Actieplan

Informatiebeveiliging in de medisch-specialistische zorg en geestelijke gezondheidszorg

Nederlandse Vereniging van Ziekenhuizen

NFU NEDERLANDSE FEDERATIE VAN UNIVERSITAIR MEDISCHE CENTRA

zkn

GGZNEDERLAND

(14 juni 2017)

1. Inleiding

Dit Actieplan is in nauwe samenwerking met de Nederlandse Vereniging van Ziekenhuizen (NVZ), Nederlandse Federatie van Universitair Medische Centra (NFU), GGZ Nederland en Zelfstandige Klinieken Nederland (ZKN) tot stand gekomen. In dit plan zijn concrete activiteiten benoemd waarmee koepelorganisaties en/of zorgaanbieders al aan de slag zijn, of gaan, of die in de komende periode breder worden uitgerold

Zorginstellingen worden regelmatig geconfronteerd met risico's op het gebied van informatiebeveiliging en privacybescherming. Dit illustreert onder andere de ransomware aanval van 12 mei jl, waar de instellingen in Nederland gelukkig geen slachtoffer van zijn geweest, maar wel leidt tot het (nog) verder aanscherpen van technische maatregelen. Op 15 december 2016 is het PBLQ-rapport over beveiliging van patiëntgegevens aan de Tweede Kamer gestuurd. De koepelorganisaties in de medisch-specialistische zorg en geestelijke gezondheidszorg (ggz) delen de urgentie om informatiebeveiliging verder te verbeteren. Zij onderschreven de conclusies en aanbevelingen uit dit rapport en hebben de handen ineengeslagen om gezamenlijk te verkennen welke doelen zij voor de komende periode stellen om de informatiebeveiliging bij instellingen in de medisch-specialistische zorg en ggz verder te verbeteren. Vanuit deze doelen worden acties vormgegeven om structureel de informatiebeveiliging op een hoger niveau te brengen. Dit actieplan richt zich allereerst op het inventariseren, delen en uitrollen van de in de praktijk bewezen 'goede voorbeelden', die gebruikt kunnen worden voor een zorgbrede implementatie. Hierbij is het van belang zowel in te zetten op cultuur, structuur en compliance. Aangezien in het PBLQ-rapport uitvoerig aandacht is besteed aan de wijze waarop ziekenhuizen en instellingen in de gzz in de dagelijkse praktijk omgaan met de beveiliging van hun patiëntgegevens en hoe hierin verbetering kan worden aangebracht zijn aanbevelingen uit dit rapport nader uitgewerkt.

Het actieplan maakt onderscheid tussen doelen en acties die gericht zijn op verschillende niveau's en onderdelen in de zorginstellingen. Het gaat daarbij om het bestuur en management, Functionaris gegevensbescherming (FG) en Information Security Officer (ISO), medewerkers (zowel zorgverleners als ondersteunend personeel) en cliënten. In de volgende paragrafen wordt ingegaan op deze verschillende onderdelen. Daarbij worden activiteiten opgebouwd vanuit activiteiten die gericht zijn op het bevorderen van goed gedrag, het delen van goede voorbeelden, het bundelen van krachten en bieden van handvatten voor het anticiperen op wet- en regelgeving en de komst van de Algemene Verordening Gegevensbescherming (AVG).

Het totaal aan activiteiten zal van alle betrokkenen een forse extra inspanning vragen.

Ook wordt inzicht gegeven in de activiteiten die brancheorganisaties, NVZ, NFU, ZKN en GGZ Nederland al ondernemen ('Ist) of voornemens zijn te ondernemen ('Soll) per organisatie weergegeven.

2. Bestuur en Management

Het PBLQ-rapport merkt het volgende op over de rol van bestuur en management: '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.'

Doelen:

- Informatiebeveiliging en bescherming van persoonsgegevens zijn onderdeel van de integrale management verantwoordelijkheid.
- Informatiebeveiliging en bescherming van persoonsgegevens zijn geïntegreerd in de governance en P&C-cyclus.
- Overzicht, inzicht in gegevensverwerkingen is geborgd.
- Bestuurders zorgen voor voldoende resources voor informatiebeveiliging en bescherming van persoonsgegevens.
- Bestuurders zorgen ervoor dat in de organisatie risico's inzichtelijk gemaakt worden en dat duidelijk is wat er gebeurt als het zich voordoet.
- De bekendheid van de risico's voor omgang met patiënteninformatie wordt bevordert onder directies en raden van toezicht, die leiden tot een hogere prioritering en actiebereidheid.

