Position paper Tweede Kameroverleg, 6 maart 2013.

Hoe privacy-innovatie in de zorg (niet) te stimuleren

Guido van 't Noordende, Universiteit van Amsterdam[i]

De Eerste Kamer riep na de afwijzing van de wet-EPD 31 466 op tot het stellen van eisen, normen en standaarden voor de beveiliging van systemen voor push- en pull communicatie binnen de wettelijke kaders van Wbp, Wet BIG, en Wgbo. Dit moest leiden tot een bottom-up verbetering van bestaande (regionale) systemen. Zeggenschap over de eigen medische gegevens was en is een belangrijk punt. De motie Tan Y stelde een onderzoek naar een autorisatiepas voor patiënten voor. De Eerste Kamer wilde geen opt-out, maar wilde een opt-in systematiek (zie o.a. Kamerstukken I, 2010-2011, 31 466 AB). De vraagstelling voor het rondetafelgesprek is: “Voldoet het wetsvoorstel aan de privacy-eisen voor het uitwisselen van medische gegevens?” Het antwoord kan kort zijn: nee.

Wetsvoorstel 33 509 regelt enkele zaken, op een problematische manier. In artikel 23a lid 2 en 15a lid 2 wordt een recht gedefinieerd waarmee cliënten (categorieën van) zorgvaanbieders kunnen *uitsluiten* van toegang. Dit creëert een opt-out systeem, gestapeld bovenop een generieke opt-in. Onder Wbp en Wgbo dient toestemming uitdrukkelijk, goed geïnformeerd, en voor een specifiek doel te zijn. Het wetsvoorstel kan echter een generieke opt-in legitimeren, doordat naar het recht op uitsluiting kan worden verwezen. Ook de MvT geeft aan dat aan een (eenmalige) generieke toestemming gedacht wordt. Gaat dit werken? Nee. Moet een patiënt straks via een internetportaal 76 categoriëen van zorgverleners uitsluiten om te zorgen dat alleen apothekers de medicatiegegevens mogen inzien? En wat bij aanpassing van de categoriëen? Een opt-out systeem is onoverzichtelijk en voldoet alleen al om die reden niet aan de wettelijke kaders van Wbp en Wgbo. Verder wil de minister bij AMvB (zonder voorhangprocedure) specifieke “functionele en technische” eisen aan het veld kunnen opleggen. Welke eisen dit zijn maakt het voorstel – bijna twee jaar na afwijzing van de wet-EPD – niet duidelijk.

Interessant is vooral wat er in het wetsvoorstel niet geregeld wordt. Het wetsvoorstel bevat geen heldere, duidelijke en generiek toepasbare beveiligingseisen om bestaande push- en pull-systemen mee te verbeteren. Het biedt geen leidraad aan zorgverleners en leveranciers over hoe zij in de praktijk om moeten gaan met beveiliging en opt-in toestemming[ii]. Hoe de zeggenschap voor de patiënt over de ontsluiting van de eigen gegevens - voor verschillende bestaande systemen in de zorg – geregeld moet worden, blijft een open vraag.

Voor een betere privacybescherming in de zorg zijn heldere kaders en stimulerend beleid nodig. Is er beleid om bestaande of nieuwe push- en pull systemen te ontwikkelen en beter te beveiligen, of om privacy-innovatie te stimuleren? Daar is in het wetsvoorstel niets van te zien.

De volgende zaken zijn mijns inziens van belang voor privacy-innovatie in de zorg:

- De zeggenschap voor patiënten (en artsen) inzake de ontsluiting van gegevens moet sterk worden verbeterd. Tenminste is een heldere uitwerking van de – uit Wbp en Wgbo volgende – uitdrukkelijke en doelgebonden toestemming nodig, waarna patiëntgegevens volgens afspraak alleen uitgewisseld worden met de vooraf vastgestelde (groep(en)) zorgaanbieder(s).
- “Goed opdrachtgeverschap” moet worden bevorderd zodat zorgverleners heldere (beveiligings)eisen aan leveranciers kunnen stellen, bijvoorbeeld ter versleuteling van praktijkgegevens in *back-end* databases. Van belang is minimaal dat zorgverleners autorisatie goed zelf kunnen regelen, en dat zij verschillende vormen van toestemming kunnen registreren.

