

AAN AANGETEKEND
Diaconessenhuis Leiden

DATUM 2 juni 2009

ONS KENMERK z2009-00213

CONTACTPERSOON

UW BRIEF VAN

UW KENMERK

ONDERWERP Beslissing om af te zien van handhaving

Geachte A,

In het kader van hun toezichhoudende taak hebben de Inspectie voor de Gezondheidszorg (IGZ) en het College bescherming persoonsgegevens (CBP) in 2007 bij Diaconessenhuis Leiden een onderzoek ingesteld naar de veilige toepassing van ICT en in het bijzonder de mate waarin de normen voor de informatiebeveiliging worden nageleefd. Naar aanleiding van dit onderzoek en het door uw ziekenhuis vervolgens ingediende Plan van Aanpak, uw schriftelijke zienswijze van 17 april 2009 en de door u bij brief van 11 mei 2009 ingezonden nadere stukken heeft het CBP het besluit genomen om af te zien van handhavend optreden.

De loop van de procedure

Op 20 april 2007 hebben IGZ en CBP een bezoek gebracht aan Diaconessenhuis Leiden in het kader van het hiervoor genoemde onderzoek.

Over de resultaten van dit onderzoek is een rapport met voorlopige bevindingen opgemaakt. Zoals in artikel 60 lid 2 Wet bescherming persoonsgegevens (Wbp) is bepaald, bent u in de gelegenheid gesteld uw zienswijze te geven op de voorlopige bevindingen van dit onderzoek. U hebt van deze gelegenheid geen gebruik gemaakt. IGZ en CBP hebben vervolgens de definitieve bevindingen en conclusie vastgesteld.

Bij brief van 16 juli 2008 is u het rapport met de definitieve bevindingen en de conclusie naar aanleiding van het onderzoek toegezonden. IGZ en CBP concluderen dat er geen sprake is van een passend beveiligingsniveau zoals bedoeld in artikel 13 Wet bescherming persoonsgegevens, en dat evenmin is voldaan aan de voorwaarden om verantwoorde zorg te leveren zoals bedoeld in artikel 2 van de Kwaliteitswet zorginstellingen.

In de brief van 16 juli 2008 is u meegedeeld dat IGZ en CBP om die reden verwachtten dat er vóór 15 oktober 2008 een Plan van Aanpak zou worden opgesteld, waarin duidelijk wordt wat het ziekenhuis onderneemt om volledig aan de NEN 7510 norm te voldoen.

In het plan diende in ieder geval te worden aangegeven wanneer het ziekenhuis welk probleem zou hebben opgelost. Dat geldt voor alle onderwerpen die in de NEN 7510 aan de orde worden gesteld.

Ook is in de brief meegedeeld dat, indien IGZ en CBP, in het licht van de hiervoor genoemde eisen concluderen dat het ziekenhuis onvoldoende voortvarend werk maakt van het verbeteren van de informatiebeveiliging, IGZ en CBP zullen overwegen om handhavend op te treden.

Bij brief van 21 augustus 2008 heeft u IGZ uw Plan van Aanpak toegezonden, welk plan in kopie naar het CBP is gestuurd. Beide toezichthouders hebben het plan beoordeeld.
Bij brief van 26 maart 2009 heeft het CBP het ziekenhuis in kennis gesteld van zijn voornemen om handhavend op te treden.
Bij brief van 17 april 2009 heeft u hierover een schriftelijke zienswijze ingediend.
Bij brief van 11 mei 2009 heeft u, op verzoek van het CBP, nadere stukken ingezonden.

Bevindingen

Het CBP heeft de door u getroffen maatregelen onderzocht, waarvan u hieronder de bevindingen aantreft.

- 1. Uitvoeren risico-analyse informatiebeveiliging*
- 2. Opstellen rapportage van de risico-analyse*

In oktober-november 2008 heeft het ziekenhuis door een externe partij een risico-analyse laten uitvoeren. De analyse bestond uit drie onderdelen. Van twee onderdelen zijn de rapportages aan het CBP gezonden, van het derde onderdeel is een samenvatting te vinden in een toegezonden overkoepelend Plan van Aanpak.

Er is sprake is van een (volwaardige) risico-analyse. Daarmee lijkt aan deze twee maatregelen te zijn voldaan.

- 3. Opstellen en vaststellen functieprofiel informatiebeveiligingsfunctionaris*

In de brief van 17 april 2009 geeft het ziekenhuis aan dat het in 2009 eerst ervaring wil opdoen met deze functionaris om pas daarna een functieprofiel op te stellen. Aan deze maatregel is niet voldaan.

- 4. Aanstellen of aanwijzen informatiebeveiligingsfunctionaris*

In de brief van 17 april 2009 schrijft het ziekenhuis dat de directiesecretaris vanaf augustus 2009 de rol van informatiebeveiligingsfunctionaris toebedeeld heeft gekregen. Of er sprake is van een typefout, die met zich mee zou brengen dat er al vanaf augustus 2008 sprake is van deze toedeling of dat men bedoelt dat dit nog moet gebeuren in augustus 2009, is niet duidelijk. Het lijkt er echter op dat aan de maatregel is of zal worden voldaan.

- 5. Opstellen procesbeschrijving voor melden, registreren en afhandelen van informatiebeveiligingsincidenten*

Het ziekenhuis geeft in de brief van 17 april 2009 aan dat het opstellen van een dergelijke procedure hoort bij de prioriteiten voor 2009. In het Informatiebeveiligingsplan 2009 (gedateerd 1 april 2009) staat vermeld dat dit project zal worden aangestuurd door de directiesecretaris (dat wil zeggen informatiebeveiligingsfunctionaris) en staat een en ander gepland voor september en oktober 2009, met als realisatiedatum 1 november 2009. Aan de maatregel lijkt op termijn te worden voldaan.

Concluderend kan worden gesteld dat op twee punten (nog) niet aan de maatregelen is voldaan. Het functieprofiel informatiebeveiligingsfunctionaris zal pas in 2010 gereed zijn, maar de betreffende functionaris lijkt aanwezig te (zullen gaan) zijn. De procesbeschrijving informatiebeveiligingsincidenten zal volgens planning per 1 november 2009 zijn afgerond en in theorie daarmee aan het eind van dit jaar beschikbaar.

Besluit

Het CBP acht het niet opportuun het (nog) niet nakomen van deze twee maatregelen af te dwingen door middel van een last onder dwangsom. Gezien de voortgang bij de overige maatregelen vertrouwt het CBP er op dat het ziekenhuis op de goede weg is om in 2010 de NEN-audit succesvol te kunnen doorstaan. Het CBP besluit om af te zien van handhavend optreden.

Het toezicht houden op de door het CBP geconstateerde tekortkomingen zal worden overgedragen aan IGZ, die deze zal meenemen in het jaarlijks overleg. Wellicht ten overvloede wijst het CBP u erop dat op u de verantwoordelijkheid rust voor het blijvend waarborgen van de naleving van de bepalingen van de Wbp.

Hoogachtend,

Het College bescherming persoonsgegevens,
Voor het College,

mr. J. Kohnstamm
voorzitter