Acties gericht op bestuur en management

Bevorderen goed gedrag

- De Raad van Toezicht controleert informatiebeveiliging-beleid van zorgconcern en legt hierover verantwoording af.
- In communicatie vanuit koepels, VWS, AP en IGZ[1] wordt het belang van naleving van relevante wet- en regelgeving op het gebied van informatiebeveiliging, waaronder de NEN-normen 7510, 7512 en 7513 benadrukt.
- Koepels verspreiden actief tools naar leden om management bewust te maken van informatiebeveiliging en bescherming van persoonsgegevens.
- Informatiebeveiliging en de naleving van NEN 7510, bestuurders zijn hiervoor eindverantwoordelijk, dienen onderdeel te zijn van de planning en control cyclus van de Raad van Bestuur.

---

[1] https://www.igz.nl/Images/20160302%20Vertrouwelijkheid%20van%20medische%20informatie%20brief%20aan%20koepels%20NFU%20AP%202%20%283%29%20def_tcm294-376620.pdf

Goede voorbeelden delen

- Checklist cyber security[2] op niveau Raad van Bestuur (voorbeeld is vragenlijst op website cybersecurity raad).
- Toolkit privacybescherming en informatieveiligheid/-beveiliging (PBIV) ggz van GGZ Nederland wordt beschikbaar gesteld voor andere sectoren.

Krachten bundelen

- Alle UMC's en een fors aantal algemene ziekenhuizen en GGZ-instellingen zijn lid van de Z-CERT[3]. Alle ziekenhuizen, GGZ-instellingen en categorale instellingen kunnen hieraan deelnemen en door een groeimodel kunnen op termijn alle zorgaanbieders zich aanmelden. Insteek is om lidmaatschap van Z-CERT verder uit te bouwen.
- In oktober 2017 start de ZEKER-campagne bij ziekenhuizen en GGZ-instellingen in samen met Alert Online[4]. De ZEKER campagne[5] zal op verschillende niveaus managers en medewerkers van zorginstellingen op een toegankelijke en aansprekende manier bewust maken hoe ze datalekken kunnen voorkomen. Het voorstel is om deze campagne uit te breiden naar andere sectoren (zorgzekeren.nl wordt aangepast).
- Het voorstel is om de Checklist cyber security op niveau Raad voor bestuur uit te breiden met privacy vragen.

Handvatten voor wet- en regelgeving / Anticiperen op de komst AVG

- Er wordt door brancheverenigingen in samenwerking met VWS een generieke Factsheet AVG voor de zorg opgesteld. Hierin wordt ook ingegaan op de consequenties voor bestuurders in de zorg. Bij het opstellen van de factsheet wordt ook gekeken naar de folder van de National Health Service folder waarin 12 aandachtspunten op het terrein van de zorg staan benoemd.
- Er wordt gekeken of de afstemming en coördinatie tussen juristen die zich bezighouden met voorbereiding op AVG verbeterd kan worden, bijvoorbeeld in het overleg dat valt onder het Informatieberaad Zorg en zich bezighoudt met informatiebeveiliging.
- De koepels passen de model bewerkersovereenkomst verder aan ter voorbereiding op komst AVG. Deze wordt generiek gemaakt voor alle zorginstellingen (najaar gereed).

---

[2] https://www.ncsc.nl/actueel/factsheets/checklist-beveiliging-van-ics-scada-systemen.html
[3] De Z-CERT is een voorziening om bij cyberincidenten snel in actie te kunnen komen, om detectie te versnellen en kennisdeling over informatie-beveiligingsincidenten te vergroten en hiermee de impact van dergelijke incidenten te beperken.
[4] Landelijke campagne van twee weken waarbij diverse activiteiten gelanceerd worden om cyberskills te vergroten en Nederland digitaal veiliger te maken
[5] www.zorgzekeren.nl

3. Functionaris Gegevensbescherming (FG) en Information Security Officer (ISO)

Het PBLQ-rapport merkt het volgende op over de rol van Functionaris Gegevensbescherming (FG) en een Information Security Officer (ISO): "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)"

Doelen

- FG's en ISO's beschikken over voldoende kennis en vaardigheden en hebben de vereiste autoriteit in de organisatie.
- Specialistische deskundigheid met betrekking tot informatiebeveiliging en privacybescherming bij privacy professionals wordt bevorderd.
- Privacy professionals kennen de wetten en normen en kunnen deze vertalen naar hun eigen praktijk.
- Privacy professionals fungeren als katalysator van de noodzakelijke (cultuur)veranderingen bij zorgverleners.

