

- **Z-CERT.** Ter bevordering van de cyber security in de zorg en mede met het oog op de 8 augustus jl. inwerking getreden Europese cybersecurityrichtlijn over Netwerk en Informatiebeveiliging (de NIB-richtlijn) hebben de NVZ, NFU en GGZ Nederland initiatief genomen tot de oprichting van een Computer Emergency Response Team voor de zorg, de Z-CERT. De richtlijn gaat digitale serviceproviders verplichten tot een hoger beveiligingsniveau voor sectoren die onder de NIB vallen. Daarnaast wordt een meldplicht voor beveiligingsincidenten geïntroduceerd.
  Het initiatief tot de oprichting van Z-CERT wordt nu gedragen door drie partijen. De partijen vertegenwoordigen ieder een branche met een eigen en onderling verschillende dynamiek, cultuur en werkwijze. De mate waarin cybersecurity op de agenda staat verschilt net als het volwassenheidsniveau waar aan dit thema in individuele zorgorganisaties inhoud wordt gegeven. Het is de bedoeling dat de Z-CERT op termijn haar doelgroep stapsgewijs uitbreidt naar andere onderdelen van de zorg, naar andere (ook kleinere) organisaties. De oprichting van Z-CERT is mogelijk door de bereidheid van private en publieke partijen financieel bij te dragen aan het compenseren van aanloopverliezen. Daarom zal de Z-CERT een financiële bijdrage vragen aan de deelnemende zorginstellingen en zal zij in haar publieke optreden vooruit moeten lopen op de uitbreiding van deelname uit andere aanpalende zorgbranches, maar ook onder de zorginstellingen uit de achterbannen van de initiatiefnemers. “The proof of the pudding is in the eating”: de Z-CERT zal zich – zeker bij eventueel voorkomende incidenten – in haar vroege operationele bestaan moeten bewijzen.

3.3 Aanbevelingen ter verbetering

Goed gedrag bevorderen

- Beleg de feitelijke eindverantwoordelijkheid voor de naleving van de informatiebeveiliging en privacybescherming bij de leiding van de zorginstelling en bespreek dit met de Raad van Toezicht.
- Neem in de jaarrapportage van de instelling een paragraaf op over de stand van zaken op het gebied van informatiebeveiliging.
- Laat de leiding ervoor zorgen dat er voldoende mensen en middelen beschikbaar zijn voor het continu monitoren en verbeteren van informatiebeveiliging en privacybescherming. Dit omvat het aanwijzen (rol of functie) van een functionaris gegevensbescherming (FG) en een information security officer (ISO).
- Laat de leiding er voor zorgen dat de belangrijkste uitgangspunten, richtlijnen en standaarden voor informatiebeveiliging en privacybescherming zijn vastgelegd in een voor ieder toegankelijk beleid en dat de naleving daarvan wordt geborgd.
- Pas '*privacy by design'* toe. Zorg bijvoorbeeld dat bij de aanschaf van nieuwe systemen daar een goed autorisatiesysteem in zit en dat er gebruik wordt gemaakt van voldoende sterke authenticatiemiddelen. Zie bijvoorbeeld het cybersecurity rapport van Herna Verhagen/CSR (Nederland Digitaal Droge Voeten), aangeboden op 6 oktober aan Mark Rutte. Met name wat de zorgplicht van leveranciers betreft.
- Maak informatiebeveiliging en privacybescherming onderdeel van de bestaande audits voor zover dit nog niet gebeurt. Waar nodig kan dit worden aangevuld met testen, zoals penetratietesten en social engineering testen.
- Zorg dat medewerkers weten wat een datalek is en hoe daarmee omgegaan dient te worden.
- Laat de FG of de ISO vanuit diens coördinerende rol voor relevante groepen medewerkers uitzoeken welke tekortkomingen er zijn op het gebied van kennis, vaardigheden en houding met betrekking tot informatieveiligheid en privacybescherming en op basis daarvan bepalen welke doelgroepgerichte opleiding en training nodig is.
- Zorg dat er dat er een leerproces gekoppeld wordt aan (de afhandeling) van meldingen en incidenten, opdat er geleerd wordt van een incident en de bewustwording hierover toeneemt. Dit zou ook moeten gelden in relatie tot meldingen aan de AP. Ook daar is een PDCA cyclus van groot belang.
- Laat de koepels samen met VWS landelijke campagnes opzetten, gericht op alle meer dan 1.1 miljoen medewerkers werkzaam in de zorg en op alle gebruikers (patiënten), waarin de basisprincipes van (informatie)veilig werken en privacybescherming op duidelijke wijze wordt uitgelegd. Dit zal de komende jaren continue aandacht vragen.

Good practices

- Maak gebruik van uitwerken van relevante normen en standaarden en good practices. Het NFU-normenkader bijvoorbeeld geeft een beeld en handvatten over hoe informatiebeveiliging en wet- en regelgeving geïntegreerd aangepakt kunnen worden. Daarnaast kunnen voorbeelden uit het handboek NEN 7510 worden gebruikt om informatiebeveiliging en privacybescherming relatief eenvoudig te handhaven door het nemen van technische en procedurele maatregelen die de zorgprocessen niet hinderen.
- Integreer systemen en processen voor informatiebeveiliging en privacybescherming bij voorkeur in de bestaande systemen en processen voor veiligheid (veiligheidsmanagementsysteem (VMS)).

- Maak informatiebeveiliging en privacybescherming (bijvoorbeeld voldoen aan de NEN 7510 en het hebben van een bewerkerscontract), voor zover dat nog niet gebeurt, onderdeel van de ICT-paragraaf van inkoopvoorwaarden.

Krachten bundelen

- Laat koepels in overleg met VWS en toezichthouders (AP en IGZ) meer sectorale afspraken maken en richtlijnen, modeldocumenten en gedragscodes opzetten en beschikbaar stellen:
    - Laat de IGZ en de AP op bestuurlijk niveau hun toezichtstaken ten aanzien van beschikbaarheid van patiëntgegevens (patiëntveiligheid) en vertrouwelijkheid (bescherming van persoonsgegevens) meer op elkaar afstemmen en hun informatieverstrekking en richtsnoeren meer baseren op door de koepels geventileerde behoeften uit de praktijk.
    - Laat de koepels en VWS gezamenlijk, op basis van de behoeften van de zorginstellingen, komen tot aanvullende sectorale afspraken, richtlijnen, modeldocumenten, standaardbewerkersovereenkomsten en gedragscodes op het gebied van informatiebeveiliging en privacybescherming, en zorgen dat hoogwaardige privacybeschermende technologie en bijbehorende protocollen worden ontwikkeld.
- Laat VWS faciliteren dat de verdere uitbouw van Z-CERT versneld en verbreed kan worden.

4. (Sub)bewerkers

AP eist betere afspraken over digitaliseren patiëntdossiers (AP 17-05-2016)
De Autoriteit Persoonsgegevens (AP) heeft geconstateerd dat drie ziekenhuizen geen goede afspraken hadden gemaakt met een bedrijf dat namens het ziekenhuis patiëntgegevens verwerkte. (…) De AP stelde vast dat één ziekenhuis geen bewerkersovereenkomst met het scanbedrijf had gesloten. Twee andere ziekenhuizen hadden wel bewerkersovereenkomsten gesloten, maar deze voldeden niet aan alle wettelijke eisen. Zo ontbraken er details over de duur van de opslag en de beveiliging van de gegevens of was er niet expliciet een plicht tot geheimhouding opgenomen (…)

Belgische gevangenen werkten met Nederlandse patiëntendossiers (NOS 25-01-2016)
Medische dossiers van Nederlandse patiënten zijn naar een gevangenis in het Belgische Leuven gestuurd om ze klaar te maken voor digitalisering. Daarbij zijn privacyregels aan de laars gelapt. Medische gegevens mogen wettelijk niet aan derden ter inzage worden gegeven zonder uitdrukkelijke toestemming van de patiënt (…)

Rel om oude röntgenfoto's Groningen (NOS 14-01-2015)
Het Universitair Medisch Centrum Groningen (UMCG) heeft opdracht gegeven de vernietiging van oude röntgenfoto's onmiddellijk te stoppen. Een bedrijf dat ermee belast is, is onzorgvuldig met het materiaal omgegaan, meldt het ziekenhuis. RTV Noord meldt dat er onder meer grappen werden gemaakt over een röntgenfoto van iemand die in de schaamstreek is geschoten (…)

Duitsers onderzoeken carnavalsconfetti van zorgdossiers (NOS 12-02-2016)
Een verzorgingscentrum in Dermbach heeft een onderzoek ingesteld nadat versnipperde patiëntendossiers bij het carnaval als confetti waren gebruikt. Bij de schoonmaak na het langsrijden van de carnavalsoptocht, zag een inwoner van de Duitse plaats de medische gegevens van haar zus op straat liggen. De dossiers waren in veel te grote stukken versnipperd (…)

4.1 Bevindingen

Zorginstellingen maken in het algemeen gebruik van verscheidene externe partijen voor het bewerken van patiëntgegevens in de zin van de Wbp. Een gemiddeld ziekenhuis heeft naar schatting van de geïnterviewden al gauw 60 bewerkers en bij UMC's gaat het om honderden. Denk daarbij bijvoorbeeld aan leveranciers van informatiesystemen, software, archivering, medische apparatuur, (secure) mail, het digitaliseren van papieren dossiers en het bewerken van medische beelden. In sommige gevallen dateert dit soort externe bewerkingen al vanaf de zeventiger jaren. Het aantal externe partijen groeit door toenemend gebruik van ICT-toepassingen, software, medische apparatuur, apps en patiëntenportalen.

