Aanbevelingen van de Nationale Raad betreffende het bijhouden van elektronische medische databanken die nominatieve en identificeerbare gegevens bevatten

Doc	a097008
Publicatiedatum	15/06/2002
Origine	NR
Thema's	Informatica Beroepsgeheim Persoonlijke levenssfeer Spoedgevallen Aansprakelijkheid van de arts (Burgerlijke- en/of strafrechtelijke-) Internet

De persoonsgegevens in verband met de gezondheid zijn commercieel (1) zeer belangrijk geworden en verwierven een politieke en handelswaarde. Meestal gaat het om medische informatie afkomstig uit databanken met persoonlijke medische gegevens die op die manier gecommercialiseerd en aangewend worden voor een ander doel dan dat waarvoor ze verzameld werden.
Tot het jaar 2000 had de meerderheid van de projecten voor servers van medische gegevens enkel betrekking op de gezondheidswerkers. Maar het verschijnen van sites waaraan patiënten vrijwillig hun medische gegevens toevertrouwen met het doel ze gemakkelijker toegankelijk te maken voor de artsen die ertoe gebracht zouden worden hen te verzorgen in een noodsituatie, doet nieuwe vragen rijzen.
Deze gegevens worden toevertrouwd aan commerciële firma's in veiligheidsomstandigheden die niet altijd getest werden.
In België wordt de verwerking van persoonsgegevens geregeld door de Wet van 8 december 1992 (2) aangevuld door het Koninklijk besluit van 13 februari 2001 (3). Ze zijn ook van toepassing op de patiëntendossiers die de artsen bijhouden. In Frankrijk mogen niet-identificeerbare gegevens afkomstig uit geneeskundige voorschriften gecommercialiseerd worden volgens modaliteiten in overeenstemming met de wetgeving en de deontologie in bijzondere gevallen onderzocht door de CNIL (4). Er valt te vrezen dat, zoals dit in de VSA gebeurt, firma's die in het bezit zijn van persoonlijke gegevens hen toevertrouwd door patiënten, op een dag geneigd zullen zijn van deze laatsten gegevens uit deze dossiers af te kopen.

Uitwisseling van medische persoonsgegevens is gerechtvaardigd tussen artsen in het belang van de patiënten. Sedert verschillende jaren heeft de Nationale Raad van de Orde richtlijnen en beveiligingstechnieken opgesteld die toegepast dienen te worden opdat de vertrouwelijkheid van de uitwisseling in die gevallen gewaarborgd zou zijn (5).
In deze materie zijn de cryptologie en de gecertificeerde digitale handtekening onontkoombaar. De gegevensbeveiliging wordt in de internationale literatuur uitvoerig behandeld (6)(7).
Het groeiend aantal projecten voor servers van gegevens en voor servers van databanken doet nieuwe problemen rijzen die de Nationale Raad ertoe brachten na te denken over de deontologische regels terzake.

ALGEMENE PRINCIPES

Bij elke verwerking van persoonsgegevens zijn een reeks regels van toepassing tijdens hun inzameling, tijdens hun introductie en hun verblijf in een databank en tijdens hun transfer langs elektronische weg.

Authenticiteit van de gegevens: dit wil zeggen de garantie dat de gegevens overeenstemmen met de werkelijkheid. De juistheid van hun inhoud moet gecertificeerd worden door de arts die ze waarnam, vaststelde of er verantwoordelijk voor is. De betrokken practicus moet geïdentificeerd worden en zijn kwalificatie dient gekend te zijn dankzij een gecertificeerde elektronische handtekening. Zo zal de practicus die de patiënt behandelt verzekerd zijn van de juistheid van de gegevens.

Integriteit van de gegevens: dit wil zeggen de garantie dat de gegevens wel degelijk deze zijn van de aangeduide patiënt, dat ze niet verdraaid werden en dus in overeenstemming zijn met het origineel. Hun bescherming tegen externe of interne aanvallen moet volledig en geactualiseerd zijn, d.w.z. gebruik makend van beschermingstechnieken regelmatig aangepast in functie van de nieuwe wetenschappelijke kennis en de vooruitgang in dit domein. De aanvallen kunnen proberen binnen te dringen in de databank, er gegevens uit te halen, er wijzigingen in aan te brengen die kunnen gaan tot de vernietiging ervan. Er moet een lijst bijgehouden en gecontroleerd worden van de niet toegestane toegangspogingen.

