COLLEGE BESCHERMING PERSOONSGEGEVENS

POSTADRES Postbus 93374, 2509 AJ Den Haag BEZOEKADRES Juliana van Stolberglaan 4-10

TEL 070 - 88 88 500 FAX 070 - 88 88 501 INTERNET www.cbpweb.nl www.mijnprivacy.nl

Ruwaard van Putten Ziekenhuis

Onderzoek naar toegangsbeveiliging van medische gegevens

z2012-00179

Rapportage van definitieve bevindingen

DATUM 31 augustus 2012

Inhoud

INLEIDING

Achtergrond

In 2007 heeft de Inspectie voor de Gezondheidszorg (IGZ) in samenwerking met het CBP onderzoek gedaan naar de informatiebeveiliging in ziekenhuizen.[1] Gelet op de uitkomsten van dat onderzoek heeft de IGZ in vervolg daarop alle Nederlandse ziekenhuizen verzocht om in 2010 een verslag in te dienen van een onafhankelijk uitgevoerde beoordeling van de informatiebeveiliging in de betreffende instellingen.

Op 25 maart 2011 heeft de IGZ een dergelijk verslag ontvangen van de Raad van Bestuur van het Ruwaard van Putten Ziekenhuis (verder: RPZ). Naar aanleiding daarvan heeft de IGZ bij brief d.d. 4 april 2011 aangegeven te verwachten dat het RPZ een plan van aanpak zou opstellen en binnen een half jaar een heraudit zou laten uitvoeren dat blijk gaf van een voldoende niveau van informatiebeveiliging.

Op 26 januari 2012 is de definitieve rapportage 'NEN 7510 heraudit Ruwaard van Putten Ziekenhuis op basis van het NVZ-toetsingsreglement' zoals opgesteld door een extern auditbureau d.d. 13 januari 2012 (verder: de auditrapportage) aangeboden aan de IGZ. Uit de auditrapportage blijkt onder meer dat ten aanzien van maatregelen die getroffen dienen te worden op het vlak van 'identificatie, authenticatie en autorisatie' (nog steeds) sprake is van tekortkomingen.

Aanleiding voor het onderzoek

Het CBP heeft diverse signalen ontvangen over het bestaan van te ruime interne toegang voor medewerkers tot gedigitaliseerde patiëntendossiers binnen zorginstellingen. Het betreft de situatie dat medewerkers toegang hebben tot meer medische gegevens dan zij gelet op hun functie nodig zouden hebben. Daarnaast is het CBP op 9 februari 2012 door de IGZ in kennis gesteld van de auditrapportage betreffende RPZ.[2] Deze omstandigheden tezamen zijn voor het CBP aanleiding geweest onderzoek te doen naar de naleving van de wettelijke vereisten ter zake van beveiliging die gelden bij de verwerking van medische gegevens door het RPZ.

Doel en reikwijdte van het onderzoek

In het RPZ worden persoonsgegevens van patiënten elektronisch verwerkt in elektronische patiëntendossiers. Het onderzoek beoogt vast te stellen of de verantwoordelijke voor die gegevensverwerking in de zin van de Wet bescherming persoonsgegevens (Wbp), zijnde de Stichting RPZ[3], passende technische en organisatorische maatregelen heeft getroffen om deze persoonsgegevens te beveiligen.

---

[1] *Informatiebeveiliging in ziekenhuizen voldoet niet aan de norm* Rapportage van een onderzoek in 2007 door het College bescherming persoonsgegevens en de Inspectie voor de Gezondheidszorg naar de informatiebeveiliging in 20 ziekenhuizen. Den Haag, november 2008.

[2] Ingevolge paragraaf VII van het Samenwerkingsprotocol CBP-IGZ. De raad van Bestuur van het RPZ is hiervan bij brief d.d. 20 april 2012 door de IGZ op de hoogte gesteld.