Acties gericht op FG/ISO

Bevorderen goed gedrag

- Inventariseren van opleidingsaanbod en beoordelen of deze voldoet aan de behoefte (o.a. accreditatie, tijd en geld).
- FG's en ISO's van zorginstellingen geven aan in hoeverre het opleidingsaanbod aansluit op de behoefte.

Goede voorbeelden delen

- Toolkit privacybescherming en informatieveiligheid/-beveiliging (PBIV) ggz van GGZ Nederland.
- Vanuit Z-CERT wordt er berichten met waarschuwingen en maatregelen verstuurd naar aanleiding van acute dreigingen (bijvoorbeeld ransomware) en kwetsbaarheden naar de deelnemers van Z-CERT.
- Z-CERT adviseert over preventieve maatregelen.
- Ingeval van ICT-beveiligingsincidenten helpt Z-CERT de technische-, privacy-, financiële-, en imagoschade zo veel mogelijk te beperken, door te adviseren en ondersteunen over de technische en organisatorische afhandeling (waaronder analyse van meldenswaardigheid) van de gemelde incidenten.

Krachten bundelen

- Voor het opleidingsaanbod wordt onderzocht in hoeverre accreditatie van opleiding geregeld moet worden. Waar nodig wordt een passend opleidingsaanbod ontwikkeld.

- Platform waarop zorg FG's en ISO's elkaar kunnen vinden en informatie uitwisselen (intervisie), Daarnaast worden door brancheorganisaties bijeenkomsten georganiseerd om kennis en ervaringen te delen en onderling af te stemmen.

Handvatten voor wet- en regelgeving / Anticiperen op de komst AVG

- Voorbereiden op de AVG door middel van coördinatie en afstemming van de juristen die hierbij betrokken zijn. Dit kan mogelijk worden versterkt door een gezamenlijk platform met alle maatregelen, uitleg en hulpmiddelen die zorgbreed toegankelijk zijn.
- Om het zorgveld voor te bereiden op de komst van de AVG zal VWS een ondersteunende rol bieden door aan brancheorganisaties in de zorg uitleg, goede voorbeelden en eventuele hulpmiddelen beschikbaar te stellen en te fungeren als informatiepunt voor de brancheorganisaties voor zorgspecifieke vragen . De AP wordt hierbij betrokken.
- Ondersteuning bij beheer van risico analyse (bijvoorbeeld door handleiding ISMS, baseline).
- In aanvulling op het Handboek Cybercrime wordt een Handboek datalekken opgesteld voor alle zorginstellingen.
- Branche-organisaties stellen het Privacy Framework beschikbaar. Om dit toegankelijker te maken wordt dit mogelijk verkort tot de belangrijkste items.

4. Medewerkers zorgaanbieders

Het PBLQ-rapport was er onder meer op gericht 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. Volgens het rapport is de bewustwording toegenomen omdat veel instellingen hiervoor meer capaciteit beschikbaar hebben gesteld. Drivers hiervoor zijn onder andere de meldplicht datalekken (artikel 34a Wet bescherming persoonsgegevens) en de toename van cyberdreigingen, zoals ransomware. Bewustwordingscampagnes hebben bij diverse zorginstellingen bijgedragen aan meer bewustwording. Hier wordt verder op ingezet.

Doelen

- Blijvende en geborgde awareness voor informatiebeveiliging en bescherming van persoonsgegevens bij medewerkers van zorgaanbieders.
- Medewerkers van zorgaanbieders beschikken over voldoende kennis en hebben een juiste houding ten aanzien van informatiebeveiliging en bescherming van persoonsgegevens en handelen hiernaar.
- Medewerkers hebben vaardigheden en middelen tot hun beschikking om juist te kunnen handelen. Inzicht in de eigen verantwoordelijkheden in relatie tot informatiebeveiliging en bescherming van persoonsgegevens.
- Bevorderen dat zorgverleners (artsen, verpleegkundigen, assistenten etc.) van klinieken de risico’s van verkeerd omgaan met patiëntgegevens inzien, en bewust zo veilig mogelijk hier mee om gaan.

Bevorderen goed gedrag

- Koepels adviseren leden om medewerkers voor zover van toepassing te laten deelnemen aan de ZEKER campagne om de bewustwording te vergroten en met name kleine datalekken te voorkomen (dit is een belangrijk onderdeel van de komende ZEKER campagne).

