Inzake het EMD en het elektronisch voorschrijven

Een oncologe raadpleegt een elektronisch patiëntendossier **zonder medeweten van de patiënt en niet op vraag van de behandelende arts**, alleen omdat de patiënt vijftien jaar geleden bij één van de leden van een dienst inwendige voor een ander probleem geconsulteerd heeft. Dit is een flagrante schending van het beroepsgeheim.

De Eed van Hippocrates en artikelen 55 tot 70 van de **Code van Geneeskundige Plichtenleer** bevatten bepalingen over het beroepsgeheim van de arts. Artikelen 38 tot 47 handelen over het medisch dossier.

Het medisch geheim is één van de laatste bastions van onze burgerlijke vrijheden. De instandhouding van het medisch geheim is de inzet van de strijd van de burger tegen alles wat hem dreigt te onderwerpen in naam van collectieve, politieke, economische en financiële belangen.

Burgerrechtelijk is ieder persoon die informatie heeft verstrekt die de privacy van de patiënt aantast aansprakelijk voor het morele en financiële nadeel veroorzaakt door zijn loslippigheid.

In het Belgische recht is de schending van het medisch geheim op de eerste plaats een delict dat **strafrechtelijk** bestraft wordt. Het beroepsgeheim zoals bepaald in artikel 458 Sw gepubliceerd in 1867, was oorspronkelijk enkel bedoeld voor de individuele arts-patiënt relatie (le colloque singulier), waarbij het verstrekken van medische gegevens aan derden slechts bij grote uitzondering toegelaten werd.

In onze geïnformatiseerde maatschappij waar het kraken van een netwerk tot gevolg kan hebben dat onbevoegden snel tot zeer gevoelige informatie toegang kunnen hebben, moet ook kunnen opgetreden worden indien onvoldoende voorzorgmaatregelen genomen zijn bij het geïnformatiseerd verwerken van gezondheidsgegevens.

De aanbeveling van 15 juni 2002 van de Nationale Raad betreffende het **bijhouden van elektronische medische databanken die nominatieve en identificeerbare gegevens bevat**, analyseert goed deze problematiek. Bij elke verwerking van persoonsgegevens zijn een reeks regels van toepassingen tijdens hun inzameling, tijdens hun introductie en hun verblijf in een databank en tijdens hun transfer langs elektronische weg.

Authenticiteit van de gegevens: De juistheid van de gegevens moet gecertificeerd worden door de arts die ze waarnam, vaststelde of er verantwoordelijk voor is. Zo zal de practicus die de patiënt behandelt verzekerd zijn van de correctheid van de gegevens.

Integriteit van de gegevens: Er moet een garantie zijn 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.

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. Elke aanvraag voor toegang tot medische persoonsgegevens ondergebracht op een server moet rekening houden met verschillende determinerende criteria of voorwaarden:

(a) **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, 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.

(b) **Het soort betrokken gegevens**: er moet een selectie gemaakt worden tussen de spoedgegevens, gedocumenteerde hypotheses, bevestigde hypotheses, werkhypotheses, genetische, psychiatrische en gevoelige gegevens...

(c) **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.

(d) **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.

(e) Voor de artsen die de patiënt behandelen is de **duur van de 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.

Vertrouwelijkheid van de gegevens. 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. Het is bijzonder belangrijk dat het geautomatiseerd medisch dossier bijgewerkt 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 medische gegevens bedraagt momenteel 30 jaar na het laatste contact met de patiënt. Dit is een eenvoudige en duidelijke gedragsregel die een goed compromis is tussen de door de wet opgelegde termijn van bewaring van medische dossiers en de termijn die vereist is voor de continuïteit van de zorg. Het geautomatiseerd dossier dat bewaard wordt in een centrale databank moet minstens identiek zijn. 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 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.

Verscheidene aanbevelingen van de Nationale Raad zijn gewijd aan de voorwaarden vereist om de veiligheid van de **systemen voor overdracht van vertrouwelijke gegevens tussen artsen** te waarborgen.
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. 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.