Uit de interviews en enquêtes blijkt dat niet alle zorginstellingen een compleet beeld hebben van welke bewerkers en subbewerkers patiëntgegevens bewerken. Mede hierdoor hebben niet alle externe (sub)bewerkers van patiëntgegevens een (sub)bewerkersovereenkomst afgesloten met de zorginstelling waar de gegevens vandaan komen. Waar wel overeenkomsten zijn afgesloten, voldoen deze niet nog altijd aan de

eisen die de AP daaraan stelt. Sommige bewerkers werken met oude contracten. Ten aanzien van deze contracten is een inhaalslag noodzakelijk.

De NFU heeft een normenkader met relevante wet- en regelgeving en (sub)bewerkerscontracten. De NVZ heeft een modelovereenkomst ontwikkeld. Artikel 7 van de modelovereenkomst legt de aansprakelijkheid bij de bewerker en uit de interviews en enquête blijkt dat veel bewerkers dit niet aanvaarden. In de praktijk leidt dit tot verschillen in bewerkersovereenkomsten tussen zorginstellingen en bewerkers.

De geïnterviewden benoemen dat veel bewerkersovereenkomsten een papieren werkelijkheid zijn. Sommige verantwoordelijken auditen hun bewerkers. De subbewerker is nu nog de verantwoordelijkheid van de bewerker. Kennisgeving aan de verantwoordelijke gebeurt nog niet altijd, maar dat is straks bij de AVG wel verplicht.

Er is weinig interne toezichtscapaciteit op naleving van het vereiste om (sub)bewerkersovereenkomsten op te stellen, als gevolg waarvan de naleving van privacybescherming niet goed getoetst kan worden.

4.2 Good practices

- **Het NFU normenkader.** Het NFU normenkader dit geeft een beeld en handvatten over hoe informatiebeveiliging en wet- en regelgeving geïntegreerd aangepakt kunnen worden.

- **Aanwezigheid FG.** Er zijn al zorginstellingen met een FG die zich tevens met bewerkersovereenkomsten bezighoudt. Een FG is straks met de komst van de AVG voor grote zorginstellingen (meer dan 250 medewerkers) verplicht. Het helpt als ook bij kleine zorginstellingen een (gezamenlijke) FG wordt aangesteld, soms gebeurt dit al.

4.3 Aanbevelingen ter verbetering

1) Inventariseer welke externe partijen patiëntgegevens verwerken en in hoeverre daarbij gebruik wordt gemaakt van diensten van subbewerkers. Benoem verantwoordelijken voor het bijhouden van de lijst met subbewerkers. Sluit met de bewerkers bewerkersovereenkomsten af die voldoen aan de eisen die de AP daaraan stelt (waaronder het inventariseren en melden van subbewerkers, alsmede het borgen van de afspraken met de subbewerkers).
2) Laat zorginstellingen in hun contracten met bewerkers opnemen dat:
    - De zorginstelling precies wil weten welke patiëntgegevens door welke subbewerkers worden bewerkt.
    - Bewerkers en (sub)bewerkerscontracten voldoen aan de voorwaarden die de AP daaraan stelt. Op deze wijze is geen verdere aanvulling van wetgeving noodzakelijk en kan door middel van de bewerkersovereenkomst een incident als de bewerking van patiëntdossiers door gevangenen worden voorkomen.
3) Laat het toetsen op de aanwezigheid van goede (sub)bewerkersovereenkomsten en het naleven van de afspraken meenemen in audits, voor zover dit nog niet gebeurt.
4) Laat de koepels (ook van leveranciers) in samenwerking met VWS onderzoeken of in aanvulling op bewerkersovereenkomsten per zorginstelling, sectorale afspraken, convenanten, modelovereenkomsten

of gedragscodes mogelijk zijn ten behoeve van de uniformering, interoperabiliteit, efficiëntie en effectiviteit. Zorg daarbij voor een standaard bewerkersovereenkomst waarmee alle partijen in de sector uit de voeten kunnen, ook de leveranciers. De standaard bewerkersovereenkomst kan per zorginstelling op maat worden gemaakt.

5) Anticipeer op de striktere voorwaarden voor bewerkers (verwerkers) die gelden in de AVG.

5. Incidenten

5.1 Bevindingen

Datalek bij drie ziekenhuizen treft ruim 158.000 patiënten (security.nl 25-01-2016)
Patiëntgegevens van twee Nederlandse ziekenhuizen en een Belgisch ziekenhuis hebben op straat gelegen. Daarover heeft het Belgische IT-bedrijf iGuana, verantwoordelijk voor het versturen van de gelekte databestanden, de ziekenhuizen maandag geïnformeerd.

Twee ziekenhuizen melden malwarebesmetting bij NCSC (NOS 12-07-2016)
Het afgelopen jaar hebben twee ziekenhuizen bij het Nationaal Cyber Security Center (NCSC) van de overheid gemeld dat ze een malwarebesmetting hadden opgelopen. Bij de Inspectie voor de Gezondheidszorg (IGZ) kwamen helemaal geen meldingen over cyber-incidenten binnen (…)

Risico's op ongeautoriseerde toegang doen zich voor. Denk aan zoekgeraakte USB-sticks met patiëntgegevens zonder wachtwoord en encryptie, open deuren met patiëntendossiers op het bureau, niet afgesloten beeldschermen, gezamenlijke logincodes of logincodes op een whiteboard en verkeerd geadresseerde e-mails. Veel van dergelijke incidenten zijn te vermijden. De informatievoorziening is echter zodanig complex en mobiel geworden dat het voor zorgverleners bijna ondoenlijk is om nooit een datalek te veroorzaken. In alle zorginstellingen zullen waarschijnlijk datalekken optreden. De meeste datalekken hebben weliswaar relatief weinig impact, maar er treden ook incidenten op die zeer grote impact hebben.

Op de enquêtevraag wat de grootste risico's met betrekking tot (het verwerken van) patiëntgegevens zijn, wordt veelal de mens genoemd: risico's ontstaan omdat medewerkers onbewust zijn, onbekwaam handelen of dat het werk zodanig ingericht is dat er te weinig ruimte is om privacy-bewust te handelen, waardoor incidenten ontstaan, zoals bijvoorbeeld gegevens onbeveiligd naar externe partijen versturen. Daarnaast worden ook technische risico's benoemd, zoals ransomware.

Voorbeelden
Voorbeelden van incidenten die tijdens de interviews zijn genoemd:

- Een onderzoeker wilde patiëntengegevens op een beveiligde USB-stick zetten om thuis verder te kunnen werken, maar omdat de eigen apparatuur de patiëntgegevens niet kon inlezen van de beveiligde USB-stick, zette de onderzoeker de patiëntgegevens op een onbeveiligde USB-stick, die vervolgens weg raakte met daarop de onderzoeksgegevens van patiënten.
- Een verkeerd geadresseerde brief of e-mail met patiëntgegevens.
- Papieren patiëntendossiers op een bureau of patiëntgegevens op een beeldscherm in een niet-afgesloten ruimte.
- Logincodes worden onbeschermd en voor anderen zichtbaar genoteerd.
- Het gebruik van commerciële e-mailaccounts voor het versturen van berichten met daarin patiëntgegevens.
- Ransomware.

De AP noemt – min of meer in lijn met de voorbeelden uit de andere interviews – de volgende soorten datalekmeldingen (zie ook recente nieuwsberichten[7]). Dat zijn in willekeurige volgorde:

- Verkeerd geadresseerde poststukken.
- Verkeerd geadresseerde e-mails met bijlagen.
- Onversleutelde USB sticks.
- Laptops die verloren gaan als gevolg van verlies of diefstal.
- In toenemende mate ransomware

Er vinden privacy-incidenten plaats die worden gemeld. In het algemeen blijkt dat goede monitoring op het gebied van privacybescherming moeilijk goed te regelen is, waardoor het aannemelijk is dat ook in zorginstellingen deze monitoring niet altijd even adequaat gerealiseerd is. Hierdoor is het waarschijnlijk dat er ook incidenten optreden die niet gedetecteerd worden.

Niet alle mensen die patiëntgegevens bewerken zijn even goed op de hoogte van wat een datalek is en waar datalekken moeten worden gemeld. De effectiviteit van het analyse- en escalatieproces voor datalekken varieert per zorginstelling.

Een veilig meldklimaat is de basis voor het voorkomen van incidenten in de toekomst. Mensen moeten kunnen leren van hun fouten. In de meeste instellingen lijkt geen afrekencultuur te bestaan ten aanzien van datalekken, maar in interviews is aangegeven dat het toch kan gebeuren dat een ogenschijnlijke incidentveroorzaker onterecht de schuld van een datalek krijgt. Er zijn ook grenzen en als willens en wetens een datalek is veroorzaakt, dient ook handhavend opgetreden te kunnen worden. Een (vooraf bekende) duidelijke aanpak is van belang.

Zorginstellingen die te maken hebben gehad met een ernstig datalek met consequenties tot in de top van de organisatie, blijken daarvan te leren en vervolgens aandacht te besteden aan bewustwording in de gehele organisatie. Vele geïnterviewden stellen dat een incident, hoe vervelend ook, vaak een bewustwordingsstimulans geeft en een groot leerpotentieel biedt.

Systemen en processen voor het registreren en afhandelen van datalekken en andere cyberincidenten, zijn niet in alle zorginstellingen gecombineerd met het registreren en afhandelen van andere incidenten. De integratie medische veiligheid en data-incidenten is nog niet in alle instellingen gerealiseerd, waardoor het afhandelen van privacy-incidenten nog niet zo gestroomlijnd loopt als andere incidenten.

