

Informatieveiligheid binnen ziekenhuizen



Voor wie is deze nieuwsbrief bestemd?

- ✓ Bestuurders
- ✓ Information Security Officer
- ✓ Functionaris privacy gegevens
- ✓ Kwaliteit medewerker
- ✓ Zorgmanager
- ✓ IT-manager

Duijnborgh Audit BV

is een middelgroot IT-audit kantoor dat zich bezig houdt met assurance en advies op het snijvlak van ICT en organisatie.



Duijnborgh Certification BV

is een onafhankelijke en onpartijdige organisatie die zich bezig houdt met certificatie activiteiten op het gebied van ICT en organisatie



NVZ toetsing doorlopen, "Hoe nu verder?"

Inmiddels hebben de meeste getoetste ziekenhuizen het rapport ingeleverd bij de IGZ en worstelen veel ziekenhuizen met de bovenstaande vraag.

Dit wordt versterkt doordat men nog niet goed weet wat de vervolgstappen van de IGZ in 2011 zullen zijn, welk accreditatie- of certificatieschema men straks moet gaan kiezen (NIAZ of NEN) en wat er dit jaar nog meer boven het hoofd hangt van de ziekenhuisbestuurders.

Budgetten worden steeds meer beperkt en de bezuinigingen zijn overal merkbaar en voelbaar. Hierdoor zullen alle ziekenhuizen overwogen met financiële middelen moeten omgaan, wat betekent dat een lange termijnplanning essentieel is. Bovenstaande onduidelijkheid met betrekking tot het onderwerp informatieveiligheid maakt een goede planning echter moeilijk.

Daarom kunt u maar beter het 'heft in eigen hand nemen'

"En nu?"

Met deze nieuwsbrief willen wij u informeren over onze ideeën om het door de ziekenhuizen in gang gezette verbeterproces van informatiebeveiliging te kunnen vasthouden en welke ondersteuning wij daarbij kunnen bieden. Want wat de eisen van externe belanghebbenden ook mogen zijn, u bent liever goed voorbereid. De ziekenhuizen hebben in het verleden veel energie en financiële middelen gestoken in de 'fundering' van goede informatieveiligheid. Net als patiëntenveiligheid en overige kwaliteitsonderwerpen dienen deze minimaal op niveau te blijven of zelfs continue te verbeteren. Hierbij kan Duijnborgh u van dienst zijn. Voor een deel is onze voorgestelde aanpak generiek, voor een belangrijk deel echter per zorginstelling specifiek, want één ding is zeker: nergens troffen wij eenzelfde situatie aan. **Maatwerk is dus gewenst!**

Leg de verantwoordelijkheid daar waar die hoort, namelijk bij het integraal management!

Onze aanpak is erop gericht dat ziekenhuizen de komende jaren een punt bereiken waarbij informatieveiligheid een vanzelfsprekend onderdeel is van de reguliere Personeel-, Informatievoorziening-, Organisatie-, Financiële, Automatisering/ Administratie- en Huisvestingtaken (PIOFAH). Kenmerkend voor dit integraal managementmodel is dat de verantwoordelijkheid voor de bedrijfsvoering zo laag mogelijk in de organisatie wordt gelegd. De leidinggevende is als integraal manager verantwoordelijk voor een deel of alle onderdelen van het PIOFAH model. Informatieveiligheid past –evenals andere kwaliteitsonderwerpen- prima daarbij.

"Hoe ziet de toekomst eruit?"

Welke standaard het gaat worden, uitbreiding van het NIAZ accreditatieschema of een certificeerbare NEN norm, achten wij op dit moment eigenlijk niet zo'n heel belangrijke vraag. Wij kunnen deze uitspraak doen omdat wij zowel nauwe contacten onderhouden met NIAZ (via onze beroepsvereniging NOREA) en NEN (via onze certificeringinstelling Duijnborgh Certification). Wat de uitkomst ook moge zijn, de door ziekenhuizen te implementeren maatregelen zullen elkaar nauwelijks gaan ontlopen. Er is dus geen enkele reden om te wachten met het (verder) implementeren van informatiebeveiliging in de organisatie. Naast het feit dat het zonde zou zijn om het huidige behaalde resultaat niet vast te houden lopen ziekenhuizen mogelijk extra risico op het ontstaan van informatieveiligheidsincidenten met als mogelijk gevolg persoonlijk leed, schadeclaims, imago schade en onnodige operationele kosten.

Waarom zou u kiezen voor vroegtijdige betrokkenheid van een externe auditor?

- ✓ Periodieke toetsing en risico rapportage richting bestuur
- ✓ Onafhankelijke evaluatie van zorg- en ICT processen door deskundige op uw vakgebied
- ✓ Voorkomt tunnelvisie!
- ✓ Kostenbesparend door tijdig sturing en suggesties
- ✓ Ervaring met zorggerelateerde informatiebeveiliging
- ✓ Hulp bij prioriteitbepaling van te nemen beheersmaatregelen
- ✓ Kennis van de processen binnen ziekenhuizen

Hoe kunnen wij ziekenhuizen helpen?

Het uiteindelijke doel kan een certificatie of derde-partij-verklaring (TPM) zijn waarmee de ziekenhuizen aan externe belanghebbenden kan aantonen dat het bewust en onderbouwd met organisatie- en patiëntengegevens om gaat waardoor de externe controledruk afneemt. In onderstaande afbeelding is grafisch weergegeven hoe een dergelijk traject er uit kan zien en wat de uiteindelijke lange termijn mogelijkheden voor een ziekenhuis kunnen zijn. Kort samengevat:

- Een ziekenhuis start in 2011 met de implementatie tegen de hoog risicogebieden vanuit de uitgevoerde risicoanalyse en/of eigen beveiligingsplan.
- Duijnborgh evalueert periodiek de gekozen werkwijze van het ziekenhuis tegen zorggerelateerde richtlijnen en rapporteert aan het ziekenhuis aandachtsgebieden om ‘overbeveiliging’, inefficiëntie en onnodige kosten te vermijden.
- Vanuit de rapportage kan het ziekenhuis het informatieveiligheid project bijsturen waar dat nodig is.
- Duijnborgh blijft tijdens het hele project aanspreekbaar voor ondersteuning tot de uiteindelijke certificering, accreditatie of TPM-verklaring.

