

## Aanbevelingen door de Orde van Geneesheren betreffende de bescherming van de vertrouwelijkheid bij de transmissie van medische persoonsgegevens via het internet.

Dr Patrick Verheijen.

Secretaris Provinciale Raad Vlaams Brabant.

Lid werkgroep Telematica van de Nationale Raad.

### INLEIDING

Op 22 april 1995 bracht de Nationale Raad voor het eerst een advies uit aangaande de veiligheidvoorwaarden die noodzakelijk zijn bij de transmissie van vertrouwelijke medische persoonsgegevens langs elektronische weg.

Het hele internetgebeuren stond toen nog in de kinderschoenen.

We moeten goed beseffen dat de evolutie op het gebied van telematica gigantisch is op de relatief korte periode van 10 jaar.

Het internet, wat nu reeds een vanzelfsprekendheid is, en zonder meer een noodzakelijk medium geworden is, bestond nog helemaal niet enkele jaren geleden.

Op 17 februari 2001 worden de adviezen van de nationale raad gepubliceerd die momenteel van kracht zijn.

Deze aanbevelingen kwamen tot stand na een uitgebreide evaluatie door de werkgroep Telematica van de Nationale Raad.

De aanbevelingen formuleren op een eenvoudige wijze hoe men op een deontologisch en ethisch verantwoorde manier vertrouwelijke gegevens kan doorzenden via het internet.

Hieronder verstaan we voornamelijk het doorsturen van gegevens zonder het medisch beroepsgeheim te schaden.

De sleutelwoorden : authenticiteit, vertrouwelijkheid en betrouwbaarheid staan in deze tekst centraal.

Ik zal van mijn spreektijd gebruik maken om een overzicht geven van deze aanbevelingen en het belang onderstrepen van de bescherming van de vertrouwelijkheid.

De orde van geneesheren is, zoals jullie wel weten, zeer begaan met het vrijwaren van het medisch beroepsgeheim.

Het is vooral sedert de opkomst van de transmissie van gegevens via het internet dat in de praktijk gebleken is dat deze overdracht niet zonder gevaar is.

Laat mij dit verduidelijken aan de hand van een praktisch voorbeeld :

Dr Katrien, huisarts, is fiere eigenaar van een PC.

Zij stelt een brief op om de geboorte te melden van haar eerste kindje en verstuurt deze via internet naar haar collega Dr Ann.

Dr Ann opent op haar PC de brief en neemt kennis van de inhoud, enkele seconden na het verzenden van de brief door Dr Katrien.

Via haar PC kan Dr Ann een geschenkje kopen van de geboortelijst.

Maar wanneer Dr Katrien een verwijsbrief over een patient wil doorsturen via haar computer naar collega Ann, dan doen er zich opeens enkele problemen voor.

Dan liggen de zaken plots helemaal anders !

Ik denk vooral aan problemen van authenticiteit en vertrouwelijkheid.

Heeft Dr Katrien dit bericht opgesteld, of wil de poetsvrouw van Dr Katrien aan vertrouwelijke informatie geraken ?

Ook de authenticiteit van de bestemming is belangrijk.

Wie zal het vertrouwelijke bericht lezen ?

Is het Dr Ann zelf, of is de verpleger van de dienst die toevallig de binnenkomende berichten van de dokter leest.

En wat met de transmissie zelf ?

Kan de inhoud van een boodschap al dan niet kwaadwillig gelezen worden tijdens de elektronische overdracht door een derde persoon.

Of kan een boodschap veranderd en aangepast worden tijdens de overdracht via internet ?

Krijgt de ontvanger de originele brief te lezen ?

Zijn er woorden of zinnen gewijzigd de originele tekst ?

Vragen die misschien voor de hand liggen, maar toch van groot belang zijn.

Het kwam er dus op aan voor de Orde van Geneesheren om zo snel mogelijk te bepalen aan welke voorwaarden een systeem moet voldoen om vertrouwelijke gegevens die onder het beroepsgeheim vallen in alle veiligheid door te sturen.

Met dit doel voor ogen heeft de werkgroep telematica van de nationale Raad aanbevelingen geformuleerd betreffende de bescherming van de vertrouwelijkheid bij de transmissie van medische persoonsgegevens via het internet.

