Project: BelRAI
Auteur: Bert Paepen
Datum: 17/01/2008

mediacentrum
K.U.LEUVEN

BelRAI privacy nota

Versies:

Versie	Datum	Auteur	Beschrijving
0.1	16/01/2008	Bert Paepen	Eerste versie
0.2	17/01/08	Bert Paepen, Anja Declerq, Nicolas Piette	Kleine correcties

Centrum voor Usability Onderzoek - K.U.Leuven
Parkstraat 45 bus 3605 – B-3000 Leuven
TEL. +32(16)32.32.09 FAX +32(16)32.32.10
http://www.kuleuven.be/cuo/

1 Inleiding

Deze nota geeft een samenvatting van de maatregelen genomen in het BelRAI project ter bescherming van de privacy van de gebruikers van het BelRAI systeem (zorgverleners) en hun zorgcliënten. Er wordt tevens een antwoord gegeven op een aantal vragen en bedenkingen in verband met privacy vanuit de sector.

2 Privacy maatregelen in belRAI.org website

Sinds het begin van het Interface project (voorloper van BelRAI) is het onderzoeksteam zich sterk bewust van de privacy problematiek die zich in het project stelt. Daarom zijn bij het ontwerp van de BelRAI applicatie de bescherming van de persoonlijke levenssfeer en van het medische geheim steeds centraal gesteld. Dit is vooral belangrijk gezien het feit dat dit een webapplicatie is waarop (para)medische gegevens over zorgcliënten gedeeld worden tussen een multidisciplinair team van zorgverstrekkers.

De beveiligingsmaatregelen in de belrai.org website houden hiermee rekening op de best mogelijke manier, voor zover de huidige status van de techniek en de beschikbare middelen in het project dit toelaten. Toegang tot de site is strikt beperkt op een “need to know” basis: zorgverleners kunnen enkel die informatie over cliënten raadplegen die ze strikt nodig hebben om hun zorgtaken uit te voeren. Dit wordt afgedwongen door een aantal veiligheidsfilters die op basis van de rol van een zorgverlener, bepalen tot welke soorten informatie over een cliënt deze toegang heeft. Vooraleer informatie over een cliënt in het systeem kan opgenomen worden dient die cliënt een “informed consent” formulier te ondertekenen waarin zijn rechten worden toegelicht en waarmee hij expliciet toestemming geeft om zijn gegevens op te nemen in het BelRAI systeem. Tenslotte fungeert de cliëntbeheerder (gestionnaire de cas) als een vertrouwenspersoon naar de cliënt toe: alleen hij bepaalt wie er toegang heeft tot de gegevens van zijn cliënt. Hij fungeert ook als contactpersoon om de cliënt toegang te verlenen tot zijn persoonlijke gegevens, verbetering te vragen, of zijn informed consent weer te laten intrekken.

Deze maatregelen zijn in meer detail beschreven in het “privacy policy” document, dat beschikbaar is op www.belrai.org voor mensen die ingelogd zijn.

Het is belangrijk te benadrukken dat de BelRAI gegevensverzameling enkel kadert in het onderzoeksproject BelRAI, dat tot doel heeft de mogelijkheden tot toekomstige implementatie van RAI in België te onderzoeken, onder meer door een analyse van de voorwaarden die nodig zijn voor een performant gebruik van dit instrument.

Vragen rond het juridische kader worden beantwoord in het document “BelRAI Nota” van Jos Dumortier dd. 14/01/08.

3 Vragen/bedenkingen uit de sector

Op 16/1 werd ons een nota bezorgd van de FAG (Forum des Associations de Généralistes ASBL) waarin bedenkingen worden geuit bij het privacy probleem in het BelRAI project (en ook in andere projecten).

We geven een toelichting bij de BelRAI privacy maatregelen om een antwoord te geven op deze vragen.

« Les données de santé transmises par informatique doivent être anonymisées, et ne peuvent en aucun cas être mises en relation avec une personne identifiée ou identifiable »

Het BelRAI systeem maakt momenteel enkel een primair gebruik van gezondheidsgegevens met als doel de zorg beter af te stemmen op de concrete zorgbehoefte van een cliënt. Dit betekent dat zorgverleners enkel toegang kunnen hebben tot gegevens over een zorgcliënt als ze bij het zorgproces van die cliënt betrokken zijn en dit op een strikte “need to know” basis. Bij dit soort van toepassing is het anoniem of gecodeerd gebruik van gegevens onmogelijk, omdat zorgverleners moeten weten voor welk cliënt ze gegevens invullen. Het voeren van het BelRAI onderzoek is bijgevolg onmogelijk met anonieme gegevens. In overeenstemming met het uitvoeringsbesluit van 13

februari 2001 wordt daarom de expliciete toestemming van de cliënt vereist in de vorm van een ondertekend informed consent formulier.

