Format

Quickscan informatiebeveiliging

voor (kleine) zorgorganisaties

Inhoudsopgave

1. Inleiding

Informatiebeveiliging wordt steeds belangrijker in de zorgsector. Zorgorganisaties zijn dagelijks verantwoordelijk voor de persoonlijke en medische gegevens van hun cliënten. Het is cruciaal om de beschikbaarheid, integriteit (juistheid) en vertrouwelijkheid, ook wel BIV genoemd, van deze gegevens te waarborgen. Dit is niet alleen essentieel voor het vertrouwen van cliënten, maar ook voor de continuïteit en kwaliteit van de dienstverlening.

Bureau eOverdracht helpt zorgorganisaties, in opdracht van het ministerie van VWS, bij het invoeren van informatiebeveiliging. De wettelijk verplichte NEN 7510 (norm voor informatiebeveiliging in de zorg) is hierbij de leidraad. Voor veel organisaties is het een grote stap om volledig volgens NEN 7510 te werken. Deze Quickscan informatiebeveiliging is bedoeld voor organisaties die nog niet klaar zijn voor de implementatie van NEN 7510, maar die wel een start willen maken met het verbeteren van de informatiebeveiliging.

Wat biedt deze quickscan?

- Inzicht of de belangrijkste maatregelen voor informatiebeveiliging zijn geïmplementeerd;
- Suggesties voor volgende stappen om de informatiebeveiliging te verbeteren.

In welke fase is deze quickscan zinvol?

- Het voldoen aan NEN 7510 is wettelijk verplicht. Zolang implementatie van NEN 7510 te groot is, is de quickscan een mooie start om richting te geven aan informatiebeveiliging.

Veel zorgorganisaties hebben te maken met dezelfde kwesties. De quickscan zal worden uitgebreid met een basis-invulling voor een deel van de normen. Organisaties kunnen deze gebruiken om te valideren en aan te vullen. Zodra dit beschikbaar is, wordt dit vermeld in een nieuwe versie van de quickscan.

Deze quickscan is gebaseerd op het Veiligheidskader GIDS Open Standaarden.

2. Handleiding

Uitvoering van de quickscan: wie en hoe

Een zorgorganisatie kan deze quickscan zelf uitvoeren of een andere organisatie vragen om dit te doen als een collegiale review. De reviewer probeert dit zo objectief en onafhankelijk mogelijk te doen. Dit proces kan beginnen met een zelfscan en later kan iemand met een onafhankelijke rol gevraagd worden om de quickscan uit te voeren. De reviewer moet basiskennis van informatiebeveiliging hebben om de maatregelen te begrijpen en te beoordelen of ze effectief zijn.

Bij een collegiale review kan de zorgorganisatie vooraf documenten opsturen die aantonen dat ze aan het kader voldoet. De organisatie kan ook ter plekke uitleggen hoe het informatiebeveiligingsbeleid in de praktijk werkt.

Het normenkader
Het normenkader bestaat uit startmaatregelen en vervolgmaatregelen. De reviewer bekijkt welke maatregelen in de organisatie aanwezig zijn. In het normenkader staan voorbeelden van hoe de organisatie kan aantonen dat een maatregel is geïmplementeerd, maar de uitvoering kan ook op een andere manier plaatsvinden.

Rapportage
De rapportage bestaat uit een ingevuld overzicht uit bijlage 1, dat ook in Excel beschikbaar is met een grafiek van de resultaten. Klik hier voor het Excelbestand.

Bij de velden 'Toelichting', 'Nog open vragen / verbeterpunten' en 'Opmerkingen' moet een korte samenvatting in begrijpelijke taal worden gegeven, zonder details over beveiligingsmaatregelen.

De reviewer rapporteert wat daadwerkelijk is geconstateerd, niet wat de organisatie van plan is. Bij een volgende review kan worden vastgesteld of verbeterplannen zijn uitgevoerd en pas dan worden deze als resultaat opgenomen.