Instellingen vragen zich af wanneer er nu precies gemeld moet worden aan de AP. Wanneer is er sprake van een ernstig incident? Net zoals bij de interne meldingen hebben de meldingen aan de AP een bewustwording - en leerpotentieel, “never let a good crisis got to waste”. De meeste geïnterviewde zorginstellingen houden een lijst bij met incidenten bij. Over meldingen gedaan aan de AP willen de meeste instellingen niet spreken. Wel wordt opgemerkt dat een melding aan de AP vaak met veel werk, stress, onzekerheid en onduidelijkheid

[7] www.zorgvisie.nl/ICT/Nieuws/2016/11/Ziekenhuizen-melden-300-datalekken.
www.trouw.nl/tr/nl/39683/nbsp/article/detail/4421103/2016/11/24/Ziekenhuizen-melden-elke-dag-datalek.dhtml.

gepaard gaat. Juist daarom zouden de zorginstellingen graag meer (situationele) feedback naar aanleiding van de melding van de AP willen ontvangen.

Bij de geïnterviewden heerst een sterke wens om (sectorgewijs) met de AP in gesprek te gaan met het oogmerk om te leren van fouten en zo te komen tot (proces)verbeteringen.

In onze digitale samenleving is cybercriminaliteit een realiteit. Uit de interviews, enquête en het ‘Cybersecurity beeld Nederland 2016’ blijkt dat ransomware bijvoorbeeld voor veel zorginstellingen een groeiend probleem is. Het beveiligen tegen cybercriminaliteit vergt aandacht vanuit de individuele organisaties. Bovendien kunnen koepels en nationale instellingen een rol spelen in het faciliteren hiervan. Een voorbeeld van dit laatste is een CERT voor de zorg (Z-CERT), gekoppeld aan de NCSC en andere CERT organisaties.

5.2 Good practices

- **Monitoring**. Alle kritische informatiesystemen, waaronder de systemen waarin patiëntgegevens opgeslagen of bewerkt worden, dienen gemonitord te worden op relevante dreigingen en mogelijke datalekken.

- **Datalekprotocol**. Veel zorginstellingen hanteren heldere en eenvoudige procedures voor het herkennen en melden van een datalek.

5.3 Aanbevelingen ter verbetering

1) Monitor alle kritische informatiesystemen, waaronder de systemen waarin patiëntgegevens opgeslagen of bewerkt worden, op relevante dreigingen en mogelijke datalekken.
2) Maak in de organisatie duidelijk wat een datalek is en richt een heldere, eenvoudige en drempelvrije procedure in voor melden van een datalek.
3) Systemen en processen voor het registreren en afhandelen van datalekken en andere cyberincidenten zijn bij voorkeur geïntegreerd in de bestaande systematiek voor de afhandeling van (andere) veiligheidsincidenten (veiligheidsincidentmeldingssysteem (VIM)).
4) Werk samen aan het afhandelen van cyberincidenten in de zorg, onder andere via Zorg-CERT.
5) Neem in de jaarrapportage van de instelling een paragraaf op over de opgetreden incidenten, alsmede wat daarmee gebeurd is.

6. Bescherming van patiëntgegevens in wetenschappelijk onderzoek

Patiëntgegevens gestolen van onderzoeker Antoni van Leeuwenhoek Ziekenhuis (NOS 03-03-2016)
Dieven hebben een externe harde schijf met daarop de gegevens van bijna 800 patiënten van het Antoni van Leeuwenhoek Ziekenhuis gestolen. De onbeveiligde gegevensdrager werd ontvreemd uit de kofferbak van de auto van een onderzoeker van het Amsterdamse ziekenhuis (…)

6.1 Bevindingen

Ten behoeve van (wetenschappelijk) onderzoek worden patiëntgegevens gebruikt. Deze dienen minimaal gepseudonimiseerd te worden, waarbij de drempel voor het koppelen van de pseudoniemen aan de patiëntgegevens voldoende hoogt ligt. Uit de interviews en de enquête blijkt dat niet altijd aan die voorwaarden wordt voldaan, ook niet bij het overdragen van persoonsgegevens aan kwaliteitsregisters.

Maatschappelijk gezien zijn registers belangrijk. Met betrekking tot privacybescherming spelen daarbij twee vragen. Ten eerste de vraag van specifieke of generieke toestemming en of de vooraf door de patiënt gegeven toestemming voor het gebruik van diens medische gegevens voor wetenschappelijk onderzoek voldoende is. Kan het principe van vooraf ingestemde goedkeuring voor wetenschappelijk onderzoek en statistiek worden gehanteerd? De komende AVG biedt de wetgever de ruimte om in nationale wetgeving het vraagstuk van medisch wetenschappelijk onderzoek verder uit te werken.

Ten tweede het vraagstuk van pseudonimisering. Bij het leveren van gegevens aan registers zitten diverse zorginstellingen met de vraag in hoeverre een pseudoniem als een persoonsgegeven gezien dient te worden, welke mate van beveiliging daarvoor nodig is en hoe pseudonimiseren (en anonimiseren) zich verhouden tot de opmars van big data. De doelstelling van pseudonimisering is juist dat het voor de onderzoekers anoniem is, maar dat in geval van nood het via een sleutel mogelijk is terug te gaan naar een individuele patiënt. Niet alle organisaties hebben de sleutels voor het pseudonimiseren goed beschermd. Daarnaast is er een wisselende variëteit aan andere beveiligingsmaatregelen van kracht.

In het onderzoek vragen FG's en ISO's van zorginstellingen en hun softwareleveranciers aandacht voor de informatiebeveiliging en privacybescherming van patiëntgegevens die zorginstellingen dienen te verstrekken aan wetenschappelijke, statistische en kwaliteitsregisters en de wijze waarop deze worden aangeleverd. Er zijn ongeveer 180 registers in Nederland waar zorginstellingen hun data aan moeten leveren. Volgens geïnterviewden omvat dit soms ook identificeerbare gegevens.

6.2 Good practices

- **Parelsnoer-instituut**. Het Parelsnoer-instituut is de infrastructuur en set van afspraken voor klinische biobanken voor wetenschappelijk onderzoek. Het Parelsnoer-instituut combineert de toestemming van de patiënt met het gebruik maken van een Trusted Third Party (TTP).

- **Privacy by design**. Privacy by design is het meenemen van het aspect privacybescherming in de ontwerpfase van een proces, systeem of dienst.

6.3 Aanbevelingen ter verbetering

1) Zorg als beveiligingsmaatregel dat gegevens minimaal gepseudonimiseerd worden voordat zij voor wetenschappelijk onderzoek verstrekt worden aan andere (onderzoeks)organisaties (bijvoorbeeld landelijke kwaliteitsregisters) en zet een procedure op om de pseudonimiseringssleutel goed te beschermen. De FG van een zorginstelling kan dan controleren of de pseudoniemen voldoende beschermd zijn en de regels hieromtrent voldoende nageleefd worden. Dit kan onder meer worden meegenomen in een privacy impact assessment (PIA).
2) Geef - na overleg tussen VWS en de AP - in de nationale uitvoeringswet behorende bij de AVG een duidelijk antwoord op de vraag of en in hoeverre en onder welke voorwaarden gepseudonimiseerde patiëntgegevens gebruikt mogen worden bij (wetenschappelijk) onderzoek en kwaliteitsregisters.
3) Laat VWS onderzoeken of het niveau van informatiebeveiliging en privacybescherming bij landelijke registraties voldoende is.

PBLQ

7. Wet- en regelgeving

7.1 Bevindingen

Er is veel wet- en regelgeving over informatiebeveiliging en privacy waar zorginstellingen compliant mee moeten zijn en er komt ook nog veel wet- en regelgeving aan, gebaseerd op Europese richtlijnen en verordeningen. Uit het onderzoek komt geen indicatie naar voren dat verdere aanvulling van wet- en regelgeving voor informatiebeveiliging en privacybescherming in zorginstellingen nodig is, mede gelet op komende wet- en regelgeving, normen en (professionele) standaarden.

Vanuit een aantal instellingen is gemeld dat een aantal relevante normen niet drempelvrij beschikbaar zijn.

Uit de interviews en enquête blijkt dat er behoefte is aan het begrijpelijker maken van wet- en regelgeving en het vertalen ervan naar basisprincipes en concrete handvatten voor de praktijk.

Met betrekking tot de decentralisaties ontbreekt er een specifiek juridisch kader voor gegevensuitwisseling ter invulling van de algemene wet- en regelgeving. Zie ook het bericht van de AP (destijds nog het CBP) van 1 juli 2014: “Het CBP constateert dat het kabinet geen duidelijke kaders geeft waarbinnen gemeenten bij de verwerking van persoonsgegevens binnen het sociaal domein moeten blijven”.

7.2 Good practices

- **Handboek NEN 7510**. Bij de NEN 7510 hoort een Handboek. In dat handboek staan nuttige goede praktijken.

