Bespreking encryptie en privacy in het kader van dataextractie uit het EMD van de huisarts.

Auteurs: Koen Thomeer, [vul aan wie meewerkt]

Status: intern

Doel: dit document heeft als doel de verschillende vormen van encryptie te bespreken die van nut kunnen zijn bij het extraheren van data in de praktijk. Daarbij wordt de privacywetgeving belicht dat van belang is bij dataverzameling.

1. encryptie en zijn toepassingen

Encryptie heeft als doel dat een derde partij, die soms noodzakelijk is voor de communicatie tussen 2 partijen, niet de inhoud van de communicatie kan zien tussen de 2 partijen. Voor de dataverzameling zal de derde partij vooral 'het internet' zijn, ttz de verschillende servers die als tussenstation dienen voor het overbrengen van het bericht van de ene partij naar de andere. In dit document worden de 2 types van encryptie besproken met zijn toepassingen in de praktijk.

1.1. symmetrische encryptie

Bij symmetrische encryptie wordt dezelfde sleutel gebruikte voor het encrypteren en het decrypteren. Voorbeelden van algoritmes zijn: AES, 3DES, RC4, ...

Voordelen:

- Het en/decrypteren gaat veel sneller dan assymetrische encryptie.

Nadelen:

- hoe gaat men de sleutel veilig overbrengen aan de andere partij, zonder dat de derde partij dit te weten komt? Men kan daarom del sleutel niet open over het internet sturen
- als er meerdere partijen zijn, is voor elke communicatie tussen 2 partijen een andere sleutel nodig. Dat brengt het aantal sleutels op n(n-1)/2, waar n het aantal partijen is.

1.2. asymmetrische encryptie

Voor asymetrische encryptie worden twee sleutels gegenereerd. Hetgeen door de ene sleutel wordt geëncrypteert kan enkel door de andere sleutel gedecrypteerd worden. In de praktijk wordt één sleutel bijgehouden (private sleutel) en de andere sleutel publiekelijk verdeeld (publieke sleutel). Als een partij een bericht wil versturen naar de houder van de private sleutel, kan zij het bericht encrypteren met de publieke sleutel en het bericht veilig verzenden over het internet. Immers enkel de eigenaar van de private sleutel kan dit bericht decrypteren met zijn private sleutel. Voorbeelden van algoritmes zijn: RSA, DSA, ...

Voordelen:

- per partij is er maar 1 sleutelpaar nodig
- publieke sleutel kan zonder probleem over het internet verspreid worden: immers een bericht dat geëncrypteerd is met een publieke sleutel kan niet gedecrypteerd worden met een publieke sleutel

Nadelen:

- Het en/decrypteren gaat langzamer dan symmetrische encryptie

1.3. Toepassing: gemengde encryptie

Om de voordelen van de 2 vorige methodes te combineren, kan men de 2 methodes tegelijk gebruiken. Indien partij B een bericht wilt verzenden naar partij A, encrypteert hij eerst symmetrisch het bericht met sleutel C. Deze encryptie gaat heel snel, aangezien het symmetrisch is. Deze sleutel C encrypteert hij met de publieke sleutel van partij A naar sleutel C'. Aangezien sleutel C veel kleiner is dan het bericht, gaat de relatief snel. Het geencrypteert bericht wordt over het internet verzonden met sleutel C' naar partij A. Niemand op het internet kan het bericht decrypteren omdat ze sleutel C niet hebben of sleutel C' decrypteren omdat de private sleutel niet gekend is. Partij A decrypteert eerst sleutel C' met zijn private sleutel naar sleutel C. Met sleutel C decrypteert hij dan het eigenlijke bericht.

1.4. Toepassing: authenticatie

Men heeft in asymetrische encryptie gezegd dat het de gewoonte is dat voor encryptie de publieke sleutel wordt gebruikt en decryptie de private. Voor authenticatie gebeurt juist het omgekeerde: de private sleutel encrypteert een stukje tekst en deze kan gedecrypteerd worden door elke andere. Iemand die zo'n stukje tekst decrypteert, weet dan dat er maar 1 persoon dit stukje tekst kan geëncrypteerd hebben: de eigenaar van de private sleutel. Dit noemt men authenticatie.

