Een juridisch kader voor Patiëntportalen

NEDERLANDSE PATIËNTEN CONSUMENTEN FEDERATIE

Betere zorg door betere informatie Nictiz

Datum 4 juli 2013 **Auteur(s)** Mr. J.A.L. Krabben	**ID Nummer** 13009		

Hoofdstuk 1 Juridisch kader voor patiëntportalen

1.1 Inleiding

Patiëntportalen worden veelvuldig ingezet door zorgaanbieders. De wet stelt eisen aan gegevensverwerking via patiëntportalen. Hoewel de betekenis van bestaande regels voor deze nieuwe ontwikkeling in de zorgverlening nog niet op alle punten is uitgekristalliseerd, biedt het wettelijk kader voldoende handvatten. Hieruit kunnen de voorwaarden worden afgeleid waar de zorgverlener in elk geval rekening mee moet houden. Deze voorwaarden worden in dit paper beschreven. In toekomstige regelgeving zullen naar verwachting aanvullende bepalingen over digitale uitwisseling van gegevens worden opgenomen.

Zorgaanbieders kunnen stapsgewijs tot invoering van diensten via een eigen portaal over gaan na zorgvuldige afweging van de manier waarop dat gebeurt. Daarmee wordt voorkomen dat patiëntgegevens onvoldoende beschermd zijn en de instelling daarvoor onverhoopt op de vingers wordt getikt.

1.2 Wat is het doel van dit kader?

Ook u vraagt zich misschien af met welke regels u rekening moet houden bij het inrichten van een patiëntportaal. In dit paper wordt een aantal uitgangspunten op een rijtje gezet.

1.3 Wie is de doelgroep?

Dit paper is geschreven voor zorgverleners en zorginstellingen die geïnteresseerd zijn in de juridische eisen aan het aanbieden van patiëntenportalen aan hun patiënten[1].

1.4 Portaalfuncties

In dit kader gaat het om patiëntportalen die worden aangeboden en beheerd door de zorgaanbieder. Portalen kennen diverse functie's.

Enkele functionaliteiten van portalen zijn:

- Registreren van gezondheidsgegevens via het portaal;
- inzage via het portaal in geregistreerde gegevens van de zorgaanbieder;
- online afspraken maken;
- berichtenfunctionaliteit via het portal;
- e-consult;
- aanvraag van herhaalrecepten;
- geven van voorlichting.

1.5 Juridisch kader in verschillende situaties

Met welke wetten en regels rekening gehouden moet worden hangt onder meer af van wie er gegevens gaat gebruiken en waar die vandaan komen. Gaat het om gegevens die de zorgverlener verwerkt of zijn het gegevens die de patiënt verstuurt? Wat ook meespeelt, is wie de gegevens opslaat en beheert, die digitaal via een patiëntportaal worden verwerkt.

Twee wetten zijn hiervoor in het bijzonder van belang: de Wet bescherming persoonsgegevens (Wbp) en de Wet op de geneeskundige behandelingsovereenkomst (WGBO).

De Wbp is van toepassing op het verwerken van persoonsgegevens. Van persoonsgegevens is sprake als gegevens herleidbaar zijn naar een individu. De Wbp vat het vastleggen en het

[1] Het juridisch kader heeft alleen betrekking op de gegevensverwerking via portalen aangeboden en beheerd door of namens de zorgaanbieders.

verdere gebruik van persoonsgegevens samen onder de noemer ‘verwerken’ van persoonsgegevens. Het verwerken slaat op alle handelingen die met betrekking tot de gegevens worden uitgevoerd. Dat kan zoal gaan om het verkrijgen, vastleggen, gebruiken, aanpassen, verzenden, samenbrengen, bewaren of vernietigen van gegevens. In welke gevallen is de Wbp van toepassing op communicatie via patiëntportalen?

De WGBO (7:446 Burgerlijk Wetboek e.v.) is van toepassing op het verwerken van gegevens door de zorgverlener die hij in het kader van de behandeling van de patiënt heeft verkregen. Die gegevens legt hij, voor zover van belang, vast in zijn dossier over de patiënt, conform de dossierplicht. Dat kunnen ook gegevens zijn die via het portaal van de zorgaanbieder zijn verwerkt. Is de WGBO steeds van toepassing?