Goede voorbeelden delen

- Bestaande e-learning modules op het terrein van informatiebeveiliging en gegevensbescherming inventariseren en die zo mogelijk breed beschikbaar stellen. Een projectleider zal in het najaar van 2017 inventariseren welke instrumenten breder inzetbaar en deelbaar zijn en zal die beschikbaar stellen aan alle zorgaanbieders.
- Brancheorganisaties bevorderen dat (nieuwe) medewerkers van zorgaanbieders e-learning cursus volgen bij het werken met een digitaal dossier / patiëntgegevens.
- Zorginstellingen stimuleren van het gebruik van hulpmiddelen voor het beheer van wachtwoorden in de zorg.
- De koepels zullen 10 geboden opstellen voor informatiebeveiliging om die door hun leden in de organisatie te verspreiden.

Krachten bundelen

- Gebruik maken van (bestaande) informatiefilmpjes als middel om boodschap over het belang van informatiebeveiliging en privacy te herhalen. Dit wordt opgepakt door de projectleider.

- De koepels adviseren hun leden om nieuwe medewerkers een introductie aan te bieden over informatiebeveiliging en privacy en hier bij de opleiding van medewerkers (binnen organisatie) hier ook aandacht aan te besteden.

Handvatten voor wet- en regelgeving / Anticiperen op de komst AVG

- De projectleider stelt een factsheet op met belangrijkste punten rond informatiebeveiliging en privacy op medewerkerniveau.
- De projectleider stelt een factsheet op om medewerkers te informeren over de komst AVG en de veranderingen die dit voor medewerkers heeft en organiseert hierover op de praktijk aansluitende workshops.

5. Cliënten

Doelen

- Bewustzijn van rechten en verantwoordelijkheden met betrekking tot informatiebeveiliging en gegevensbescherming.
- Bewustzijn van de eigen verantwoordelijkheid voor informatiebeveiliging en de bescherming van de eigen gegevens.
- De cliënt heeft kennis van rechten en plichten (toestemming, inzage, recht op vergeten).
- De cliënt wordt zo veel mogelijk geholpen met vaardigheden en middelen om juist te kunnen handelen.

Bevorderen goed gedrag

- Cliënt laten helpen privacylekken te melden bijvoorbeeld door meldpunt binnen organisatie in te richten waar cliënten terecht kunnen. Koepels geven aan deze optie onder de aandacht van hun leden te brengen.
- Zorgaanbieders kunnen de eigen verantwoordelijkheid van cliënt expliciet maken door cliënten hierover met een heldere folder te informeren.

Krachten bundelen

- Generieke patiëntenfolder opstellen .

6. Activiteiten van de brancheorganisaties

Acties bestuur & management				
	ZKN	**NVZ**	**NFU**	**GGZ NL**
IST	-Beperkt aantal instellingen NEN 7510 gecertificeerd - Bereidheid tot deelname aan Z-CERT -Aandacht voor privacy en cyber security in ledenbijeenkomsten	-Awareness communicatie materiaal -Beperkt aantal instellingen NEN 7510 gecertificeerd -Deelname (deels) aan Z-CERT -Kennis en ervaring met melding datalekken -Brede bestuurlijke aandacht voor privacy	-Diverse communicatiemiddelen voor awareness. -Certificering ISO27001 / NEN7510 is bij diverse UMC's aanwezig. -Tweejaarlijkse benchmark NEN7510. -Kennis en ervaring met meldplicht datalekken.	- Awareness communicatie materiaal - Aantal ggz-instellingen NEN 7510 gecertificeerd - Aantal ggz-instellingen nemen deel aan Z-CERT -Kennis en ervaring met melding datalekken - Continue bestuurlijke aandacht voor privacy
SOLL	-Bevorderen van de bekendheid van de risico's voor omgang met patiënten informatie onder directies en raden van toezicht - ZKN Product- dienstencatalogus uitbreiden op thema informatiebeveiliging	-Informatiebeveiliging en privacy moeten op bestuurlijk niveau geïntegreerd zijn in governance. -Sturing en controle met behulp van ISMS -Goed bestuurlijk beeld op basis van risicomanagement	-Informatiebeveiliging en bescherming van persoonsgegevens moeten op bestuurlijk niveau worden geïntegreerd. -Sturing op basis van privacyframework en ISMS. Invoering van integraal risicomanagement. -Verder op sterkte brengen van capaciteit voor Informatiebeveiliging en Privacybescherming	-Bestuurlijke adaptie van informatiebeveiliging en gegevensbescherming. - Sturing met behulp van een lean SMS of Raamwerk PBIV -Handzame ondersteuning voor bestuurders, waar beginnen, hoe beginnen? -Kennisdeling en intervisie naar volwassenheidniveau (bijvoorbeeld masterclass voor NEN gecertificeerd)