7.3 Aanbevelingen ter verbetering

Het bieden van handvatten voor wet- en regelgeving

1) Maak vigerende wet- en regelgeving voor zorgmedewerkers behapbaar in sectorale en beroepsgerichte gedragscodes en thematische richtsnoeren.
2) Blijf faciliteren dat privacywet-en regelgeving en uitspraken van de AP eenvoudig en vrijelijk beschikbaar zijn en helder geduid worden, met name ook met toekomstige wet- en regelgeving, zoals de AVG.
3) Maak informatiebeveiliging en privacybescherming onderdeel van de subsidievoorwaarden (bijvoorbeeld aangesloten zijn op Z-CERT en voldoen aan de NEN 7510).
4) Laat de koepels en VWS er gezamenlijk voor zorgen dat de relevante normen en standaarden, voor zover dit nog niet het geval is, drempelvrij beschikbaar komen voor zorginstellingen.
5) Bevorder dat authenticatiemiddelen met een hoog betrouwbaarheidsniveau landelijk worden toegepast binnen de zorg. Mede door het bij wet aangenomen digitale inzagerecht en de komst van patiëntportalen en persoonlijke gezondheidsomgevingen worden authenticatiemiddelen met een hoog betrouwbaarheidsniveau noodzakelijk.
6) Geef aan zorginstellingen en gemeenten duidelijke handvatten over hoe zij om dienen te gaan met het medisch beroepsgeheim en het verwerken van patiëntgegevens, bijvoorbeeld in de jeugd-GGZ

vanwege de uitvoering van de decentralisatiewetten. Overweeg pas aanvullende wet- of regelgeving als de handvatten onvoldoende blijken.

7) Zorg voor bewustwording, duiding en gebruik van de iWMO en iJeugdstandaarden bij uitwisseling van patiëntgegevens.
8) Laat organisaties verantwoording afleggen over informatiebeveiliging en privacybescherming binnen de organisatie, bijvoorbeeld als paragraaf in het jaarverslag.

8. Aanvullende vragen

In aanvulling op de vijf onderzoeksvragen die in de voorafgaande hoofdstukken zijn behandeld heeft de minister van VWS naar aanleiding van vragen tijdens het Algemeen Overleg van 29 juni jl. vanuit de Tweede Kamer nog de volgende drie vragen aan PBLQ gesteld:

1) Hoe is het gesteld met de verantwoordelijkheidsverdeling in de praktijk (wie hebben er in de praktijk toegang tot het dossier en hoe is dit formeel geregeld) ?
2) Wat is de stand van zaken met betrekking tot het digitaliseren van papieren dossiers?
3) Worden er opleidingen/ trainingen over informatiebeveiliging gegeven? Zo ja; aan wie?

In het navolgende worden deze drie vragen beantwoord.

Verantwoordelijkheidsverdeling in de praktijk (wie hebben er in de praktijk toegang tot het dossier en hoe is dit formeel geregeld)?

De bevindingen:
In de meeste onderzochte instellingen wordt als uitgangspunt gehanteerd dat autorisatie voor systemen wordt verleend op grond van de functie die medewerkers vervullen en/of de werkcontext waarin de medewerkers die functie vervullen.

De praktijk laat zien dat, naast iedereen die direct bij een behandelrelatie betrokken is, veelal ook anderen mensen, bijvoorbeeld indirect bij de behandeling betrokken zorgmedewerkers en ondersteunende medewerkers, bij de gegevens kunnen komen of deze onder ogen kunnen krijgen, en dat soms ook derden toegang tot gegevens in het dossier krijgen, bijvoorbeeld voor regionale samenwerking en kwaliteitsregisters.

Aanbevelingen ter verbetering:
1) Beleg de feitelijke eindverantwoordelijkheid voor de naleving van de informatiebeveiliging en privacybescherming bij de leiding van de zorginstelling en bespreek dit met de Raad van Toezicht.
2) Laat de FG's of ISO's erop toezien dat alleen medewerkers die rechtstreeks bij de behandeling betrokken zijn, toegang hebben tot de patiëntinformatie, bijvoorbeeld door het monitoren van logging.
3) De medewerkers in het primaire zorgproces moeten weten dat alleen wanneer er sprake is van een directe behandelrelatie, zij patiëntinformatie mogen delen en inzien. Bovendien moeten zij de kennis en vaardigheden hebben om zorgvuldig met patiëntgegevens om te gaan. Dit vraagt om hoogwaardige privacybeschermende technologie en bijbehorende protocollen. Het ligt niet voor de hand dat alle zorginstellingen deze informatietechnische problematiek zelf op gaan lossen. De aanbeveling is dan ook dat VWS samen met koepelorganisaties projecten initieert die zich organisatieoverstijgend op deze problematiek richten. Hierbij moet ook gekeken worden naar de rol die het veld en de leveranciers hierin kunnen spelen en in welke mate VWS dit kan faciliteren.

PBLQ

Digitaliseren van papieren dossiers

De bevindingen:
Uit het onderzoek komt het beeld naar voren dat de meeste zorginstellingen ver zijn met het digitaliseren van patiëntendossiers, hoewel er ook nog met papieren dossiers wordt gewerkt. Zo zijn bijvoorbeeld ziekenhuizen gemiddeld verder met het digitaliseren dan GGZ-instellingen.

Een papieren dossier is bij de geïnterviewde partijen, veelal voorlopers, op weg om een uitzondering te worden. Deze partijen zijn geraadpleegd met het oog op good practices en verbetervoorstellen, maar niet geheel representatief.

Opleidingen en trainingen over informatiebeveiliging in ziekenhuizen

De bevindingen:
Naast campagnes om bewustwording te generen worden er binnen de meeste zorginstellingen trainingen en cursussen gegeven over informatiebeveiliging en privacybescherming, bijvoorbeeld door middel van online modules.

Opleidingen en trainingen zijn vaak niet gericht op diegenen in het primaire zorgproces, maar vaak op medewerkers die betrokken zijn bij informatiebeveiliging en privacybescherming. Tijdens de interviews is gebleken dat de medewerkers in het primaire zorgproces en de mensen die zich in de zorginstelling met informatiebeveiliging en privacybescherming bezig houden in gescheiden werelden leven, met eigen prioriteiten, opleidingen en trainingen.

Aanbevelingen ter verbetering:
1) Laat de koepels samen met VWS landelijke campagnes opzetten, gericht op alle meer dan 1.1 miljoen medewerkers werkzaam in de zorg en op alle gebruikers (patiënten), waarin de basisprincipes van (informatie)veilig werken en privacybescherming op duidelijke wijze wordt uitgelegd. Dit zal de komende jaren continue aandacht vragen.
2) Laat de FG of de ISO vanuit diens coördinerende rol voor relevante groepen medewerkers uitzoeken welke tekortkomingen er zijn op het gebied van kennis, vaardigheden en houding met betrekking tot informatieveiligheid en privacybescherming en op basis daarvan bepalen welke doelgroepgerichte opleiding en training nodig is.
3) Laat VWS agenderen dat thema's als informatiebeveiliging en privacybescherming voldoende in (medische) opleidingen aan bod komen, opdat het digibewustzijn wordt vergroot.

PBLQ

9. Conclusies en aanbevelingen

Zoals in de inleiding vermeld zijn er acht onderzoeksvragen geformuleerd voor het door PBLQ uitgevoerde onderzoek. Hieronder worden voor iedere onderzoeksvraag de bevindingen en belangrijkste aanbevelingen geresumeerd.

9.1 Bescherming patiëntgegevens in de praktijk, gedrag én in cultuur

De belangrijkste bevindingen:

1) De vertrouwelijkheid van patiëntgegevens is een kernwaarde voor zowel patiënten als zorgaanbieders, en is ook de grond onder het medisch beroepsgeheim. Daarnaast is goede, veilige zorg een kernwaarde. In de praktijk van zorgverlening leidt dit tot een belangenafweging tussen zorgkwaliteit en vertrouwelijkheid. De positie van vertrouwelijkheid kan worden versterkt, door enerzijds bewustwording en anderzijds het inzetten van ondersteunende technische en organisatorische maatregelen. Een voorbeeld is het gebruik van authenticatie met behulp van een toegangspas die tevens uitlogt als de werkplek wordt verlaten en automatisch inlogt in iedere volgende werkplek, alsook medische apparatuur.
2) In de afgelopen jaren lijkt de positie van informatiebeveiliging en privacybescherming te zijn verbeterd. Veel instellingen hebben hiervoor meer capaciteit beschikbaar gesteld. Drivers hiervoor zijn onder andere de meldplicht datalekken (artikel 34a Wbp) en de toename van cyberdreigingen, zoals ransomware. Bewustwordingscampagnes hebben bij diverse zorginstellingen geleid tot meer bewustwording. De NVZ campagne “Je bent zelf een datalek” van de tool “Zeker-Check” wordt positief gewaardeerd door zorginstellingen.
3) De externe omgeving van zorginstellingen wordt door de vergevorderde digitalisering van patiëntendossiers, de vlucht van eHealth, gezondheidsapps en big data en de toename van cyberdreigingen steeds complexer, alsook door wijzigingen in het zorgdomein zelf, zoals de decentralisaties. Steeds meer (digitale) patiëntgegevens worden verwerkt en steeds meer daarvan worden buiten de kring van rechtstreeks bij de behandeling betrokkenen verwerkt, als gevolg waarvan de risico’s op incidenten met patiëntgegevens toenemen. Informatiebeveiliging en privacybescherming vergen constante aandacht. In die zin is er sprake van een continu verbeterpotentieel.
4) Informatiebeveiliging en privacybescherming landen alleen in een organisatie als dit van hoog naar laag door de organisatie gedragen wordt en op een realistische wijze kan worden uitgevoerd. Wat betreft leiderschap is het daarom van belang dat de leiding het belang van informatiebeveiliging en privacybescherming begrijpt, dit actief uitdraagt binnen en buiten de organisatie en de uitvoering ervan faciliteert, bijvoorbeeld door voldoende personeel en ondersteunende middelen hiervoor beschikbaar te stellen.
5) Niet alle zorginstellingen voldoen aan de NEN 7510, terwijl deze baseline voor informatiebeveiliging en privacybescherming beschouwd kan worden als een minimum beveiligingsniveau. Er zijn verschillende methoden om vast te stellen in hoeverre en in welke mate de NEN 7510 is geïmplementeerd. UMC’s benchmarken zich al meer dan 12 jaar iedere 2 jaar tegen de norm en hebben daarvoor instrumenten ontwikkeld en beschikbaar gesteld aan de ziekenhuizen.
6) Privacy staat bij sommige organisaties los van patiëntveiligheid en de fysieke veiligheid, terwijl er ook zorginstellingen zijn die informatiebeveiliging integreren met andere soorten veiligheid.