1.5 Toepassing: elektronisch handtekenen

Hiervoor moet het begrip hashing worden uitgelegd. Hashing is een algoritmisch extract van een grote tekst naar een klein stukje tekst. Elke identieke grote tekst heeft exact hetzelfde hashing resultaat. Indien een enkele verandering aangebracht wordt aan de grote tekst zal het hash resultaat totaal verschillend zijn. Uit de kleine hash tekst is het niet mogelijk om de grote tekst te reconstrueren. Vormen van hashing zijn: SHA, MD5, ...

Voor het elektronisch tekenen van een bericht, doet men het volgende. Bericht A wordt gehasht door partij 1. Hieruit komt de kleine hash tekst B. Deze hash tekst B wordt geëncrypteert door partij 1 met zijn private sleutel naar tekst B'. Bericht A verstuurt partij 1 samen met hash tekst B' naar de ander partij 2. Partij 2 wilt weten of dit bericht echt is getekend door partij 1. Hij hasht hiervoor het ontvangen bericht A: hij krijgt hiervoor dezelfde hash tekst B. (Immers elke tekst dat gehasht wordt door hetzelfde hashalgoritme, moet hetzelfde resultaat B geven. Of dit nu door partij 1 of 2 gedaan wordt, maakt niet uit.) Hij decrypteert tekst B' met de publieke sleutel van partij 1. Indien dit resultaat hetzelfde is (= tekst B), als het hash resultaat van grote tekst A, weet hij zeker dat partij 1 de gehashde tekst geëncrypteerd heeft. Vormen van elektronisch tekenen zijn: md5DSA, sha1RSA, ...

Een tekst elektronisch tekenen is dus de tekst hashen en het resultaat encrypteren met de private sleutel. Een elektronische handtekening controleren is het gehashte resultaat decrypteren met de publieke sleutel en nakijken of dit resultaat overeen komt met het resultaat van de gehashte tekst.

1.6. Toepassing: certificaten

Een probleem in de internetwereld is te weten of een publieke sleutel nu echt wel de eigendom is van partij A. Dit lost men op met certificaten: partij C geniet het vertrouwen van alle partijen. Hetgeen partij C tekent, wordt algemeen aanvaard. Partij C kan naast de publieke sleutel van partij A de naam van partij A bijvoegen. Dit geheel (publieke sleutel en naam van partij A) tekent partij C met zijn private sleutel, omdat partij C gecontroleerd heeft of de sleutel toebehoort aan partij A. Partij B die zo'n getekende sleutel met tekst ontvangt, kan op de tekst lezen van wij deze sleutel is. Aangezien dit getekend is door partij C, die hij vertrouwt, weet hij zeker dat deze publieke van

partij A is. Zo'n getekende publieke sleutel met tekst noemt men een certificaat. Een internationale standaard van zo'n certificaat is de x509.

1.7 Encryptie bij dataverzameling.

Aangezien de data over het internet wordt verzonden, is encryptie noodzakelijk. Vermoedelijk zal asymetrische encryptie voldoen, aangezien de data klein is (gemengde encryptie is niet nodig).

Om de publieke sleutels van de partijen te certificieren, zou men voor gemeenschappelijke vertrouwde partner ehealth kunnen kiezen. Een andere mogelijkheid is ict-health.be.

2. Privacywetgeving

In dit onderdeel wordt eerst de theorie weergegeven over de privacywetgeving, dewelke van belang is bij een dataverzameling. Daarna wordt zijn toepassing besproken in het kader van dataverzameling.

2.1. Toepassingsgebied

De privacywetgeving is van toepassing op alle persoonsgegevens, al dan niet gecodeerd. Anonieme gegevens vallen buiten de privacywetgeving, omdat dit geen persoonsgegevens zijn. Voor de definitie anoniem is de privacywetgeving zeer strik. “Persoonsgegevens zijn maar anoniem indien niemand ooit in staat is om te achterhalen over wie het gaat. Dit veronderstelt niet alleen dat naam en adres worden weggelaten, maar ook dat andere ruim of gemakkelijke gekende gegevens worden vervaagd: geen geboortedatum, maar enkel leeftijdscategorie, geen woonplaats, maar eerder arrondissement, geen precieze beroepscategorie en zo verder tot er geen enkele kans op herkenning meer is.”[i] De interpretatie tot de kans op herkenning behoort toe tot de privacycommissie of diens sectoraal comités.