Acties FG / ISO				
	ZKN	**NVZ**	**NFU**	**GGZ NL**
IST	- Onderwerp op agenda commissie Kwaliteit & Veiligheid -ZKN ledenportal voor uitwisseling inhoudelijke documentatie	-Grote deelname aan overlegstructuur ISO's en FG's. (FG's niet geformaliseerd) -Deelname aan online platform voor informatiebeveiliging NVZ instellingen -Deelname FG's en ISO's aan trainingsprogramma's en opleidingen -Gezamenlijke ontwikkeling van tools, hulpmiddelen en handreikingen -Deelname ZORG-ISAC	-Periodiek overleg NFU voor ISO's en FG's. -Trainingsprogramma's FG's en ISO's. -Deelname door FG's aan leergang FG (Duthler). -Certificeringen ISO's (o.a. CISSP). -Privacyframework NFU. -ISMS ingericht in diverse UMC's. -Praktijkgids NEN7510. -Diverse middelen (IB-beleid, model bewerkersovereenkomst, procedure datalekken).	-Deelname FG's en ISO's aan trainingsprogramma's -Deelname FG's en ISO's aan netwerk PBIV (GGZ N) -Framework BPIV van GGZ N -Diverse hulpmiddelen zoals de handreiking autorisaties EPD en de functiebeschrijving FG.
SOLL	- Samenwerking met VWS en koepels voor ontwikkelen tools/cursussen	-Opleiding voor FG's. -Deelname alle ISO's aan intervisie/kennisdeling sessies, o.a. bijvoorbeeld te organiseren vanuit de Z-CERT -Opzet van een netwerk voor FG's. -Introductie AVG, actuele hanteerbare informatiebron voor AVG inclusief handreikingen, tools enz.	-Accreditatie en certificering FG's Kennisportaal voor de security en privacy professional. -Invoering van een PDCA-cyclus voor bescherming van persoonsgegevens.	-Deelname ISO's aan intervisie/kennisdeling sessies, bijvoorbeeld te organiseren vanuit de Z-CERT -Deelname FG's aan intervisie/kennisdeling bijvoorbeeld via GGZ NL -Introductie AVG, e-learning, awareness en handzame instructie, ook via app.

Medewerkers				
	ZKN	**NVZ**	**NFU**	**GGZ NL**
IST	ZKN Academie scholingsplatform	Inzicht in de eigen verantwoordelijkheden in relatie tot informatiebeveiliging en bescherming van persoonsgegevens. Zorgverleners en ander personeel hebben adequate vaardigheden en hulpmiddelen tot hun beschikking.	Diverse communicatiemiddelen voor awareness. Gedragscodes voor medewerkers.	Inzicht in de eigen verantwoordelijkheden in relatie tot informatiebeveiliging en bescherming van persoonsgegevens. Zorgverleners en ander personeel hebben adequate vaardigheden en hulpmiddelen tot hun beschikking. Aandacht in opleidingen en gedragscode voor medisch beroepssgeheim en het privacy-gevoelige karakter van geestelijke gezondheidszorg
SOLL	Samenwerking met VWS en koepels voor ontwikkelen tools/cursussen Aandacht voor opleidingen in ZKN Academie opleidingsprogramma	Aandacht in opleidingen en gedragscode voor medisch beroepsgeheim en het privacy-gevoelige karakter van medische informatie	Onderhoud awareness (toekomstige ontwikkelingen). Faciliteren van gewenst gedrag door het invoeren van veilige en betrouwbare middelen (bijv. secure mail, authenticatiemiddelen, veilige ICT-infrastructuur in de zorg). Informatieverstrekking en e-learning modules (bijv. wanneer informed	Diverse communicatiemiddelen met betrekking tot awareness

Cliënten				
	ZKN	**NVZ**	**NFU**	**GGZ NL**
IST	Aandacht voor voorlichting in ZKN-keurmerk	In patiëntenfolders en op websites wordt informatie verstrekt. Eigen per instelling.	Patiëntenfolders met aandacht voor bescherming persoonsgegevens.	
SOLL	Samenwerking met VWS en koepels voor ontwikkelen communicatiemateriaal	Eenduidige informatie voor de zorg met betrekking tot rechten en plichten. Invoering van betrouwbare middelen voor authenticatie	Faciliteren van gewenst gedrag door het invoeren van veilige en betrouwbare middelen (portaal, authenticatiemiddelen).	Patiëntenfolders met aandacht voor bescherming persoonsgegevens.