5 AANDACHTSPUNTEN BIJ BOUW PATIËNTPORTAAL

Juridisch kader rond medische gegevens is complex

Bij de implementatie van patiëntportalen komt heel wat kijken. Er moet worden voldaan aan verschillende wetten en normen. De interpretatie van dit alles roept veel vragen op. Natascha van Duuren en Anton Ekker zetten de juridische aandachtspunten op een rij. Vijf belangrijke adviezen.

door: NATASCHA VAN DUUREN & ANTON EKKER

De laatste jaren worden steeds meer patiëntportalen op de markt gebracht. Volgens een rapport van het Nationaal ICT Instituut in de Zorg (Nictiz) en de Nederlandse Patiënten Consumenten Federatie (NPCF) waren eind 2010 al ruim veertig patiëntportalen in de lucht. Naar verwachting zal dit aantal de komende jaren snel toenemen.
Een patiëntportaal is een online toegangspoort die de patiënt regie geeft bij het vergaren en delen van medische gegevens en overige informatie over zijn gezondheid. De aard en de opzet van deze portalen is divers. De meeste portalen bieden naast inzage in informatie over de gezondheid aanvullende functionaliteiten aan, zoals een patiëntenforum, het invoeren van zelfmetingen of alerts bij een afspraak of uitslag.
Bij de implementatie van een patiëntportaal dient rekening te worden gehouden met een complex juridisch kader. Zo dient in ieder geval te worden voldaan aan de wet op de geneeskundige behandelingsovereenkomst (WGBO) en de wet bescherming persoonsgegevens (Wbp). Indien gebruik wordt gemaakt van het BSN geldt ook de wet gebruik burgerservicenummer in de zorg (Wgbsn-z). Daarnaast zijn er verschillende beroepsnormen en zogenaamde NEN-normen van toepassing. In de praktijk blijkt de interpretatie van dit geheel aan deels overlappende wetten en normen, veel vragen op te roepen. Vijf belangrijke adviezen.

1. Bepaal duidelijk wie de verantwoordelijke is

Een van de eerste aandachtspunten betreft vaak de vraag welke partij of partijen optreden als 'verantwoordelijke' in de zin van de wet bescherming persoonsgegevens. De verantwoordelijke is degene die het doel en de middelen van de gegevensverwerking bepaalt. In veel gevallen worden bij de gegevensverwerking daarnaast derde partijen ingeschakeld die onder het gezag van de verantwoordelijke handelen. Het kan gaan om bijvoorbeeld een IT-leverancier of een hostingpartij. De verantwoordelijke is verplicht om met een dergelijke 'bewerker' contractuele afspraken te maken, onder andere over informatiebeveiliging.
Aangezien bij een patiëntportaal vaak meerdere partijen betrokken zijn, is niet altijd duidelijk wie voor een specifieke verwerking de verantwoordelijke is. Voor het voldoen aan de Wbp en voor het uitoefenen van patiëntenrechten is het echter wel van essentieel belang de verschillende rollen vast te stellen en deze contractueel vast te leggen.

2. Garandeer patiëntenrechten

De gebruiker van een patiëntportaal heeft verschillende rechten met betrekking tot de verwerking van zijn gegevens. Zo dient de verantwoordelijke de gebruiker vooraf te informeren over het doel van het portaal en wie daarvoor verantwoordelijk is. Daarnaast is de uitdrukkelijke toestemming van de gebruiker vereist voor de verwerking van diens patiëntgegevens. Bovendien dient de gebruiker er op te worden gewezen dat hij bezwaar kan maken tegen de verwerking van zijn gegevens en dat hij zijn toestemming op elk moment kan intrekken (en op welke wijze). Dit volgt uit zowel de Wbp als de Wgbo. Vereist is dat deze toestemming 'uitdrukkelijk' is gegeven. Op degene die patiëntgegevens verwerkt rust een dubbele bewijslast: in de eerste plaats moet bij twijfel bewezen kunnen worden dat een bepaalde toestemming is verleend en waarvoor. Daarnaast zal zo nodig bewezen moeten worden dat de toestemming aan de gestelde eisen voldoet. Het gevolg van het niet voldoen aan dit vereiste is verstrekkend: als de toestemming niet aan bovenstaande vereisten voldoet, is zij nietig en kan de informatie van de desbetreffende gebruiker dus niet via het portaal worden verwerkt.

3. Zorg voor beveiligde toegang

Op grond van de wet bescherming persoonsgegevens (Wbp) dient de verantwoordelijke 'passende technische en organisatorische maatregelen' te treffen om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Een van die passende technische en organisatorische maatregelen is identificatie en authenticatie. Gegarandeerd dient te worden dat veilige toegang wordt geboden, middels identificatie en authenticatie ('zeggen wie je bent' en 'bewijzen dat je bent wie je zegt dat je bent').
Er is momenteel nog veel onduidelijkheid over de vraag hoe deze veilige toegang kan worden gegarandeerd. De eerste vraag die daarbij dient te worden gesteld is: welke soort informatie of diensten worden via het portaal ontsloten en welk veiligheidsniveau is daarbij vereist? Authenticatie ('bewijzen dat je bent wie je zegt dat je bent') wordt op dit moment op verschillende manieren geregeld (zie kader). Voor identificatie kan gebruik worden gemaakt van het burgerservicenummer (BSN). Het gebruik van het BSN is echter uitsluitend voorbehouden aan zorgaanbieders.