De persoon die de quickscan uitvoert, rapporteert de bevindingen en voegt, indien gewenst, een reactie van de zorgorganisatie toe. Deze reactie kan maatregelen vermelden die naar aanleiding van de bevindingen zijn genomen.

Vervolg na de quickscan
Op basis van de rapportage maakt de zorgorganisatie een plan van aanpak om de informatiebeveiliging te verbeteren, inclusief de route en termijnen om aan NEN 7510 te voldoen.

Bij voorkeur wordt direct ook de volgende review met gebruik van deze quickscan ingepland. De quickscan moet minimaal jaarlijks worden uitgevoerd om de voortgang te volgen. Bij veranderingen, zoals in het informatiebeveiligingsbeleid, kan eerder een nieuwe review worden uitgevoerd.

3. Normenkader

De *cursief gedrukte tekst* bevat voorbeelden van manieren om iets vast te stellen, maar deze zijn niet leidend.

3.1 Deel 1: Maatregelen om mee te starten

1. Informatieveiligheid en privacy zijn een prioriteit van de eigenaar/eigenaren en de directie

Het beleid voor informatiebeveiliging en privacy is effectief wanneer de leiding dit actief ondersteunt en uitdraagt. Tijdens de evaluatie moet deze betrokkenheid van de leiding duidelijk zichtbaar zijn.

Voorbeelden van manieren waarop dat aangetoond kan worden:

- *De eigenaren zijn actief betrokken bij de evaluatie en tonen aan goed op de hoogte te zijn van de details.*
- *Er zijn duidelijke voorbeelden van beslissingen op directieniveau waarbij beveiliging en privacy voorrang kregen.*
- *Medewerkers voelen zich gesteund door de directie bij het uitvoeren van beveiligingsmaatregelen.*

2. Directie en verantwoordelijk medewerkers weten aan welke wetten en andere verplichtingen ze moeten voldoen en welke (leveranciers van) informatiesystemen er zijn

Het doel van deze maatregel is om inzicht te verkrijgen in de wetten en verplichtingen waaraan de organisatie moet voldoen. Dit overzicht helpt bij het plannen van acties om aan deze verplichtingen te voldoen.
Het omvat zowel **algemene wetten**, zoals de AVG, als sectorspecifieke wetten en andere contractuele verplichtingen.

Informatiesystemen ondersteunen de informatievoorziening, en het is essentieel dat de organisatie een duidelijk overzicht heeft van deze systemen. Het overzicht van informatiesystemen en hun leveranciers helpt om te begrijpen waar de informatie van de organisatie zich bevindt, wat cruciaal is voor de beveiliging van deze informatie.

Voorbeelden van specifieke wetten/verplichtingen:

- *WGBO* (Wet geneeskundige behandelingsovereenkomst)
- *Wegiz* (Wet Elektronische Gegevensuitwisseling in de Zorg)
- *NEN 7510* (Norm Informatiebeveiliging in de zorg)
- *NIS2* (Network and Information Systems directive).
  Let op! Deze cybersecurityrichtlijn is niet voor heel kleine zorgorganisaties van toepassing. Doe de zelf-evaluatie om te weten of NIS2 van toepassing is.

- Contractuele verplichtingen, zoals eisen van het zorgkantoor of de gemeente.

Voorbeelden van manieren waarop dat aangetoond kan worden:
- *Er is een overzicht beschikbaar van de verplichtingen waaraan voldaan moet worden.*
- *Directie en medewerkers kunnen direct de voor het werk relevante eisen noemen.*
- *Er is een overzicht beschikbaar van informatiesystemen en bijbehorende leveranciers.*

Voorbeelden van (leveranciers van) informatiesystemen:
- Elektronisch Cliënten Dossier (ECD) van leverancier X
- Kantoorautomatisering (apparatuur en/of applicaties)
- Personeelsadministratie
- Financiële administratie
- Medicatiedossier
- Leverancier van datacentrum

3. Er is begrip van de risico's die voor de doelgroep en/of de organisatie relevant zijn

Bij informatiebeveiliging draait het om risico's, incidenten en maatregelen.

