COLLEGE BESCHERMING PERSOONSGEGEVENS

Toegang tot digitale patiëntendossiers binnen zorginstellingen

ONDERZOEKSRAPPORT JUNI 2013

COLLEGE BESCHERMING PERSOONSGEGEVENS

Toegang tot digitale patiëntendossiers binnen zorginstellingen

ONDERZOEKSRAPPORT | JUNI 2013

Inleiding

Voor een effectieve en efficiënte hulpverlening werken zorginstellingen met digitale patiëntendossiers. Als het gebruik ervan goed en zorgvuldig is, hebben dergelijke dossiers grote voordelen. Informatie over de patiënt is beter toegankelijk voor zorgverleners. Gegevens kunnen dag en nacht worden opgevraagd en zijn snel beschikbaar. Hierdoor kunnen fouten worden voorkomen, hoeven niet telkens dezelfde gegevens te worden ingevoerd en kunnen zorgverleners ook in geval van nood snel over gegevens beschikken. De kwaliteit van zorg kan aanzienlijk toenemen en er zijn kostenbesparingen mogelijk.

Tegelijkertijd kunnen door de digitalisering van patiëntendossiers privacygevoelige gegevens gemakkelijker onder ogen komen van mensen die daar niets mee te maken hebben. Wettelijk is vereist dat medische gegevens over patiënten alléén toegankelijk zijn voor zorgverleners die rechtstreeks bij de behandeling van die patiënten betrokken zijn. Dat dit in de praktijk niet altijd het geval is, blijkt uit eerdere onderzoeken[1] en uit signalen die het CBP hierover in 2011 en 2012 ontving. Een student liet bijvoorbeeld weten niet geconfronteerd te willen worden met een medestudent die parttime werkend op de administratie van een ggz-instelling in zijn ggz-dossier kan kijken; een doktersassistent gaf aan niet te willen dat collega's op een andere huisartsenpost in zijn behandeldossier kunnen kijken; een buurman wilde niet dat de buurvrouw die als secretaresse in een ggz-instelling werkt, zijn dossier kan inzien om te controleren of hij daadwerkelijk in behandeling is.

Het bestuur van een zorginstelling heeft de wettelijke verantwoordelijkheid ervoor te zorgen dat medewerkers in de betreffende instelling zorgvuldig omgaan met de medische gegevens die patiënten aan hun hulpverleners toevertrouwen. Mensen moeten daarop kunnen vertrouwen. De patiënt moet kunnen rekenen op én een goede medische behandeling én een zorgvuldige omgang met zíjn vertrouwelijke gegevens. Van het bestuur van een zorginstelling mag worden verwacht dat het zijn medewerkers bewust maakt van de privacyrisico's die een onzorgvuldige omgang met patiëntgegevens met zich meebrengt. Voorkomen moet worden dat onbevoegde medewerkers medische gegevens van grote groepen mensen inzien doordat zorgaanbieders hun autorisatiebeleid niet op orde hebben. Het is niet voor niets dat in de Wet bescherming persoonsgegevens (Wbp) medische gegevens onder de categorie 'bijzondere gegevens' vallen, waarvoor strengere wettelijke eisen gelden. Het CBP heeft de zorgvuldige omgang met medische gegevens dan ook hoog op de toezichtagenda staan.

AANLEIDING, VRAAGSTELLING EN DOEL

In 2011 en 2012 ontving het CBP signalen over een – naar de indruk van de signaalgevers – te ruime toegang van medewerkers van zorginstellingen tot gedigitaliseerde patiëntendossiers. Die signalen betreffen zowel de toegang tot patiëntgegevens door medewerkers met een functie in de administratief-ondersteunende sfeer als de toegang door zorgverleners (artsen, verpleegkundigen).

Het CBP zag in deze signalen aanleiding een onderzoek te starten bij zorginstellingen naar de manier waarop zij de toegang van medewerkers tot digitale patiëntendossiers hebben geregeld en of op dit punt de beveiliging van persoonsgegevens in de zorgsector op het door de Wbp vereiste 'passende niveau' is. Het onderhavige onderzoek is specifiek gericht op de vraag of de verantwoordelijken voor de zorginstelling (het bestuur) de toegang tot gedigitaliseerde patiëntendossiers zodanig hebben ingericht dat medewerkers in zorginstellingen alleen dán toegang krijgen tot patiëntgegevens als zij een behandelrelatie met de betreffende patiënt hebben of als de toegang voor de beheersmatige afwikkeling van de behandeling noodzakelijk is. Daarnaast is het onderzoek gericht op de vraag of wordt bijgehouden wie wanneer een dossier raadpleegt (logging) en of dit wordt gecontroleerd. Met deze logging en de controle daarop kan onbevoegde toegang tot medische gegevens worden opgespoord en kan het bestuur van de zorginstelling actie ondernemen.

Met dit onderzoek heeft het CBP de praktijk op het gebied van toegang van medewerkers tot digitale patiëntendossiers in beeld gebracht en inzicht verkregen in de keuzen die de besturen van zorginstellingen hierbij maken. Door toetsing van de bevindingen aan de wettelijke vereisten wordt vervolgens inzichtelijk gemaakt in hoeverre zorginstellingen voldoen aan die vereisten en op welke punten verbetering van de praktijk noodzakelijk is. Het bestuur van de betreffende instelling heeft de verplichting dergelijke verbeteringen aan te brengen.

WERKWIJZE

In het eerste en tweede kwartaal van 2012 heeft het CBP schriftelijke verzoeken om inlichtingen gedaan aan in het onderzoek betrokken zorginstellingen. Hierbij is verzocht om inlichtingen over de getroffen maatregelen in technische en organisatorische zin met betrekking tot de toegang van medewerkers tot digitale patiëntendossiers. Het doel hiervan was te beoordelen of de wijze waarop die toegang is vormgegeven, voldoet aan het vereiste van artikel 13 Wbp.

Uit de verkregen informatie is het beeld ontstaan dat binnen de onderzochte zorginstellingen niet in overeenstemming met artikel 13 Wbp wordt gehandeld als het gaat om autorisatiebeleid. Dit is in juli 2012 aan in het onderzoek betrokken zorginstellingen medegedeeld. Om meer inzicht in de keuzen van de zorginstellingen te krijgen en tot een goede beoordeling te komen, heeft het CBP vervolgens in gesprekken nadere informatie gevraagd. Deze gesprekken met zorginstellingen zijn gevoerd in de periode september-oktober 2012. Naar aanleiding hiervan heeft het CBP de betreffende zorginstellingen de gelegenheid geboden om maatregelen te nemen en verbetertrajecten in gang te zetten. In de periode november 2012-januari 2013 hebben de zorginstellingen daarover nadere informatie aan het CBP verstrekt.

BEELD OVER DE ZORGSECTOR

Het onderzoek strekte zich uit tot negen zorginstellingen, waaronder algemene ziekenhuizen, ggz-instellingen en huisartsenposten. Deze instellingen behandelen gezamenlijk ruim een miljoen patiënten per jaar. Uit het onderzoek blijkt dat in geen van de onderzochte zorginstellingen het bestuur de toegang tot gedigitaliseerde patiëntendossiers zodanig heeft ingericht dat medewerkers in zorginstellingen alleen dán toegang kunnen krijgen tot patiëntgegevens indien zij een behandelrelatie met de betreffende patiënt hebben of als toegang voor de beheersmatige afwikkeling van de behandeling noodzakelijk is. Geen van de onderzochte instellingen voldoet dus

[1] IGZ, *ICT in ziekenhuizen - Beveiliging van informatie nog onvoldoende voor een betrouwbare papierloze patiëntenzorg*, Den Haag, 2004; CBP en IGZ, *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 informatiebeveiliging in 20 ziekenhuizen*, Den Haag, november 2008.

aan hetgeen wettelijk vereist is. De onderzochte zorginstellingen laten op een aantal belangrijke punten echter ook aanzienlijke verschillen zien. Zo acht het bestuur in sommige zorginstellingen privacybescherming ondergeschikt aan verantwoorde patiëntenzorg. In andere zorginstellingen heeft het bestuur de verantwoordelijkheid voor het realiseren van een adequate bescherming van patiëntgegevens wél genomen en vertaald in maatregelen, zonder dat dit ten koste gaat van de patiëntveiligheid. Deze maatregelen zijn echter nog niet voldoende om aan de wet te voldoen. Andere verschillen tussen de instellingen hebben te maken met de gebruikte technologie. In een aantal zorginstellingen is sprake van gebruik van verouderde technologie waarmee niet aan de wettelijke vereisten kán worden voldaan. Andere instellingen hebben modernere technologie, maar maken hier niet optimaal gebruik van.