4. Wees voorbereid op datalekken

De Nederlandse overheid en de Europese Commissie dienden onlangs voorstellen in voor een wettelijke meldplicht bij datalekken. Het Nederlandse wetsvoorstel zal naar verwachting als eerste in werking treden en introduceert de plicht voor bedrijven en overheden om een datalek zo snel mogelijk te melden bij het College Bescherming Persoonsgegevens. Als een datalek niet wordt gemeld, kan het CBP de desbetreffende verantwoordelijke een boete opleggen van maximaal 200.000 euro.
Wanneer een datalek zich voordoet bij een patiëntenportaal zal de verantwoordelijke verschillende stappen moeten zetten om aan zijn wettelijke verplichtingen te voldoen. Het is daarom belangrijk om na te denken over een heldere interne procedure. Hierin kan onder andere worden geregeld wie er intern op de hoogte moet worden gesteld en hoe wordt bepaald of er een melding moet worden gedaan. Daarnaast moeten zo snel mogelijk maatregelen worden getroffen om de negatieve gevolgen van de inbreuk te beperken. Ten slotte moeten de betrokkenen snel en adequaat worden geïnformeerd.
Ook voor IT-leveranciers van patiëntportalen brengt de meldplicht vergaande verplichtingen met zich mee. Zij zijn verplicht de zorgverlener of zorginstelling actief bij te staan en te waarschuwen als zij een inbreuk vaststellen.

5. Houd rekening met komende regelgeving

Er is een nieuwe Europese Privacyverordening op komst waarin strengere regels zijn opgenomen. Zo moeten betrokkenen een kopie van hun opgeslagen persoonsgegevens kunnen krijgen om deze gegevens over te kunnen dragen aan een ander (recht van gegevensoverdraagbaarheid). Bovendien krijgen betrokkenen 'het recht om vergeten te worden'. Verantwoordelijken zullen op verzoek van betrokkenen onmiddellijk actie dienen te ondernemen om alle persoonsgegevens van betrokkenen te verwijderen. Zij moeten er daarbij voor zorgen dat ook derde partijen aan wie zij de gegevens hebben verstrekt, deze gegevens verwijderen. Deze regels leggen strenge eisen op aan de (technische) werking en inrichting van patiëntportalen. Het is de vraag of de huidige patiëntportalen, technisch gezien, al aan deze eisen kunnen voldoen.
Door in een vroeg stadium rekening te houden met de genoemde aandachtspunten worden de rollen en verantwoordelijkheden van de verschillende betrokken partijen duidelijker. Daarnaast wordt de kans verkleind dat de rechten van de patiënt worden geschonden. Hiermee worden ook de aansprakelijkheidsrisico's beperkt. «

Patiëntportalen

Eind 2010 waren er al meer dan veertig patiëntportalen in de lucht. Naar schatting zijn dit er inmiddels bijna honderd. Een van deze patiëntportalen is Zorgportaal Rijnmond (www.zorgportaalrijnmond.nl). Dit portaal biedt onder meer de volgende functionaliteiten:

- ZorgInfo TV, internetvideovoorlichting met de mogelijkheid om schriftelijk te reageren tijdens live-uitzending;
- afspraak plannen bij ziekenhuizen in de regio Rijnmond;
- zelfmetingen invoeren;
- digitale VraagWijzer;
- diverse onlineformulieren (waaronder anamnese).

Voor een beperkt aantal patiënten(groepen):

- inzage in brieven van specialisten aan huisartsen;
- zelfmanagement dagboeken;
- toegang tot kerndossier.

AL BIJNA HONDERD PATIËNTPORTALEN IN DE LUCHT

AUTHENTICATIE

Authenticatieniveaus worden in NEN 7512 onderverdeeld in zwak, matig en sterk. De NEN 7512 schrijft voor dat het authenticatieniveau moet worden vastgesteld op grond van een risicoanalyse. In de praktijk zijn onder meer de volgende authenticatiewijzen te onderscheiden:

- gebruikersnaam en wachtwoord;
- gebruikersnaam en wachtwoord met een (bijvoorbeeld via SMS verstuurde) eenmalige code;
- DigiD (laag en midden);
- certificaat met persoonlijke gebruikerscode;
- certificaat aangebracht op een smartcard (persoonlijke pas), met persoonlijke gebruikerscode.


Anton Ekker is juridisch adviseur bij het Nationaal ICT Instituut in de Zorg (Nictiz) en advocaat te Amsterdam (www.ehealthlaw.nl).

Natascha van Duuren is advocaat en partner bij De Clercq Advocaten Notarissen te Leiden (www.declercq.com).

Voor reacties en nieuwe bijdragen van IT-experts:
Henk Ester,
070 3780397
h.ester@sdu.nl