2.2. Aangifte aan de privacycommissie

Art. 17. §1. “Voordat wordt overgegaan tot één of meer volledig of gedeeltelijk geautomatiseerde verwerkingen van gegevens die voor de verwezenlijking van een doeleinde of van verscheidene samenhangende doeleinden bestemd zijn, doet de verantwoordelijke voor de verwerking of, in voorkomend geval, diens vertegenwoordiger, daarvan aangifte bij de Commissie voor de bescherming van de persoonlijke levenssfeer.”

Dat betekent dat alle verwerking moeten aangegeven worden. Niet alleen de dataverzameling voor het wetenschappelijk onderzoek, echter ook elk EMD dat door de huisarts gebruikt wordt moet aangegeven worden aan de privacycommissie. Een EMD is immers ook een verwerking, immers art. 1. §3. zegt: “Onder “verwerking” wordt verstaan elke bewerking of elk geheel van bewerkingen met betrekking tot persoonsgegevens, al dan niet uitgevoerd met behulp van geautomatiseerde procédés, zoals het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op enigerlei andere wijze ter beschikking stellen, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van persoonsgegevens.”

2.3. “De verwerking van persoonsgegevens die de gezondheid betreffen, is verboden”

Dit is art. 7. §1 van de privacywet. In §2 worden de uitzondering besproken, dewelke werken met een EMD, als het verzamelen van data voor wetenschappelijk onderzoek mogelijk maakt.

2.3.1. Uitzondering: "wanneer de verwerking noodzakelijk is voor doeleinden van preventieve geneeskunde of medische diagnose, het verstrekken van zorg of behandelingen aan de betrokkene of een verwant, of het beheer van de gezondheidsdiensten handelend in het belang van de betrokkene en de gegevens worden verwerkt onder het toezicht van een beroepsbeoefenaar in de gezondheidszorg" (sub j, art 7 §2)

Dit wil dus zeggen, dat alle verwerking in het kader van de zorg, mogelijk is. Er zijn hier ook geen beperkingen opgelegd, buiten dat de verwerker een beroepsbeoefenaar moet zijn en dat er ook een aangifte moet gebeuren volgens art. 17.

Praktisch wilt dit zeggen dat verzameling van gegevens in het kader van de zorg ('zorgproject': zorgpaden, zorgtrajecten, ...) onder deze regeling vallen. Er is dus geen nood aan een Trusted Third Party, zoals hieronder besproken voor een wetenschappelijk onderzoek, zolang de gegevens in het kader van de zorg gebruikt worden.

2.3.2. Uitzondering: "wanneer de verwerking noodzakelijk is voor het wetenschappelijk onderzoek en verricht wordt onder de voorwaarden vastgesteld door de Koning bij een in Ministerraad overlegd besluit, na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer" (sub k, art 7 §2)

Dit artikel maakt wetenschappelijk onderzoek op gezondheidsgegevens dus mogelijk. In dit artikel wordt verwezen naar toekomstige voorwaarden. Deze zijn gepubliceerd in de uitvoerinsbesluiten van 13 februari 2001, onder de noemer "Latere verwerking van persoonsgegevens voor historische, statistische of wetenschappelijke doeleinden".

2.3.2.1. Bewaartermijn

Persoonsgegevens dienen in een vorm die het mogelijk maakt de betrokkenen te identificeren, niet langer te worden bewaard dan voor de verwezenlijking van de doeleinden waarvoor zij worden verkregen of verder worden verwerkt, noodzakelijk is. (art 4, §1 5° PrivacyWet).

Dat wil dus zeggen dat ALLE persoonsgegevens maar een beperkte duur hebben. Anonieme gegevens vallen dus hier niet onder.

2.3.2.2. Verwerking (anoniem – gecodeerd – niet gecodeerd)

1. *De verwerking van persoonsgegevens gebeurt aan de hand van **anonieme gegevens** (art 3 uitvoeringsbesluiten).*

Dit is de preferentiële manier waarop wetenschappelijk onderzoek zou moeten gebeuren. Dit heeft echter zware beperkingen: het is dan niet mogelijk om een longitudinaal onderzoek op te zetten, aangezien men de gegevens niet met elkaar kan linken. Ze zijn immers anoniem, of zoals de wet zegt: "gegevens die niet met een geïdentificeerd of identificeerbaar persoon in verband kunnen worden gebracht".