Er is slechts één systeem dat waarschijnlijk voldoende veilig is om in te staan voor de transmissie van vertrouwelijke gegevens, namelijk de asymmetrische encryptie, door ons beter gekend als het dubbelsleutelsysteem.

### WAT IS NU EIGENLIJK DIT FAMEUZE SYSTEEM ?

Encryptie betekent in deze context de gegevens beveiligen en onleesbaar maken voor een buitenstaander.

Bij de asymmetrische encryptie AE zijn er twee sleutels : een publieke en een private sleutel. Deze twee sleutels zijn elkaars tegengestelde en ze heffen mekaar op.

Ik verklaar mij nader : als je iets codeert met de publieke sleutel, dan kan je enkel decoderen met de private sleutel en omgekeerd.

De twee sleutels neutraliseren mekaar en toch is het onmogelijk om uit de ene sleutelcode de ander af te leiden.

Stel dat persoon A een gecodeerd bericht wil sturen naar persoon B.

Persoon B zorgt er dan voor in het bezit te zijn van de publieke sleutel van persoon A.

Publieke sleutel wil zeggen, een code die algemeen verspreid werd door persoon A.

Persoon B kan dan met zijn strikt geheime private sleutel dit bericht lezen.

Geen enkele andere persoon wereldwijd heeft deze private sleutel, en persoon A weet dit.

Persoon A weet dan ook met zekerheid dat zijn bericht enkel en alleen door B kan gelezen worden !

De Private of geheime sleutel blijft strikt geheim door de beveiliging met een paszin of met een pin-code op een chipcard.

De publieke sleutel mag wereldwijd verspreid worden op het internet, bijvoorbeeld via een website of e-mails.

De publieke sleutel moet dan wel gekoppeld worden aan een persoon.

In de praktijk gebeurt dit door een CA of certification authority .

Deze CA zal de publieke sleutel van een persoon of dienst tekenen met de private sleutel van de CA na verificatie van de identiteit van de persoon of dienst.

Zo ontstaat een digitaal certificaat, een soort uniek identiteitsbewijs.

Certificatie van de gegevens die onder het beroepsgeheim vallen, dienen aan de hoogste veiligheidsnormen te voldoen.

De veiligheid hangt o.a. af van de lengte van de digitale sleutels.

Men zal dan ook eerder spreken van een paszin in plaats van een wachtwoord.

Bij uitgebreide versleuteling is de kans op decodering quasi nul.

Echter onder voorwaarde van regelmatig nieuwe sleutels aan te maken .

Dit systeem wordt actueel door de Orde als veilig aanzien en komt in aanmerking voor het verzenden van medische gegevens.

De orde eist wel in verband met de veiligheid dat de private sleutel, opgeslagen op een beveiligde cd of ucb sleutel, bij de orde wordt bewaard.

Bij het vergeten van een paszin, of een chipcard heeft men dan alsnog toegang tot de gegevens.

Wanneer een certificaat dan toch zou gekraakt worden, dan moet men dit certificaat revoken. De CA houdt een lijst bij van alle certificaten die gerevoked werden.

Ik ga nu concreet een woordje zeggen over de zogenaamde  
RICHTLIJNEN VAN DE NATIONALE RAAD VAN DE ORDE VAN GENEESHEREN  
AANGAANDE DE ELECTRONISCHE GEGEVENSOVERDRACHT

Alhoewel ik het liever als : “ aanbevelingen om problemen te vermijden “  
zou willen omschrijven en niet zozeer als richtlijnen of een verordening.

**KRACHTENS ARTIKEL 458 VAN HET STRAFWETBOEK IS DE ARTS WETTELIJK  
VERPLICHT HET BEROEPSGEHEIM TE EERBIEDINGEN.**

De elektronische transmissie van gegevens die geheime persoonsgegevens bevat, ontkomt niet aan deze wettelijke en deontologische verplichting.

1.

Medische gegevens gedekt door het beroepsgeheim van de arts mogen enkel door een arts als natuurlijke persoon doorgezonden en ontvangen worden.

Binnen een instelling mag een arts alleen in eigen naam gegevens doorzenden of ontvangen.