7) Bij de informatiebeveiliging en privacybescherming van systemen is de authenticatie en autorisatie een zorgpunt. Dit zorgpunt wordt groter door ontwikkelingen als complexere medische apparatuur, beheer op afstand, steeds meer mobiele eHealth hulpmiddelen, de opkomst van patiëntportalen en persoonlijke gezondheidsomgevingen.
8) De zorginstellingen in dit onderzoek vragen nadrukkelijk om een concrete duiding van de privacywet- en regelgeving en de informatieveiligheid en een dialoog met de AP, gericht op continu verbeteren.
9) Zorginstellingen zijn zoekende waar het gaat om uitwisseling van gegevens met onder meer gemeenten, bijvoorbeeld in het kader van de decentralisaties in de (jeugd)zorg. Duiding, bewustwording en voorlichting zijn ook hier noodzakelijk.

Conclusie
Uit het onderzoek komt het beeld naar voren dat ten opzichte van het onderzoek 'Toegang tot digitale patiëntendossiers binnen zorginstellingen' van de Autoriteit Persoonsgegevens uit 2013 (toen CBP), informatiebeveiliging en privacybescherming in de meeste instellingen meer aandacht krijgt en dat er veel (nieuwe) good practices zijn. Toch is continue aandacht vereist, mede vanwege de voortschrijdende digitalisering en de steeds complexere externe omgeving van zorginstellingen en een toenemend cybersecurity dreigingsbeeld.

Aanbevelingen ter verbetering:

Goed gedrag bevorderen

- Beleg de feitelijke eindverantwoordelijkheid voor de naleving van de informatiebeveiliging en privacybescherming bij de leiding van de zorginstelling en bespreek dit met de Raad van Toezicht.
- Neem in de jaarrapportage van de instelling een paragraaf op over de stand van zaken op het gebied van informatiebeveiliging.
- Laat de leiding ervoor zorgen dat er voldoende mensen en middelen beschikbaar zijn voor het continu monitoren en verbeteren van informatiebeveiliging en privacybescherming. Dit omvat het aanwijzen (rol of functie) van een functionaris gegevensbescherming (FG) en een information security officer (ISO).
- Laat de leiding er voor zorgen dat de belangrijkste uitgangspunten, richtlijnen en standaarden voor informatiebeveiliging en privacybescherming zijn vastgelegd in een voor ieder toegankelijk beleid en dat de naleving daarvan wordt geborgd.
- Pas '*privacy by design'* toe. Zorg bijvoorbeeld dat in nieuwe systemen een goed autorisatiesysteem zit en dat er gebruik wordt gemaakt van voldoende sterke authenticatiemiddelen.
- Maak informatiebeveiliging en privacybescherming onderdeel van bestaande audits voor zover dit nog niet gebeurt.
- Zorg dat medewerkers weten wat een datalek is en hoe daarmee omgegaan dient te worden.

Good practices

- Maak gebruik van reeds uitgewerkte relevante normen en standaarden en good practices. Het NFU-normenkader bijvoorbeeld geeft een beeld over hoe informatiebeveiliging en wet- en regelgeving geïntegreerd aangepakt kunnen worden en biedt hiervoor handvatten. Daarnaast kunnen voorbeelden uit het handboek NEN 7510 worden gebruikt om informatiebeveiliging en privacybescherming relatief eenvoudig te handhaven door het nemen van technische en procedurele maatregelen die de zorgprocessen niet hinderen.

- Integreer systemen en processen voor informatiebeveiliging en privacybescherming bij voorkeur in de bestaande systemen en processen voor veiligheid (veiligheidsmanagementsysteem (VMS)).
- Maak informatiebeveiliging en privacybescherming (bijvoorbeeld voldoen aan de NEN 7510 en het hebben van een bewerkerscontract), voor zover dat nog niet gebeurt, onderdeel van de ICT-paragraaf van inkoopvoorwaarden.

Krachten bundelen

- Laat koepels in overleg met VWS en toezichthouders (AP en IGZ) meer sectorale afspraken maken en richtlijnen, modeldocumenten en gedragscodes opzetten en beschikbaar stellen:
  - Laat de IGZ en de AP op bestuurlijk niveau hun toezichtstaken ten aanzien van beschikbaarheid van patiëntgegevens (patiëntveiligheid) en vertrouwelijkheid (bescherming van persoonsgegevens) meer op elkaar afstemmen en hun informatieverstrekking en richtsnoeren meer baseren op door de koepels geventileerde behoeften uit de praktijk.
  - Laat de koepels en VWS gezamenlijk, op basis van de behoeften van de zorginstellingen, komen tot aanvullende sectorale afspraken, richtlijnen, modeldocumenten, standaardbewerkersovereenkomsten en gedragscodes op het gebied van informatiebeveiliging en privacybescherming, en zorgen dat hoogwaardige privacybeschermende technologie en bijbehorende protocollen worden ontwikkeld.
- Laat VWS faciliteren dat de verdere uitbouw van Z-CERT versneld en verbreed kan worden.

9.2 (Sub)bewerkers

De belangrijkste bevindingen:

1) Zorginstellingen maken in het algemeen gebruik van verscheidene externe partijen voor het bewerken van patiëntgegevens in de zin van de Wbp. Een gemiddeld ziekenhuis heeft naar schatting van de geïnterviewden al gauw 60 bewerkers en bij UMC's gaat het om honderden. Denk daarbij bijvoorbeeld aan leveranciers van informatiesystemen, software, archivering, medische apparatuur, (secure) mail, het digitaliseren van papieren dossiers en het bewerken van medische beelden. Het aantal externe partijen groeit door toenemend gebruik van ICT-toepassingen, software, medische apparatuur, apps en patiëntportalen.
2) Niet alle zorginstellingen hebben een compleet beeld van welke bewerkers en subbewerkers patiëntgegevens bewerken. Mede hierdoor hebben niet alle externe (sub)bewerkers van patiëntgegevens een (sub)bewerkersovereenkomst afgesloten met de zorginstelling waar de gegevens vandaan komen. Waar wel overeenkomsten zijn afgesloten, voldoen deze niet altijd aan de eisen die de AP daaraan stelt.
3) De NFU heeft een normenkader met relevante wet- en regelgeving en (sub)bewerkerscontracten. De NVZ heeft een modelovereenkomst. Artikel 7 van de modelovereenkomst legt de aansprakelijkheid bij de bewerker en dat aanvaarden veel bewerkers niet. In de praktijk leidt dit tot verschillen in bewerkersovereenkomsten tussen zorginstellingen en bewerkers.
4) De geïnterviewden benoemen dat veel bewerkersovereenkomsten een papieren werkelijkheid zijn. Sommige verantwoordelijken auditen hun bewerkers. De subbewerker is nu nog de verantwoordelijkheid van de bewerker. Kennisgeving aan de verantwoordelijke gebeurt nog niet altijd, maar is straks bij de AVG wel verplicht.

Conclusie
Uit de interviews en de enquête blijkt dat niet alle zorginstellingen een compleet beeld hebben van welke bewerkers en subbewerkers zij patiëntgegevens bewerken. Niet alle zorginstellingen blijken met bewerkers contracten te hebben afgesloten die voldoen aan de voorwaarden die de AP daaraan stelt. De borging van de bescherming van patiëntgegevens tussen zorginstellingen en (sub)bewerkers verschilt per zorginstelling.

Aanbevelingen ter verbetering:

1) Inventariseer welke externe partijen patiëntgegevens verwerken en in hoeverre daarbij gebruik wordt gemaakt van diensten van subbewerkers. Benoem verantwoordelijken voor het bijhouden van de lijst met subbewerkers. Sluit met de bewerkers bewerkersovereenkomsten af die voldoen aan de eisen die de AP daaraan stelt (waaronder het inventariseren en melden van subbewerkers, alsmede het borgen van de afspraken met de subbewerkers).
2) Laat zorginstellingen in hun contracten met bewerkers opnemen dat:
    - De zorginstelling precies wil weten welke patiëntgegevens door welke subbewerkers worden bewerkt.
    - Bewerkers en subbewerkerscontracten voldoen aan de voorwaarden die de AP daaraan stelt. Op deze wijze is geen verdere aanvulling van wetgeving nodig en kan door middel van de bewerkersovereenkomst een incident als de bewerking van patiëntdossiers door gevangenen worden voorkomen.
3) Laat het toetsen op de aanwezigheid van goede (sub)bewerkersovereenkomsten en het naleven van de afspraken meenemen in audits, voor zover dit nog niet gebeurt.
4) Laat de koepels (ook van leveranciers) in samenwerking met VWS onderzoeken of in aanvulling op bewerkersovereenkomsten per zorginstelling, sectorale afspraken, convenanten, modelovereenkomsten of gedragscodes mogelijk zijn ten behoeve van de uniformering, interoperabiliteit, efficiëntie en effectiviteit. Zorg daarbij voor een standaard bewerkersovereenkomst waarmee alle partijen in de sector uit de voeten kunnen, ook de leveranciers. De standaard bewerkersovereenkomst kan per zorginstelling op maat worden gemaakt.
5) Anticipeer op de striktere voorwaarden voor bewerkers (verwerkers) die gelden in de AVG.