2. *Indien een latere verwerking van anonieme gegevens niet de mogelijkheid biedt de historische, statistische of wetenschappelijke doeleinden te verwezenlijken, mag de verantwoordelijke voor de latere verwerking voor historische, statistische of wetenschappelijke doeleinden overeenkomstig de bepalingen van afdeling 2 van dit hoofdstuk **gecodeerde persoonsgegevens** verwerken (art 4 uitvoeringsbesluiten).*

Op deze manier kan men wel een longitudinaal onderzoek verrichten, immer men kan de persoonsgegevens die op verschillende momenten zijn verzameld met elkaar verbinden aan de hand van een code. De wet zegt over gecodeerde persoonsgegevens: "persoonsgegevens die slechts door middel van een code in verband kunnen worden gebracht met een geïdentificeerd of identificeerbaar

persoon".

3. *Indien een latere verwerking van gecodeerde gegevens niet de mogelijkheid biedt de historische, statistische of wetenschappelijke doeleinden te verwezenlijken, mag de verantwoordelijke voor de latere verwerking overeenkomstig afdeling 3 van dit hoofdstuk* ***niet gecodeerde persoonsgegevens*** *verwerken (art 5 uitvoeringsbesluiten).*

Niet gecodeerde persoonsgegevens zijn meestal niet nodig voor het uitvoeren van wetenschappelijk onderzoek. Ze zijn hier dus niet van toepassing.

4. *De verantwoordelijke voor de latere verwerking van persoonsgegevens voor historische, statistische of wetenschappelijke doeleinden mag geen handelingen verrichten die zijn gericht op de omzetting van anonieme gegevens in persoonsgegevens of van gecodeerde persoonsgegevens in niet-gecodeerde persoonsgegevens (art 6 uitvoeringsbesluiten).*

Dit is logisch. Dat wil zeggen dat er toch een vorm van supervisie en eindverantwoordelijkheid noodzakelijk is voor het uitvoeren van het wetenschappelijk onderzoek. Daarbij stelt art 7 §4 van de privacywet dat de verwerker van gezondheidsgegevens een arts moet zijn. Dit geldt ook voor wetenschappelijk onderzoek van medische gegevens.

2.3.2.3. Codering

1. "*Persoonsgegevens worden gecodeerd alvorens later op enigerlei wijze voor historische, statistische of wetenschappelijke doeleinden te worden verwerkt" (art 7 uitvoeringsbesluiten).*

Art 8 tem 10 geven de verschillende modaliteiten hoe persoonsgegevens moeten worden gecodeerd. Men spreekt hier van intermediaire organisatie, dat door de wet als volgt wordt geformuleerd: *"de natuurlijke persoon, de rechtspersoon, de feitelijke vereniging of de openbare overheid, andere dan de verantwoordelijke voor de verwerking van de niet-gecodeerde gegevens, die voornoemde gegevens codeert"*. In de omgangstaal spreekt men over een Trusted Third Party (TTP). Er zijn dus niet veel voorwaarden voor een TTP, behalve dat het niet de verantwoordelijk mag zijn van de verwerking.

2.1. *"Ingeval de verantwoordelijke voor de verwerking van persoonsgegevens verzameld voor bepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden die persoonsgegevens later verwerkt voor historische, statistische of wetenschappelijke doeleinden of die verwerking toevertrouwt aan een verwerker, worden die persoonsgegevens voorafgaand aan de latere verwerking ervan gecodeerd, hetzij door de verantwoordelijke voor de verwerking, hetzij door de verwerker, hetzij door een intermediaire organisatie.*

In dit laatste geval wordt de intermediaire organisatie beschouwd als een verwerker in de zin van artikel 1, § 5, van de wet." (art. 8 uitvoeringsbesluiten).