Toegangsrecht: de toegang tot het geheel of een deel van een medisch dossier wordt essentieel bepaald door het statuut van “verzorgend persoon momenteel met de patiënt belast”. Hij is beperkt tot de gegevens waarvan de kennis noodzakelijk is voor de verzorging en tijdens de duur ervan (8).
Er moet een hiërarchische volgorde opgesteld worden in functie van eenieders bekwaamheden en specialisme, evenals een selectie van de gegevens onderling.
Elke aanvraag voor toegang tot medische persoonsgegevens ondergebracht op een server moet rekening houden met verschillende determinerende criteria of voorwaarden:
De identiteit en de kwalificatie van de aanvrager: het kan gaan om een arts of een gezondheidswerker die de patiënt verzorgt, om een vertrouwensarts gekozen door de patiënt, om een arts verbonden aan een verzekeringsorganisme of aan een private verzekering, of om een lid van het verzorgend personeel van een ziekenhuis, of om de patiënt zelf die zijn medisch dossier wenst in te zien. De gecertificeerde elektronische handtekening moet gebruikt worden om de identiteit en de hoedanigheid van de aanvrager na te gaan wanneer deze aanvraag elektronisch gebeurt.
Het soort betrokken gegevens: er moet een selectie gemaakt worden tussen de gegevens : spoedgegevens, gedocumenteerde hypotheses, bevestigde hypotheses, werkhypotheses, genetische, psychiatrische en gevoelige gegevens...
De vertrouwelijkheidsgraad die hun auteur of de patiënt hen toekende dient geëerbiedigd te worden. Er moet rekening gehouden worden met de toestemming van de patiënt, die digitaal gematerialiseerd moet worden.
Het doel van de aanvraag moet duidelijk gedefinieerd worden door de aanvrager : beheerder van het globaal medisch dossier van de patiënt (huisarts), arts bijgeroepen om de patiënt voor een specifiek probleem te verzorgen (arts die wachtdienst heeft of specialist), spoedsituatie, adviserend arts van een verzekeringsorganisme, controle-arts, arbeidsarts, arts deskundige voor een verzekering of voor een rechtbank, arts inspecteur van het Riziv, enz.
Voor de artsen die de patiënt behandelen is **de duur** van deze toegang strikt beperkt tot de periode waarvoor de patiënt de aanvrager raadpleegt.. Voor de andere artsen is de toegang beperkt tot de gegevens nodig voor de uitoefening van hun wettelijke opdracht.
De creatie van een project voor een server van medische gegevens zal deze verschillende factoren moeten opnemen in een matrixrooster waardoor de toegangsaanvraag zal gefilterd worden teneinde de private levenssfeer van de patiënten te beschermen en het medisch geheim te eerbiedigen.

Het nasporen van de toegangen. Het is belangrijk een bewijskrachtig spoor te bewaren van de

elektronische transacties om, indien nodig, te kunnen bewijzen dat ze plaats hadden. Om dit te bereiken kan alleen een elektronisch notariaat een tracering van de transacties waarborgen. Dit notariaat zou niet gerealiseerd moeten worden binnen de server maar wel bij een derde organisme dat de rol kan spelen van getuige van de documentenuitwisseling. De identiteit van de aanvrager zal aan dit organisme doorgegeven worden.

Vertrouwelijkheid van de gegevens: de persoonlijke gegevens van de patiënten zijn gedekt door het beroepsgeheim van de arts (Strafwetboek art. 458, Code van geneeskundige plichtenleer art. 55 tot 70). De vertrouwelijkheid wordt bepaald door de beveiliging en door het rooster met de rechthebbenden op toegang tot de gegevens. Artsen mogen geen persoonsgegevens toevertrouwen aan informaticasystemen die niet of niet voldoende aan deze voorwaarden voldoen.

Inhoud: Alleen de objectieve gegevens aangaande een patiënt maken deel uit van zijn dossier en mogen bewaard worden in een nominatieve medische databank. Het is bijzonder belangrijk dat het geautomatiseerd medisch dossier van een patiënt bijgehouden wordt. Dit houdt in dat de artsen die de patiënt momenteel verzorgen toegang hebben tot dit dossier en dat beide partijen akkoord zijn er de nieuwe objectieve gegevens aan toe te voegen.