« Le traitement de données de santé est interdit, sauf s'il est nécessaire à l'administration de soins dans l'intérêt de la personne concernée, et que les données sont traitées sous la surveillance d'un professionnel des soins de santé. (Art 7 Loi du 08/12/1992)»

L'article 7.§2 de ce loi dit que "l''interdiction de traiter les données à caractère personnel visées au § 1er ne s'applique pas dans les cas suivants : (suit une liste de 12 cas dans lesquels le traitement de données relatives à la santé est autorisé). Sous la lettre k) de cette liste on lit: "lorsque le traitement est nécessaire à la recherche scientifique et est effectué conformément aux conditions fixées par le Roi, par arrêté délibéré en Conseil des ministres, après avis de la Commission de la protection de la vie privée".

Het gaat hier om wetenschappelijk onderzoek, uitgevoerd in opdracht van de FOD Volksgezondheid, Veiligheid van de Voedselketen en Leefmilieu.

« Le traitement automatisé de données de santé doit faire l'objet d'une déclaration préalable à la Commission de Protection de la Vie Privée (CPVP) et mentionner l'identité du responsable du traitement, les finalités du traitement, l'existence d'un droit de s'opposer à un usage à des fins de « direct marketing », les catégories de données de santé, la liste des catégories de personnes ayant accès aux données, et l'existence d'un droit d'accès et de rectification des données.... »

Deze aanvraag werd reeds gedaan tijdens het Interface project en wordt momenteel voorbereid voor het BelRAI onderzoek. Onduidelijkheid rond wie deze aanvraag moet indienen (FOD of onderzoeksequipe) zorgde voor enige vertraging.

De verantwoordelijke, doel van het onderzoek, recht op weigering, recht op toegang en verbetering worden vermeld in de privacy policy en het informed consent formulier. De categorieën van gezondheidsgegevens en een lijst van categorieën van zorgverleners die toegang hebben tot de informatie, zijn momenteel nog niet publiek beschikbaar maar zullen gepubliceerd worden.

« Les données doivent être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont obtenues. (Art 4 Loi du 08/12/1992)

Les données à caractère personnel relatives à la santé doivent être collectées auprès de la personne concernée, et ne peuvent être collectées auprès d'autres sources qu'à condition que la collecte soit nécessaire aux fins de traitement ou que la personne concernée ne soit pas en mesure de les fournir elle-même. (Art 7 Loi du 08/12/1992) »

In het BelRAI systeem worden enkel die gegevens verzameld die essentieel zijn om de zorgbehoefte van een cliënt op een zo objectief mogelijke manier in kaart te brengen en dit volgens een internationaal gevalideerd instrument (RAI). Ze worden ingebracht door een multidisciplinair team van zorgprofessionals om een zo objectief mogelijk beeld te krijgen.

« Seul un médecin, personne physique, peut transmettre et recevoir des données médicales couvertes par le secret professionnel du médecin. (Avis du Conseil National de l'Ordre des Médecins du 22/04/1995) »

Het rolgebaseerde toegangssysteem van BelRAI zorgt ervoor dat medische gegevens kunnen afgeschermd worden van alle zorgverleners, behalve artsen. In het systeem kan bepaald worden welke de standaard toegang is van elke rol tot elk soort van gegevens. Daarbij kan men bepalen dat enkel artsen toegang hebben tot medische gegevens.

Bij sommige soorten van gegevens is het mogelijk deze standaard toegang aan te passen voor een specifiek dossier (in functie van het team van zorgprofessionals die het dossier invullen) maar bij erg gevoelige of medische gegevens kan men beslissen om dit niet toe te laten. Bijvoorbeeld: men kan

instellen dat medische gegevens enkel door een arts kunnen geraadpleegd of ingevuld worden en dat men van deze algemene regel nooit kan afwijken.

Momenteel wordt in het onderzoeksproject gebruik gemaakt van de rol “formele zorgverstrekker” voor alle zorgprofessionals die aan het onderzoek deelnemen en zij hebben toegang tot alle soorten informatie. Dit moet zeker in de toekomst verfijnd worden; hoe dit best gebeurt, maakt deel uit van de onderzoeksvragen in het huidige BelRAI project.

« Le traitement de données à caractère personnel relatives à des litiges soumis aux cours et tribunaux ainsi qu'à des juridictions administratives, à des suspicions, des poursuites ou des condamnations est interdit. »

Niet van toepassing voor BelRAI.

« Le traitement de données à caractère personnel qui relèvent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale ainsi que le traitement des données relatives à la vie sexuelle est interdit. »

Niet van toepassing voor BelRAI, behalve gegevens over “Geloofsovertuiging en daarmee samenhangende wensen of noden..”. Deze informatie heeft als doel de zorg beter af te stemmen op de behoeftes of wensen van de cliënt, maar kan best anders verwoord worden als “Wensen of noden samenhangend met geloofsovertuiging” zodat niet de overtuiging dient opgegeven te worden maar enkel de wensen of noden die eruit voortvloeien.