In het volgende hoofdstuk wordt op de toepasselijkheid van deze wetten verder ingegaan.

Hoofdstuk 2 Wet op de geneeskundige behandelingsovereenkomst

2.1 Toepasselijkheid

De WGBO is van toepassing op het verwerken van gegevens door de zorgverlener die hij in het kader van de behandeling van de patiënt heeft verkregen. Die wet verplicht hem de noodzakelijke gegevens vast te leggen in zijn dossier over de patiënt. Wanneer de zorgverlener gegevens over de patiënt wil delen heeft hij te maken met het beroepsgeheim dat in de WGBO verankerd is[2]. Aan anderen dan de patiënt verstrekt de zorgverlener alleen gegevens omtrent de patiënt met zijn toestemming. Die toestemming is niet nodig als het gaat om rechtstreeks bij de behandelingsovereenkomst betrokkenen en de betreffende informatie nodig is voor de behandeling. De patiënt heeft recht op inzage in de vastgelegde gegevens.

Bij het gebruik van patiëntenportalen door zorginstellingen speelt de vraag of de WGBO steeds van toepassing is. Nagegaan moet worden voor welke functies het portaal gebruikt wordt. In alle gevallen dat het portaal gebruikt wordt voor communicatie tussen patiënt en zorgverlener of patiënt en zorgaanbieder in het kader van de (aanstaande) behandeling van de patiënt is de WGBO van toepassing. De relevante gegevens worden opgeslagen in het dossier van de zorgaanbieder. Sommige gegevens zijn bedoeld voor de patiëntenadministratie. Al deze gegevens van de patiënt vallen onder de WGBO en de geheimhoudingsplicht van de zorgverlener en de instelling. Niet alleen de gegevens die daadwerkelijk in het dossier worden vastgelegd vallen onder de geheimhoudingsplicht. Deze plicht geldt ook voor informatie over de patiënt die ter kennis van de zorgverlener is gekomen bij de behandeling, welke niet in het dossier wordt opgenomen.

De zorgverlener neemt de relevante gegevens op in het dossier.
Niet alles dat wordt besproken wordt ook vastgelegd. Ook niet alles dat de zorgverlener ziet of ervaart wordt opgenomen in het dossier.
De geheimhoudingsplicht strekt zich wel uit tot deze gegevens.

Communicatie via het portaal tussen niet-patiënten of andere geïnteresseerden en de zorginstelling valt niet onder de WGBO. Dat verandert als bepaalde informatie later alsnog wordt opgenomen in het dossier, bij de aanvang van een behandeling.

2.2 Persoonlijk Gezondheidsdossiers

Een portaal kan ook de mogelijkheid tot het bijhouden van een Persoonlijke Gezondheidsdossier (PGD) bieden (zie kader op de volgende pagina voor een definitie). In dat geval is de toepassing van de WGBO niet geheel eenduidig[3]. De vraag is of het PGD ook de dossierbescherming van de WGBO heeft. Als dat niet of niet geheel het geval kan zijn, is vervolgens de vraag of de betreffende gegevens onder de geheimhoudingsplicht van de zorgverlener en de instelling vallen zoals bedoeld in artikel 88 Wet BIG of artikel 7:457 BW (WGBO). Gegevens die in het kader van de behandeling van de patiënt ter kennis van de zorgverlener zijn gekomen vallen onder de geheimhoudingsverplichting. Ook als het gegevens zijn die in het PGD zijn opgenomen. Die plicht geldt niet alleen voor de betrokken zorgverlener maar ook voor de zorgaanbieder die het informatiesysteem beheert waarin het dossier is opgenomen. Dat betekent dat de zorgaanbieder zich tegenover anderen dan de patiënt moet beroepen op die verplichting.

[2] Het medisch beroepsgeheim vloeit voor zorgverleners ook voort uit artikel 88 Wet BIG. In de WGBO is het beroepsgeheim in de behandelrelatie nader uitgewerkt.
[3] Op dat punt is nog duidelijkheid nodig van de wetgever, toezichthouder of rechter.

Een PGD is een gezondheidsdossier dat wordt geïnitieerd en onderhouden door een patiënt, waarin de eigen medische gegevens bijgehouden kunnen worden, maar ook gegevens afkomstig van anderen zoals zorgverleners opgenomen kunnen worden.

