

Achter de feiten aan

Auteur's: Jaap van der Wel en Berend de Vries
Foto: Frank Muller

De regionale gegevensuitwisseling is nog niet veilig genoeg. EPD-wetgeving zou hier in kunnen voorzien. Echter die laat vooralsnog op zich wachten.

Het College Bescherming Persoonsgegevens (CBP) onderzocht twee regionale informatie-uitwisselingen in de zorg en signaleerde medio 2009 ernstige tekortkomingen in de privacybescherming. Waarschijnlijk kunnen meer regio's de toets der kritiek niet doorstaan. Dit is een serieus probleem. Binnen de regio's bestaan vele banden - tussen familie, bekenden, school, werk, sportvereniging - en juist die kunnen aanleiding zijn voor gegevensmisbruik. En dit probleem betreft het grootste deel van alle Nederlandse patiënten want dat is inmiddels het bereik van de gezamenlijke regionale informatiesystemen. Het CBP onderzocht de beveiliging aan de hand van een toetslijst die werd afgeleid uit de Wet bescherming persoonsgegevens (Wbp) en de bepalingen over de geneeskundige behandelingsovereenkomst, zie kader 1. Eén toetspunt van die lijst, informeren van patiënten over de gegevensuitwisseling, volgde direct uit de wet. Andere punten zijn uitwerkingen, bijvoorbeeld de eis van gestructureerde logging waarbij op 'verdachte situaties' wordt gecontroleerd. Dat laatste is voor het CBP een middel om onbevoegde artsen te weren door achteraf vast te stellen of de behandelrelatie bestaat. Onduidelijk is of men

ook denkt aan controle op gegevensverkeer dat wijst op aanvallen van hackers. Er zijn wel meer beveiligingsmaatregelen te bedenken dan die van de toetslijst van het CBP. Zo is voor informatievoorziening over internet belangrijk dat een arts zich identificeert met méér dan alleen een wachtwoord. Bij elektronisch bankieren is al jaren een extra beveiliging in zwang, voor de ING TAN-codes en de voor de Rabobank en de ABNAMRO de chip en pincode van de bankpas, afgelezen door

Duidelijk is dat de toetspunten van het CBP onvolledig zijn voor de veiligheid van het patiëntendossier

een speciaal leesapparaat. De techniek van de UZI-pas voor het landelijk Patiëntendossier is daarmee vergelijkbaar. Een hacker heeft zo niets aan een afgeluisterd wachtwoord. Duidelijk is dat de toetspunten van het CBP onvolledig zijn voor de veiligheid van het patiëntendossier. Een volledige toets zou echter te veel werk zijn geweest. Vragen naar een risicoanalyse informatieveiligheid was in theorie ook mogelijk geweest. Dit zou echter hebben geleid tot veel dubbel werk tussen alle regio-organisaties: kostbaar en vertragend. En het ontbreekt dan nog aan de standaardisatie die nodig is voor de invoering van toegangspassen. Die zijn hard nodig in de eerste lijn want bij tal van internettoepassingen - gelukkig niet alle - volstaat een gebruikersnaam en een wachtwoord om vertrouwelijke patiëntgegevens in te zien.

Dat het CBP problemen constateert, is terecht. Maar bij een poging om die op te lossen, berispt het de zorginstanties publiekelijk op basis van regels die ad hoc uit de wet worden afgeleid, in het zorgveld niet vooraf bekend waren en blind zijn voor vele essentiële beveiligingsrisico's. Dit is dweilen met de kraan open, een weinig productieve en voor het zorgveld frustrerende aanpak. Begin 2009 constateerden de kamerleden Omtzigt (CDA) en Vermeij (PvdA) deze hiaten in de regelgeving ook al. Bij de behandeling van het wetsvoorstel voor het landelijk EPD dienden zij een motie in om het toepassingsgebied van het wetsvoorstel uit te breiden naar alle grootschalige zorginformatiesystemen (kader 2).

Discussie

Dit wetsvoorstel ligt nu bij de Eerste Kamer. De Eerste Kamer heeft vorig jaar vragen gesteld die na de zomer zijn beantwoord. Eind 2009 heeft er een expertmeeting plaatsgevonden en eind maart zal er nog een tweede expertmeeting plaatsvinden, waarna de behandeling zal volgen. Ondertussen woeden discussies in de pers zoals begin februari in Webwereld.nl en Medisch Contact over de ontbrekende controle vooraf op de patiëntrelatie. In vergelijking met de vele problemen bij de regionale dossiers is dit probleem niet urgent. Het wetsvoorstel verplicht namelijk al tot een dergelijke controle achteraf met een logprocedure en een klantloket waar patiënten kunnen nagaan wie in het dossier heeft gekeken, een novum. De controle vooraf op de behandelrelatie is zelfs deels al gerealiseerd door te toegang te beperken tot het domein van de raadpleger maar kan nog beter. Dat kost tijd omdat onder andere de informatiesystemen van aangesloten zorgverleners moeten worden aangepast. Vooruitlopend op de wetgeving zijn al 'proeftuinen' voor het landelijk EPD ingericht en de beveiliging daarvan steekt gunstig af tegen menig bestaand systeem in de regio en voor beroepsgroepen. Dat hoeft niet te verbazen want die proeftuinen zijn van recenter datum. Ondersteund met de conceptwetgeving voor het landelijk EPD konden