Het CBP heeft aanleiding om aan te nemen dat het beeld dat bij de onderzochte instellingen is aangetroffen, ook geldt voor andere zorginstellingen. Zo ontving het CBP ook in 2013 signalen over toegangsbeveiliging in – andere dan de onderzochte – zorginstellingen.

Met de publicatie van dit rapport wil het CBP ook bij de verantwoordelijken in andere zorginstellingen bereiken dat zij zich daadwerkelijk verantwoordelijk tonen voor het realiseren van adequate bescherming van patiëntgegevens en dat zij de daartoe benodigde maatregelen en voorzieningen treffen. De uitkomsten van het onderhavige onderzoek zijn een signaal voor de gehele zorgsector om te voldoen aan de wettelijke verantwoordelijkheid om zorgvuldig om te gaan met de gegevens van de aan de betreffende instelling toevertrouwde patiënten en daarbij te zorgen voor een passend beveiligingsniveau om onrechtmatige toegang van medewerkers te voorkomen.

VERVOLG

De in dit onderzoek betrokken zorginstellingen hebben aan het CBP informatie verstrekt over door hen opgestelde plannen en in gang gezette acties om de wijze van toegangsverlening voor medewerkers tot patiëntendossiers en de controle op die toegang te verbeteren. Het CBP heeft in reactie daarop aan de zorginstellingen kenbaar gemaakt dat aanvullende acties noodzakelijk zijn om te voldoen aan artikel 13 Wbp. Over de fasering van en de redelijke termijn waarbinnen realisatie van dergelijke – veelal complexe – aanpassingen in technologie en werkwijze mogelijk is, is het CBP in overleg met de betreffende zorginstellingen en de koepelorganisaties. Indien het CBP echter constateert dat zorginstellingen onvoldoende voortvarend werk maken van de verbeterpunten, zal het CBP bij die zorginstellingen handhavend optreden.

Het CBP beoogt dat ook de overige zorginstellingen in Nederland naar aanleiding van dit rapport beoordelen of zij de benodigde maatregelen hebben getroffen om ervoor te zorgen dat gegevens van patiënten in hun instelling goed beveiligd zijn en alleen toegankelijk zijn voor bevoegde medewerkers. Als dit niet het geval blijkt te zijn, dienen deze instellingen over te gaan tot het nemen van maatregelen.

Het CBP zal mogelijk op termijn ook bij andere dan de nu onderzochte zorginstellingen op dit punt inlichtingen inwinnen en daarover in voorkomende gevallen rapporteren en publiceren, zeker als over specifieke instellingen signalen zijn binnengekomen.

LEESWIJZER

Hoofdstuk 1 van dit rapport geeft de bevindingen van het onderzoek weer. In hoofdstuk 2 staat de beoordeling door het CBP van deze bevindingen. Ook gaat dit hoofdstuk in op de verschillende redenen die de zorginstellingen aanvoeren waarom zij, volgens hen, geen maatregelen hoeven te treffen om het risico op onrechtmatige verwerking door medewerkers verder terug te brengen. Hoofdstuk 3 geeft de conclusies weer. De bijlage bevat het normenkader dat binnen dit onderzoek van belang is. Delen van dit normenkader zijn tevens in hoofdstuk 2 opgenomen.

In 2007 deed het CBP samen met de Inspectie voor de Gezondheidszorg (IGZ) onderzoek naar informatiebeveiliging in twintig ziekenhuizen en naar de daarop genomen vervolgacties van de IGZ. In het in november 2008 door CBP en IGZ gezamenlijk uitgebrachte rapport[2] werd geconcludeerd dat ziekenhuizen voor het merendeel onvoldoende maatregelen nemen om de beveiliging van hun informatieverwerking op een voldoende niveau te krijgen en dat de meeste ziekenhuizen nog niet aan de NEN 7510-norm voldoen. Het onderhavige onderzoek van het CBP bij een aantal zorginstellingen kijkt specifieker naar het punt van de beheersing van toegang voor medewerkers tot patiëntendossiers en naar de vraag welke maatregelen ter zake in zorginstellingen daadwerkelijk zijn geïmplementeerd.

[2] CBP en IGZ, *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 informatiebeveiliging in 20 ziekenhuizen*, Den Haag, november 2008.

1 Bevindingen

De bevindingen uit dit onderzoek naar toegangsbeveiliging van medische gegevens binnen de zorgsector vallen uiteen in twee onderwerpen:

- De wijze van autoriseren: hoe bepaalt de verantwoordelijke wie wanneer toegang tot welke patiëntendossiers krijgt?
- Logging en controle: houdt de verantwoordelijke bij wie wanneer een dossier raadpleegt en wordt dit gecontroleerd?

VERANTWOORDELIJKE

In zorginstellingen worden het doel en de middelen voor de verwerking van persoonsgegevens bepaald door de raad van bestuur. De raad van bestuur is daarmee de verantwoordelijke in de zin van de Wet bescherming persoonsgegevens (Wbp). De raad van bestuur van de zorginstelling is derhalve gehouden tot naleving van de in de Wbp aan de verantwoordelijke opgelegde verplichtingen.

De verplichting om te voldoen aan het bepaalde in artikel 7:457 eerste en tweede lid Burgerlijk Wetboek (BW) rust eveneens[3] op de raad van bestuur van de zorginstelling, als contractspartij bij de geneeskundige behandelingsovereenkomst met de patiënt.

1.1 Wijze van autoriseren

Uit de wet vloeit voort dat zorginstellingen alleen toegang tot patiëntgegevens mogen verlenen aan zorgmedewerkers als deze rechtstreeks betrokken zijn bij de behandeling van de patiënt en dat overige medewerkers slechts toegang mogen krijgen voor zover dat voor hun functie in het beheer noodzakelijk is. In zorginstellingen zijn derhalve procedures nodig aan de hand waarvan wordt bepaald welke medewerkers onder welke omstandigheden toegang krijgen tot bepaalde patiëntgegevens. Naast procedures om te bepalen wie al dan niet bevoegd is tot toegang, zijn er technische voorzieningen nodig om toegang door bevoegde medewerkers mogelijk te maken en toegang door onbevoegde medewerkers te voorkomen.

Het CBP constateert dat alle in het onderzoek betrokken instellingen onderkennen dat op grond van de wet is vereist dat medewerkers in zorginstellingen alleen dán toegang mogen hebben tot patiëntgegevens indien zij een behandelrelatie met de betreffende patiënt hebben of als toegang voor de beheersmatige afwikkeling van de behandeling noodzakelijk is.

Het CBP constateert dat zorginstellingen verschillende criteria hanteren om te bepalen of medewerkers worden geautoriseerd voor toegang tot gedigitaliseerde patiëntdossiers. De diverse wijzen van autoriseren zoals aangetroffen in de onderzochte zorginstellingen laten zich op hoofdlijnen als volgt beschrijven:

[3] Zie normenkader in bijlage.