Denk bijvoorbeeld aan het risico dat iemand onbevoegd inlogt. Het incident is een uitgelekt wachtwoord. De maatregel is het implementeren van twee-factor-authenticatie.

Welke risico's relevant zijn, hangt sterk van de context en de doelgroep af. Daarom is het van belang om eerst algemeen vast te stellen op welke manieren patiënten/cliënten in de problemen kunnen komen, bijvoorbeeld: "ik wil niet dat mijn zorginformatie uitlekt: mijn buren kijken op mij neer als zij weten welke problemen ik heb" of "ik kan geen goede zorg krijgen als de informatie niet beschikbaar is of niet klopt".

De risico's liggen op het vlak van:
- Beschikbaarheid (informatie is beschikbaar op de tijd en de plaats waar het nodig is);
- Integriteit (informatie is juist en volledig);
- Vertrouwelijkheid (informatie is alleen in te zien en te wijzigen door geautoriseerde personen).

Deze lijst van risico's zal in de loop der tijd gedetailleerder worden naarmate het risicomanagement zich ontwikkelt van een beginstadium (3a) naar een meer uitgebreid niveau (tot en met 3e).

Stel vast welke elementen al aanwezig zijn.

3	Eis	*Voorbeelden van manieren waarop dat aangetoond kan worden*
3a	Er is een overzicht van • risico's die voor de patiënten/cliënten relevant zijn en • risico's die voor de organisatie relevant zijn.	• *Er kan mondeling weergegeven worden welke risico's relevant zijn.* • *Er kan een lijst met risico's overlegd worden.* • *Er is documentatie van de risicoanalyse.*
3b	Aan elk risico is een gewicht toegekend op basis van de waarschijnlijkheid van optreden en mogelijke schade (kans x impact).	• *Er is documentatie van de risicoanalyse.* • *Er is een tool voor risicomanagement waarin risicoanalyse is vastgelegd.*
3c	Het overzicht van de risico's is in samenwerking met medewerkers vastgesteld.	• *Er kan mondeling weergegeven worden welke nieuwe inzichten de gesprekken met medewerkers opgeleverd hebben.* • *Er is een gespreksverslag van een overleg met medewerkers hierover.*
3d	Het overzicht van de risico's is onderbouwd.	• *Het beveiligingsnieuws, bijvoorbeeld de nieuwsberichten van SANS of Security.nl, wordt gevolgd en er kan uitgelegd worden welke nieuwe relevante bedreigingen er uit een nieuwsbericht volgen.* • *De eigen analyse is vergeleken met de analyse van andere partijen en de verschillen kunnen verklaard worden.*
3e	Bij elk van de benoemde risico's is beoordeeld of deze acceptabel zijn of niet, en dus of maatregelen noodzakelijk zijn	• *Er kan mondeling weergegeven worden welke risico's niet acceptabel zijn en dus maatregelen behoeven.* • *Er kan een lijst worden overlegd met aangegeven welke risico's niet acceptabel zijn en dus maatregelen behoeven.*

4. Basisbeveiligingsmaatregelen

Tegen alle bij 3b genoemde incidenten, met een **niet-acceptabel** risico, zijn maatregelen genomen.

Voorbeelden van zulke maatregelen zijn:

- Opstellen en goedkeuren van informatiebeveiligingsbeleid;

- Beheer van toegangsrechten;
- Twee-factor-authenticatie;
- Maatregelen om door te kunnen werken bij uitval van systemen.

Als software en/of hardware door een derde partij geleverd wordt, dan heeft de organisatie met deze derde partij afspraken gemaakt over informatiebeveiliging. Minstens zijn er afspraken voor:

- het maken van back-ups en het terugzetten van back-ups. Het terugzetten van een back-up is getest op juistheid en volledigheid;
- monitoring van de systemen;
- beveiliging en beheer gebruikersapparaten;
- bestrijding en preventie van malware;
- software op bedrijfsmiddelen up-to-date houden;
- omgang met (persoons-)gegevens/verwerkersovereenkomst.