[3] Uit de statuten van de Stichting Ruwaard van Putten Ziekenhuis, getiteld Statutenwijziging en opgemaakt d.d. 8 juni 2007, blijkt dat de Stichting ten doel heeft de bevordering van de gezondheidszorg in verschillende daarin genoemde gemeenten en dat de Stichting dit doel tracht te bereiken door het beheer en de exploitatie van een algemeen ziekenhuis met bijbehorende voorzieningen in Spijkenisse (artikelen 1 en 2). Uit artikel 4 volgt dat de Stichting wordt bestuurd door een Raad van Bestuur, onder toezicht van een Raad van Toezicht.

Het onderzoek is beperkt tot de maatregelen die betrekking hebben op het voorkomen van onrechtmatige toegang door medewerkers van het RPZ, zowel door artsen/hulpverleners als door medewerkers met een functie in het beheer van de instelling.

Onderzoeksvraag

Onderzocht wordt of de verantwoordelijke passende technische en organisatorische maatregelen ten uitvoer heeft gelegd teneinde persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking, zoals bedoeld in artikel 13 Wet bescherming persoonsgegevens (Wbp). Het onderzoek richt zich in dit kader op de wijze waarop binnen de zorginstelling de toegangsmogelijkheden tot het gedigitaliseerde patiëntendossier voor de diverse medewerkers worden beheerd, in technische en organisatorische zin.

Werkwijze

In de auditrapportage heeft het externe auditbureau aangegeven dat zowel de audit als de heraudit zijn uitgevoerd in lijn met de reikwijdte zoals omschreven in het NVZ-toetsingsreglement.[4] Het externe auditbureau heeft ten aanzien van de toetselementen het zogenoemde volwassenheidsniveau bepaald op basis van de volwassenheidsniveaus die in het NVZ-toetsingsreglement zijn opgenomen. Dit betreft de niveaus 1 tot en met 4.

Nadat het daarvan door de IGZ in kennis is gesteld, heeft het CBP de auditrapportage bestudeerd. Het CBP heeft kennis genomen van de bevindingen die daarin zijn opgenomen en deze beoordeeld. Op grond hiervan is de rapportage van voorlopige bevindingen opgesteld[5]. De Raad van Bestuur van de Stichting RPZ is bij brief van 24 mei 2012 door het CBP ingelicht over de gehanteerde werkwijze.

Bij brief van 4 juli 2012 heeft de Stichting RPZ haar zienswijze kenbaar gemaakt. Hierin zijn de bevindingen die opgenomen zijn in de auditrapportage niet betwist. Wel is aangegeven dat deze rapportage heeft geleid tot een verbetertraject. Naar aanleiding hiervan heeft het CBP op 12 juli 2012 per e-mail nadere vragen gesteld. Op 25 juli 2012 heeft het CBP hierop -eveneens per e-mail- de antwoorden en een bijbehorende bijlage ontvangen.

De zienswijze en aanvullende antwoorden van de Stichting RPZ hebben geleid tot aanvulling van de feiten en de beoordeling zoals weergegeven in de voorlopige bevindingen. Dit leidt echter niet tot een gewijzigde conclusie ten opzichte van de voorlopige bevindingen.

Gelet op het voorgaande worden de bevindingen van het CBP hiermee definitief vastgesteld.

---

[4] Auditrapportage pagina 4 van 30.

[5] Waar in de auditrapportage is uitgegaan van NEN 7510:2004, heeft het CBP gebruik gemaakt van NEN 7510:2011. Gelet op de aard en inhoud van de daarin aangebrachte wijzigingen in het licht van de beoordeling van de feiten en omstandigheden binnen het kader van artikel 13 Wbp, zag het CBP geen aanleiding de verouderde versie te gebruiken. Dat dit niet in het nadeel bleek te zijn van het RPZ droeg daar in grote mate aan bij.