- Het is belangrijk om bestaande systemen te behouden en te verbeteren die van evidente waarde zijn voor zorgverleners in verschillende situaties in de praktijk. Bijvoorbeeld beveiligde email voor *push* communicatie, zoals Edifact berichtenverkeer[iii].
- Scheid zorginhoudelijke standaarden van communicatie- en beveiligings-standaarden. Gestandaardiseerde berichten kunnen in verschillende uitwisselingssystemen gebruikt kunnen worden. *Lock-in* van een specifieke infrastructuur (zoals het LSP) moet vermeden worden.
- Leg eenvoudige regels vast rond beveiliging kunnen als basis voor veilige communicatie in bestaande en toekomstige systemen. Zoals publieke sleutel (PKI) technologie voor de versleuteling en authenticatie van berichten in push- en pullsystemen, bij email, en bij het *uploaden* van gegevens naar *personal health records*. Daarnaast kunnen regels en richtlijnen gesteld worden rond (lokale) authenticatie, autorisatie en logging in zorgsystemen.
- Geef patiënten die dat willen het recht om voor de beveiliging van hun gegevens een authenticatie (en PKI identificatie) pas te gebruiken, als zij dat willen, ten behoeve van onder meer *autorisatie van zorgverleners* via een digitale handtekening[iv].
- Verplicht PIA's en stimuleer gebruik van beveiligingstechnieken die *'feature creep'* en toegang tot gegevens door derden - zoals vreemde mogendheden - op voorhand voorkomen (zoals *end-to-end* authenticatie en versleuteling van berichtenverkeer).
- Ontwikkel een visie rond kwaliteitsbewaking van (medicatie)dossiers. Wie is de *dossierhouder*? Ontwikkel communicatiemodellen om dossierhouders van informatie te voorzien, ook wanneer patiënten niet mee willen doen met (grootschalige) pull systemen zoals het LSP.
- Voorkom dat de zorg afhankelijk wordt van één of enkele systemen. Niemand is gebaat bij een risicovolle *systeemafhankelijkheid*, ook vanuit het oogpunt van *cybersecurity* dreigingen. Schep daarom kaders rond beslissingsvrijheid, concurrentie en financiering om een vrij speelveld voor communicatietechnieken mogelijk te maken.

Gegeven recente ontwikkelingen rond het LSP lijken ook de volgende punten van belang:

- Garandeer dat zorgverleners vanuit hun professionele rol de eindverantwoordelijkheid -en (financiële) beslissingsruimte- behouden om zelfstandig keuzes te maken ten aanzien van de manier (techniek) van ontsluiting van dossiers, afhankelijk van de patiënt en de situatie.
- Zorg voor reële, neutrale vergoedingen voor zorgverleners zodat zij objectief voorlichting kunnen geven over communicatiesystemen, en zodat zij ICT functionaliteiten kunnen (laten) ontwikkelen die privacy beter beschermen.
- Garandeer dat zorgverzekeraars of andere private partijen geen (financiële, morele) invloed kunnen en mogen uitoefenen op de beslissingen die op micro-nivo (bij de arts in de spreekkamer) binnen de arts-patiënt relatie worden genomen - zoals over het al dan niet uitwisselen van gegevens.

Het wetsvoorstel geeft, bijna twee jaar na de afwijzing van de wet-EPD, geen antwoord op kernvragen rond beveiliging en zeggenschap over de ontsluiting van patiëntgegevens. De manier waarop Wbp en Wgbo uitdrukkelijke toestemming wordt uitgebreid met een “recht op uitsluiting” van (groepen van) zorgaanbieders is vanuit privacyperspectief contraproductief.

Het wetsvoorstel en beleid lijken niet erg gericht op het beschermen van privacy in de praktijk, of op het stimuleren van technieken die privacy en beveiliging echt kunnen verbeteren. Praktische richtlijnen voor beveiliging en privacybescherming (toestemmingsprocedures, autorisatie) en privacy-innovatie zijn belangrijk. Hiervoor is geen wijziging van wet nodig, maar op privacy gericht beleid.

[i] De uitnodiging voor het rondetafelgesprek is gebaseerd op kennis en ervaring met het onderwerp opgebouwd sinds mijn onderzoek naar de beveiliging en privacybescherming van het Landelijke EPD/LSP in 2010 [1], [2], waarover ook naar de Eerste Kamer en het ministerie van VWS is gerapporteerd [3]. Informatie hierover en latere aanvullingen zijn te vinden op http://www.science.uva.nl/~noordend/epd/ .

