

Definitieve bevindingen SPITZ Midden-Holland

In het kader van zijn toezichhoudende taak heeft het College bescherming persoonsgegevens (CBP) onderzocht of de Stichting Schakelpunt Informatie Transmurale Zorg Midden-Holland (hierna: SPITZ-MH) de artikelen 13, 33 en 34 Wet bescherming persoonsgegevens (Wbp) naleeft bij haar gegevensuitwisseling tussen zorgverleners in de regio. Deze artikelen hebben betrekking op beveiliging respectievelijk informatieplicht. Het onderzoek naar de beveiliging is beperkt tot de aspecten toegang en logging.

Conclusie

Door middel van het Zorgportal heeft een deelnemende zorgverlener via het Regionaal Schakelpunt (RSP) toegang tot alle beschikbare patiëntinformatie van alle andere aangesloten zorgverleners. Aan de patiënten is hiervoor geen toestemming gevraagd. Behoudens het tonen van een waarschuwingsscherm heeft SPITZ-MH geen maatregelen getroffen om te voorkomen dat een aangesloten zorgverlener via het RSP gegevens inziet van een patiënt die op dat moment niet bij hem in behandeling is. Hierdoor handelt SPITZ-MH in strijd met artikel 13 Wbp juncto artikel 7:457 Burgerlijk Wetboek.

Uit het onderzoek blijkt dat alle raadplegingen door SPITZ-MH worden gelogd. De logging is echter niet specifiek gericht op verdachte situaties, waardoor de logging niet effectief kan worden gebruikt voor structurele controle op rechtmatige toegang tot patiëntendossiers. Er zijn evenmin duidelijke afspraken gemaakt tussen SPITZ-MH en de zorgverleners omtrent structurele en incidentele controle van de logging.

SPITZ-MH heeft daardoor onvoldoende geborgd dat onrechtmatige verwerking van patiëntgegevens wordt voorkomen. Dit is in strijd met artikel 13 Wbp.

Het CBP concludeert voorts dat SPITZ-MH in strijd handelt met artikel 34 Wbp omdat het verzuimt patiënten persoonlijk te informeren op het moment dat hun persoonsgegevens worden opgenomen in het RSP.

Verloop onderzoek

Op 2 maart 2009 hebben drie medewerkers van het CBP een onderzoek ter plaatse uitgevoerd bij SPITZ-MH. In het kader van het onderzoek zijn interviews afgenomen bij A en B. Daarnaast is informatie gebruikt uit systeemdocumentatie, papieren voorlichtingsmateriaal van SPITZ-MH en de website www.spitz-mh.nl.

Op 9 april 2009 heeft het CBP aan SPITZ-MH de voorlopige bevindingen van het onderzoek toegezonden. SPITZ-MH heeft hierop bij brief van 22 april 2009 gereageerd. Het CBP heeft SPITZ-MH per brief van 7 mei 2009 laten weten dat deze reactie geen aanleiding vormt om de bevindingen aan te passen.

Bevindingen

Toegangsbeveiliging

Artikel 7:457 BW ziet op de voorwaarden waaronder een hulpverlener - de in het kader van een behandelingsrelatie verzamelde - gegevens mag verstrekken aan anderen dan de patiënt.

Artikel 7:457 lid 1 formuleert het vereiste van toestemming van de patiënt voor een dergelijke gegevensverstrekking.

Aan de patiënten is geen toestemming gevraagd voor het uitwisselen van zijn gegevens via het RSP.

Het tweede lid van artikel 7:457 bevat een uitzondering op het toestemmingsvereiste voor zover het gaat om verstrekking van informatie aan degenen die betrokken zijn bij de uitvoering van de tussen de hulpverlener zelf en de patiënt gesloten behandelingsovereenkomst en voor gegevensverstrekking aan de waarnemer. Een en ander voor zover dergelijke gegevensverstrekking noodzakelijk is voor de door hen in dat kader te verrichten werkzaamheden.

Artikel 13 Wbp vereist dat de verantwoordelijke passende technische en organisatorische maatregelen ten uitvoer legt om persoonsgegevens te beveiligen tegen enige vorm van onrechtmatige verwerking. Deze maatregelen moeten, rekening houdend met de stand van de techniek en de kosten van tenuitvoerlegging, een passend beveiligingsniveau garanderen, gelet op de risico's die de verwerking en de aard van de te beschermen gegevens met zich brengt.