Onderzoek regionale EPD's

Bij het onderzoek aan de regionale EPD's ging het CBP uit van de Wet bescherming persoonsgegevens en de bepalingen over de Geneeskundige Behandelingsovereenkomst uit het Burgerlijk Wetboek. Het CBP concretiseerde dit alles met de volgende eisen:

- De zorgverlener moet een behandelrelatie hebben met de patiënt voor gegevenstoegang;
- Raadpleging wordt gelogd;
- Deze logging wordt gecontroleerd waarbij een selectie mogelijk is op verdachte situaties;
- Over deze logging worden afspraken gemaakt met de zorgverleners;
- Patiënten worden persoonlijk geïnformeerd en kunnen afzien van deelname.



De zorgverlener moet een behandelrelatie hebben met de patiënt voor gegevenstoegang.

daarin de nieuwste beveiligingsinzichten worden toegepast.

De wetgever kan de ontwikkelingen van ict in de zorg niet bijbenen. Het huidige wetgevingstraject is rond 2004 gestart, vier jaar na het begin aan het Landelijk EPD met de oprichting van Nictiz. Als de Eerste Kamer in de zomer van 2010 akkoord gaat - zeker is dat nog niet - dan kost het nog minimaal twee jaar om tot uitvoering van de wet

komen. Waarschijnlijk duurt dit langer omdat in het wetsvoorstel is gekozen voor de tijdrovende weg om de uitvoeringsbesluiten aan het parlement voor te leggen. Na de late start van het wetgevingstraject kost het zo nog eens minimaal acht jaar om van idee tot realisatie te komen. De uitgroei van het internet van medium voor freaks met inbelijnen tot cruciale infrastructuur gebaseerd op 'elektronische snelwegen', verliep veel

sneller. En inmiddels groeit ook de proeftuin van het landelijk EPD pijlsnel: het zou naar verluid nu al van circa één miljoen dossiers de gegevens uitwisselen en is daarmee al één van de meest grootschalige systemen binnen de Nederlandse zorg.

Het landelijk EPD is nu al één van de meest grootschalige systemen binnen de Nederlandse zorg

Motie Omtzigt / Vermeij

De motie Omtzigt / Vermeij heeft betrekking op de 'Wijziging van de Wet gebruik burgerservicenummer in de zorg in verband met de elektronische informatie-uitwisseling in de zorg'. Deze wetswijziging is nodig voor de invoering van het landelijk EPD die nu bij de Eerste Kamer ligt.

Artikel 13hb van dit voorstel is afkomstig van de motie Omtzigt / Vermeij die door de Tweede Kamer werd aangenomen. Hiermee werd de werking van het wetsvoorstel uitgebreid naar zorginformatiesystemen:

- die op elkaar zijn aangesloten anders dan via het landelijk schakelpunt, of
- waarvan meer dan één zorgaanbieder gebruik kan maken.

Voor de uitwerking van de details verwijst het artikel naar uitvoeringsbesluiten. In de motie staat ook wat moet worden uitgewerkt:

- alleen beroepsbeoefenaren hebben toegang;
- alleen toegang als er een behandelrelatie is met de betreffende cliënt;
- de cliënt moet bezwaar kunnen maken tegen opname van gegevens en de mogelijkheid hebben om die te laten wissen;
- de cliënt heeft inzage in de gegevens zelf en in de loggegevens. Bij voorkeur moet een cliënt die kunnen inzien op dezelfde manier en plaats als dat mogelijk wordt gemaakt voor het landelijk EPD;
- de toegang vereist een UZI-pas als dat technisch uitvoerbaar is;
- de eisen voor goed beheerd zorgsysteem zijn van toepassing;
- bestuurlijke boete bij overtreding van de bepalingen.

Kortom, alle - terechte - zorgen bij de volksvertegenwoordigers over de patiëntenprivacy leiden er paradoxaal genoeg toe dat dringend noodzakelijke verbeteringen van de informatiebeveiliging niet kunnen worden gebaseerd op wettelijke maatregelen. Op lager niveau van regelgeving is de norm voor Goed Beheerd zorgsysteem van het Nictiz een belangrijke stimulans voor verbeteringen gebleken voor de systemen die gaan aansluiten op het landelijk EPD. Dat neemt niet weg dat een vlotte realisatie van het wettelijk kader van groot belang is, zeker voor de vele systemen die nog niet gaan aansluiten. Eventuele gaten kunnen later wel gerepareerd worden. <

Jaap van der Wel is auteur van 'Informatiebeveiliging in de Zorg' en met drs. Berend de Vries verbonden aan Comfort-IA (www.comfort-ia.nl)