Er is echter een aantal complicerende aspecten aanwezig. Het PGD is in de eerste plaats de werkomgeving van de patiënt, waar hij zijn zorginformatie opslaat[4]. Als dat betekent dat (alleen) de patiënt bevoegd is tot het autoriseren van toegang door anderen, dan kan de WGBO zorgplicht om de toegang tot het dossier door derden te voorkomen niet (in zijn huidige omvang of betekenis) aan de zorgaanbieder worden opgelegd. Zonder de macht erover te beschikken kan hij niet de verantwoordelijkheid ervoor dragen. En hoewel de geheimhoudingsplicht geldt voor alles wat ter kennis van de zorgverlener is gekomen in het kader van de behandeling, is het de vraag of alle in een PGD beschikbare informatie als zodanig kan worden beschouwd.

Overigens wordt deze juridische 'situatie' deels ondervangen door de bepalingen en verplichtingen, ook met betrekking tot geheimhouding, uit de Wbp. De Wbp komt hierna aan de orde. Toch maakt wel uit of de WGBO van toepassing is en het medisch beroepsgeheim geldt. Dat biedt namelijk betere bescherming van vertrouwelijke gegevens van de patiënt. Omdat er niet zoiets bestaat als een patiëntgeheim, zijn dossiergegevens die buiten de bescherming van het beroepsgeheim (en met name de bescherming van het dossier onder de WGBO) zouden vallen gemakkelijker door anderen te verkrijgen. Denk aan het verlangen van gegevens door politie en het openbaar ministerie of anderen met bijzondere bevoegdheden[5].

2.3 Praktisch omgaan met verschillende regimes

Bij de meeste portaalfuncties geldt dat de WGBO van toepassing zal zijn, maar zoals beschreven is het soms onduidelijk hoever de toepassing reikt. U kunt een aantal uitgangspunten hanteren om daarmee zorgvuldig om te gaan:

- U gaat ervan uit dat de WGBO steeds van toepassing is. De vereisten uit de Wbp voor het verwerken van gezondheidsgegevens leiden tot een vergelijkbaar streng regime ten aanzien van de bescherming en beveiliging van de gegevens. (Zie hoofdstuk 3 over de Wbp)
- Naar derden toe beroept u zich zo nodig op het medisch beroepsgeheim ten aanzien van alle onder verantwoordelijkheid van de zorgaanbieder opgeslagen gegevens van de patiënt. U hoeft dan niet steeds na te gaan of dat zo is en kunt u één lijn hanteren, terwijl u er geen risico mee loopt.
- U zorgt ervoor dat de gegevens uitsluitend worden verwerkt door beroepsbeoefenaars die een geheimhoudingsverplichting hebben of door personen aan wie een geheimhoudingsplicht is opgelegd[6].

Voor het gebruik van het patiëntportaal als communicatiemiddel in de behandeling heeft de zorgverlener de toestemming van de patiënt nodig. Die kan aan hem verleend worden via het portaal of op andere wijze. Toestemming is in elk geval nodig omdat de patiënt de gelegenheid moet hebben in te stemmen met deze manier van digitale gegevensverwerking die naast de

[4] eHealth en recht. Inleiding op het thema. Nouwt en Hooghiemstra, Computerrecht, afl. 6, December 2011

[5] Ook is er geen mogelijkheid zich als zorgverlener te verschonen bij de rechter als er geen sprake is van gegevens die onder het medisch beroepsgeheim vallen.

[6] In de eerste plaats worden de gegevens alleen door (afgeleid) geheimhoudingsplichtigen verwerkt. Mocht er toch noodzaak van verwerking bestaan door iemand die niet op grond van de wet geheimhoudingspichtig is (bijvoorbeeld de ICT bewerker) dan dient er sprake te zijn van een opgelegde geheimhoudingsverplichting.

reguliere communicatie en gegevensverwerking zal plaatsvinden. De patiënt moet daarvoor toereikend geïnformeerd worden. Dat biedt hem de gelegenheid in te stemmen met de voorwaarden van de dienstverlening en met de inherente risico's van de gegevensverwerking via het portaal, zonder dat dit de zorgaanbieder ontslaat van de verplichting tot het treffen van passende maatregelen van gegevensbescherming en beveiliging[7].