- Variant I: autorisatie gebeurt op basis van de *functie* die medewerkers vervullen.
- Variant II: autorisatie gebeurt niet alleen op basis van de functie die medewerkers vervullen, maar ook op basis van de *werkcontext* waarin medewerkers die functie vervullen.
- Variant III: autorisatie gebeurt nadat is *vastgesteld dat er rechtstreekse betrokkenheid* bij de behandeling van een patiënt is.

Het CBP stelt hierbij vast dat alleen bij variant III wordt voldaan aan hetgeen op grond van de wet is vereist. Het CBP constateert echter dat deze wijze van autoriseren nauwelijks voorkomt: deze is slechts bij één van de onderzochte zorginstellingen aangetroffen en dan nog maar alleen op een aantal afdelingen.

1.1.1 Variant I: autorisatie op basis van functie

Een aantal van de onderzochte zorginstellingen maakt voor autorisatie onderscheid naar de functie die medewerkers vervullen. Afhankelijk van de functie en/of de functiegroep waarin een functie is ingedeeld, wordt bepaald welke bevoegdheden iemand krijgt voor toegang tot patiëntgegevens. Hierbij kijkt de instelling naar de rol die medewerkers in een bepaalde functie vervullen in de behandeling van of zorgverlening aan patiënten of in het beheer van de instelling. De benodigde toegangsrechten worden gerelateerd aan wat redelijkerwijs noodzakelijk is voor een goede vervulling van die rol.

Hierbij wordt onderscheid gemaakt tussen medewerkers die zijn betrokken bij het beheer van de instelling en medewerkers die zijn betrokken zijn bij de zorgverlening aan of behandeling van patiënten.

MEDEWERKERS BETROKKEN BIJ BEHEER

Medewerkers die zijn betrokken bij het beheer van de onderzochte instellingen krijgen in het algemeen geen toegang tot medische persoonsgegevens, aangezien dat voor de vervulling van hun taken niet nodig is. Zij hebben vaak wel toegang tot algemenere gegevens van patiënten, voor zover dat noodzakelijk is voor hun taakuitoefening. Zo kunnen medewerkers van de zorgadministratie toegang hebben tot de algemene patiëntgegevens (zoals naam, adres, woonplaats) van alle patiënten en medewerkers van het opnamebureau tot afsprakenregistratiegegevens van alle patiënten.

Voor een beperkt aantal medewerkers belast met de financiële afhandeling van diagnosebehandelcombinaties (DBC's) is vaak wel voorzien in toegang tot medische persoonsgegevens. Zij hebben deze toegang nodig om in plaats van de behandelend artsen een aantal administratieve handelingen in de DBC-procedure te kunnen verrichten.

MEDEWERKERS BETROKKEN BIJ ZORGVERLENING/BEHANDELING

Ook bij de toekenning van toegangsrechten aan medewerkers die betrokken zijn bij de zorgverlening aan of behandeling van patiënten, wordt binnen de onderzochte instellingen nader onderscheid gemaakt op basis van functie of functiegroep. Daarbij krijgen artsen de ruimste bevoegdheden, waardoor zij toegang hebben tot alle gegevens van alle patiënten die in de instelling zijn opgenomen (geweest) en/of daar worden of werden behandeld. In de onderzochte ziekenhuizen geldt dit veelal wel met uitzondering van patiëntgegevens van de afdeling Psychiatrie. Ook kan soms een arts in het systeem de gegevens van een specifieke patiënt als vertrouwelijk aanmerken, waardoor deze gegevens uitsluitend voor leden van de eigen vakgroep zijn in te zien.

Voor andere medewerkers dan artsen wordt een beperking aangebracht in de aard en omvang van de bevoegdheden met betrekking tot (medische) gegevens. Vaak kunnen

deze medewerkers bijvoorbeeld die gegevens wel raadplegen maar niet wijzigen. Verpleegkundigen kunnen soms alleen gegevens registreren in het verpleegkundig dossier van patiënten die zijn opgenomen of worden verpleegd op de afdeling waar een verpleegkundige werkzaam is.

AFDWINGEN BEPERKING VAN TOEGANG

Het CBP constateert dat in de zorginstellingen autorisaties op basis van functie met technologische middelen worden afgedwongen. Medewerkers kunnen hierdoor via het systeem geen toegang verkrijgen tot andere of meer gegevens dan aan de betreffende functie toegewezen. Het is in deze situaties vervolgens aan de medewerkers zelf om zorgvuldig om te gaan met hun toegangsbevoegdheden en daarvan alléén gebruik te maken als er daadwerkelijk sprake is van een behandelrelatie met een specifieke patiënt. Een en ander wordt in communicatie over en in beleidsdocumenten, zoals gedragscodes en autorisatiebeleid, onder de aandacht van medewerkers gebracht. Met technologische middelen wordt die beperking van toegang tot situaties waarin daadwerkelijk sprake is van een behandelrelatie echter niet afgedwongen. Hierdoor hebben medewerkers feitelijk via het systeem ook toegang tot gegevens van patiënten met wie zij geen behandelrelatie hebben.

In de meeste onderzochte zorginstellingen is de mogelijkheid voor medewerkers om toegang te krijgen tot gegevens van patiënten niet in tijd afgebakend. Hierdoor is het bijvoorbeeld mogelijk dat medewerkers ook na het ontslag van een patiënt uit de zorginstelling diens gegevens nog onbeperkt via het systeem kunnen raadplegen. Slechts in enkele onderzochte zorginstellingen wordt met technologische middelen afgedwongen dat pas als voor een patiënt een activiteit gepland is (afspraak op de poli of opname) medewerkers via het systeem toegang kunnen krijgen tot diens gegevens. Die mogelijkheid vervalt vervolgens na het verstrijken van een vooraf bepaalde periode na het laatste contact met de patiënt.

NOODKNOPPROCEDURE

In noodsituaties en/of in verband met patiëntveiligheid kunnen zorgmedewerkers gebruikmaken van een zogenoemde noodknopprocedure, ook wel aangeduid als 'breaking the glass'-procedure. Daarmee kunnen zij toegang verkrijgen tot meer gegevens dan aan hun functie toegewezen. Veelal bestaat zo'n procedure uit een extra pop-up op het scherm. Hiermee worden medewerkers erop gewezen dat zij niet bevoegd zijn om toegang te krijgen tot deze specifieke patiëntgegevens. Medewerkers wordt gevraagd een reden aan te geven waarom toegang toch noodzakelijk is. Met behulp van die procedure kunnen medewerkers dan alsnog ruimer toegang verkrijgen tot gegevens van patiënten.

VIPS

Veel zorginstellingen uit dit onderzoek kennen een bijzondere regeling voor toegang tot patiëntdossiers van 'vips', onder wie bekende Nederlanders, leden van de raad van bestuur en sóms ook de medewerkers van de zorginstelling zelf. De patiëntdossiers van dergelijke vips zijn afgeschermd van de overige dossiers en slechts voor een beperkte groep zorgmedewerkers te raadplegen, veelal via de noodknopprocedure.

1.1.2 Variant II: autorisatie op basis van functie en werkcontext

Bij sommige van de onderzochte zorginstellingen wordt bij de toekenning van toegangsrechten tot patiëntgegevens niet alleen rekening gehouden met de functie die medewerkers vervullen, maar ook met de werkcontext (afdeling, organisatorische eenheid, discipline, vakgroep). De aan een bepaalde functie toegekende bevoegdheden zijn dan alleen geldig voor zover het gaat om patiënten die binnen een bepaalde werkcontext vallen. Afhankelijk van het type zorginstelling varieert het aantal patiënten dat binnen zo'n werkcontext valt aanzienlijk. Er zal dan ook niet altijd sprake zijn van daadwerkelijke betrokkenheid van een specifieke medewerker bij de behandeling van alle onder die werkcontext vallende patiënten.