BEVINDINGEN

Juridisch kader

Ingevolge artikel 1 onder d Wbp is de verantwoordelijke de natuurlijke persoon, rechtspersoon of ieder ander die, alleen of tezamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt.

Een persoonsgegeven is elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon. Medische persoonsgegevens zijn bijzondere persoonsgegevens in de zin van artikel 16 Wbp. De verwerking daarvan is verboden tenzij -onder andere- deze ingevolge artikel 21, eerste lid onder a Wbp geschiedt door hulpverleners, instellingen of voorzieningen voor gezondheidszorg voor zover dat met het oog op een goede behandeling of verzorging van de betrokkene, dan wel het beheer van de betreffende instelling of beroepspraktijk noodzakelijk is.

Artikel 9, vierde lid Wbp beperkt vervolgens de rechtmatige verwerking van medische persoonsgegevens in die zin dat de verwerking daarvan, waaronder het raadplegen van die gegevens, achterwege blijft voor zover een geheimhoudingsplicht uit hoofde van ambt, beroep of wettelijk voorschrift daaraan in de weg staat. In artikel 7:457 eerste lid Burgerlijk Wetboek (BW; Wet op de Geneeskundige Behandelings-Overeenkomst) is - voor zover hier relevant - opgenomen dat de hulpverlener zorg draagt dat aan anderen dan de patiënt geen inlichtingen over de patiënt dan wel inzage in of afschrift van het medisch dossier wordt verstrekt dan met toestemming van de patiënt of indien het bij of krachtens de wet bepaalde daartoe verplicht. Ingevolge lid 2 van dit artikel zijn onder anderen dan de patiënt niet begrepen degenen die rechtstreeks betrokken zijn bij de uitvoering van de behandelingsovereenkomst en degene die optreedt als vervanger van de hulpverlener, voor zover de verstrekking noodzakelijk is voor de door hen in dat kader te verrichten werkzaamheden.

Het verlenen van toegang tot medische persoonsgegevens in elektronische patiëntendossiers is zodoende slechts toegestaan voor zover het gaat om medewerkers die rechtstreeks betrokken zijn bij de behandeling of verzorging van betrokkene, dan wel bij het beheer van de betreffende instelling, en in beide gevallen alleen voor zover dat noodzakelijk is voor hun werkzaamheden.

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

Ter voorkoming van onrechtmatige verwerking van persoonsgegevens door medewerkers in de instelling dient de verantwoordelijke de toegang tot de elektronische patiëntendossiers afdoende te beveiligen door het treffen van passende maatregelen ter beheersing van die toegang. Door passende organisatorische en technische maatregelen te treffen moet de toegang tot de medische persoonsgegevens

zodanig worden ingericht dat uitsluitend de bevoegde medewerkers toegang wordt verleend.

Bij de toetsing van de beveiligingsmaatregelen aan artikel 13 Wbp is de NEN 7510[6] referentiekader. De NEN-norm is een gezaghebbende sectorale uitwerking van artikel 13 Wbp: als een zorginstelling in de NEN-norm aangegeven maatregelen heeft getroffen, mag ervan uit worden gegaan dat het ook voldoet aan voornoemde wettelijke bepaling. Andersom is dit overigens geen volstrekt automatisme: een zorginstelling kan ook op andere wijze aantonen dat de beveiliging in orde is, bijvoorbeeld door te voldoen aan de Code voor Informatiebeveiliging (ISO 17799).