De Wet van 8 december 1992 tot **bescherming van de Persoonlijke Levenssfeer ten opzichte van de verwerking van persoonsgegevens** neemt het artikel 458 Sw over zeggende dat elke verwerker van persoonsgegevens eerlijk en rechtmatig moet zijn. De verwerking moet gebeuren volgens de wettelijke bepalingen. Wanneer een betrokkene schade kan aantonen door een onrechtmatige verwerking, hij de verantwoordelijke aansprakelijk kan stellen.

Artikel 4 §1, 2° van de Wet Verwerking Persoonsgegevens mag aanzien worden als de hoeksteen van deze wet. Dit beginsel houdt in dat het doel van de verwerking aangegeven en omschreven moet zijn. Dit **finaliteitsbeginsel** omvat drie aspecten.

(1) Het doeleinde van de gegevensverwerking moet specifiek omschreven zijn, dus voor elkeen, in het bijzonder de gemiddelde burger, **begrijpelijk**.

(2) Het doeleinde moet gerechtvaardigd en niet overmatig zijn, dus **proportioneel** en niet verder reikend dan noodzakelijk voor het verwezenlijken van het doel.
(3) De gegevens mogen niet verder worden verwerkt op een wijze die onverenigbaar is met de doeleinden.

De verwerking voor een **onverenigbaar doel** houdt in dat de verantwoordelijke de betrokkene voorafgaandelijk zal moeten informeren over het nieuw doeleinde.

De verwerking dient te beschikken over een **noodzakelijk karakter**. Indien de verwerking enkel maar nuttig of interessant is, wordt niet voldaan aan de toelaatbaarheidvereiste.

De verwerking van persoonsgegevens die de gezondheid betreffen, is verboden. Doch dit principe is niet absoluut. Artikel 7 §2 somt een limitatief aantal gevallen op waarin verwerking van de gezondheidsgegevens kan worden toegelaten. Hier volgt de limitatieve lijst met elf **uitzonderingen waardoor de verwerking van gezondheidsgegevens een legaal karakter krijgen**.

(1) De schriftelijke toestemming.
Artikel 26 van het uitvoeringsbesluit legt op haar beurt de verplichting op om een lijst op te stellen van personen die tot de gezondheidsgegevens toegang hebben.
(2) Verplichtingen en rechten met betrekking tot het arbeidersrecht.
(3) Verdediging van vitale belangen wanneer deze persoon fysisch of juridisch niet in staat is om zijn toestemming te geven.
(4) Gegevens die duidelijk en met die intentie door de betrokkene zijn openbaar gemaakt.
(5) Verwerking noodzakelijk voor de vaststelling, uitoefening of verdediging van een recht in rechte.
(6) Verwerking noodzakelijk voor doeleinden van
a. preventieve geneeskunde
b. medische diagnose
c. verstrekken van zorg of behandelingen aan de betrokkene of een verwant
d. het beheer van gezondheidsdiensten handelend in het belang van de betrokkene.
(7) Verwerking noodzakelijk voor de beteugeling van een strafrechtelijke inbreuk.
(8) Verwerking noodzakelijk voor de doelstelling van de Sociale Zekerheid.
(9) Verwerking noodzakelijk voor de bevordering en de bescherming van de volksgezondheid met inbegrip van bevolkingsonderzoek.
(10) Wet, decreet of ordonnantie van zwaarwichtig algemeen belang.
(11) Verwerking noodzakelijk voor het wetenschappelijk onderzoek na KB en advies door de Commissie voor de bescherming van de persoonlijke levenssfeer.

Met de komst van de **wet patiëntenrechten** van 22 augustus 2002 werden een aantal fundamentele rechten ingebouwd voor de patiënt. Sinds het van kracht worden van deze wet spreekt men terecht over het “patiëntendossier”, dat alle documenten moet bevatten die opgesteld zijn in het kader van de professionele relatie tussen patiënt en zorgverstrekker. De patiënt heeft recht op bescherming van de persoonlijke levenssfeer bij iedere tussenkomst van de beroepsbeoefenaar. Er is geen inmenging toegestaan ten opzichte van dit recht, tenzij dit is voorzien bij wet en nodig is voor de bescherming van de volksgezondheid of voor de bescherming van de rechten en de vrijheden van anderen.