« La transmission informatique de données couvertes par le secret médical doit être cryptée et certifiée par une signature digitale. »

De gegevens die tussen het BelRAI systeem en zijn gebruikers worden verzonden, worden versleuteld volgens het HTTPS/SSL protocol. Certificatie door een digitale handtekening is vandaag nog niet mogelijk omdat er nog geen universeel verspreide elektronische identiteitskaart voorhanden is. Dit wordt in de toekomst voorzien via het e-ID systeem en via be.health.

4 Aanpassingen op korte termijn

Het is duidelijk dat de communicatie in verband met privacy maatregelen vanuit het BelRAI project naar zorgprofessionals toe, vandaag onvoldoende adequaat is. Daarom zal op korte termijn gezorgd worden voor een meer transparante communicatie hierover, die publiek beschikbaar wordt gemaakt. Tevens worden enkele bijkomende aanpassingen gedaan om tegemoet te komen aan de opmerkingen vanuit de sector.

1. De aanvraag aan de Privacy Commissie wordt ingediend (deadline 25/1/2008)
2. Aan het informed consent formulier wordt informatie toegevoegd over welke categorieën van zorgverleners toegang hebben tot de gegevens van een cliënt en over het inzagerecht door de cliënt. Er wordt ook toegevoegd dat de informatie, als die in de toekomst zou worden gebruikt om statistische informatie af te leiden, geanonimiseerd zal worden. (deadline 25/1/2008)
3. De BelRAI wiki site, waarop het hele BelRAI systeem uitvoerig wordt toegelicht, zal uitgebreid worden met een hoofdstuk rond privacy. (deadline 31/1/2008) Hierin worden de volgende zaken opgenomen:
    a. Privacy policy: tekst met huidige privacy maatregelen
    b. Aangepaste informed consent formulier
    c. Lijst van categorieën van zorgverleners (“rollen”) en welke toegang ze hebben in het systeem (matrices “Toegang van Rollen op Vraagtypes” en “Toegang van Rollen op Systeemfuncties”)

d. “Flow chart” van groepen en hoe toegang wordt georganiseerd.

e. De rol van cliëntbeheerder met betrekking tot de bescherming van de privacy van de zorgcliënt

f. Bijkomende privacy maatregelen voorzien voor de toekomst

De BelRAI wiki site is beschikbaar op de volgende adressen:

- Nederlandstalig: http://wiki.belrai.org/nl/
- Franstalig: http://wiki.belrai.org/fr/

5 Toekomstige aanpassingen

De volgende aanpassingen om de privacy nog beter te beschermen, zijn gepland voor toekomstige BelRAI projecten:

1. Password policy: veiligere wachtwoorden afdwingen
2. Logging en controletools zodat veiligheidsconsulenten kunnen controleren of er geen privacy inbreuken zijn in het systeem.
3. Veiligheidsconsulent: elke groep in het systeem (bv. een ziekenhuis) zal een veiligheidsconsulent hebben die vragen rond de veiligheid van het systeem kan beantwoorden en die de veiligheid mee garandeert.
4. Encryptie van de databank en connectie tussen de databank en de software code. Dit gebeurt vandaag op één afgeschermde server zodat deze encryptie nog niet essentieel is. Uiteraard gebeurt de encryptie van de overgedragen gegevens tussen de server en de gebruiker nu al (zie hoger).
5. Individuele role based access: vandaag wordt de toegang tot soorten gegevens bepaald per rol, en dit voor alle zorgcliënten in het hele systeem. In de toekomst is het best dit uit te breiden tot individuele rolgebaseerde toegang, zodat per cliënt kan bepaald worden welke rollen tot welk soort informatie toegang hebben.
6. Inzagerecht: een lijst van verwerkingbevoegde personen of rollen beschikbaar maken op de site, zodat van elke zorgcliënt kan opgevraagd worden wie er toegang heeft tot welke van zijn gegevens. Hierbij is er mogelijk een conflict met het recht op privacy van de zorgprofessionals zelf. Dit moet juridisch nog verder onderzocht worden.
7. e-ID login en koppeling aan be.health om toegangsrechten van zorgverstrekkers op cliënten te bepalen
8. Anonimiseren van gegevens bij secundaire verwerking, bijvoorbeeld statistieken over verschillende instellingen heen.

Het privacy beleid in het BelRAI project is uitgewerkt in samenspraak met de groep ICRI van K.U.Leuven, maar tijdens de vorige BelRAI projecten was niet het nodige budget voorhanden om een meer uitgebreide juridische studie te maken. Het wettelijke kader is zeer divers en soms sectorspecifiek. Daarom kan niet gegarandeerd worden dat alle juridische aspecten 100% zijn afgedekt. Ook is er nog geen onderzoek gevoerd naar een toekomstig gebruik van het BelRAI systeem op grote schaal, buiten de context van het wetenschappelijk onderzoek. We pleiten er daarom sterk voor om bijkomend privacy onderzoek in toekomstige BelRAI projecten op te nemen.