Hoofdstuk 3 Wet bescherming persoonsgegevens

3.1 Begrippen Wbp

De Wbp hanteert het begrip 'verantwoordelijke' voor degene die het doel en de middelen van de gegevensverwerking vaststelt. Dat is degene die bepaalt waarvoor de gegevensverwerking noodzakelijk en gerechtvaardigd is en die de wijze van verwerking bepaalt. Het is kort gezegd degene met de zeggenschap over de gegevensverwerking. Die natuurlijke of rechtspersoon is aan te spreken op de naleving van de verplichtingen uit de Wbp, die grotendeels aan hem gericht zijn.

Een verantwoordelijke kan een deel van de gegevensverwerking uitbesteden aan een dienstverlener die niet onder zijn rechtstreeks gezag staat. Die dienstverlener treedt dan op als 'bewerker' in de zin van de Wbp[8]. Een klein aantal verplichtingen uit de Wbp zijn gericht op deze bewerkersrol. Zo moet de bewerker zorgen voor adequate beveiliging van de gegevens die hij in opdracht van de verantwoordelijke verwerkt. Bij digitale communicatie wordt veel gebruik gemaakt van bewerkers. Die hebben de kennis en techniek in huis om de gegevensverwerking goed uit te voeren. De bewerker verwerkt de gegevens alleen in opdracht van de verantwoordelijke. Zo niet, dan is hij (mede-) verantwoordelijke. Dit laatste is in de zorg onwenselijk in verband met de vertrouwelijkheid van gegevens. In de afspraken tussen de verantwoordelijke en de bewerker wordt dit daarom duidelijk vastgelegd.

De Wet bescherming persoonsgegevens
De Wet bescherming persoonsgegevens (Wbp) gaat uit van het 'verwerken' van persoonsgegevens. Het verwerken slaat op alle handelingen die met betrekking tot de persoonsgegevens worden uitgevoerd. Dat kan bijvoorbeeld gaan om het verkrijgen, vastleggen, gebruiken, aanpassen, verzenden, samenbrengen, bewaren of vernietigen van gegevens.

Op dienstverlening door zorgverleners via een portaal is de Wbp van toepassing. Dat is anders als geanonimiseerd gebruik kan worden gemaakt van bepaalde diensten en de daarbij verwerkte gegevens verder ook niet herleidbaar zijn naar patiënt of zorgverlener. De meeste functionaliteiten in portalen verlangen echter een persoonlijk en geïdentificeerd gebruik.

3.2 Toepassing Wbp op patiëntportaal

De Wbp is van toepassing op de verwerking van persoonsgegevens via een patiëntportaal van de zorgaanbieder. De zorgaanbieder is de verantwoordelijke voor deze gegevensverwerking via het patiëntportaal. Hij stelt het doel en de middelen voor de gegevensverwerking vast. Hij bepaalt welk systeem hij aanbiedt en de functionaliteiten die hij wil aanbieden. De verantwoordelijkheid voor de

[7] Ook moet de zorgaanbieder zorg blijven dragen voor het verlenen van verantwoorde zorg. De zorgaanbieder moet de dienstverlening dus zo inrichten dat hij ook aan andere wettelijke voorwaarden voor zorgverlening blijft voldoen.
[8] Een bewerker kan een hostingpartij zijn, maar ook een partij die een bepaalde verwerking uitvoert voor de verantwoordelijke. Leveranciers van patiëntportalen van zorginstellingen zijn vaak 'bewerker' zoals de wet bedoelt.

inhoudelijke juistheid van de verwerkte gegevens is voor de zorgaanbieder op sommige punten beperkt, wanneer deze door de gebruikers van het portaal worden aangeleverd. Wel moet hij ervoor zorgen dat de gegevens die worden opgeslagen overeenkomen met de door gebruikers aangeleverde gegevens en dient hij identificerende gegevens te controleren op juistheid. De gebruikers zijn de zorgverleners en de patiënt.