Het CBP constateert dat, net als bij variant I, deze wijze van autorisatie in de betreffende zorginstellingen met technologische middelen wordt afgedwongen. Hiermee wordt bereikt dat medewerkers via het systeem uitsluitend toegang hebben tot gegevens van patiënten die behoren tot hun werkcontext en dat zij geen toegang hebben tot gegevens van patiënten daarbuiten. Dit betekent bijvoorbeeld dat administratief medewerkers geen toegang hebben tot gegevens van patiënten die op een andere locatie in behandeling zijn. Voor artsen kan het betekenen dat zij uitsluitend toegang hebben tot de gegevens van patiënten die in behandeling zijn bij de discipline/vakgroep waartoe zij behoren. Hoewel zorgmedewerkers door deze wijze van autoriseren bijvoorbeeld uitsluitend toegang hebben tot de gegevens van patiënten van de afdeling waarvoor zij werken, betekent dit niet automatisch dat de toegang beperkt is tot uitsluitend de gegevens van patiënten waarmee zij een behandelrelatie hebben. Niet elke zorgmedewerker zal namelijk daadwerkelijk betrokken zijn bij de behandeling van alle patiënten die binnen zijn werkcontext vallen.

De onderzochte instellingen maken bij deze wijze van autoriseren een uitzondering voor medewerkers van wie de werkcontext niet exact kan worden vastgesteld, bijvoorbeeld omdat zij bij alle patiënten bij de behandeling betrokken kunnen raken. Dit geldt bijvoorbeeld voor ziekenhuishygiënisten, radiologen en geriaters. Voor dit type medewerkers wordt gekozen voor een autorisatie die toegang geeft tot alle patiënten.

In de onderzochte zorginstellingen die deze wijze van autoriseren toepassen, is net als bij variant I voorzien in een noodknopprocedure. Hiermee kunnen medewerkers als het noodzakelijk is toegang krijgen tot gegevens van patiënten die buiten hun werkcontext vallen, bijvoorbeeld bij spoedgevallen. Deze zorginstellingen geven aan dat het bij deze striktere wijze van autorisatie vaker noodzakelijk is om van de noodknopprocedure gebruik te maken dan wanneer medewerkers toegangsrechten krijgen op basis van alleen hun functie.

1.1.3 Variant III: autorisatie na vaststelling rechtstreekse betrokkenheid

Het CBP stelt vast dat op enkele afdelingen van één van de onderzochte zorginstellingen medewerkers pas toegangsrechten krijgen tot de medische gegevens van (groepen) patiënten nádat is vastgesteld dat de betreffende medewerker daadwerkelijk betrokken is bij de behandeling van die patiënten. Op deze afdelingen vindt autorisatie plaats op basis van een voor een specifieke patiënt opgesteld behandelplan. Pas als in dat behandelplan is voorzien dat een medewerker met een bepaalde functie onderdeel gaat uitmaken van het behandelteam, krijgt die medewerker toegang tot de gegevens van die patiënt. Een en ander wordt met technologische middelen afgedwongen, waardoor medewerkers uitsluitend via het systeem toegang hebben tot gegevens van patiënten bij wie zij een rol vervullen in de behandeling.

1.2 Logging en controle

Uit de wet vloeit voort dat zorginstellingen structureel moeten bijhouden wie wanneer welk patiëntendossier heeft geraadpleegd (logging) en dat dit wordt gecontroleerd. Op deze manier kan de instelling onbevoegde toegang opsporen en maatregelen nemen.

Naarmate de beheersing van de toegang tot patiëntgegevens minder technologisch wordt afgedwongen, is het des te belangrijker om achteraf goed te controleren wie op welk moment welke gegevens heeft geraadpleegd. Ook kan het bestuur van een instelling door analyse van de logging beoordelen of er op punten bijstelling van de autorisaties nodig is.

1.2.1 Logging

Het CBP constateert dat de meeste onderzochte zorginstellingen niet structureel bijhouden wie wanneer welk patiëntendossier heeft geraadpleegd (logging). Soms ontbreken daartoe de technische mogelijkheden. In andere gevallen geven zorginstellingen aan te hebben afgezien van het gebruik van de technische mogelijkheden, omdat daar risico's aan verbonden zijn voor de werking van het systeem. Logging zou het systeem vertragen. In de meeste onderzochte zorginstellingen wordt wel structureel bijgehouden wie wanneer voor welk doel gebruikmaakt van de noodknopprocedure.

1.2.3 Controle van gegevens uit logging

Uit het onderzoek blijkt dat de zorginstellingen de gegevens van het loggen alleen controleren bij het gebruik van de noodknopprocedure, ook in de zorginstellingen waar sprake is van logging van alle acties op patiëntendossiers. Deze controles gebeuren meestal bij vermoedens van misbruik of bij klachten en in een aantal instellingen steekproefsgewijs.

2 Beoordeling

In het vorige hoofdstuk zijn de bevindingen weergegeven over de wijze waarop de onderzochte zorginstellingen omgaan met de toegangsbeveiliging voor gegevens in digitale patiëntendossiers. Dit hoofdstuk beschrijft de voor dit onderzoek relevante wettelijke bepalingen en de beoordeling van de bevindingen vanuit dit normenkader.

2.1 Normenkader

Het CBP heeft de bevindingen uit het onderzoek beoordeeld aan de hand van de voor dit onderzoek relevante wettelijke bepalingen. In de bijlage is het gehele normenkader opgenomen.

RECHTMATIGHEID GEGEVENSVERWERKING

Voor medewerkers van zorginstellingen is toegang tot gegevens in gedigitaliseerde patiëntendossiers alleen rechtmatig indien en voor zover een medewerker rechtstreeks betrokken is bij de behandeling van of zorgverlening aan een patiënt en/of bij de beheersmatige afwikkeling van die zorgverlening en de toegang beperkt blijft tot de gegevens die noodzakelijk zijn voor de uitvoering van de taken van die medewerker. Dit vloeit voort uit het bepaalde in artikel 21, eerste lid onder a, juncto artikel 9, vierde lid Wet bescherming persoonsgegevens (Wbp) juncto artikel 7:457, eerste en tweede lid Burgerlijk Wetboek (BW).

TE TREFFEN BEVEILIGINGSMAATREGELEN

Door het treffen van passende technische en organisatorische maatregelen om persoonsgegevens te beveiligen tegen verlies of enige vorm van onrechtmatige verwerking moet de verantwoordelijke voor de gegevensverwerking een passend beveiligingsniveau garanderen. Dit vloeit voort uit het bepaalde in artikel 13 Wbp.

Voor de zorgsector is met name van belang de nadere uitwerking van de Code voor Informatiebeveiliging (ISO 17799) in de standaard NEN 7510. Het CBP heeft inmiddels ook in de publicatie *Richtsnoeren beveiliging van persoonsgegevens* aanbevolen om ter bepaling van hetgeen in een concrete situatie 'passend' is in de zin van artikel 13 Wbp, gebruik te maken van algemeen geaccepteerde beveiligingsstandaarden. Deze standaarden geven houvast bij het daadwerkelijk treffen van passende maatregelen om beveiligingsrisico's af te dekken. De NEN 7510 is een gezaghebbende sectorale uitwerking van artikel 13 Wbp. Als een ziekenhuis voldoet aan NEN 7510, mag ervan uit worden gegaan dat het ook voldoet aan bovengenoemde wettelijke bepaling. Een ziekenhuis kan ook op andere wijze aantonen dat de beveiliging op orde is, bijvoorbeeld door te voldoen aan de Code voor Informatiebeveiliging. Bij de toetsing van beveiligingsmaatregelen van zorginstellingen aan artikel 13 Wbp gebruikt het CBP het bepaalde in NEN 7510 als ijkpunt.