Dit wilt zeggen, dat indien het de verantwoordelijke van de primaire verwerking ook de medische gegevens later verwerkt voor wetenschappelijk onderzoek (of indien de resultaten voor hem bestemd zijn), de codering mag gedaan worden door de volgende:

- de verantwoordelijke van de verwerking
- de uitvoerder van het wetenschappelijk onderzoek
- een intermediaire organisatie (TTP)

Men is hier dus niet verplicht een (dure) TTP te betrekken.

In de praktijk kan dit van toepassing zijn, indien men de medische gegevens reeds verzameld is in het kader van de zorg, zoals gezegd bij bevoorbeeld een zorgproject (zorgtraject, zorgpad, ...). De verantwoordelijke van het zorgproject kan dan zelf de gegevens coderen om het later te gebruiken voor wetenschappelijk onderzoek.

2.2. *“Ingeval de verantwoordelijke voor de verwerking van persoonsgegevens verzameld voor bepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden deze persoonsgegevens aan een derde meedeelt met het oog op een latere verwerking voor historische, statistische of wetenschappelijke doeleinden, worden die persoonsgegevens voorafgaand aan die mededeling gecodeerd door de verantwoordelijke voor de verwerking of door een intermediaire organisatie.*

In dit laatste geval wordt de intermediaire organisatie beschouwd als een verwerker in de zin van artikel 1, § 5, van de wet.” (art. 9 uitvoeringsbesluiten).

In tegenstelling tot het vorige punt (art. 8) is de verantwoordelijke van de primaire verwerking niet de uitvoerder van het wetenschappelijk onderzoek. De codering mag dan slechts gedaan worden door de volgende:

- de verantwoordelijke van de verwerking
- een intermediaire organisatie (TTP)

Dit kan bijvoorbeeld het RIZIV zijn die zijn gegevens laat onderzoeken door het Federaal Kenniscentrum (KCE) voor wetenschappelijk onderzoek. Het RIZIV zal dan eerst zijn gegevens coderen, alvorens het door te sturen naar het KCE.

2.3. *“Ingeval verscheidene verantwoordelijken voor verwerkingen van persoonsgegevens verzameld voor bepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden aan dezelfde derde(n) persoonsgegevens meedelen met het oog op de latere verwerking ervan voor historische, statistische of wetenschappelijke doeleinden, worden die persoonsgegevens voorafgaand aan die mededeling gecodeerd door een intermediaire organisatie.*

In dit geval wordt de intermediaire organisatie beschouwd als een verantwoordelijke voor de verwerking in de zin van artikel 1, § 4, van de wet.” (art. 10 uitvoeringsbesluiten).

In tegenstelling tot het vorige punt (art. 9) zijn er meerdere primaire verwerkers. De codering mag dan slechts gedaan worden door:

- een intermediaire organisatie (TTP)

De TTP verzamelt dan val alle mogelijk bronnen de gegevens, codeert deze en geeft deze dan gecodeerd door aan de wetenschappelijke onderzoeker. Men kan zich afvragen waarom elke verantwoordelijke van de verwerking niet zelf mag coderen en dan doorsturen naar de onderzoeker. Hiervoor zijn verschillende redenen:

- indien de gegevens komen van de TTP is de bron van de gegevens niet traceerbaar voor de onderzoeker. Indien het direct komt van de bron (=primaire verwerker), dan kan de onderzoeker markeren in zijn gegevens van welke bron deze gegevens afkomstig zijn.
- de TTP kan de gegevens met elkaar linken (bvb aan de hand van het INSZ) en deze dan doorgeven aan de onderzoeker zonder INSZ

In de praktijk is dit onderdeel van toepassing indien men data wilt verzameling het EMD's van huisartsen. De TTP ontvangt deze, codeert en stuurt het door naar de onderzoeker.

3. Voorwaarden voor codering

- art 11 van de uitvoeringsbesluiten stelt dat een TTP onafhankelijk is van de onderzoeker
- art 12 van de uitvoeringsbesluiten stelt dat de codeerder de gepaste maatregelen neem om te verhinderen dat de gecodeerde gegevens kunnen omgezet worden in niet-gecodeerde gegevens
- art 13 van de uitvoeringsbesluiten stelt dat de onderzoeker een aangifte moet indienen voor het onderzoek met gecodeerde gegevens aan de privacycommissie. Letterlijk staat erin dat de codeerder de gecodeerde gegevens pas mag vrijgeven aan de onderzoeker tegen

voorlegging van het bewijs van aangifte aan de privacycommissie.