9.3 Incidenten

De belangrijkste bevindingen:

1) Risico's op ongeautoriseerde toegang doen zich voor. Denk aan zoekgeraakte USB-sticks met patiëntgegevens zonder wachtwoord en encryptie, open deuren met patiëntendossiers op het bureau, niet afgesloten beeldschermen, gezamenlijke logincodes of logincodes op een whiteboard en verkeerd geadresseerde e-mails. Veel van dergelijke incidenten zijn te vermijden. De informatievoorziening is echter zodanig complex en mobiel geworden dat het voor zorgverleners bijna ondoenlijk is om nooit een datalek te veroorzaken. In alle zorginstellingen zullen dus datalekken optreden. De meeste datalekken hebben weliswaar relatief weinig impact maar er treden ook incidenten op die zeer grote impact hebben.
2) In het algemeen blijkt dat goede monitoring op het gebied van privacybescherming moeilijk goed te regelen is, waardoor het aannemelijk is dat ook in zorginstellingen deze monitoring niet altijd even adequaat gerealiseerd is.
3) Niet alle mensen die patiëntgegevens bewerken zijn even goed op de hoogte van wat een datalek is, en waar dat gemeld moet worden. De effectiviteit van het analyse- en escalatieproces voor datalekken varieert per zorginstelling.

4) Een veilig meldklimaat is de basis voor het voorkomen van incidenten in de toekomst. Mensen moeten kunnen leren van hun fouten. Maar er zijn ook grenzen en als willens en wetens een datalek is veroorzaakt, dient ook handhavend opgetreden te kunnen worden. Een (vooraf bekende) duidelijke aanpak is van belang.
5) Zorginstellingen die te maken hebben gehad met een ernstig datalek met consequenties tot in de top van de organisatie, blijken daarvan te leren en vervolgens aandacht te besteden aan bewustwording in de gehele organisatie.
6) Systemen en processen voor het registreren en afhandelen van datalekken en andere cyberincidenten, zijn niet in alle zorginstellingen gecombineerd met het registreren en afhandelen van andere incidenten.
7) De geïnterviewden willen meer (situationele) feedback bij meldingen aan de AP. Overigens vragen veel instellingen zich af wanneer er nu precies gemeld moet worden aan de AP. Net zoals bij de interne meldingen hebben de meldingen aan de AP een bewustwording -en leerpotentieel, “never let a good crisis got to waste”.
8) Bij de geïnterviewden heerst een sterke wens om (sectorgewijs) met de AP in gesprek te gaan met het oogmerk om te leren van fouten en zo te komen tot (proces)verbeteringen.
9) In onze digitale samenleving is cybercriminaliteit een realiteit. Uit de interviews, enquête en het ‘Cybersecurity beeld Nederland 2016’ blijkt dat ransomware bijvoorbeeld voor veel zorginstellingen een groeiend probleem is. Het beveiligen tegen cybercriminaliteit vergt aandacht vanuit de individuele organisaties. Bovendien kunnen koepels en nationale instellingen een rol spelen in het faciliteren hiervan. Een voorbeeld van dit laatste is een CERT voor de zorg (Z-CERT), gekoppeld aan de NCSC en andere CERT organisaties.

Conclusie
Incidenten zijn niet te voorkomen. Het gaat er om dat ervan wordt geleerd en dat de informatiebeveiliging en privacybescherming op basis daarvan worden verbeterd. Niet alle zorginstellingen integreren het afhandelen van cyberincidenten met dat van andere incidenten.

Aanbevelingen ter verbetering:
1) Laat zorginstellingen al hun kritische informatiesystemen, waaronder de systemen waarin patiëntgegevens opgeslagen of bewerkt worden, monitoren op relevante dreigingen en mogelijke datalekken.
2) Maak in de organisatie duidelijk wat een datalek is en richt een heldere, eenvoudige en drempelvrije procedure in voor melden van een datalek.
3) Werk samen aan het afhandelen van cyberincidenten in de zorg, onder andere via Zorg-CERT.

9.4 Bescherming van patiëntgegevens in wetenschappelijk onderzoek

De belangrijkste bevindingen:
1) Ten behoeve van (wetenschappelijk) onderzoek worden patiëntgegevens gebruikt. Deze dienen minimaal gepseudonimiseerd te worden, waarbij de drempel voor het koppelen van de pseudoniemen aan de patiëntgegevens voldoende hoogt ligt. Uit de interviews en de enquête blijkt dat niet altijd aan die voorwaarden wordt voldaan, ook niet bij het overdragen van persoonsgegevens aan kwaliteitsregisters.
2) Bij het leveren van gegevens aan registers zitten diverse zorginstellingen met de vraag of vooraf gegeven toestemming van de patiënt voor wetenschappelijk onderzoek voldoende is, in hoeverre een

pseudoniem als een persoonsgegeven gezien dient te worden, welke mate van beveiliging daarvoor nodig is en hoe pseudonimiseren (en anonimiseren) zich verhouden tot de opmars van big data.

3) In het onderzoek vragen FG's en ISO's van zorginstellingen en hun softwareleveranciers aandacht voor de informatiebeveiliging en privacybescherming van patiëntgegevens die zorginstellingen dienen te verstrekken aan wetenschappelijke, statistische en kwaliteitsregisters en de wijze waarop deze worden aangeleverd. Er zijn ongeveer 180 registers in Nederland waar zorginstellingen hun data aan moeten leveren. Volgens geïnterviewden omvat dit soms ook identificeerbare gegevens.

Conclusie

Uit de op de interviews en de enquête gestoelde bevindingen blijkt dat de bescherming van patiëntgegevens in de onderzoekspraktijk en bij het aanleveren aan kwaliteitsregisters niet altijd afdoende is geborgd.

Aanbevelingen ter verbetering:

1) Zorg als beveiligingsmaatregel dat gegevens minimaal gepseudonimiseerd worden voordat zij voor wetenschappelijk onderzoek verstrekt worden aan andere (onderzoeks)organisaties (bijvoorbeeld landelijke kwaliteitsregisters) en zet een procedure op om de pseudonimiseringssleutel goed te beschermen. De FG van een zorginstelling kan dan controleren of de pseudoniemen voldoende beschermd zijn en de regels hieromtrent voldoende nageleefd worden. Dit kan onder meer worden meegenomen in een privacy impact assessment (PIA).
2) Geef - na overleg tussen VWS en de AP - in de nationale uitvoeringswet behorende bij de AVG een duidelijk antwoord op de vraag of en in hoeverre en onder welke voorwaarden gepseudonimiseerde patiëntgegevens gebruikt mogen worden bij (wetenschappelijk) onderzoek en kwaliteitsregisters.
3) Laat VWS onderzoeken of het niveau van informatiebeveiliging en privacybescherming bij landelijke registraties voldoende is.

9.5 Wet- en regelgeving

De belangrijkste bevindingen:

1) Er is veel wet- en regelgeving over informatiebeveiliging en privacy waar zorginstellingen compliant mee moeten zijn en er komt ook nog veel meer wet- en regelgeving aan, gebaseerd op Europese richtlijnen en verordeningen. Uit het onderzoek komt geen indicatie naar voren dat verdere aanvulling van wet- en regelgeving voor informatiebeveiliging en privacybescherming in zorginstellingen nodig is, mede gelet op komende wet- en regelgeving, normen en (professionele) standaarden.
2) Vanuit een aantal instellingen is gemeld dat een aantal relevante normen niet drempelvrij beschikbaar zijn.
3) Uit de interviews en enquête blijkt dat er behoefte is aan het begrijpelijker maken van wet- en regelgeving en het vertalen ervan naar basisprincipes en concrete handvatten voor de praktijk.

Conclusie

Over het algemeen is er voldoende wet- en regelgeving ten aanzien van het werken met patiëntgegevens, maar is het vooral veel en complex. Uit de interviews en enquête blijkt dat er behoefte is aan het begrijpelijker maken van wet- en regelgeving en het vertalen ervan naar basisprincipes en concrete handvatten voor de praktijk.

Aanbevelingen ter verbetering:

Het bieden van handvatten voor wet- en regelgeving

1) Maak vigerende wet- en regelgeving voor zorgmedewerkers behapbaar in sectorale en beroepsgerichte gedragscodes en thematische richtsnoeren.
2) Blijf faciliteren dat privacywet-en regelgeving en uitspraken van de AP eenvoudig en vrijelijk beschikbaar zijn en helder geduid worden, met name ook met toekomstige wet- en regelgeving, zoals de AVG.
3) Maak informatiebeveiliging en privacybescherming onderdeel van de subsidievoorwaarden (bijvoorbeeld aangesloten zijn op Z-CERT en voldoen aan de NEN 7510).
4) Laat de koepels en VWS er gezamenlijk voor zorgen dat de relevante normen en standaarden, voor zover dit nog niet het geval is, drempelvrij beschikbaar komen voor zorginstellingen.
5) Bevorder dat authenticatiemiddelen met een hoog betrouwbaarheidsniveau landelijk worden toegepast binnen de zorg. Mede door het bij wet aangenomen digitale inzagerecht en de komst van patiëntportalen en persoonlijke gezondheidsomgevingen worden authenticatiemiddelen met een hoog betrouwbaarheidsniveau noodzakelijk.
6) Geef aan zorginstellingen en gemeenten duidelijke handvatten over hoe zij om dienen te gaan met het medisch beroepsgeheim en het verwerken van patiëntgegevens, bijvoorbeeld in de jeugd-GGZ vanwege de uitvoering van de decentralisatiewetten. Overweeg pas aanvullende wet- of regelgeving als de handvatten onvoldoende blijken.
7) Zorg voor bewustwording, duiding en gebruik van de iWMO en iJeugdstandaarden bij uitwisseling.