De patiënt is verantwoordelijk voor de juistheid van door hem ingevoerde gegevens. Ook kan er zeggenschap bij de patiënt liggen betreffende de (exclusieve) mogelijkheid om anderen toegang te bieden tot delen van zijn PGD, wanneer dat een functionaliteit is. De Wbp is volledig van toepassing op de door de patiënt toegevoegde gegevens. De zorgaanbieder die het portaal aanbiedt is verantwoordelijk voor het opslaan van de ingevoerde gegevens en voor de gegevensverwerking die noodzakelijk is om de gegevensuitwisseling via het portaal tot stand te brengen. Hierbij kan hij gebruik maken van een dienstverlener die als bewerker van de persoonsgegevens optreedt[9].

De zorgaanbieder zal bij deze gegevensverwerking dus rekening moeten houden met de verplichtingen die de Wbp aan hem oplegt. Daarbij gaat het onder meer om het volgende:

- De zorgaanbieder stelt het **doeleinde** van een bepaalde gegevensverwerking vast en kiest daarvoor de geschikte toepassing. Het doel bepaalt de gegevensbehoefte zodat vastgesteld kan worden welke gegevens verwerkt mogen worden.
- De wet vereist een **grondslag**[10] voor de inzet van een bepaalde portaalvoorziening door de zorgaanbieder. Een daarvan is de toestemming van betrokken patiënten.
- In de meeste gevallen gaat het bij de verwerkte gegevens via het portaal om **gegevens betreffende de gezondheid** zoals bedoeld in artikel 16 Wbp. Voor het verwerken daarvan verlangt de Wbp een ontheffing zoals in de wet opgesomd. Wanneer de patiënt heeft ingestemd met het gebruik van het portaal voor de zorgtoepassing, dan zorgt dat voor de ontheffing.
- Het verwerken van gezondheidsgegevens stelt zwaardere eisen aan de **beveiliging** van de gegevens dan het verwerken van niet-bijzondere gegevens[11]. Daarbij speelt ook de identificatie, authenticatie en autorisatie van gebruikers een rol.
- Patiënten moeten **geïnformeerd** worden over het gebruik van de toepassingen van het portaal. Daarbij worden de keuzes die de patiënt ter beschikking staan uitgelegd en wordt verteld wat zijn **rechten** zijn.
- De zorgaanbieder maakt **schriftelijke afspraken met de bewerker** over de voorwaarden waaronder de gegevens voor hem zullen worden verwerkt voor de zorgaanbieder. De afspraken gaan onder andere over de bewaartermijn van gegevens, de beveiliging door de bewerker en het toezicht door de verantwoordelijke op de naleving van de afspraken en geheimhouding.
- Het voldoen aan de **Wbp meldplicht**[12].

In het hoofdstuk hierna wordt ingegaan op enkele van de hier genoemde verplichtingen. Achtereenvolgens komt daarin aan de orde de toestemming als grondslag voor het gebruik van het portaal als communicatiemiddel, het uitoefenen van patiëntenrechten waaronder inzage en tot slot de beveiliging van persoonsgegevens.

[9] Er kunnen ook meerdere bewerkers zijn.
[10] Een 'grondslag' heeft hier de betekenis van een bij wet geregelde rechtvaardiging.
[11] Alle 'bijzondere gegevens' waarvoor een aanvullend regime geldt worden beschreven in artikel 16 Wbp. Het gaat onder andere om gezondheidsgegevens en strafrechtelijke gegevens.
[12] Niet vrijgestelde verwerkingen moeten op grond van artikel 27 Wbp worden gemeld aan het CBP ten behoeve van opname in het openbare meldingsregister, tenzij er een Functionaris Gegevensbescherming is ingesteld door de verantwoordelijke. In dat geval ontvangt die de melding. Meer informatie over het melden vindt u op www.cbpweb.nl. Gegevensverwerking via een portaal is niet vrijgesteld van melding.