[ii] Dat richtlijnen nodig zijn blijkt uit de huidige opt-in praktijk bij het LSP. Hier krijgen patiënten soms een folder van VZVZ mee waaruit een brede toestmming blijkt, terwijl hen wordt gevraagd “mogen wij toestemming om uw gegevens uit te wisselen met de huisartsenpost?” en een ja op die vraag wordt als toestemming genoteerd. De gestelde vraag is helder en begrijpelijk. Echter, de onderliggende LSP infrastructuur implementeert de beperking “huisartsenpost” helemaal niet, en de VZVZ folder maakt duidelijk dat uitbreiding van toegang in de toekomst mogelijk is. Gegeven de brede toestemming is opnieuw toestemming vragen niet nodig. De toestemmingsvraag die aan patiënten gesteld is deugt dus niet.

[iii] Enkele ideëen. In plaats van (of naast) een landeijk schakelpunt kan gedacht worden aan regionale pull systemen op basis van moderne, flexibele standaarden (bijv. IHE), die op de regio-randen eventueel koppelbaar zijn via een bovenregionale index. Dit kan worden aangevuld met push communicatie tussen regio's (bijvoorbeeld voor ontslag- en \medicatie-berichten naar dossierhouder, en voor doorverwijzing naar ziekenhuizen). Daarnaast kan een landelijke noodgegevens-database (allergieëen, medicatie-samenvatting van complexe patiënten) worden opgezet. Zo kunnen voor verschillende functies, toepassingen en soorten zorgverleners/patiëntgegevens verschillende 'netwerken' worden opgebouwd, elk met een in de betreffende conrtext eenvoudig begrijpelijke specifieke toestemming, en daarmee bescherming en zeggenschap. Met eventueel, slechts dan wanneer nodig en met toestemming van de patiënt, aan elkaar gekoppelde netwerken voor grootschaliger ontsluiting. In aanvulling kan een autorisatiepas worden uitgegeven voor patiënten die dat willen, voor betere bescherming van gegevens naarmate de ontsluiting van gegevens op grotere schaal plaatsvindt envoor het veiliger inloggen op portalen. Er bestaan online persoonlijke gezondheidsdossiers waarin (alleen op verzoek van patiënten) medische gegevens kunnen worden geüpload, welke eventueel door patiënten zelf kunnen worden aangevuld. Aldus ontstaat een systeem van ieder op zichzelf kleinschaliger en beheersbaarder systemen, zodat het mogelijk wordt om op elke zorgbehoefte afgestemd elektronisch te communceren, maar wel met zeggenschap en concrete controle voor patiënt en zorgverlener.

[iv] Een dergelijke pas wordt soms ten onrechte een 'zorgpas' genoemd. Uit overleg in de Eerste Kamer (Kamerstukkken I vergader jaar 2010-2011, 31466 AB) blijkt dat senator Tan een autorisatie pas zinvol achtte voor de autorisatie van zorgverleners. Echter, de minister liet alleen onderzoek doen naar een *opslagpas* (zie rapport “Digitale toegang tot het eigen medische dossier, PriceWaterhouseCoopers, 25-11-2011) en naar het inloggen op portalen. Een (optionele) autorisatiepas (digitale sleutel) waarmee patiënten hun zorgverleners kunnen autoriseren is nooit afdoende onderzocht. In de concept-gedragscode voor communicatie in de zorg *EGiZ* wordt de mogelijkheid van gebruik van zo'n pas ('digitale handtekening voor autorisatie') overigens wél genoemd.

Referenties

[1] G.J. van 't Noordende "A Security Analysis of the Dutch Electronic Patient Record System", Technical Report UVA-SNE-2010-01, Universiteit van Amsterdam, 2010

[2] G.J. van 't Noordende, "Security in the Dutch Electronic Patient Record System", 2nd ACM CCS Workshop on Security and Privacy in Medical and Home-Care Systems (SPIMACS), Chicago, Illinois, USA, October 8, 2010.

[3] Brieven aan de vaste Kamercommissie VWS/JG van de Eerste Kamer, en aan de minister van Volksgezondheid, Welzijn en Sport (VWS), 18 februari 2010., te vinden via http://staff.science.uva.nl/~noordend/epd/letter.html .