Det is niet meteen duidelijk tot wie de patiënt zijn **verzoek tot inzage** in het patiëntendossier moet richten. Volgens artikel 9 §1 van de Wet Patiëntenrechten heeft de patiënt ten opzichte van de beroepsbeoefenaar recht op een zorgvuldig en veilig bewaard patiëntendossier. Vaak is de verantwoordelijke voor het patiëntendossier door de wetgever bepaald, zoals de huisarts voor het Algemeen Medisch dossier (Art 3 van het KB van 3 mei 1999), de hoofdgeneesheer in verband met het medisch dossier en het verpleegkundig dossier in het ziekenhuis (art 3 van het KB van 28 december 2006 inzake de minimumvoorwaarden waaraan een verpleegkundig dossier in het ziekenhuis moet voldoen en art 25 van het KB 10 juli 2008 houdende coördinatie van de wet betreffende de ziekenhuizen en andere zorginstellingen), de arbeidsgeneesheer-preventieadviseur (Art 93 van het KB gezondheidstoezicht werknemers) of de beroepsbeoefenaar bij het Centrum voor leerlingenbegeleiding (Art 3 van het besluit 12 september 2008 betreffende de CLB).
Maar niet in alle gevallen is de verantwoordelijke voor het beheer van het medisch dossier ook de beroepsbeoefenaar tot wie de patiënt in relatie staat. Zo wordt het medisch dossier in het ziekenhuis beheerd door de hoofdgeneesheer, terwijl hij niet de beroepsbeoefenaar is die de gezondheidszorg levert.

E-health is een federaal **beveiligd** elektronisch platform waar alle spelers uit de gezondheidszorg samenwerken om de veiligheid van de patiënt te verbeteren. Het platform zal ook de administratieve formaliteiten trachten terug te dringen. Gevoelige persoonsgegevens zullen aan de hand van dit systeem via elektronische weg consulteerbaar worden door verschillende gezondheidswerkers en de patiënt.
Interoperabiliteit tussen de diverse actoren in de binnen de gezondheidszorg kan pas gerealiseerd worden wanneer er duidelijke afspraken gemaakt worden. De regels handelen over gegevensuitwisselingen, de algemene architectuur van het uitwisselingssysteem, de uitgewisselde berichten, de structuur van medische documenten en de codificatie van de informatie.

Elke (poging tot) toegang tot het netwerk en de consultatie of publicatie van persoonsgegevens die de gezondheid betreffen, worden geregistreerd. Met deze maatregel kan een controle worden uitgevoerd op de correcte werking van het toegangsbeheer en kunnen (pogingen tot) inbreuken worden gecontroleerd zowel door de beheerders in het kader van de correcte werking van het systeem als op vraag van de patiënt bij de uitoefening van zijn patiëntenrechten.

Wij pleiten er ook voor dat deze **veiligheidsloggings** niet zo maar bewaard worden, doch ook opgevolgd worden. De opspoorbaarheid van ongeoorloofde inzage is het beste middel om deze ongezonde nieuwsgierigheid te bannen. In dit verband weten we dat ongeoorloofde inzage al wel eens gebeurt door onze informatici. Zij zitten aan de bron en kunnen nadien de sporen hiervan uitwissen. Binnen een netwerk waarin medische gegevens circuleren is een logging van de bewegingen door een onafhankelijke superviserende entiteit noodzakelijk.
Timestamping van de loggings via het e-healthplatform kan zo goed als gratis en weinig omslachtig een irreversibel bewijs vormen.

In het kader van de uitwisseling van gezondheidsgegevens tussen de Belgische gemeenschap van ziekenhuizen en artsen, kan het e-health platform rekenen op de technische ondersteuning van de Belgian Care Providers Telematic Advisory Group, ook gekend als de **G19**. Deze groep formuleert onder meer voorstellen op het vlak van de algemene architectuur van het

platform. De globale architectuur van het uitwisselingssysteem "**hubs-metahub**" wordt aldus besproken binnen deze groep.

Patiënt moet de mogelijkheid hebben om te weigeren dat bepaalde persoonsgegevens die de gezondheid betreffen, worden uitgewisseld, evenals dat een welbepaalde zorgverstrekker of –instelling kennis kan krijgen van een deel of het geheel van zijn persoonsgegevens die de gezondheid betreffen. Patiënt heeft tevens de mogelijkheid om aan bepaalde personen (familieleden, vertrouwenspersonen) toegangsrechten tot de elektronisch gedeelde persoonsgegevens die de gezondheid betreffen te verlenen door middel van mandaten. Identificatie en authenticatie van patiënten zijn essentieel voor een adequate toegangsbeheer.