Hoofdstuk 4 Enkele Wbp verplichtingen toegelicht

4.1 Toestemming

Voor het gebruik van functionaliteit(en) van het portaal in de zorgverlening en behandeling is instemming van de patiënt nodig. 'Uitdrukkelijke' toestemming zoals genoemd in de Wbp is niet nodig wanneer het verwerken van de gezondheidsgegevens noodzakelijk is voor de zorg aan de patiënt of voor het beheer van de instelling[13]. Dit zou bij bepaalde functionaliteiten van het portaal zo kunnen zijn, zoals bijvoorbeeld bij e-consult. Maar vaak zal niet kunnen worden vastgesteld of aan deze voorwaarde is voldaan, in elk geval niet door de verantwoordelijke zorgaanbieder[14]. In dat geval moet worden uitgegaan van uitdrukkelijke toestemming[15]. Voor de praktijk is het niet zo belangrijk om het onderscheid tussen de noodzaak van toestemming of uitdrukkelijke toestemming steeds vast te stellen: het moment van face to face uitgifte van toegangsmiddelen en inloggegevens aan gebruikers leent zich uitstekend voor het vastleggen van toestemming. Zorgverleners zullen die toestemming toch willen vastleggen in verband met een zorgvuldige procedure. Aan uitdrukkelijkheid is in die gevallen dan steeds voldaan. Ook kan men binnen de toepassing de patiënt vragen akkoord te gaan met de voorwaarden van het gebruik[16].

De patiënt moet van toereikende informatie worden voorzien om toestemming voor het gebruik van de toepassing te kunnen geven. Die informatie kan via het publiekelijk toegankelijke deel van de website of het portaal worden gegeven. Ook kan de informatie aan de balie worden verstrekt, alvorens tot vastleggen van toestemming en uitgifte van toegangsgegevens over te gaan.

4.2 Patiëntenrechten via het portaal

Het patiëntportaal is ideaal als hulpmiddel bij het uitvoering geven aan patiëntenrechten. Via het portaal kan informatie worden gegeven en kunnen formulieren worden aangeboden om bijvoorbeeld een afspraak voor inzage in het dossier te maken of een verzoek tot correctie van gegevens in te dienen. De formulieren kunnen in de beveiligde omgeving van het portaal worden verzonden. Het verzoek heeft betrekking op verwerking van gezondheidsgegevens in het dossier waarop het beroepsgeheim rust. De identificatie en authenticatie van de verzoeker dient dan ook zorgvuldig plaats te hebben.

Met de komst van het patiëntportaal heeft de verantwoordelijke er een gegevensverwerking bij gekregen waarop de patiënt zijn rechten kan uitoefenen. Voor zover hij er met de functionaliteit niet zelf toe in staat is gesteld, kan hij ook correctie en verwijdering vragen van gegevens die in deze toepassing worden verwerkt. In elk geval gelden alle Wbp rechten van betrokkenen zoals recht op inzage, afschrift en verbeteren. Maar ook het recht van aanvullen, verwijderen, of afschermen indien de gegevens feitelijk onjuist zijn. Gelet op wat hierboven over de toepassing van de WGBO is opgenomen zijn de daaruit volgende rechten op correctie, aanvulling en vernietiging mogelijk niet in alle gevallen van toepassing. Daarom kan het goed zijn het vernietigingsrecht en wijzigingsrecht van gegevens in de portaalomgeving in de gebruiksvoorwaarden (voor alle gevallen gelijk) te regelen.

4.3 Inzage in medische gegevens

Via het portaal kan de patiënt ook digitale inzage in (onderdelen van) zijn medisch dossier geboden worden. Een patiënt heeft recht op inzage in zijn medische gegevens. Er is nog geen recht op digitale inzage. Dit recht is in nieuwe wetgeving wel voorzien[17]. Een dergelijk recht kan ingevoerd worden wanneer organisatie en techniek gereed zijn om dat op een veilige manier overal te implementeren.

---

[13] Artikel 21 lid 1 onder a Wbp.
[14] Dit kan spelen bij het verwerken van gegevens in een PGD.
[15] Artikel 23 lid 1 onder a Wbp.
[16] De voorwaarden moeten in lijn zijn met de eisen die de wet aan de zorgaanbieder stelt.
[17] Zie bijvoorbeeld Kamerstukken II, 33509 en het voorstel voor de Algemene Verordening Gegevensverwerking.