In hoofdstuk 11 van de NEN-norm 7510[7] wordt ter zake van toegangsbeveiliging in algemene zin aangegeven: "Toegangsbeveiliging moet ervoor zorgen dat toegang tot voorzieningen en gegevens wordt verleend aan gebruikers die daartoe zijn gerechtigd en wordt geweigerd aan anderen." Meer specifiek (artikel 11.1.1 Toegangsbeleid) wordt bepaald dat: "(…) toegangsbeleid [behoort] te worden vastgesteld, gedocumenteerd en beoordeeld op basis van bedrijfseisen en beveiligingseisen voor toegang." En: "Leg in een beleidsverklaring voor toegangsbeveiliging voor elke gebruiker of gebruikersgroep duidelijke regels en rechten vast; Baseer het toegangsbeleid op vooraf gedefinieerde rollen met gerelateerde rechten die nodig zijn voor de rol en niet verder strekken. Zorg ervoor dat goedkeuringen in zorgprocessen, waar dat nodig is, worden gekoppeld aan verschillende rollen en afgedwongen door applicatiefuncties in het informatiesysteem; In het algemeen geldt dat gebruikers van zorginformatiesystemen alleen toegang mogen krijgen tot patiëntgegevens indien er een behandelrelatie bestaat tussen de gebruiker en de patiënt, op het moment dat de gebruiker een zorgactiviteit uitvoert ten behoeve van die patiënt en indien er ook noodzaak is voor bedoelde gegevens om deze activiteit te ondersteunen. "
Daarnaast is in artikel 11.2.1. (Registratie van gebruikers) vastgelegd dat er formele procedures voor het registeren en afmelden van gebruikers behoren te zijn vastgesteld, voor het verlenen en intrekken van toegangsrechten tot alle informatiesystemen en –diensten.

Feitelijke bevindingen

De Stichting RPZ houdt zich bezig met het beheer en de exploitatie van het RPZ. De Stichting wordt bestuurd door de Raad van Bestuur. Dit volgt uit de statuten van de Stichting[8] en kan afgeleid worden uit het organogram van het RPZ d.d. mei 2012.[9] De auditrapportage van het externe auditbureau is bij brief van 26 januari 2012 door de Raad van Bestuur toegezonden aan de IGZ.

De audit is in maart 2011 uitgevoerd, terwijl de heraudit tussen 11 november en 22 december 2011 heeft plaatsgevonden. "Met de toetsingswerkzaamheden is zowel de opzet als het bestaan van de toetselementen getoetst. Dit wil zeggen dat zowel gecontroleerd is, voor zover van toepassing, of er documentatie is opgesteld waarin beschreven is op welke wijze invulling wordt gegeven aan de norm, als de

[6] NEN 7510, Medische informatica – Informatiebeveiliging in de zorg, oktober 2011.
[7] Zie noot 2.
[8] Zie noot 3.
[9] http://www.rpz.nl/media//organogram-per-afdeling-mei-20122.pdf.

daadwerkelijke implementatie van de beschrijving. De werking van de maatregelen over een bepaalde periode valt buiten de reikwijdte van de heraudit."[10]
In de auditrapportage zijn op basis van de NEN-ID met bijbehorende NEN-normtekst en de bevindingen zoals die in maart 2011 en november 2011 zijn vastgesteld, scores toegekend aan de individuele toetselementen per cluster.[11] Wanneer op een toetselement een NVZ-score van 1 is toegekend, betekent dit dat het toetselement weinig of geen aandacht krijgt of dat er uitsluitend plannen zijn om met het normelement aan de slag te gaan.

Het CBP heeft kennisgenomen van de bevindingen voor het cluster "Identificatie, authenticatie en autorisatie". Voor zover binnen dit cluster de NVZ-score 1 is toegekend, betreft het de volgende "belangrijkste bevindingen"[12] (gestoeld op de in de auditrapportage opgenomen "detailbevindingen"[13]):

- Er zijn geen autorisatiematrices voor de informatiesystemen waarmee medische gegevens worden verwerkt. Verder worden autorisaties niet periodiek gecontroleerd op juistheid en volledigheid.
- Er bestaan geen centrale processen voor de toekenning en intrekking van autorisaties.
- Er zijn geen procedures vastgesteld voor het registreren en afmelden van gebruikers.