Duurzaamheid van de databank op internet: De bewaartijd van de medische gegevens bedraagt momenteel 30 jaar (9) na het laatste contact met de patiënt, behalve bij een bijzondere situatie. Het geautomatiseerd dossier dat bewaard wordt in een centrale databank moet minstens identiek zijn. Stelt zich dus de vraag wat er gebeurt met de ingewonnen gegevens wanneer het verzamelend organisme verdwijnt. Een burgerlijke firma kan haar eigen bestaansduur niet garanderen. Men kan niet aanvaarden dat nominatieve gegevens met een therapeutisch doel verzameld worden door firma's die niet in staat zijn de bewaring ervan te verzorgen gedurende de wettelijke en deontologische termijn.

Aangifte van de bestanden: De Wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens bepaalt de voorwaarden waaraan deze verwerkingen moeten voldoen (10). De geautomatiseerde verwerking moet aangegeven worden bij de Commissie voor de bescherming van de persoonlijke levenssfeer. Deze aangifte moet ondermeer het doel bevatten waarvoor deze gegevens verzameld worden.

Medische aansprakelijkheid: het registreren door de arts van medische persoonsgegevens in een databank impliceert de aansprakelijkheid van de arts die de patiënt behandelt. Het is dus aangeraden zich te beperken tot de gedocumenteerde, gedateerde objectieve gegevens waarvan de auteur geïdentificeerd is.

Informaticastandaarden: Er moet een gemeenschappelijk kader van interoperabiliteit opgesteld worden voor de uitwisselingen en de boekhouding van de systemen. Het gaat hier om een initiatief dat afhangt van de overheid. Op die manier zal de gegevensuitwisseling tussen verschillende gebruikers mogelijk worden.

SYSTEMEN BESTEMD VOOR HET INFORMEREN VAN DE SPOEDGEVALLENDIENSTEN

Het betreft medische inlichtingen die nuttig geacht worden en die toegankelijk zijn op internet voor onbekende artsen die ertoe zouden gebracht worden dringende zorgen te verlenen aan patiënten die deel uitmaken van het systeem. De toegang gebeurt gewoonlijk door middel van een code die in het bezit is van de patiënt.

Zonder het nut ervan in bepaalde gevallen te ontkennen, moet er opgemerkt worden dat er geen enkel wetenschappelijk bewijs geleverd werd (11) van een kwaliteitsverbetering van de spoedgevallen dankzij deze methode. Alle urgentiediensten verifiëren immers altijd onmiddellijk een reeks parameters zoals de bloedgroep, de glykemie, het ecg, enz. Het informeren van de artsen, urgentisten of anderen, is daarentegen ongetwijfeld nuttig in andere spoedgevallen zoals ernstige anafylactische reacties, epilepsie … De vermelding van deze pathologie op een document dat de

patiënt bij zijn identiteitspapieren bewaart voldoet goed aan deze behoefte : grotere veiligheid, gemakkelijke toegang.

Authenticiteit van de gegevens :

1. De gegevens ingebracht door de patiënt kunnen twijfelachtig zijn. De patiënt is immers niet noodzakelijk op de hoogte van hun belang, hun relevantie, hun betekenis, hun juistheid. Het kan bijvoorbeeld vitaal zijn de grote geneesmiddelenallergieën te kennen, maar men mag zich echter niet baseren op een allergielijst gemeld door de patiënt die zou kunnen ofwel onjuiste inlichtingen ofwel teveel inlichtingen geven. Bovendien wordt er in de documentatie van de betrokken firma's "aangeraden zich te laten helpen door zijn vertrouwde huisarts".
2. De medische validatie is inderdaad onontbeerlijk. Ze impliceert de aansprakelijkheid van de arts en dient gematerialiseerd te worden op de server door zijn handtekening.
3. Indien de gegevens ingebracht worden door een arts kan zijn aansprakelijkheid geïmpliceerd worden. De arts moet minstens de zekerheid hebben dat de gegevens niet konden of niet kunnen gewijzigd worden. Hij dient zich te beperken tot de gedocumenteerde objectieve gegevens en zich te identificeren.
4. Het probleem van het permanent actualiseren van de gegevens is niet opgelost wanneer de patiënt er verantwoordelijk voor is. Dit zou mogelijk zijn indien deze taak ten laste zou vallen van de arts die het aanvaard heeft.