De Code voor Informatiebeveiliging en NEN 7510 zijn beveiligingsstandaarden die het hele terrein van de informatiebeveiliging binnen een organisatie afdekken. De volgende aspecten van NEN 7510 worden betrokken bij de beoordeling van het passend niveau van de maatregelen die zorginstellingen hebben getroffen op het gebied van toegangsverlening aan medewerkers tot gegevens in gedigitaliseerde patiëntendossiers:

- Er is beleid voor het verlenen van toegang tot informatie:
  - Er zijn procedures om bevoegde gebruikers toegang te geven tot de informatiesystemen en -diensten die ze voor de uitvoering van hun taken nodig hebben en om onbevoegde toegang tot informatiesystemen te voorkomen.
  - Dit beleid is zodanig dat uitsluitend toegang wordt verleend aan medewerkers indien en voor zover zij direct betrokken zijn bij de behandeling van de specifieke patiënt en/of betrokken zijn bij de beheersmatige afwikkeling daarvan en dit beleid wordt ook door inzet van technologische middelen afgedwongen.
- Activiteiten die gebruikers uitvoeren met persoonsgegevens worden vastgelegd in logbestanden (logging).
- De logbestanden worden periodiek gecontroleerd op indicaties van onrechtmatige toegang of onrechtmatig gebruik van persoonsgegevens en waar nodig wordt actie ondernomen.

2.2 Constateringen

Het CBP heeft de bevindingen uit het onderhavige onderzoek beoordeeld op basis van het voor dit onderzoek gehanteerde normenkader. Dit leidt tot constatering van tekortkomingen op het gebied van autorisatie van zorgmedewerkers, autorisatie van administratief-ondersteunende medewerkers, logging en de controle van logging.

AUTORISATIE ZORGMEDEWERKERS

Het CBP constateert dat de wijze van autoriseren van zorgmedewerkers waarbij onderscheid wordt gemaakt op basis van functie (variant I) of op basis van functie en werkcontext (variant II) niet zodanig zijn dat daarmee wordt bereikt dat uitsluitend toegang mogelijk is tot gegevens in patiëntendossiers voor medewerkers voor wie dat gelet op een rechtstreekse betrokkenheid bij de behandeling/verzorging van een patiënt noodzakelijk is. Een zodanige beperking van de toegang van medewerkers is vereist op grond van het bepaalde in artikel 21, eerste lid onder a juncto artikel 9, vierde lid Wbp juncto artikel 7:457 eerste en tweede lid BW. Daar waar bij toegangsverlening aan zorgmedewerkers niet wordt voorzien in de vaststelling van een behandelrelatie tussen de specifieke zorgmedewerker en de specifieke patiënt, is sprake van een wijze van toegangsverlening die niet voldoet aan het vereiste van artikel 13 Wbp.

In variant III is sprake van een zodanige werkwijze dat pas nadat is vastgesteld dat er een behandelrelatie is tussen een specifieke medewerker en een patiënt, de medewerker toegang wordt verleend tot de patiëntgegevens. Een dergelijke werkwijze voldoet wel aan het wettelijke vereiste inzake het voorkomen van onrechtmatige gegevensverwerking door medewerkers. Deze werkwijze is in het onderzoek overigens slechts op een aantal afdelingen binnen één zorginstelling aangetroffen. Wel gebruiken meerdere zorginstellingen deze werkwijze voor toegang tot patiëntgegevens van vips, waarbij toegang alleen wordt toegekend nadat is vastgesteld dat de betreffende zorgmedewerker daadwerkelijk is betrokken bij de behandeling van de vip.

AUTORISATIE ADMINISTRATIEF-ONDERSTEUNENDE MEDEWERKERS

Het CBP constateert dat de wijze van autoriseren van administratief-ondersteunende medewerkers waarbij onderscheid wordt gemaakt op basis van functie (variant I) erin voorziet dat dergelijke medewerkers geen toegang hebben tot de medische persoonsgegevens van patiënten. Maar deze medewerkers hebben feitelijk wel vaak toegang tot de algemene gegevens van alle patiënten. Op grond van het bepaalde in artikel 21, eerste lid onder a juncto artikel 9, vierde lid Wbp juncto artikel 7:457 eerste en tweede lid BW is ook ten aanzien van administratief-ondersteunende medewerkers vereist dat zij slechts toegang krijgen tot gegevens van patiënten indien en voor zover noodzakelijk. Die noodzaak bestaat alleen indien en voor zover patiënten tot hun werkcontext behoren. Als deze werkcontext niet wordt betrokken in de autorisatie van administratief-ondersteunende medewerkers, is sprake van autorisatie die niet voldoet aan het vereiste van artikel 13 Wbp.

LOGGING EN CONTROLE

Het CBP stelt over logging vast dat niet in alle onderzochte zorginstellingen de logging voldoet aan hetgeen op grond van NEN 7510 en NEN 7513 ter zake is aangegeven, omdat niet van alle acties op patiëntgegevens logging plaatsvindt. Zorginstellingen waar geen logging plaatsvindt van alle acties, voldoen niet aan artikel 13 Wbp.

Ook stelt het CBP vast dat in de onderzochte zorginstellingen niet is voorzien in een systematische, consequente controle van alle logging. Hoogstens is sprake van controle van de logging bij gebruik van de noodknop, hetgeen – veelal – ook beperkt blijft tot steekproefsgewijze controles of controle op basis van klachten. Zorginstellingen waar geen systematische controle van alle logging plaatsvindt, voldoen derhalve niet aan artikel 13 Wbp.

2.3 Betoog zorginstellingen en reactie CBP

De onderzochte zorginstellingen voeren verschillende redenen aan waarom zij – in ieder geval vooralsnog – niet gehouden zouden kunnen worden om maatregelen te treffen op het niveau zoals vereist op grond van artikel 13 Wbp om het risico op onrechtmatige verwerking door medewerkers terug te brengen.

2.3.1 Technologische beperkingen in (de software van) het instellings-EPD

Sommige zorginstellingen geven aan dat het in het door hen aangeschafte elektronische patiëntendossier, het zogeheten instellings-EPD, ontbreekt aan technologische ondersteuning voor verdergaande maatregelen om toegangsbeperkingen voor medewerkers conform de wettelijke vereisten te (kunnen) realiseren. Ook wordt genoemd dat logging van alle acties in hun instellings-EPD technisch niet mogelijk is en/of leidt tot risico's voor de werking van het systeem. Eén zorginstelling geeft aan dat het bestuur van de instelling zich vrij snel na de aanschaf van het instellings-EPD realiseerde dat daarmee niet aan de wettelijke vereisten kon worden voldaan, maar daar vervolgens in berustte. Soms stelt een zorginstelling dat deze meende te kunnen vertrouwen op de mededeling van de desbetreffende leverancier dat diens instellings-EPD 'Wbp-proof' zou zijn.

Het CBP merkt op dat 'de huidige stand van de techniek' maatgevend is voor hetgeen als passende maatregelen in de zin van artikel 13 Wbp wordt beschouwd. Argumenten ontleend aan beperkingen gelegen in het gebruik van verouderde techniek zijn derhalve niet valide. De stappen gezet door zorginstellingen om te komen tot een update/upgrade van het door hen gebruikte (verouderde) instellings-EPD, onder meer door het gezamenlijk formuleren van nadere eisen aan de betreffende softwareleverancier, zijn dan ook aangewezen. Dat geldt ook voor de stappen van zorginstellingen om de in het bestaande instellings-EPD aanwezige technologische mogelijkheden daadwerkelijk in te (gaan) zetten.