Voorbeelden van manieren waarop dat aangetoond kan worden:

- *De maatregelen kunnen, met mondelinge toelichting, ter plekke getoond worden.*
- *Er kan getoond worden dat er een actief informatiebeveiligingsbeleid is voor de leveranciers van apparatuur en applicaties.*

3.2 Deel 2: Vervolgmaatregelen

In dit deel bespreken we extra beveiligingsmaatregelen die organisaties kunnen overwegen. Naarmate een organisatie verder gevorderd is in informatiebeveiliging, worden deze maatregelen belangrijker. Soms worden ze ook vereist door andere partijen of wettelijke voorschriften. Deze maatregelen zijn niet in Deel 1 opgenomen omdat ze niet voor alle zorgorganisaties relevant zijn of omdat ze voor kleinere organisaties een onnodige belasting kunnen vormen.

5. Er zijn concrete beveiligingsregels voor de medewerkers en vrijwilligers/informele zorgverleners

Het gedrag van medewerkers, vrijwilligers en informele zorgverleners heeft invloed op het niveau van informatiebeveiliging. Daarom is het belangrijk dat de organisatie heldere richtlijnen biedt.

Het is raadzaam om medewerkers niet meer dan nodig te belasten. Waar mogelijk, verdient een technische oplossing de voorkeur.

Voorbeelden van richtlijnen voor gebruikers

- het kiezen en gebruiken van wachtwoorden;
- het gebruik van USB-sticks;
- het gebruik van open WiFi;
- het delen van gegevens met samenwerkingspartners en verwanten;
- het gebruik van informatie door vrijwilligers en informele zorgverleners;
- ‘Clear desk’ (leeg bureau) en ‘clear screen’ (schermvergrendeling);

- veilig communiceren/veilig mailen;
- het gebruik van informatie op papier (wanneer wel of niet printen);
- het delen van gegevens op social media;
- omgaan met phishing/smishing/vishing;
- het melden van incidenten en datalekken;

en dergelijke.

Voorbeelden van manieren waarop dat aangetoond kan worden:

- *De medewerkers, vrijwilligers en informele zorg hebben een lijst met do's en don'ts en kunnen deze informatie makkelijk reproduceren.*
- *In contracten zoals arbeidsovereenkomsten en vrijwilligersovereenkomsten staan regels waaraan men zich moet houden.*
- *Er is een gedragscode, die door medewerkers en vrijwilligers ondertekend is. Belangrijke onderwerpen hierin zijn onder meer regels voor gebruik van bedrijfsmiddelen, geheimhouding, en het naleven van specifieke beleidsregels rondom informatiebeveiliging en privacy (bijv. het melden van incidenten of werken op externe locaties).*

6. Het is intern duidelijk wie waar verantwoordelijk voor is

Er zijn verschillende taken op het gebied van informatiebeveiliging, zoals het zijn van een aanspreekpunt voor informatiebeveiliging, het beheren en opvolgen van incidenten, het toewijzen van toegangsrechten, en dergelijke. Voor elk van deze taken is duidelijk wie verantwoordelijk is en wie de vervanger is bij afwezigheid. Voor taken die onafhankelijkheid vereisen, zoals die van de Functionaris Gegevensbescherming, zijn er maatregelen getroffen om die onafhankelijkheid te waarborgen.

Voorbeelden van manieren waarop dat aangetoond kan worden:

- *Er is een lijst met informatiebeveiligingstaken, inclusief de naam of functie van de verantwoordelijke en de vervanger.*
- *Bij elke taak kunnen direct de naam van de verantwoordelijke en de naam van de vervanger worden genoemd.*
- *Er is een verdeling van rollen en verantwoordelijkheden aanwezig zoals toegelicht in:*
    - *§ 5.3 van NEN 7510-1:2024; en*
    - *§ 5.2 van NEN 7510-2:2024.*

7. Er is een noodplan voor informatievoorziening

Er zijn plannen, procedures en voorbereidingen voor als er iets mis gaat met applicaties en apparatuur. Deze zijn bij voorkeur ook getest, zodat de organisatie weet dat ze werken.