Vertrouwelijkheid van de gegevens: de bescherming van de geïdentificeerde persoonsgegevens moet gewaarborgd worden wanneer ze op internet circuleren (codering en gecertificeerde handtekening) en ook wanneer ze op de server van de databank voorkomen : bescherming tegen niet toegestane toegang, tegen hackers, tegen elke niet toegestane wijziging, maar ook tegen de schending van het privé leven van de patiënt door de verantwoordelijke firma zelf.
Een eenvoudige toegangscode is een onvoldoende bescherming. Bovendien zou de patiënt, indien hij de codehouder is, verplicht kunnen worden, onder morele dwang of bij gebrek aan informatie, de inhoud van zijn dossier vrij te geven voor een niet-therapeutisch doeleinde.

Medische aansprakelijkheid van de gebruiker van de gegevens: De arts die ertoe zal gebracht worden deze gegevens te gebruiken wanneer hij zorgen verstrekt, impliceert op gevaarlijke wijze zijn aansprakelijkheid indien hij zijn therapeutisch gedrag baseert op gegevens die niet gevalideerd werden. Vandaar de noodzaak van veiligheid, authenticiteit en vertrouwelijkheid.
De problemen verbonden met de duurzaamheid van de databank en met de aangifte van de bestanden zijn eveneens van toepassing op deze systemen.

SYSTEMEN VOOR OVERDRACHT VAN VERTROUWELIJKE GEGEVENS TUSSEN ARTSEN

Medische documenten worden meer en meer onder digitale vorm verstuurd. Deze werkwijze is geleidelijk aan bezig de klassieke postuitwisseling te vervangen. Er werd geregeld de aandacht gevestigd op de onveiligheid van de uitwisseling via elektronische weg. Verscheidene aanbevelingen van de Nationale Raad zijn gewijd aan de voorwaarden vereist om de veiligheid van dit soort transmissie te waarborgen (12)(13).
De elektronische communicatie van documenten tussen artsen kan rechtstreeks gebeuren of door tussenkomst van een mailprovider (elektronische brievenbus). In beide gevallen dienen de veiligheidsregels gerespecteerd te worden. De cryptografie en de gecertificeerde elektronische handtekening staan hierbij op de eerste plaats.
De encryptie moet asymmetrisch zijn en een beroep doen op beproefde algoritmes; de encryptiesleutel moet voldoende lang zijn. Bij hun gebruik dient het programma alle maatregelen te bevatten nodig voor de bescherming van de private sleutel.
De elektronische handtekening van de arts moet gecertificeerd worden in overeenstemming met de wettelijke bepalingen (14)(15). Deze handtekening moet, wanneer ze op een gedigitaliseerd document geplaatst wordt, de identiteit en de hoedanigheid van de arts legaliseren, net zoals zijn manuele handtekening op papier. Ze biedt het bijkomend voordeel de integriteit van het

ondertekende document te certificeren. Momenteel en ondanks de aanbevelingen en wetgevingen, leveren de commerciële systemen van elektronische brievenbus geen gecertificeerde handtekening in overeenstemming met de wetgeving en laten ze niet toe medische documenten te versturen buiten hun eigen klantenkring. De gegevensuitwisseling is dus op het terrein zeer beperkt bij gebrek aan interoperabiliteit. Dit brengt een strenge beperking mee in de elektronische verspreiding van de medische post en vormt een ernstige hinderpaal voor de uitbreiding en de wereldwijde verbreiding van deze dienst. Bovendien kan het gebruik van onmiskenbaar ontoereikende systemen ter identificatie van de artsen leiden tot veiligheidsgebreken.

De aanbevelingen van de Nationale Raad (16) blijven momenteel van toepassing :

1. Alleen een arts, natuurlijke persoon, mag medische gegevens gedekt door het beroepsgeheim van de arts doorgeven en ontvangen. Binnen een instelling mag de arts die medische gegevens doorgeeft of ontvangt dit enkel doen in zijn naam. Het is dus de persoonlijke handtekening van de arts verantwoordelijke afzender die, zoals op een papieren document, de inhoud van het verstuurde document moet valideren en certificeren.
2. De codering door een systeem met dubbele sleutel, ook nog asymmetrisch wiskundig systeem genoemd, geeft voldoende veiligheid.
3. De arts maakt zelf de sleutels aan op zijn persoonlijke computer met een programma verkregen bij een onafhankelijke provider.
4. Teneinde de elektronische handtekening te legaliseren dient de publieke sleutel van de handtekening gecertificeerd te worden door een certificatiedienstverlener die gekwalificeerde certificaten aflevert en die onafhankelijk is van de mailserver.
5. De toegang tot de geheime sleutel is definitief beperkt tot de eigenaar ervan.
6. Het gebruikte algoritme moet gekend en voldoende lang zijn zowel wat betreft het symmetrische als wat betreft het asymmetrische deel.
7. De codering en de decodering van de gegevens gebeuren respectievelijk in de computer van de afzender en van de bestemmeling. Deze operaties mogen in geen geval uitgevoerd worden in een tussenliggende computer gewijd aan of verbonden met de elektronische brievenbus.