Doel van een EPD is het faciliteren van de elektronische uitwisseling van zorginformatie tussen hulpverleners voor zover dat voor de behandeling of verzorging van de patiënt aangewezen is. Gebruik van EPD-gegevens buiten de context van een behandelrelatie past niet binnen die doelstelling en is (derhalve) onrechtmatig.

Tegen de achtergrond van deze bepalingen is bij een EPD als passende beveiligingsmaatregel ter voorkoming van onrechtmatige verwerking vereist dat voorafgaand aan het verlenen van toegang tot EPD-gegevens zo mogelijk de aanwezigheid van een behandelrelatie tussen patiënt en de raadplegend hulpverlener wordt geverifieerd.

Door middel van het Zorgportal kan een deelnemende zorgverlener via het RSP zoeken naar medische informatie van alle patiënten van alle andere aangesloten zorgverleners. Na selectie van een patiënt verschijnt een tussenscherm met - onder meer - de volgende vraag:

“Heeft u met deze persoon, waarvan u het dossier wilt inzien, op dit moment een actuele behandel/zorgverleningsrelatie, en/of heeft u de informatie nodig in het kader van spoedeisende zorgverlening/behandeling?”.

Pas na een bevestigend antwoord op deze vraag (klikken op “Ja”) worden alle beschikbare gegevens van de geselecteerde patiënt daadwerkelijk getoond. Gegevens zijn niet beschikbaar indien de patiënt (delen van) zijn dossier bij de zorgverlener heeft laten afschermen.

Behoudens het tonen van dit waarschuwingsscherm heeft SPITZ-MH geen maatregelen getroffen om te voorkomen dat een aangesloten zorgverlener via het RSP gegevens inziet van een patiënt die op dat moment niet bij hem in behandeling is.

Logging

Op grond van artikel 13 Wbp dient SPITZ-MH passende technische en organisatorische maatregelen ten uitvoer te leggen om persoonsgegevens te beveiligen tegen enige vorm van onrechtmatige verwerking.

Eén van de in dit geval benodigde maatregelen is logging van de raadplegingen van de patiëntgegevens. De logging dient op zodanige wijze plaats te vinden, dat op elk willekeurig moment met terugwerkende kracht kan worden nagegaan welke persoon toegang heeft gehad tot de gegevens van een patiënt. Daarnaast dient de logging regelmatig te worden gecontroleerd op onbevoegde raadplegingen.

In het onderzoek is aannemelijk geworden dat alle raadplegingen door SPITZ-MH worden gelogd. De logs worden iedere week door de projectleider bekeken.

Daarnaast worden de logs doorgestuurd naar de zorgverlener wiens patiëntgegevens zijn opgevraagd. Of de logs daadwerkelijk zichtbaar worden voor de zorgverlener is echter afhankelijk van de door hem gebruikte software.

De logging is niet specifiek gericht op verdachte situaties, waardoor de logging niet effectief kan worden gebruikt voor structurele controle op rechtmatige toegang tot patiëntendossiers.

Er zijn evenmin duidelijke afspraken gemaakt tussen SPITZ-MH en de zorgverleners omtrent structurele en incidentele controle van de logging.

Informatieplicht

SPITZ-MH verwerkt in het kader van gegevensuitwisseling tussen zorgverleners in haar regio persoonsgegevens vanaf het moment dat een zorgverlener persoonsgegevens van zijn patiënten laat opnemen in het RSP. Deelnemende zorgaanbieders hebben via het RSP de mogelijkheid om medische persoonsgegevens van de betrokken patiënten op te vragen uit de systemen van aangesloten zorgaanbieders.

Op grond van artikel 34 Wbp dient SPITZ-MH de patiënt te informeren over de hem betreffende gegevensverwerking door SPITZ-MH, tenzij de patiënt hiervan reeds op de hoogte is. Uit het onderzoek blijkt dat SPITZ-MH bij het opnemen van de persoonsgegevens in het RSP niet vaststelt of patiënten hiervan reeds op de hoogte zijn.

SPITZ-MH dient de patiënt te informeren uiterlijk op het moment dat diens persoonsgegevens worden opgenomen in het RSP (artikel 34 lid 1 sub a Wbp). Uitgangspunt is dat een verantwoordelijke de informatie zodanig moet verstrekken dat de betrokkene daarover daadwerkelijk beschikt. SPITZ-MH dient patiënten wiens persoonsgegevens hij verwerkt derhalve persoonlijk te informeren opdat de patiënt daadwerkelijk beschikt over de informatie.

SPITZ-MH informeert patiënten echter uitsluitend via huis-aan-huisbladen, folders en posters in openbare ruimten, apotheken en huisartspraktijken en via haar website www.spitz-mh.nl.