In haar zienswijze en aanvullend toegestuurde informatie heeft de Stichting RPZ de auditrapportage van het externe auditbureau niet betwist, maar aangegeven dat naar aanleiding daarvan een aanvang is genomen met een verbetertraject. Een stuurgroep heeft in dit kader de opdracht gekregen zo snel als mogelijk het RPZ voldoende te laten scoren daar waar dat nu nog niet het geval is.

Er zal volgens de Stichting RPZ alsnog worden voorzien in het koppelen van de autorisaties aan functies en aan de daarbij behorende bevoegdheden (inzien, vastleggen, muteren). In het personeelssysteem zal iedere medewerker worden gekoppeld aan een functie. De afdeling ICT zal per systeem(deel) het bestand met bevoegdheden dat gekoppeld is aan de verschillende functies en daarmee aan de medewerkers gaan beheren. Dit beleid zal volgens RPZ in 2012 gerealiseerd zijn en zal vervolgens jaarlijks gecontroleerd worden op juistheid. Volgens het toegestuurde tijdspad voor implementatie van de autorisaties en bevoegdheden van alle medewerkers[14] is voltooiing voorzien in week 39, dat wil zeggen de laatste week van september 2012[15].

Daarnaast is in het (vernieuwde) personeelssysteem voorzien in het registreren en afmelden van alle gebruikers binnen het ziekenhuis en daarmee ook van de informatievoorziening van het RPZ, aldus de zienswijze van RPZ. Het proces voor af- en aanmelden van gebruikers zal worden gevat in een workflow in het

[10] Auditrapportage pagina 5 van 30.
[11] Auditrapportage pagina's 8 tot en met 25 van 30.
[12] Auditrapportage pagina 7 van 30.
[13] Auditrapportage pagina's 22 tot en met 25 van 30.
[14] Tijdspad implementatie CBP, opgesteld door de kwaliteitsfunctionaris, datum onbekend.
[15] Het CBP begrijpt week 39 van 2012.

personeelssysteem. Het project voor het opleveren van de benodigde workflows is reeds gestart en zal in de tweede helft van 2012 gereed zijn.
Momenteel wordt het aan- en afmelden van gebruikers via een maandelijkse lijst 'uit- en in dienst' vanuit de afdeling P&O naar ICT gecommuniceerd, de afdeling ICT verwerkt deze uit- en indiensttredingen vervolgens in de diverse systemen.

Beoordeling

Het CBP stelt vast, mede gelet op het aangegeven tijdspad, dat de maatregelen die door de Stichting RPZ in het kader van het verbetertraject zijn voorzien ten tijde van het opstellen van de onderhavige rapportage van definitieve bevindingen (nog) niet zijn gerealiseerd. Dit betekent dat maatregelen voor toegangsbeleid zoals voorgeschreven in NEN 7510 vooralsnog ontbreken. Het RPZ beschikt nog niet over geïmplementeerd autorisatiebeleid gebaseerd op vooraf gedefinieerde rollen met gerelateerde rechten nu een autorisatiematrix en centrale processen voor de toekenning en intrekking van autorisaties nog niet in werking zijn. Bovendien ontbreekt tot op heden een geformaliseerde en geïmplementeerde gebruikersregistratie ten behoeve van het registeren en afmelden van gebruikers en het verlenen en intrekken van toegangsrechten tot alle informatiesystemen en –diensten; het aan- en afmelden van gebruikers via een maandelijkse lijst 'uit- en indienst' vanuit de afdeling P&O naar ICT voldoet hier niet aan.

Uit het bovenstaande vloeit voort dat de Stichting RPZ niet voorziet in de in NEN 7510 op dit punt voorgeschreven maatregelen. Dit betekent dat niet is zeker gesteld dat in het RPZ toegang tot medische persoonsgegevens uitsluitend mogelijk is voor medewerkers die daartoe gerechtigd zijn, dat wil zeggen die betrokken zijn bij de behandeling van de betreffende patiënt en voor wie kennisname van de gegevens noodzakelijk is en/of voor wie het gelet op zijn functie in het beheer van de instelling noodzakelijk is om toegang tot (bepaalde) gegevens te verkrijgen.

