Informatiebeveiliging in de zorg: NEN 7510 nieuw en afgewogen

Omdat het beter kan

Wanneer ICT wordt toegepast, moet het veilig voor de patiënt zijn. Daarnaast brengt de toepassing van ICT, risico's voor de privacy van de patiënt met zich, terwijl het hier gaat om gevoelige gegevens die juist extra bescherming verdienen. Toch zijn het risicobewustzijn en maatregelen om informatiebeveiliging op een voldoende niveau te krijgen, tot op de dag van vandaag maar beperkt aanwezig[1].
Maar ook de Nederlandse norm voor informatiebeveiliging (IB) in de zorg, NEN 7510, was voor verbetering vatbaar. In 2011 wordt deze opnieuw uitgebracht, waarbij risicobeoordeling duidelijker als startpunt wordt neergezet voor de *keuze* aan beveiligingsmaatregelen, in een zich herhalend proces.[2]

Voor alle zorgprofessionals

Alle ziekenhuizen in Nederland moeten aan de inspectie met een externe audit aantonen dat zij voldoen aan een voldoende mate van informatiebeveiliging[3].
Maar informatiebeveiliging, daar waar mensen worden onderzocht, behandeld en verzorgd beperkt zich niet alleen tot ziekenhuizen. Ook in de eerstelijn, thuiszorg, verzorgingshuizen, ambulante hulpverlening en gespecialiseerde klinieken moet men kunnen rekenen op integere, vertrouwelijke en beschikbare informatie. Door toepassing van een schaalbare norm kan ook een solopraktijk eenvoudig aantonen, dat zij bewust omgaat met risico's voor informatiebeveiliging en privacy.

In de praktijk

Het behalen van een certificaat en mogen voeren van een logo is een mooie mijlpaal, maar tegelijkertijd ook maar een momentopname.
Wat toetsbaar moet zijn, zijn uw ambities, uw activiteiten en in hoeverre deze met elkaar in overeenstemming zijn of gebracht zullen worden.
In feite is dit de meest beknopte definitie van een kwaliteitssysteem, ook voor informatiebeveiliging.
NEN7510:2010 i.o. is een hulpmiddel om dit te bereiken, dat stoelt op internationaal erkende normen als ISO 27001, 27002 en 27799. Maar uiteraard dient ook wetgeving (WBP, KWZ, WGBO, WBIG) gevolgd te worden.

---

[1] IGZ/CBP rapport nov. 2008; M&I/partners juli 2009; NVZ/Q-consult feb. 2011; E&Y mei 2011
[2] http://www.nen7510.org/publicaties/3887
[3] Jaarplan rijksinspecties ziekenhuizen 2011,

Informatiebeveiliging stapsgewijs invoeren

1. Integratie met bestaande werkwijze

Door de combinatie met ISO27001 is de nieuwe NEN7510 in feite een kwaliteitsmanagementsysteem geworden naar analogie van ISO9001. Dit betekent dat ook informatiebeveiliging wordt vorm gegeven in een iteratief proces volgens de bekende stappen van plan-do-check-act. Niet door een 2e kwaliteitssysteem te ontwikkelen maar door informatiebeveiliging in uw bestaande werkwijze te integreren.

2. Risicobeoordeling

Essentieel voor een pragmatische invoering van informatiebeveiliging is een risicoanalyse en -beoordeling van de informatiestromen en hulpmiddelen (informatiesystemen). Dan zal blijken of de 39 hoofdcategorieën (beveiligingsdoelstellingen) allemaal even relevant zijn. Wanneer de motivatie om hier van af te wijken wordt vastgelegd, wordt duidelijk voor interne en externe geïnteresseerden (auditors) en andere belanghebbenden (uw klanten) dat men met een beheerste organisatie te maken heeft.

3. IB-baseline vaststellen en invoeren

Na een inventarisatie van de status quo wordt met de uitkomsten van de risicobeoordeling vastgesteld wat er tenminste moet gebeuren om informatiebeveiliging op een acceptabel niveau te krijgen en te houden. Daarbij wordt *gekozen* welke van de 129 beheersmaatregelen uit de NEN7510 moeten worden ingevoerd om een beheerste situatie te onderhouden.

NEN7510 / NEN-ISO/IEC 27002 hoofdstukken	Beheers-maatregelen
5 Beveiligingsbeleid	2
6 Organisatie van informatiebeveiliging	11
7 Beheer van bedrijfsmiddelen	5
8 Personeel	9
9 Fysieke beveiliging en beveiliging van de omgeving	13
10 Beheer van communicatie- en bedieningsprocessen	32
11 Toegangsbeveiliging	25
12 informatiesystemen	12
13 Beheer van informatiebeveiligingsincidenten	5
14 Bedrijfscontinuïteitsbeheer	5
15 Naleving	10
	129

4. Meten en bijstellen

Net als de jaarlijkse financiële planning en control cyclus bestaat ook kwaliteitsmanagement uit periodiek herhaalde activiteiten om resultaten te meten en nieuwe begrotingen te maken. Voor informatiemanagement betekent dat incidentrapportages evalueren, resultaten meten en vergelijken (benchmarkstudies), processen opnieuw analyseren en beleid bijsturen en vaststellen.

Aan de slag

Neem contact op met HuibHezemans.nl voor een kennismakingsgesprek of om uw situatie voor te leggen. HuibHezemans.nl werkt bij de beoordeling en verbetering van informatiebeveiliging in organisaties nauw samen met Audittrail en BITTI.

www.huibhezemans.nl
IBzorg@huibhezemans.nl
06-23953453

www.audittrail.nl

www.bitti.nl