Zorginstellingen geven ook aan dat het vaststellen van een behandelrelatie tussen een medewerker en een patiënt voor de autorisatie vooralsnog niet door inzet van

technologische middelen kan worden gerealiseerd en dat daarmee derhalve de inzet van (een aanzienlijke hoeveelheid) menskracht is gemoeid.

Het CBP merkt daarover op dat de stand van techniek niet als statisch, maar dynamisch moet worden opgevat. Redelijkerwijs kan daarom van zorginstellingen of hun brancheorganisaties worden verlangd dat zij samen met leveranciers van instellings-EPD's verder onderzoeken hoe c.q. in hoeverre eventuele technologische belemmeringen/beperkingen in volgende versies/upgrades van die instellings-EPD's kunnen worden ondervangen. Ook merkt het CBP op dat in artikel 13 Wbp niet alleen wordt gerefereerd aan de inzet van passende technische maatregelen, maar ook aan de inzet van organisatorische maatregelen. Bij het ontbreken van technologische voorzieningen voor adequate informatiebeveiliging is derhalve de inzet van (voldoende) menskracht aangewezen om het vereiste passende beveiligingsniveau te garanderen.

2.3.2 Geheimhoudingsplicht van medewerkers als waarborg

Zorginstellingen wijzen op de maatregelen die zijn getroffen om te stimuleren dat (zorg)medewerkers uitsluitend gebruikmaken van de hun toegekende toegangsrechten als dit noodzakelijk is om hun rol te vervullen bij de behandeling/verzorging van een specifieke patiënt. Met maatregelen als gedragscodes, personeelsbeleid (waaronder screening van medewerkers met een verklaring omtrent het gedrag (VOG), training, binding aan geheimhoudingsplicht en bewustwordingscampagnes) en sancties (ontslag c.q. ontbinding van toelatingsovereenkomst) kan worden bevorderd dat medewerkers zich bewust zijn dat zij zorgvuldig moeten omgaan met de hun toegekende autorisaties.

Het CBP is positief over maatregelen van zorginstellingen voor bewustwording van het personeel met gedragscodes, personeelsbeleid en sancties. Het CBP merkt echter op dat hiermee geen compensatie kan worden geboden voor het niet inzetten van voldoende technologische maatregelen waarmee 'beheersing vooraf' in voldoende mate kan worden gerealiseerd. Het succes van maatregelen mag niet grotendeels afhankelijk zijn van de zelfbeheersing van de medewerkers. Dat in voorkomende gevallen medewerkers bij onrechtmatige raadpleging van patiëntendossiers kunnen worden ontslagen, doet aan die constatering niet af.[4]

2.3.3 Eventuele risico's voor verantwoorde, veilige zorgverlening (patiëntveiligheid)

Enkele zorginstelling refereren aan potentiële strijdigheid van eisen die aan zorginstellingen worden gesteld in de sfeer van verantwoorde, veilige zorgverlening en eisen op het gebied van de bescherming van de persoonlijke levenssfeer van patiënten. Aan extra maatregelen voor toegangsbeperking voor zorgmedewerkers tot gegevens in patiëntendossiers zouden zodanige risico's kleven voor de patiëntveiligheid, dat zij daarom menen van het treffen van dergelijke maatregelen te mogen afzien.

Het CBP stelt voorop dat het bestuur van een zorginstelling behalve verantwoordelijk voor de patiëntveiligheid óók (wettelijk) verantwoordelijk is voor de bescherming van de persoonlijke levenssfeer van de aan de instelling toevertrouwde patiënten. Er is in dezen geen sprake van tegenstrijdige, maar van nevengeschikte verantwoordelijkheden. De patiënt mag rekenen op én een goede medische behandeling én een zorgvuldige omgang met zijn vertrouwelijke gegevens.

Het CBP constateert dat zorginstellingen de argumentatie rond eventuele risico's voor verantwoorde, veilige zorgverlening niet voorzien van een nadere specificatie en onderbouwing van de eventuele risico's voor de patiëntveiligheid. Daarbij wordt evenmin aangegeven waarom in situaties waarin dit risico reëel aanwezig is, niet zou kunnen worden volstaan met voorzieningen als een noodknopprocedure en/of uitzonderingen bijvoorbeeld voor bepaalde afdelingen, zoals spoedeisende hulp en intensive care. Dergelijke uitzonderingen kunnen worden gemaakt vanwege het spoedeisende en/of complexe karakter van hulpverlening in bepaalde situaties, maar dienen dan wel goed onderbouwd en proportioneel te zijn. Ook dient de logging en de controle adequaat te zijn. De noodzaak om voor bepaalde situaties een uitzondering te maken hoeft dus niet in de weg te staan aan invoering van de hoofdregel.

Overigens geven zorginstellingen die wel verdere maatregelen voor toegangsbeperking hebben ingezet aan dat – ter compensatie van mogelijke risico's van het gehanteerde autorisatiebeleid – dergelijke noodvoorzieningen volstaan en dat zich geen extra incidenten op het gebied van patiëntveiligheid hebben voorgedaan die kunnen worden geweten aan onvoldoende toegang tot patiëntgegevens in noodsituaties. Ook eventuele weerstand bij zorgmedewerkers vanwege gepercipieerde risico's voor de patiëntveiligheid en/of het gebruiksgemak blijkt na een gewenningsperiode en/of door gerichte acties effectief weg te nemen.

2.3.4 Financiële beperkingen

De zorginstellingen wijzen op de aanzienlijke kosten die gemoeid zijn met het aanschaffen en updaten van een instellings-EPD en stellen dat dit daarom niet altijd de hoogste prioriteit kan hebben.

Het CBP merkt op dat kosten in wettelijke zin geen valide reden kunnen zijn voor zorginstellingen om blijvend een achterstand op te lopen in het gebruik van een instellings-EPD dat voldoet aan de actuele stand van de techniek. Het CBP merkt daarnaast op dat het bestuur van een zorginstelling gehouden is om ook de juiste prioriteit toe te (blijven) kennen aan bescherming van de persoonlijke levenssfeer en hierin te investeren.

2.3.5 Ontbreken van voldoende menskracht voor controle van logging

Sommige onderzochte zorginstellingen geven aan dat zij vooralsnog afzien van de controle van de loggegevens van alle acties op dossiers, omdat daarmee te veel menskracht is gemoeid. Deze zorginstellingen zijn op zoek naar manieren voor intelligentere analyse van loggegevens, waarmee het beslag op tijd en menskracht bij controle kan worden verminderd. Zorginstellingen in de Verenigde Staten experimenteren hier al mee. Ook geven zorginstellingen aan dat de hoofdbehandelaar van een patiënt inhoudelijk de controletaak het beste zou kunnen uitvoeren, maar dat artsen/zorgverleners over het algemeen geen tijd kunnen of willen vrijmaken voor een dergelijke taak. De implementatie van controle op logging strandt in zorginstellingen daarom vooralsnog vaak op de vraag 'door wie en hoe?'.

Het CBP merkt op dat het vereiste van passende maatregelen in artikel 13 Wbp niet impliceert dat bij het – vooralsnog – ontbreken van 'ideale' maatregelen kan worden afgezien van (tijdsintensievere) maatregelen waarmee resultaat kan worden geboekt.

[4] Rechtbank Den Haag, 2 juni 2010, *Tijdschrift voor Gezondheidsrecht* 2010/27.

De verplichting tot logging om onrechtmatige toegang te voorkomen zoals opgenomen in de NEN-normen impliceert dat de logging ook daadwerkelijk wordt gecontroleerd. Die controle vormt een wezenlijk onderdeel van de toegangsbeveiliging en is des te belangrijker daar waar in zorginstellingen de autorisatie – vooralsnog – tekortschiet. Als zorginstellingen die autorisaties verbeteren, zal de analyse van de logging mogelijkerwijs ook 'intelligenter' aangepakt kunnen worden.