9.6 Aanvullende vragen

Verantwoordelijkheidsverdeling in de praktijk (wie hebben er in de praktijk toegang tot het dossier en hoe is dit formeel geregeld)?

De belangrijkste bevindingen:

1) In de meeste onderzochte instellingen wordt als uitgangspunt gehanteerd dat autorisatie voor systemen wordt verleend op grond van de functie die medewerkers vervullen en/of de werkcontext waarin de medewerkers die functie vervullen.
2) Uit de interviews komt het beeld naar voren dat, naast iedereen die bij een behandelrelatie betrokken is, veelal ook anderen mensen, bijvoorbeeld indirect bij de behandeling betrokken zorgmedewerkers en ondersteunende medewerkers, bij de gegevens kunnen komen of deze onder ogen kunnen krijgen, en dat soms ook derden toegang tot gegevens in het dossier krijgen, bijvoorbeeld voor regionale samenwerking en kwaliteitsregisters.

Conclusie

De verantwoordelijkheidsverdeling voor toegang tot het dossier in de praktijk van zorginstellingen is formeel meestal geregeld op grond van de functie van medewerkers, maar patiëntgegevens komen in de praktijk ook buiten de kring van rechtstreeks betrokkenen bij de behandeling terecht. De zorg voor de naleving van informatiebeveiliging en privacy behoort bij de leiding van de zorginstelling te liggen, maar is daar niet altijd daadwerkelijk belegd.

Aanbevelingen ter verbetering:

1) Laat de FG's of ISO's erop toezien dat alleen medewerkers die rechtstreeks bij de behandeling betrokken zijn, toegang hebben tot de patiëntinformatie, bijvoorbeeld door het monitoren van logging.
2) De medewerkers in het primaire zorgproces moeten weten dat alleen wanneer er sprake is van een directe behandelrelatie, zij patiëntinformatie mogen delen en inzien. Bovendien moeten zij de kennis en vaardigheden hebben om zorgvuldig met patiëntgegevens om te gaan. Dit vraagt om hoogwaardige privacybeschermende technologie en bijbehorende protocollen. Het ligt niet voor de hand dat alle zorginstellingen deze informatie-technische problematiek zelf op gaan lossen. De aanbeveling is dan ook dat VWS projecten initieert die zich organisatie overstijgend op deze problematiek richten. Hierbij moet ook gekeken worden naar de rol die het veld en de leveranciers hierin kunnen spelen en in welke mate VWS dit kan faciliteren.

Digitaliseren van papieren dossiers

De belangrijkste bevindingen:

1) Uit het onderzoek komt het beeld naar voren dat de meeste zorginstellingen ver zijn met het digitaliseren van patiëntendossiers, hoewel er ook nog met papieren dossiers wordt gewerkt. Zo zijn bijvoorbeeld ziekenhuizen gemiddeld verder met het digitaliseren dan GGZ-instellingen.
2) Een papieren dossier is bij de geïnterviewde partijen, veelal voorlopers, op weg om een uitzondering te worden. Deze partijen zijn geraadpleegd met het oog op good practices en verbetervoorstellen, maar niet geheel representatief.

Conclusie

De meeste zorginstellingen digitaliseren papieren dossiers, maar er zijn ook nog steeds veel papieren dossiers bij de Nederlandse zorginstellingen.

Opleidingen / trainingen over informatiebeveiliging en privacybescherming

De belangrijkste bevindingen:

1) Naast campagnes om bewustwording te generen worden er binnen de meeste zorginstellingen trainingen en cursussen gegeven over informatiebeveiliging en privacybescherming, bijvoorbeeld door middel van online modules.
2) Opleidingen en trainingen zijn vaak niet gericht op diegenen in het primaire zorgproces, maar vaak op medewerkers die betrokken zijn bij informatiebeveiliging en privacybescherming. Tijdens de interviews is gebleken dat de medewerkers in het primaire zorgproces en de mensen die zich in de zorginstelling met informatiebeveiliging en privacybescherming bezig houden in gescheiden werelden leven, met eigen prioriteiten, opleidingen en trainingen.

Conclusie

Via diverse campagnes is en wordt binnen de meeste zorginstellingen bewustwording versterkt. Medewerkers in het primaire zorgproces en de mensen die zich in de zorginstelling met informatiebeveiliging en privacybescherming bezighouden, leven nog teveel in gescheiden werelden, met eigen prioriteiten, opleidingen en trainingen.

Aanbevelingen ter verbetering:

1) Laat de koepels samen met VWS landelijke campagnes opzetten, gericht op alle meer dan 1.1 miljoen medewerkers werkzaam in de zorg en op alle gebruikers (patiënten), waarin de basisprincipes van (informatie)veilig werken en privacybescherming op duidelijke wijze wordt uitgelegd. Dit zal de komende jaren continue aandacht vragen.
2) Laat de FG of de ISO vanuit diens coördinerende rol voor relevante groepen medewerkers uitzoeken welke tekortkomingen er zijn op het gebied van kennis, vaardigheden en houding met betrekking tot informatieveiligheid en privacybescherming en op basis daarvan bepalen welke doelgroepgerichte opleiding en training nodig is.
3) Laat VWS agenderen dat thema's als informatiebeveiliging en privacybescherming voldoende in (medische) opleidingen aan bod komen, opdat het digibewustzijn wordt vergroot.

PBLQ

Bijlage A Geïnterviewde personen

Naam	Functie	Organisatie
Maarten Fischer	Beleidsadviseur ICT/EPD	NVZ
Trudy Boshuizen	Senior beleidsadviseur Kwaliteit & Organisatie Onderwerp	NVZ
Karel van Lambalgen	Directeur ICT en CIO	NFU/ LUMC
Jacques Landman	Directeur	NFU
Paul van Rooij	Directeur	GGZ Nederland
Marloes Jonkers	Juridisch adviseur	GGZ Nederland
Jaap Schrieke	Programmaleider	GGZ Nederland
Robert Geertsma	Senior onderzoeker	RIVM (ihkv afstemming RIVM onderzoek)
Hanneke Landman	Secretaris Medische Technologie	IGZ (ihkv afstemming RIVM onderzoek)
Joke de Vries	Hoofdinspecteur	IGZ
Paul van Zeijst	Programma Directeur Medische Technologie	IGZ
Sjaak Nouwt	Adviseur gezondheidsrecht	KNMG
Dianda Veldman	Directeur	NPCF
Marcel Heldoorn	Manager Digitale Zorg	NPCF
Reinier ter Kuile	Programmadirecteur Informatievoorziening Sociaal Domein	VNG/I-Sociaal Domein
Ton Monasso	Adviseur	VNG/I-Sociaal Domein
Mark van Houdenhove	Voorzitter RvB	Sint Maartenskliniek
Marcel van de Haagen	Stafadviseur Privacybescherming en Informatiebeveiliging	VU MC
Guido van de Bogaert	Bestuurder	Rijndam
Jan Willem Schoemaker	CISO/ Business Continuity Manager	Erasmus MC
Peter van Hoogdalem	FG	Erasmus MC
Peter Roos	Hoofd farmaceutische afdeling	Erasmus MC
Bob Zietse	Hoofd afdeling inwendige geneeskunde	Erasmus MC
Peter Bakker	Manager ICT	Groene Hart Ziekenhuis
Marjolein ten Kroode	Voorzitter RvB	GGZ Rivierduinen
Emile Barkhof	Geneesheer-Directeur	GGZ Rivierduinen
Sonja Distelbrink	Jurist	GGZ Rivierduinen

Bart Fennema	FG	GGZ Rivierduinen
Dennis van der Wal	Hoofd Bedrijfsondersteuning	GGZ Delfland
Jolanda Plessius	Informatiemanager/manager CZA	GGZ Delfland
Koen Arnoldus	Technical manager	Epic
Bonne Datema	Directeur	VIR E-care Solutions
Florian Visser	Directeur	RijnmondNet
Ton van Lieshout	Directeur	Triaspect
Pim Südmeijer	Partner	Triaspect
Gerrit Mulder	COO	Chipsoft
Robert Hardholt	CTO	Chipsoft
Wilbert Tomesen	Vice-voorzitter	Autoriteit Persoonsgegevens
Alex Commandeur	Afdelingshoofd Toezicht sector Publiek	Autoriteit Persoonsgegevens
Jan Vlug	Senior Inspecteur	Autoriteit Persoonsgegevens
Igor van Ulst	Security Officer / FG	MC Groep / MC Slotervaart
Margriet Witteveen	Hoofd Verenigingszaken en voorheen hoofd verpleegkundige	V&VN

Aan de EffectenArena op 31 oktober 2016 namen deel:

Pieter van Bemmel (VWS)
Nicole Troisfontaine (VWS)
Annemarie Drent (VWS)
Marcel Heldoorn (Patiëntenfederatie)
Jan Willem Schoemaker (Erasmus Medisch Centrum)
Marcel van der Haagen (VUmc)
Jaap Schrieke (GGZ Nederland)
Rien Meijerink (PBLQ, voorzitter)
Marcel Spruit (PBLQ)
Mano Radema (PBLQ)
Jelle Oud (PBLQ)
Theo Hooghiemstra (PBLQ, onderzoeksleider)