*Het mag dus niet dat een niet-arts toegang heeft tot deze gegevens.*

*Men is duidelijk hierover: zowel het versturen, als het ontvangen van deze gegevens moet door de betrokken arts zelf gebeuren.*

*Deze taak kan niet gedelegeerd worden aan bv een medische secretaresse.*

*De arts stuurt en ontvangt de gegevens die onder het beroepsgeheim vallen.*

2.

Het dubbele sleutelsysteem, ook nog asymmetrisch mathematisch systeem genoemd, biedt voldoende veiligheid.

*Dit hebben we U daarnet uitgelegd*

3.

Teneinde het geheim karakter ervan te bewaren, dient te arts zelf zijn eigen sleutels aan te maken op zijn PC.

Tijdens deze handeling mag deze computer niet aangesloten zijn op het netwerk.

*Met deze richtlijn wil men voorkomen dat buitenstaanders toegang hebben tot uw geheime code. Bij het aanmaken van sleutels op een andere PC dan de uwe is er onmiddellijk een probleem van beveiliging.*

*Dit geldt eveneens voor het aanmaken van sleutels terwijl de PC aangesloten is op het netwerk.*

4.

De toegang tot de geheime sleutel is strikt voorbehouden tot de eigenaar ervan.

Deze toegang moet beveiligd worden met een paswoord, dat niet mag medegedeeld worden.

*Inderdaad, moest je uw geheime sleutel aan een andere persoon meedelen zelfs aan personen met wie je nauw samenwerkt, dan is het geheim verbroken en is een veilige overdracht van gegevens niet meer mogelijk. Uw correspondent moet absoluut zeker zijn dat jij alleen toegang hebt tot het bericht. Niet uw echtgenote, uw verpleegster, zelfs niet uw collega met wie je samenwerkt.*

5.

De arts dient een kopie van de geheime sleutel op cd-rom of usb-sleutel toe te vertrouwen aan de Raad van de Orde onder wiens bevoegdheid hij valt.

De toegang tot deze informatie moet beveiligd worden met een paswoord of paszin, die afzonderlijk in een verzegelde omslag wordt bewaard.

*Dit is belangrijk om bij verlies van uw geheime sleutel, toch nog een mogelijkheid te hebben om uw gegevens op te vragen. U alleen kan bij de Orde de sleutel opvragen bij verlies ervan. Dit blijkt geen nutteloze maatregel te zijn, aangezien het wel eens voorkomt dat een paszin vergeten wordt.*

*Denk maar eens aan alle pin-codes en paswoorden die je nu al moet onthouden in het dagelijks leven.*

*Ook wanneer de sleutel op een token staat, bestaat de mogelijkheid deze te verliezen.*

*Vandaar deze aanbeveling.*

6.

De publieke sleutel mag medegedeeld worden aan de firma die instaat voor de bestelling van de elektronische post.

*Deze firma dient er zich toe te verbinden deze publieke code enkel door te geven aan artsen die meewerken aan de uitwisseling van medische vertrouwelijke gegevens.*

*Zij moeten alle mogelijke maatregelen treffen om te verhinderen dat deze sleutel voor andere doeleinden gebruikt zou worden.*

7.

Deze publieke sleutels worden het best bewaard en naar de gebruiker doorgezonden via een server die verschillend is van deze die gebruikt wordt voor de transmissie van gegevens.

De numerieke fingerprint van de publieke sleutel die toelaat de authenticiteit ervan te controleren, moet bewaard en doorgezonden worden door een betrouwbare autoriteit.

*Hiermee bedoelt men de “certification authority “ waarover ik daarnet gesproken heb.*

8.

De codering en decodering van de gegevens vinden respectievelijk plaats in de PC van de afzender en van de bestemming.

Deze procedures mogen in geen geval via een tussencomputer gebeuren.

( hoasting, netwerkserver )

*Hier ook weer dezelfde reden, namelijk het voorkomen dat uw persoonlijke gegevens door een derde persoon zouden kunnen gelezen worden.*

WAT MOET U NU CONCREET DOEN OM IN VEILIGHEID UW MEDISCHE GEGEVENS DOOR TE ZENDEN AAN EEN COLLEGA.