2.3.6 Samenvatting

Samenvattend constateert het CBP dat er geen valide redenen in de sfeer van stand der techniek, patiëntveiligheid en kosten van tenuitvoerlegging zijn voor de onderzochte zorginstellingen om niet te voldoen aan hetgeen vereist is ex artikel 13 Wbp als het gaat om beperking van toegang voor medewerkers tot gegevens van patiënten, logging en de controle daarop. Het argument van sommige zorginstellingen dat patiëntveiligheid in de weg staat bij het treffen van de vereiste maatregelen wordt alleen al weerlegd door de constatering dat andere zorginstellingen dergelijke maatregelen wel blijken te (kunnen) implementeren. Daarnaast kunnen voor de inschakeling van hulpverleners in spoedeisende en/of complexe situaties andere, passende regelingen voor de toegang tot patiëntgegevens worden getroffen, mits onderbouwd en proportioneel.

Van het bestuur van zorginstellingen mag worden verwacht dat zij in de praktijk goed uitwerking geven aan de nevengeschikte verantwoordelijkheden van het leveren van verantwoorde zorg en de bescherming van de persoonlijke levenssfeer van patiënten.

Bij de aanschaf van een instellings-EPD, moet het bestuur van een zorginstelling al in een vroegtijdig stadium nadenken over de mogelijke privacyrisico's en een adequate beveiliging van persoonsgegevens. Uit het onderhavige onderzoek komt het beeld naar voren dat er bij sommige, zo niet de meeste, zorginstellingen pas in een (te) laat stadium aandacht is voor dit onderwerp.

3 Conclusie

Het CBP concludeert na onderzoek bij negen zorginstellingen dat deze instellingen vooralsnog niet voorzien in voldoende passend te achten maatregelen om de toegang tot gedigitaliseerde patiëntendossiers te beperken, zodanig dat medewerkers alleen dán toegang krijgen tot patiëntgegevens indien zij een behandelrelatie met de betreffende patiënt hebben en/of de toegang noodzakelijk is voor de beheersmatige afwikkeling van de behandeling. Een dergelijke beperking van de toegang voor medewerkers is vereist gelet op het bepaalde in artikel 21, eerste lid onder a juncto artikel 9, vierde lid Wet bescherming persoonsgegevens (Wbp) juncto artikel 7:457 eerste en tweede lid Burgerlijk Wetboek (BW). In slechts één zorginstelling is sprake van een werkwijze bij autorisatie die wel aan de wettelijke vereisten voldoet, maar die werkwijze wordt niet in de gehele zorginstelling toegepast.

Het CBP concludeert dat een aantal zorginstellingen gebruikmaakt van een gedigitaliseerd patiëntendossier, instellings-EPD genoemd, dat niet (meer) voldoet aan de huidige stand van de techniek. Op grond van artikel 13 Wbp is vereist dat zorginstellingen bij het treffen van passende maatregelen, zoals bedoeld in artikel 13, letten op hetgeen bij de stand van de techniek mogelijk is. Zorginstellingen die geen stappen hebben gezet om gebruik te (gaan) maken van verbeteringen in de techniek waarmee (ook) de naleving van de Wbp kan worden verbeterd, voldoen daardoor niet aan artikel 13 Wbp.

Het CBP concludeert daarnaast dat binnen zorginstellingen die wél beschikken over een instellings-EPD dat voldoet aan de huidige stand van de techniek, sprake is van een onvoldoende niveau van passende maatregelen zoals vereist door artikel 13 Wbp. Het gaat daarbij om zorginstellingen die de aanwezige technische mogelijkheden niet gebruiken en/of niet voldoende menskracht inzetten om tot naleving van de Wbp te (kunnen) komen. Naar het oordeel van het CBP geven deze zorginstellingen onvoldoende onderbouwing waarom deze inzet van techniek en/of menskracht redelijkerwijs van hen niet kan worden gevergd.

Het CBP concludeert verder dat niet in alle onderzochte zorginstellingen de logging voldoet aan hetgeen op grond van NEN 7510 en NEN 7513 ter zake is aangegeven, omdat niet van alle acties op patiëntgegevens logging plaatsvindt. Zorginstellingen waar geen logging plaatsvindt van alle acties, voldoen niet aan artikel 13 Wbp.

In de onderzochte zorginstellingen is verder niet voorzien in een systematische, consequente controle van alle logging. Hoogstens is sprake van controle van de logging bij gebruik van de noodknop, hetgeen – veelal – ook beperkt blijft tot steekproefsgewijze controles of controle op basis van klachten. De verplichting tot controle van de logging teneinde te controleren of toegang tot patiëntgegevens beperkt blijft tot situaties waarin dat rechtmatig is, vloeit logischerwijs voort uit de verplichting tot logging zoals opgenomen in NEN 7510 en NEN 7513. Zorginstellingen waar geen systematische controle van alle logging plaatsvindt, voldoen derhalve niet aan artikel 13 Wbp.

'Vips' (BN'ers, leden van de raad van bestuur en soms ook medewerkers van de zorginstelling) hebben in de onderzochte zorginstellingen vaak wél meer bescherming tegen onrechtmatige toegang tot patiëntgegevens door medewerkers van de instellingen. Deze mate van bescherming komt op grond van de wet (Wbp en Wgbo) aan iedere

patiënt toe. Studenten willen ook niet dat medestudenten die bijverdienen op de administratie van een zorginstelling in hun dossier kunnen kijken; doktersassistenten willen evenmin dat collega's op een andere huisartsenpost in hun behandeldossier kunnen kijken; buren willen niet dat de buurvrouw die als secretaresse in een zorginstelling werkt, hun dossier kan inzien.

Verantwoordelijken in de zorgsector lijken tot op heden weinig 'sense of urgency' te ervaren om de toegang tot digitale patiëntendossiers te beperken. Pas naar aanleiding van het onderhavige onderzoek door het CBP heeft een aantal van de onderzochte zorginstellingen stappen gezet om ten opzichte van de softwareleverancier gezamenlijk op te trekken (organisatie van 'gebruikersmacht') om zo de benodigde aanpassingen in het instellings-EPD van die leverancier af te dwingen.

Er is vooralsnog alleen in de ggz-sector sprake van een – mede door de koepelorganisatie georganiseerde – gemeenschappelijke set van eisen voor instellings-EPD's en toetsing van de producten van verschillende leveranciers aan die eisen. Daardoor kunnen ggz-instellingen een keuze maken uit gecertificeerde instellings-EPD's en hoeven zij niet langer alleen te varen op de mededelingen van softwareleveranciers over hun product en/of hoeven zij zich niet langer zelfstandig te oriënteren op hetgeen gelet op de praktijk in de sector en de in de sector gebruikte techniek als 'passend' moet worden beschouwd.

De onderzochte zorginstellingen hebben aan het CBP informatie verstrekt over door hen opgestelde plannen en in gang gezette acties om de wijze van toegangsverlening voor medewerkers tot patiëntendossiers en de controle op die toegang te verbeteren. Het CBP heeft in reactie daarop aan die zorginstellingen kenbaar gemaakt dat aanvullende acties noodzakelijk zijn om te voldoen aan artikel 13 Wbp. Over de fasering van en de redelijke termijn waarbinnen realisatie van dergelijke – veelal complexe – aanpassingen in technologie en werkwijze mogelijk is, is het CBP in overleg getreden met de betreffende zorginstellingen en de koepelorganisaties. Indien het CBP echter constateert dat zorginstellingen onvoldoende voortvarend werk maken van de verbeterpunten, treedt het CBP bij die zorginstellingen handhavend op.