PBLQ

Bijlage B Documenten

Document	Versie	Datum
VWS documenten		
Factsheet Medisch beroepsgeheim		Juni 2016
Documenten van koepelorganisaties		
PBIV 1 Privacykader en reglement ggz 160119, Toolkit PBIV (GGZ NL)	Versie 160119	2016
Handreiking verantwoordelijkheidsverdeling bij samenwerking in de zorg (GGZ NL)		Januari 2010
Het beroepsgeheim in samenwerkingsverbanden: een wegwijzer voor zorgprofessionals (GGZ NL)		
Referentiedomeinenmodel spreadsheet ggz versie 1.00, Toolkit PBIV (GGZ NL)		
PBIV Modelbewerkersovereenkomst NVZ, Toolkit PBIV		
Model speerpunten beleid, Toolkit PBIV (GGZ NL)		
Handreiking Gegevensuitwisseling in de bemoeizorg (GGZ NL)		
PBIV 3 Model procedure binnenkomende externe post, Toolkit PBIV (GGZ NL)	Versie 160412	
PBIV 3 Model protocol Meldplicht Datalekken, Toolkit PBIV (GGZ NL)		
Handreiking WGBO (GGZ NL)		Juli 2013
PBIV 2 Handreiking autorisatie EPD, Toolkit PBIV (GGZ NL)	Versie 1.1	Maart 2014
PBIV 3 Model Handleiding Receptie onaangekondigd bezoek toezichthouder, Toolkit PBIV (GGZ NL)		
PBIV 3 Model patiënteninformatie verstrekken door receptie en secretariaat, Toolkit PBIV (GGZ NL)		Maart 2016
PBIV 1 Model VvT obv NEN 7510 Tactus, Toolkit PBIV (GGZ NL)		
PBIV 1 Model Registratie privacyhuishouding en verwerkingen persoonsgegevens binnen de instelling, Toolkit PBIV (GGZ NL)		
Identity Management starterkit, Toolkit PBIV (GGZ NL)		
PBIV 1 Model voor Beleid Management Systeem voor Informatiebeveiliging, Toolkit PBIV (GGZ NL)		Mei 2016
PBIV 1 Competentieprofiel Functionaris voor de Gegevensbescherming FG, Toolkit PBIV (GGZ NL)		
PBIV 1 Model Classificatie en Risicoanalyse Gegevensverwerkingen, Toolkit PBIV (GGZ NL)		April 2016
Autorisatiebeleid stappen, Toolkit PBIV (GGZ NL)		2009

Stappen voor aanbevelingen voor implementatie PB, Toolkit PBIV (GGZ NL)		
Aanbevelingen voor implementatie PB (2), Toolkit PBIV (GGZ NL)		
Toelichting SG, Toolkit PBIV (GGZ NL)		
Governancecode UMC's (NFU)		Januari 2010
Convenant Veilige Toepassing van Medische Technologie in de medisch specialistische zorg (NFU)	Tweede druk	2016
NFU Normenkader informatiebeveiliging		
Parelsnoer-instituut (NFU)		
Manifest In Goed Vertrouwen - Privacy jeugd borgen (GGZ NL / VNG e.a.)		Juni 2016
Vuistregels voor professionals bij gegevensuitwisseling en privacy (GGZ NL / VNG e.a.)		2016
Alert Online campagne (NVZ)		2016
Online zelftest informatiebeveiliging (NVZ)		
Convenant "Veilige toepassing van medische technologie in het ziekenhuis' (NVZ)		
Richtlijn Omgaan met medische gegevens (KNMG)		September 2016
Handleiding Privacy bij regionale uitwisseling van patiëntgegevens (KNMG)		2010
Gedragscode Elektronische Gegevensuitwisseling in de Zorg (EGiZ)		November 2014
Handreiking Artsen en Social Media (KNMG)		2011
Medical App Checker: a Guide to assessing Mobile Medical Apps (KNMG)		
Handreiking voor naleving meldplicht datalekken (KNMG)		
Zorgbrede govenancecode 2017		September 2016
Wet- en regelgeving en normenkaders		
Wet bescherming persoonsgegevens (Wbp), inclusief meldplicht datalekken (artikel 34a Wbp)		
Wbp-naslag (AP)		
Handleiding Wet bescherming persoonsgegevens		Juli 2006
Beleidsregels meldplicht datalekken (AP)		December 2015
Richtsnoeren voor de Beveiliging van patiëntgegevens (CBP)		Februari 2013
Toegang tot digitale patiëntendossiers binnen zorginstellingen, Onderzoeksrapport (CBP)		Juni 2013
Informatiebeveiliging ziekenhuizen voldoet niet aan de norm,		November 2008

Onderzoeksrapport (CBP & IGZ)	
Eisen bewerkersovereenkomst (AP)	Mei 2016
CBP: gemeenten mogen bij decentralisatie privacywetgeving niet negeren	Juli 2014
Archiefwet	
Auteurswet	
Grondwet (vooral artikel 10 en 13)	
Wet kwaliteit, klachten en geschillen zorg	
Richtlijnen Centrale Commissie Mensgebonden Onderzoek (CCMO)	
Richtlijnen van de International Conference on Harmonisation of technical requirements for registration of pharmaceutical for human use. Good Clinical Practice.	
Telecommunicatiewet	
Wet beroepen in de individuele gezondheidszorg (Wet BIG)	
Wetsvoorstel Computercriminaliteit III	
Wet gebruik Burgerservicenummer in de zorg (Wbsn-z)	
Wet geneeskundige behandelingsovereenkomst (WGBO), eigenlijk boek 7 BW artikel 7:446 e.v.	
Wet cliëntenrechten bij elektronische verwerking gegevens Wet medisch-wetenschappelijk onderzoek met mensen (WMO, niet te verwarren met de andere Wmo voor maatschappelijk ondersteuning)	
Wet maatschappelijke ondersteuning (Wmo)	
Jeugdwet	
Wet langdurige zorg	
Wet op het hoger onderwijs en wetenschappelijk onderzoek	
Algemene Verordening Gegevensbescherming (AVG)	
eIDAS-Verordening	
EU-Richtlijn Netwerk en Informatiebeveiliging (NIB)	
Europese richtlijn medische apps	
(herziene) Convenant medische technologie (IGZ)	
NEN 7510 (Informatiebeveiliging in de zorg)	
NEN 7512 (Vertrouwensbasis voor gegevensuitwisseling)	
NEN 7513 (Logging)	
Grip op datalekken - Handreiking voor het beheersen van datalekrisico's	2015
T.F.M. Hooghiemstra en S. Nouwt, SDU Commentaar, Wet bescherming persoonsgegevens, editie 2016	Juni 2016

J. Krabben (PrivacyCare) en T.F.M. Hooghiemstra (PBLQ), Patiëntauthenticatie, advies in opdracht van minister van VWS.		Augustus 2016
Wet gegevensverwerking en meldplicht cybersecurity		2016
Handreiking Betrouwbaarheidsniveaus (Versie 4) (Forum Standaardisatie)		November 2016
Algemeen		
Cyber security of networkconnected medical devices in (EMEA) Hospitals 2016		2016
Wet- en regelgeving in de zorg (Nictiz)		2013
Veilig omgaan met e-mail in de zorg (NICTIZ)		2015
Voorbeeld procedure melding datalek (RPCG)		2015
Bijlage 1: Formulier melding datalek (RPCG)		2015
Bijlage 3: Informatie voor leden van de Datalekken Commissie (RPCG)		2015
Bijlage 4: Informatie voor te interviewen interne personen (RPCG)		2015
Bijlage 5: Informatie voor te interviewen medewerkers van derden (RPCG)		2015
Bijlage 6A: Format rapportage Datalekken Commissie - met toelichting (RPCG)		2015
Bijlage 6B: Format rapportage Datalekken Commissie (RPCG)		2015
Grondslag samenwerken aan Zorg en Veiligheid. Naar een handelingskader gegevensdeling (Leertuin Zorg en Veiligheid)	Werkdocument	Oktober 2013
S. Nouwt, Gemeentezorg en privacyzorgen (NJB)		2014 (42)
Big data in de gezondheidszorg (Nictiz)		2015
Nederland digitaal droge voeten – Cybersecurity adviesrapport Herna Verhagen (in opdracht van de Cyber Security Raad)		Oktober 2016
Handreiking cybersecurity voor de bestuurder (Cyber Security Raad)		April 2015
“Informatiebeveiliging is een issue voor de zorg” (Zorgvisie)		Oktober 2016
Zorgmedewerkers letten op informatiebeveiliging (NVZ)		Oktober 2016
Zwarte markt voor medische gegevens groeit (Zorgvisie)		Oktober 2016
Licht op de digitale schaduw. Verantwoord innoveren met big data (Rapport van de expertgroep Big data en privacy aan de minister van Economische Zaken)		Oktober 2016
Ziekenhuizen melden 300 datalekken (Zorgvisie)		24 november 2016
Ziekenhuizen melden elke dag datalek (Trouw)		24 november 2016
Cybersecuritybeeld Nederland 2016 (NCSC)		2016
P. van Houten, M. Spruit & K. Wolters, Informatiebeveiliging onder controle, Pearson, Amsterdam.		2015

PBLQ

M. Spruit, Volwassenheid informatiebeveiliging, RAAK-project Veilig Water, Haagse Hogeschool.	2016
M. Spruit & M. de Graaf, Een twee-sporenaanpak voor informatiebeveiliging (Management Executive, nr. 1, pag. 34-37).	2004