Nu de NEN 7510 als gezaghebbende sectorale invulling van hetgeen op het gebied van informatiebeveiliging voor zorginstellingen moet worden beschouwd als 'passende technische en organisatorische maatregelen', het RPZ niet aan NEN 7510 voldoet en vooralsnog uit de verkregen informatie niet is gebleken dat de verantwoordelijke op andere wijze technische en organisatorische maatregelen heeft getroffen teneinde de gegevens te beveiligen tegen verlies of enige vorm van onrechtmatige verwerking van te voorkomen, voldoet de verantwoordelijke niet aan artikel 13 Wbp. Aannemelijk is dat de Stichting RPZ het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt, zodat zij als de verantwoordelijke voor de verwerking van medische persoonsgegevens binnen het RPZ dient te worden aangemerkt.

Conclusie: De Stichting RPZ handelt in strijd met artikel 13 Wbp nu zij tekortschiet in het treffen van passende organisatorische en technische beveiligingsmaatregelen om medische persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking.

CONCLUSIE

Verwerking van medische persoonsgegevens in het elektronische patiëntendossier, daaronder begrepen de toegang daartoe, is slechts toegestaan door medewerkers die rechtstreeks betrokken zijn bij de behandeling of verzorging van betrokkene, dan wel bij het beheer van de betreffende instelling, en in beide gevallen alleen voor zover dat noodzakelijk is voor hun werkzaamheden. Ter voorkoming van onrechtmatige verwerking van persoonsgegevens door medewerkers in de instelling dient de verantwoordelijke derhalve de toegang voor medewerkers tot elektronische patiëntendossiers zodanig in te richten dat uitsluitend de medewerkers die direct betrokken zijn bij de behandeling of verzorging van de patiënt toegang tot diens elektronisch patiëntendossier kunnen krijgen. Voor andere medewerkers zou dit slechts mogelijk moeten zijn indien en voor zover dat gelet op hun functie in het beheer van de instelling noodzakelijk is te achten.

In de auditrapportage opgesteld door het externe auditbureau zijn bevindingen vastgelegd waaruit blijkt dat in het RPZ niet is zeker gesteld dat toegang tot medische persoonsgegevens uitsluitend mogelijk is voor medewerkers die betrokken zijn bij de behandeling van de betreffende patiënt en voor wie kennisname van de gegevens noodzakelijk is en/of voor wie het gelet op hun functie in het beheer van de instelling noodzakelijk is om toegang tot (bepaalde) gegevens te verkrijgen. Dit vloeit voort uit het ontbreken van (geïmplementeerde) maatregelen voor toegangsbeleid zoals voorgeschreven in NEN 7510, waaronder autorisatiebeleid en –procedures en een geformaliseerde gebruikersregistratie. Dat het RPZ naar aanleiding van de auditrapportage een aanvang heeft gemaakt met een verbetertraject om deze situatie op te heffen doet, mede in het licht van het geschetste tijdspad ten behoeve van de uitvoering van de maatregelen, vooralsnog niet af aan deze omstandigheid.

De NEN 7510 geldt als gezaghebbende sectorale invulling van hetgeen op het gebied van informatiebeveiliging voor zorginstellingen moet worden beschouwd als passende technische en organisatorische maatregelen teneinde onrechtmatige verwerking te voorkomen. Nu het RPZ deze maatregelen niet heeft getroffen en vooralsnog uit de verkregen informatie niet is gebleken dat op andere wijze technische en organisatorische maatregelen zijn getroffen teneinde de gegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking, voldoet het RPZ niet aan artikel 13 Wbp. De Stichting RPZ is hiervoor de verantwoordelijke in de zin van de Wbp.