Ten aanzien van alle andere, nog niet onderzochte zorginstellingen in Nederland verwacht het CBP dat zij naar aanleiding van dit rapport ook acties ondernemen om te beoordelen of zij de benodigde maatregelen hebben getroffen om te voldoen aan hetgeen vereist is op grond van artikel 13 Wbp.

Het CBP zal mogelijk op termijn ook bij andere dan de nu onderzochte zorginstellingen op dit punt inlichtingen inwinnen en daarover in voorkomende gevallen rapporteren en publiceren, zeker als over specifieke instellingen signalen zijn binnengekomen.

Bijlage:

Toelichting normenkader

Aan de in dit onderzoek toepasselijke wettelijke bepalingen geeft het CBP de navolgende uitleg:

RECHTMATIGHEID GEGEVENSVERWERKING

Voor medewerkers van zorginstellingen is toegang tot gegevens in gedigitaliseerde patiëntendossiers alleen rechtmatig indien en voor zover een medewerker rechtstreeks betrokken is bij de behandeling van of zorgverlening aan een patiënt en/of bij de beheersmatige afwikkeling van die behandeling/zorgverlening en de toegang beperkt blijft tot de gegevens die noodzakelijk zijn voor de uitvoering van de taken van die medewerker. Dit vloeit voort uit het bepaalde in artikel 21, eerste lid onder a, juncto artikel 9, vierde lid Wet bescherming persoonsgegevens (Wbp) juncto artikel 7:457, eerste en tweede lid Burgerlijk Wetboek (BW).

VERANTWOORDELIJKE

In zorginstellingen worden het doel en de middelen voor de verwerking van persoonsgegevens bepaald door de raad van bestuur en is als zodanig de raad van bestuur de verantwoordelijke in de zin van de Wbp. De raad van bestuur van de zorginstelling is derhalve gehouden tot naleving van de in de Wbp aan de verantwoordelijke opgelegde verplichtingen.

De verplichting om te voldoen aan het bepaalde in artikel 7:457 eerste en tweede lid BW inzake geheimhouding rust eveneens[5] op de raad van bestuur van de zorginstelling, zijnde contractspartij bij de geneeskundige behandelingsovereenkomst met de patiënt.

In dit kader is (in relatie tot werkzaamheden van op 'toelatingsovereenkomst' werkzame specialisten in zorginstellingen) ook van belang hetgeen in de memorie van antwoord bij de Wet op de geneeskundige behandelingsovereenkomst is opgemerkt over de verantwoordelijkheid van (het bestuur van) de rechtspersoon als (mede) hulpverlener/contractspartij in de zin van artikel 7:446 BW. Met betrekking tot de omgang met (medische) persoonsgegevens en het verlenen van toegang tot die gegevens aan medewerkers is daarin aangegeven: '(..) dat het voor het bereik van de geheimhoudingsplicht niet meer ter zake doet of een natuurlijke persoon als hulpverlener optreedt dan wel een rechtspersoon, zoals een ziekenhuis of andere instelling (…) Naar onze mening is het ongewenst de reikwijdte van de geheimhoudingsplicht te laten afhangen van de rechtsverhoudingen binnen een ziekenhuis. Ook als het ziekenhuis hulpverlener is, mogen patiëntengegevens niet worden verstrekt aan onbevoegden, ongeacht of deze zich binnen of buiten de instelling bevinden. De tekst (…) beoogt dit te bereiken door het creëren van een zorgplicht

[5] Indien er sprake is van op toelatingsovereenkomsten werkzame artsen in de instelling komt tussen die artsen en de patiënt ook een geneeskundige behandelingsovereenkomst tot stand en zijn zowel de instelling als de arts aangemerkt als 'hulpverlener' in de zin van artikel 7:446 BW en gehouden tot naleving van artikel 7:457 BW, terwijl voor de arts ook het in artikel 88 Wet Big neergelegde (medisch) beroepsgeheim van belang is.

voor de hulpverlener dat met de in het kader van de behandelingsrelatie verkregen gegevens op een juiste wijze wordt omgegaan. Dit betekent dat ook de nodige maatregelen moeten worden getroffen om de gegevens te beveiligen. (…) De kern van de voorgestelde tekst is echter, dat de hulpverlener verantwoordelijk is voor een juist beheer van de in het kader van de behandeling aan hem toevertrouwde gegevens.'[6]

TE TREFFEN BEVEILIGINGSMAATREGELEN

In artikel 13 Wbp is bepaald: de verantwoordelijke legt passende technische en organisatorische maatregelen ten uitvoer om persoonsgegevens te beveiligen tegen verlies of enige vorm van onrechtmatige verwerking. Deze maatregelen garanderen, rekening houdend met de stand van de techniek en de kosten van tenuitvoerlegging, een passend beveiligingsniveau gelet op de risico's die de verwerking en de aard van de te beschermen gegevens met zich meebrengen. De maatregelen zijn er mede op gericht onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen.

Voor de zorgsector is met name van belang de nadere uitwerking van de Code voor Informatiebeveiliging (ISO 17799) in de standaard NEN 7510. Het CBP heeft inmiddels ook in de publicatie *Richtsnoeren beveiliging van persoonsgegevens*[7] aanbevolen om ter bepaling van hetgeen in een concrete situatie 'passend' is in de zin van artikel 13 Wbp, gebruik te maken van algemeen geaccepteerde beveiligingsstandaarden. Deze standaarden geven houvast bij het daadwerkelijk treffen van passende maatregelen om beveiligingsrisico's af te dekken. De NEN 7510 is een gezaghebbende sectorale uitwerking van artikel 13 Wbp. Als een ziekenhuis voldoet aan NEN 7510, mag ervan uit worden gegaan dat het ook voldoet aan bovengenoemde wettelijke bepaling. Een ziekenhuis kan ook op andere wijze aantonen dat de beveiliging op orde is, bijvoorbeeld door te voldoen aan de Code voor Informatiebeveiliging. Bij de toetsing van beveiligingsmaatregelen van zorginstellingen aan artikel 13 Wbp gebruikt het CBP het bepaalde in NEN 7510 als ijkpunt.

De Code voor Informatiebeveiliging en NEN 7510 zijn beveiligingsstandaarden die het hele terrein van de informatiebeveiliging binnen een organisatie afdekken. De volgende aspecten van NEN 7510 zijn betrokken bij de beoordeling van het passend niveau van de maatregelen die zorginstellingen hebben getroffen op het gebied van toegangsverlening aan medewerkers tot gegevens in gedigitaliseerde patiëntendossiers:

- Er is beleid voor het verlenen van toegang tot informatie:
  - Er zijn procedures om bevoegde gebruikers toegang te geven tot de informatiesystemen en -diensten die ze voor de uitvoering van hun taken nodig hebben en om onbevoegde toegang tot informatiesystemen te voorkomen.
  - Dit beleid is zodanig dat uitsluitend toegang wordt verleend aan medewerkers indien en voor zover zij direct betrokken zijn bij de behandeling van de specifieke patiënt en/of betrokken zijn bij de beheersmatige afwikkeling daarvan en dit beleid wordt ook door inzet van technologische middelen afgedwongen.
- Activiteiten die gebruikers uitvoeren met persoonsgegevens worden vastgelegd in logbestanden (logging).
- De logbestanden worden periodiek gecontroleerd op indicaties van onrechtmatige toegang of onrechtmatig gebruik van persoonsgegevens en waar nodig wordt actie ondernomen.

[6] TK, 1990-1991, 21 561, nr. 6, pp. 38-39.
[7] CBP, *Richtsnoeren Beveiliging persoonsgegevens*, februari 2013.

COLLEGE BESCHERMING PERSOONSGEGEVENS

Postbus 93374
2509 AJ Den Haag

www.cbpweb.nl
www.mijnprivacy.nl