Voorbeeld
Als je ECD het niet doet, wat doe je dan? Denk hierbij aan de continuïteit van zorg, maar ook wat je doet om het ECD te herstellen. Deze stappen staan in een noodplan beschreven.

Voorbeelden van manieren waarop dat aangetoond kan worden:
- *Medewerkers kunnen benoemen wat ze moeten doen als er iets mis gaat.*
- *Er is een handboek voor noodsituaties.*
- *Er zijn afspraken voor noodgevallen en noodvoorzieningen, zoals kanalen voor nood-communicatie, fall-back systemen, manieren om snel inzicht te krijgen in de situatie en prioriteitenlijsten voor mogelijke acties.*
- *Er zijn verslagen van tests van de noodplannen.*

8. Er zijn procedures rond informatiebeveiliging

Er zijn procedures of richtlijnen voor taken zoals
- het melden van incidenten en datalekken bij de aangewezen autoriteiten;
- het aannemen en inwerken van nieuw personeel;
- het in gebruik nemen, inleveren en afdanken van apparatuur; en
- het afhandelen van informatiebeveiligingsmeldingen.

Andere taken kunnen ook aan bod komen.

Een procedure hoeft niet altijd schriftelijk vastgelegd te zijn. Het kan ook op een andere manier zijn ingericht en gewaarborgd.

Voorbeelden van manieren waarop dat aangetoond kan worden:
- *De procedures zijn gedocumenteerd.*
- *Er kan aangetoond worden dat de procedures in de praktijk werken.*
- *Er is een formulier of een knop op intranet, waarmee een geautomatiseerde procedure (workflow) in werking wordt gezet, bijvoorbeeld voor het melden van datalekken en incidenten.*

9. Er is een systeem voor het beheren van informatiebeveiliging actief

Deze quickscan gaat uit van een aantal losse maatregelen. Voor een meer georganiseerde aanpak van informatiebeveiliging zou de organisatie een managementsysteem voor informatiebeveiliging (ISMS) moeten opzetten. Zo'n ISMS is gebaseerd op normen zoals NEN 7510 of ISO 27001 en volgt een Plan-Do-Check-Act-(PDCA-)cyclus.

Voorbeelden van manieren waarop dat aangetoond kan worden:

- *Documentatie van het managementsysteem voor informatiebeveiliging.*
- *Er is een actielijst om maatregelen te implementeren.*
- *Auditverslag van het managementsysteem voor informatiebeveiliging.*
- *Informatiebeveiliging is opgenomen in het kwaliteitsmanagementsysteem voor ISO 9001 of HKZ.*

10. Er zijn specifieke informatiebeveiligingsmaatregelen genomen

Afhankelijk van de situatie kunnen specifieke maatregelen nuttig zijn, zoals het inrichten van tweefactor-authenticatie en het gebruik van versleutelde gegevensdragers (bv. USB-sticks).

Voorbeelden van manieren waarop dat aangetoond kan worden:

- *Mondelinge toelichting op de maatregelen.*
- *Schriftelijke beschrijving van de maatregelen.*

11. De medewerkers worden geschoold op het gebied van informatiebeveiliging

Dit gaat om activiteiten voor bewustwording en gedrag. Denk aan het onderwerp bespreken in het teamoverleg, opleidingen gericht op kennis (bijvoorbeeld een cursus of e-learning), en trainingen om veilig gedrag te versterken (bijvoorbeeld les in specifieke vaardigheden als het gebruik van een wachtwoordkluis of het gebruik van twee-factor-authenticatie).