In de mate dat persoonsgegevens worden meegedeeld tussen beroepsbeoefenaars in de gezondheidszorg in het kader van de behandeling van een specifieke patiënt en er aldus sprake is van een gedeeld beroepsgeheim, kunnen **enkel** die gegevens worden gebruikt die **relevant, noodzakelijk en pertinent** zijn voor de concrete behandeling van de patiënt en meer algemeen voor het verzekeren van de continuïteit van de zorgen.

In een ziekenhuis is het bewijs van een therapeutische relatie de gewone inschrijvingsprocedure. Het lezen van de elektronische identiteitskaart is een sterk authenticatiemiddel van de patiënt. Dit kan nog versterkt worden indien de bijhorende pincode wordt gevraagd. Hoewel er , in tegenstelling tot de eID, geen authenticatiecertificaat op de SIS-kaart aanwezig is, kan ook het lezen van de SIS-kaart aan de patiënt in de ziekenhuissetting wijzen op een therapeutische relatie tussen de patiënt en de behandelende ziekenhuisgeneesheer. Mits fysische controle van de identiteitsgegevens van de SIS-kaart aan de hand van andere bronnen (bv. de identiteitskaart), kan het lezen van de SIS-kaart eveneens als een sterk bewijsmiddel van de therapeutische relatie beschouwd worden.
De geldigheidsduur van de toegangsrechten is beperkt tot drie maanden indien de behandeling wordt verstrekt in het kader van een hospitalisatie of een ambulante behandeling.
De geldigheidsduur is beperkt tot één maand op de spoedgevallendienst of naar aanleiding van een MUG-interventie. Indien patiënt evenwel gehospitaliseerd wordt, geldt voor de toegangsrechten de geldigheidsduur van de hospitalisatie.

Op het niveau van de geneesheer-specialist buiten het ziekenhuis is het bewijs van de therapeutische relatie:
- het lezen van de e-ID van de patiënt
- het lezen van de SIS-kaart van de patiënt
- de aanwezigheid van een zorgtraject

De geldigheidsduur van de toegangsrechten bedraagt zes maanden behalve bij aanwezigheid van een zorgtraject behoudens vroegtijdige beëindiging de periode van het zorgtraject bedragen. (in principe vier jaar)
Indien de geneesheer-specialist een andere geneesheer-specialist vervangt, zal de vervangen geneesheer-specialist zijn bestaande toegangsrechten moeten delegeren voor de periode waarin hij wordt vervangen voor zover de vervangende geneesheer-specialist niet in staat zou zijn om met betrekking tot een specifieke patiënt beroep te doen op zijn eigen toegangsrechten. Dit neemt niet weg dat de geneesheer-specialist die de vervanging uitvoert, gelet op het recht van de patiënt op de vrije keuze van zorgverstrekker, slechts gebruik mag maken van de hem overgedragen toegangsrechten voor zover de patiënt in kwestie zijn of haar al dan niet impliciete toestemming heeft verleend aan de tussenkomst van de geneesheer-specialist die de vervanging uitvoert.

Op niveau van de huisarts is het bewijs van therapeutische relatie:
- het statuut van GMD-houder
- het lezen van de e-ID van de patiënt
- het lezen van de SIS-kaart
- de aanwezigheid van een zorgtraject
- inschrijving in een Medisch Huis

De geldigheidsduur bedraagt maximum 12 maanden voor de GMD-houder.
De geldigheidsduur bedraagt 6 maanden bij bewijs via e-ID en SIS-kaart.
De geldigheidsduur bedraagt 4 jaar voor een zorgtraject.
De inschrijving in een Medisch Huis is niet beperkt in tijd en dus geldig tot beëindiging van de inschrijving.

Op niveau van groepspraktijken of netwerken zal in afwachting van de concrete uitvoering van de registratie van groepspraktijken van huisartsen, verplicht zijn een mandaat te verlenen aan zijn collega's opdat zij zich zouden kunnen beroepen op de bewijsmiddelen van een therapeutische relatie waarover de huisarts in kwestie beschikt.