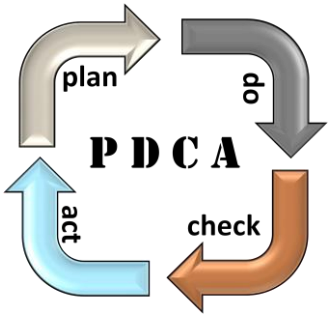
Via patiëntportalen wordt al een stap gezet tot digitale inzage. Deze portalen bieden toegang tot de medische gegevens uit informatiesystemen in het ziekenhuis, zoals inzage in brieven aan de huisarts, inzage in onderzoeksverslagen en in röntgenfoto's. Andere portalen bieden in plaats daarvan inzage in een uittreksel van het dossier waarin onder andere betrokken hulpverleners worden vermeld, medicatiegegevens, laboratoriumuitslagen en afspraken.

Het spreekt voor zich dat rechtstreekse toegang tot informatiesystemen van de zorgaanbieder vanuit beveiligingsoogpunt risicovoller is dan inzage in een afgescheiden, in omvang beperkt, deel. Bij het verlenen van digitale inzage in het dossier gelden alle voorwaarden die ook voor de andere vormen van gegevensverwerking van patiëntengegevens uit de Wbp en de WGBO voortvloeien voor de zorgaanbieder. De belangrijkste zijn hierboven aan bod gekomen.

4.4 Beveiliging van persoonsgegevens

Artikel 13 Wbp schrijft voor dat passende technische en organisatorische maatregelen getroffen moeten worden om persoonsgegevens te beveiligingen tegen onrechtmatige verwerking. Wat passend is hangt af van de aard van de gegevens en de risico's die samenhangen met de voorgenomen verwerking. Gaat het om een complexe of grootschalige verwerking van persoonsgegevens? Wat zijn de gevolgen van een ongeoorloofde inbreuk? Daarnaast bepaalt de stand van de techniek wat haalbaar en reëel is, mede gelet op de kosten van te treffen maatregelen.

Kwaliteitscirkel van Deming
William Edwards Deming (Sioux City (Iowa), 14 oktober 1900 - Washington D.C., 20 december 1993) was een Amerikaanse statisticus. Deming ontwikkelde een 'kwaliteitscirkel' die vier activiteiten beschrijft die op alle verbeteringen in organisaties van toepassing zijn. De vier activiteiten zorgen voor een betere kwaliteit. Het cyclische karakter garandeert dat de kwaliteitsverbetering continu onder de aandacht is.



Zorgaanbieders die een portaal aanbieden zijn verantwoordelijke in de zin van de Wbp voor de gegevensverwerking. De beveiligingsverplichting richt zich daarom tot hen. De verantwoordelijke moet in kaart brengen welk risico gemoeid is met de gegevensverwerkingen. Uit de recent uitgebrachte Richtsnoeren Beveiliging van persoonsgegevens van het CBP volgt dat het inrichten van een Plan Do Check Act (PDCA) cyclus in de organisatie daarvoor nodig is[18]. Het verwerken van gezondheidsgegevens brengt bijzondere risico's met zich mee, mede in verband met de vertrouwelijkheid van de gegevens. Bij elektronische inzage in medische gegevens, zoals hierboven besproken, moet worden uitgegaan van een hoog betrouwbaarheidsniveau of een hoog risico, zoals verwoord in de handreiking Betrouwbaarheidsniveaus voor authenticatie bij elektronische overheidsdiensten van het Forum Standaardisatie[19] en de daarin verwerkte achtergrondstudie van het College Bescherming Persoonsgegevens uit 2001[20]. De toegang tot de inzage-functionaliteit moet daarop ingericht zijn. Hoewel de recente richtsnoeren de eerdere achtergrondstudie opvolgen, is de risicoklasse-indeling uit de achtergrondstudie nog bruikbaar en indicatief voor risico-inschatting.

De eisen aan gegevensbeveiliging bij het verwerken van gezondheidsgegevens, van belang bij de inzet van portalen door de zorgverlener, worden beschreven in NEN-normen voor

[18] CBP Richtsnoeren, Beveiliging van persoonsgegevens, College Bescherming Persoonsgegevens, februari 2013.
[19] Een handreiking voor overheidsorganisaties, Betrouwbaarheidsniveaus voor authenticatie bij elektronische overheidsdiensten, Forum Standaardisatie (BZK).

[20] Achtergrondstudie 23 Beveiliging van persoonsgegevens, College Bescherming Persoonsgegevens, Blarkom & Borking, 2001.

informatiebeveiliging in de zorg[21]. De NEN-normen scheppen een kader voor de te treffen maatregelen en technische vereisten. Daarmee kan een voldoende veilige omgeving voor uitwisseling van patiëntgegevens worden ingericht.