Voorbeelden van manieren waarop dat aangetoond kan worden:

- *Medewerkers kunnen uitleggen hoe de organisatie hun kennis over informatiebeveiliging actueel houdt.*
- *Het onderwerp is vermeld op de agenda van het werkoverleg.*
- *Er is een opleidingsplan voor medewerkers.*
- *Er zijn certificaten voor gevolgde opleidingen en trainingen aanwezig.*
- *De gevolgde opleidingen zijn geregistreerd in een LeerManagementSysteem (LMS).*

4. Bijlagen

4.1 Bijlage 1: Resultaten Beoordeling Informatiebeveiliging

NB: Van deze tabel is ook een werkbladversie beschikbaar in Excel, inclusief grafiek van de resultaten. Klik hier voor het Excelbestand.

Organisatie / product:

Reviewers (namen + organisaties):

Datum review:

Maatregelen om mee te starten				
Item	**Omschrijving**	**Bevinding**	**Toelichting**	**Nog open vragen/verbeterpunten**
1	Informatieveiligheid en privacy zijn een prioriteit van de eigenaar/-eigenaren en de directie	ja/gedeeltelijk/nee		
2	Directie en verantwoordelijk medewerkers weten aan welke wetten en andere verplichtingen ze moeten voldoen en welke	ja/gedeeltelijk/nee		

Item	Omschrijving	Bevinding	Toelichting	Nog open vragen/verbeterpunten
	(leveranciers van) informatiesystemen er zijn			
3a	Er is overzicht van • risico's die voor de patiënten/cliënten relevant zijn en • risico's die voor de organisatie relevant zijn.	ja/gedeeltelijk/nee		
3b	Aan elk risico is een gewicht toegekend op basis van de waarschijnlijkheid van optreden en mogelijke schade (kans x impact).	ja/gedeeltelijk/nee		
3c	Het overzicht van de risico's is in samenwerking met medewerkers vastgesteld.	ja/gedeeltelijk/nee		
3d	Het overzicht van de risico's is onderbouwd.	ja/gedeeltelijk/nee		
3e	Bij elk van de benoemde risico's is beoordeeld of deze acceptabel zijn of	ja/gedeeltelijk/nee		

Item	Omschrijving	Bevinding	Toelichting	Nog open vragen/verbeterpunten
	niet, en dus of maatregelen noodzakelijk zijn			
4	Maatregelen voor een basisniveau van informatiebeveiliging zijn genomen	ja/gedeeltelijk/nee	*[Benoem de genomen maatregelen]*	

Vervolgmaatregelen

Item	Omschrijving	Bevinding	Toelichting	Nog open vragen/verbeterpunten
5	Er zijn concrete beveiligingsregels voor de medewerkers en vrijwilligers/informele zorgverleners	ja/gedeeltelijk/nee		
6	Het is intern duidelijk wie waar verantwoordelijk voor is	ja/gedeeltelijk/nee		
7	Er is een noodplan voor informatievoorziening	ja/gedeeltelijk/nee		
8	Er zijn procedures rond informatiebeveiliging	ja/gedeeltelijk/nee		

Item	Omschrijving	Bevinding	Toelichting	Nog open vragen/verbeterpunten
9	Er is een systeem voor het beheren van informatiebeveiliging actief	ja/gedeeltelijk/nee	*[Benoem de gebruikte norm]*	
10	Er zijn specifieke informatiebeveiligings-maatregelen genomen	ja/gedeeltelijk/nee	*[Benoem de maatregelen]*	
11	De medewerkers worden geschoold op het gebied van informatiebeveiliging	ja/gedeeltelijk/nee		

Reactie organisatie:

.....

Quickscan informatiebeveiliging voor (kleine) zorgorganisaties

Deze quickscan is onderdeel van het programma eOverdracht
en is tot stand gekomen met ondersteuning van
het Ministerie van Volksgezondheid, Welzijn en Sport

Meer informatie op www.startjekickstart.nl

Versie 1.1
December 2024

Samen werken aan eOverdracht