Thans zijn ook pilootprojecten gelanceerd voor een **elektronisch medisch voorschrift.** Het principe is eenvoudig. De arts maakt op zijn computer een voorschrift aan. Dit kan worden afgedrukt en meegegeven met de patiënt, maar wordt tegelijk ook verzonden naar een centrale server. De uitvoerende apotheker, kinesist of verpleegkundige heeft dan de mogelijkheid om langs deze weg de informatie op te vragen, uit te voeren en eventueel via dezelfde weg feedback te geven. Bedoeling is dat het systeem ook gekoppeld wordt aan andere reeds bestaande elektronische platformen zoals e-health en myCareNet. Het elektronisch voorschrift heeft verschillende voordelen: een groter comfort voor de patiënt, winst aan doeltreffendheid, een afname van de kosten dankzij de vereenvoudiging en een kleiner risico op verkeerd lezen en vervalste voorschriften. Er is ook een betere controle op het antibioticabeleid en de workflow voor cytostaticavoorschriften. Elk jaar worden in ons land zowat 100 miljoen medische voorschriften verstrekt.

Het elektronisch voorschrift is een etappe naar de ontwikkeling van een **farmaceutisch dossier**. Dit geeft meer inzicht bij consultatie en een betere opvolging van huis-, ambulante en chronische medicatie. Voor het eerst heeft de apotheker zicht op de volledige medicamenteuze therapie en kan hij daarmee rekening houden bij de beslissing om een bepaald medicijn af te leveren. Naar de toekomst wordt het systeem uitgebreid met mobiele oplossingen en verbreding van het project naar niet-medische voorschriften. Het zal nog een hele klus zijn om de wetgeving betreffende de privacy en het beroepsgeheim strikt te respecteren. Voor de arts is zorgvuldigheid essentieel. Er is nood aan werkzame oplossingen voor de elektronische identificatie en authenticatie van personen, niet in het bezitvan een elektronische identiteitskaart. Bijvoorbeeld personen die niet in de Belgische bevolkingsregisters ingeschreven zijn, kinderen jonger dan 12 jaar, verloren of vergeten eID…

Ter aanpassing van het wettelijk kader is op 15 juli 2004 art 21 van het KB 78 aangepast. Indien gebruik gemaakt wordt van de **elektronische handtekening** dient deze geavanceerd te zijn, gerealiseerd op basis van een gekwalificeerde certificaat en aangemaakt door een veilig middel. De koning kan eventuele aanpassingsmodaliteiten bepalen, alsook voorzien in

mogelijke afwijkingen van deze vereisten voor het gebruik van de elektronische handtekening binnen de ziekenhuizen.
In het KB van 7 juni 2009 worden de criteria bepaald voor het gebruik van een elektronisch voorschrift binnen het ziekenhuis. Meer bepaald wordt de opstelling voorzien van een informaticaprotocol tussen enerzijds de directie van het ziekenhuis, de hoofdgeneesheer, de apotheker-titularis of hoofdapotheker en de verantwoordelijke van de informatica en anderzijds elke voorschrijvende geneesheer en beoefenaar van de tandheelkunde.

Als slot mag ik U melden dat er op dit ogenblik reeds 12.000 artsen hun beveiligde **e-mail verbinding met de Nationale Raad geactiveerd** hebben. Vanuit de provincie Antwerpen zijn er dat ongeveer 2.300. Onze provincie is koploper, zowel in absoluut aantal, als in dekkingsgraad met 35 %. Wij vragen dat alle artsen zonder uitstel hun persoonlijke account zou willen activeren. Artsen die hun toegangscode niet meer bezitten of die problemen ondervinden met het activeren, kunnen hiervoor contact opnemen met de Nationale Raad door een bericht te sturen naar info@ordomedic.be.
Samengevat zijn de voordelen van het intranet:

1. een beveiligde e-mail communicatie tussen één of meerdere collega's
2. het op de hoogte blijven van de belangrijke informatie door de nieuwsbrieven van de Nationale Raad
3. het is een eenvoudige manier om de adviezen van de Nationale Raad op te zoeken.
4. het is de aanzet naar **elektronische verkiezingen** in 2012, zeker voor degenen die vorige verkiezingen met lange benen naar de post liepen om hun aangetekende stemformulieren te gaan afhalen en terug te bezorgen.