De NEN normen voor informatiebeveiliging in de zorg zijn ook richtinggevend voor de uitwerking van het identiteits management[22]. De keuze van authenticatiemiddelen moet passend zijn gelet op de risico's, de stand der techniek en de kosten. Een werkgroep van het door Nictiz gefaciliteerde platform 'patiënt en eHealth' heeft in februari 2013 een handreiking patiëntauthenticatie gepubliceerd, met handvatten om tot een keuze van authenticatiemiddelen voor patiënten te komen, op basis van een use-case-gebaseerde risicobenadering. Deze handreiking is tot mei 2013 open voor publieke review en zal daarna geactualiseerd worden. De handreiking zal in overeenstemming moeten zijn met de recent gepubliceerde richtsnoeren van het CBP.

Een belangrijk aspect is daarnaast hoe het verlenen van toegangsrechten (autorisatie) tot gegevens is ingericht. Daarbij moet rekening gehouden worden met de vertrouwelijkheid van de gegevens. Voor een PGD van de patiënt is het een breed aanvaard uitgangspunt dat de patiënt het beheer over de toegang tot de gegevens zou moeten hebben[23]. Toch zou het in de praktijk ook zo kunnen zijn dat de zorgverlener mede-behandelaars toegang kan verlenen, binnen de geldende wetgeving.

Het is dus van belang dat de voorwaarden van het gebruik van de toepassing duidelijk zijn, zodat de verwachtingen van de patiënt en de zorgverlener over en weer beantwoord worden. Omdat zorgaanbieders portalen en PGD's aanbieden met elk verschillende functionaliteiten is dit extra belangrijk.

4.5 Tot slot

De ontwikkelingen in toepassingen van het patiëntportaal in de zorgverlening kunnen het juridisch kader nog beïnvloeden, net als andersom. Met een aantal aanvullingen op de wetgeving kan nog beter op nieuwe situaties worden aangesloten. Het huidige kader stelt echter voldoende duidelijke regels zoals in dit paper beschreven. Het is daarbij van belang dat de zorgaanbieder afspraken met de patiënt maakt over de wederzijdse verwachtingen van het gebruik van het portaal. Via informatie en gebruiksvoorwaarden kan worden aangegeven wat de patiënt van de zorgverlener mag verwachten.

Meer informatie

Wilt u meer informatie over wat u in dit paper heeft gelezen? Neem dan contact op met Marinka de Jong van Nictiz (mdejong@nictiz.nl) of Jacqueline Krabben (krabben@privacycare.nl).

Over de auteur

Mr. J.A.L. Krabben is als zelfstandig adviseur op het gebied van gezondheidsrecht, privacywetgeving en IT-recht betrokken bij Nictiz, het landelijke expertisecentrum dat ontwikkeling van ICT in de zorg faciliteert.

[21] NEN 7510/7512 en NEN 7513.
[22] NEN 7510 Informatiebeveiliging in de zorg en NEN 7512 Vertrouwensbasis voor gegevensuitwisseling. De norm NEN 7521 Toegang en uitwisselen van patiëntgegevens is in de maak.
[23] Zie ook Patiëntportalen in Nederland, uitgave Nictiz en NPCF, 16 mei 2011, RP 110013 en De informatiepositie van de patiënt, Het Expertise Centrum, § 3.4

Patiëntenfederatie NPCF is een samenwerkingsverband van patiënten- en consumentenorganisaties die zich sterk maken voor alle mensen die zorg nodig hebben, nu of in de toekomst.

NPCF
@npcf
npcf@npcf.nl
www.npcf.nl

Optimale toepassing van eHealth en ICT in de zorg kan niet zonder standaardisatie. In nauwe samenwerking met zorgverleners, koepelorganisaties, standaardisatieorganisaties en industrie draagt Nictiz zorg voor de ontwikkeling en beschikbaarheid van de noodzakelijke standaarden. We doen dit door het organiseren van gemeenschappelijke ontwikkelprojecten, kennisoverdracht en kwaliteitstoetsing.

Nictiz
@Nictiz
info@nictiz.nl
www.nictiz.nl