De Nationale Raad heeft een infrastructuur van publieke sleutels opgezet die aan elke ingeschreven arts toelaat een gecertificeerde sleutel te bekomen in overeenstemming met de wettelijke bepalingen. Hij beveelt het gebruik ervan aan bij de uitwisseling van medische gegevens via elektronische weg. Elke arts wordt uitgenodigd contact op te nemen met zijn provinciale raad om de aanmaakprocedure van zijn digitale identificatie gecertificeerd door de Orde van geneesheren op te starten en zijn telematische dienst te vragen deze identificatie te gebruiken.

SERVERS VAN MEDISCHE DATABANKEN

Naargelang het geval kunnen de gegevens bewaard worden op de schijf van een individuele computer, binnen een centraal archiefsysteem in de verzorgingsinstellingen of binnen een gecentraliseerde server bestemd voor distributie van diensten.
In elk geval dienen er betrouwbare**beveiligingsmaatregelen** toegepast te worden. Ze betreffen zowel de fysieke bescherming van de installaties als de bescherming tegen de incidentele vernietiging van gegevens of tegen niet toegestane toegang tot de gestockeerde gegevens. De duurzaamheid van de databank dient eveneens gewaarborgd te worden.
Het belang van de **toegangscontrolemaatregelen** is evenredig met het aantal en de verschillende kwalificaties van de personen die toegang kunnen hebben. Hetzelfde geldt voor de beschermingsmaatregelen.

(1) La commercialisation des informations médicales est-elle “déontologiquement correcte”? Nationale Raad van de Orde van geneesheren, Frankrijk, 29-30 juni 2000.
(2) Wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens.
(3) Koninklijk besluit ter uitvoering van de wet van 8 december 1992 tot bescherming van de

persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens. 13 februari 2001.
(4) Commission Nationale Informatique et Liberté. Frankrijk.
(5) Aanbevelingen betreffende de bescherming van de vertrouwelijkheid bij de transmissie van medische persoonsgegevens via internet (17 februari 2001). Tijdschrift Nationale Raad nr. 92, juni 2001, p. 4.
(6) Hanka, R., Buchan, I.E. : Security measures in open communication systems. hanka@medschl.cam.ac.uk
(7) CEN/TC 251/Wi 6.10: Framework fo Security of Health Care Communication.
(8) Toegangsrecht tot het dossier, Geautomatiseerd globaal medisch dossier (12 december 1998). Tijdschrift Nationale Raad nr. 84, juni 1999, p. 14.
(9) Code van geneeskundige plichtenleer, art. 46.
(10) Zie hierover het advies van de Nationale Raad van 18 januari 1997, Tijdschrift Nationale Raad nr. 75, maart 1997, p. 32.
(11) Commissie Telematica van het ministerie van Volksgezondheid, 12 november 2001.
(12) Elektronische post (22 februari 1995), Tijdschrift Nationale Raad nr. 69, september 1995, p. 13.
(13) Aanbevelingen betreffende de bescherming van de vertrouwelijkheid bij de transmissie van medische persoonsgegevens via internet (17 februari 2001), Tijdschrift Nationale Raad nr. 92, juni 2001, p. 4.
(14) Richtlijn 1999/93/EG van het Europese Parlement en van de Raad, van 3 december 1999, over een gemeenschappelijk kader voor de elektronische handtekeningen.
(15) Wet betreffende de activiteit van certificatiedienstverlener met het oog op het gebruik van elektronische handtekeningen. 14 juni 2001.
(16) Aanbevelingen betreffende de bescherming van de vertrouwelijkheid bij de transmissie van medische persoonsgegevens via internet (17 februari 2001), Tijdschrift Nationale Raad nr. 92, juni 2001, p. 4.