- art 14 van de uitvoeringsbesluiten stelt dat bij data dat gezondheidsgegevens bevat, de betrokken personen (van wie de gegevens komen: dus niet de primaire verwerker, maar de patient zelf) moeten verwittigd worden indien de data gaat gecodeerd worden (en dus later gebruikt voor wetenschappelijk onderzoek). Volgende elementen moeten gemeld worden aan de patiënt:
    - de identiteit van de verantwoordelijke voor de verwerking,
    - de verwerkte categoriee¨n van persoonsgegevens,
    - de herkomst van de gegevens,
    - een precieze omschrijving van de historische, statistische of wetenschappelijke doeleinden van de verwerking,
    - de personen of de categorieën van personen voor wie de persoonsgegevens bestemd zijn,
    - het bestaan van een recht op raadpleging van zijn eigen persoonsgegevens, alsook van een recht op verbetering ervan,
    - het bestaan van een recht van verzet in hoofde van de betrokken persoon.
- art 15 van de uitvoeringsbesluiten zegt dat art. 14 niet moet uitgevoerd worden,
    - indien deze verplichting onmogelijk blijkt of onevenredig veel moeite kost. Men moet dan wel aan de verplichting voldoen van art 16 van het besluit. Dit zal vooral van toepassing zijn bij dataverzameling bij huisartsen.
    - indien de intermediaire organisatie een administratieve overheid is die door of krachtens de wet de uitdrukkelijke opdracht heeft om persoonsgegevens samen te brengen en te coderen, en hierbij onderworpen is aan door of krachtens de wet vastgelegde specifieke maatregelen die de bescherming van de persoonlijke levenssfeer tot doel hebben.
- art 16 van de uitvoeringsbesluiten stelt dat men aan aangifte moet doen aan de privacycommissie, indien men niet aan de verplichtingen van art 14 kan voldoen omdat het onmogelijk blijkt of indien het onevenredig veel moeite kost. Volgende elementen moeten in de aangifte staan:
    - de precieze omschrijving van de historische, statistische of wetenschappelijke doeleinden van de verwerking,
    - de redenen ter verantwoording van de verwerking van persoonsgegevens bedoeld in de artikelen 6 tot 8 van de wet,
    - de redenen waarom aan de betrokken persoon de gegevens vermeld in artikel 14 niet kunnen worden meegedeeld of de onevenredigheid van de moeite nodig om zulks te doen,
    - de categorieën van personen van wie persoonsgegevens bedoeld in de artikelen 6 tot 8 van de wet worden verwerkt,
    - de personen of de categoriee¨n van personen die de persoonsgegevens kunnen raadplegen;
    - de herkomst van de gegevens.

  De privacycommissie moet dan binnen een termijn van 45 werkdagen (kan éénmalig verlengd worden) een aanbeveling geven met eventueel de bijkomende voorwaarden voor later wetenschappelijk onderzoek.

Meestal stelt de privacycommissie de volgende voorwaarden in het kader van dataverzameling bij huisartsen:

  - poster in de wachtzaal
  - folder voor de patiënt
  - actieve bevraging door de huisarts zelf

  De aanbeveling van de commissie wordt publiek gemaakt.

- art 17 van de uitvoeringsbesluiten stelt dat elke wijziging in de gegevens aan de privacycommissie medegedeeld, weer gemeld moet worden.

2.4 Praktische toepassingen

Na de uiteenzetting van de wet gaan we dit in de praktijk brengen met 2 vormen van dataverzameling die op het vlak van huisartsgeneeskunde van toepassing zijn.

2.4.1. De medische gegevens zijn reeds verzameld (in het kader van de zorg).

Dit zou kunnen zijn in het kader van een zorgproject. Een kring verzorgt de wachdienst en het medisch dossier hiervan staat op één centrale server. Of een kring heeft een zorgpad diabetes waar de gegevens worden opgeslagen op één centrale server.

Vooraleerst moet elke verwerking, ook in het kader van de zorg, aangegeven worden aan de privacycommissie. Dit kan éénvoudig op de website gebeuren. Men noemt dit de primaire verwerking. Dit heeft nog niks te maken met het wetenschappelijk onderzoek.

Men heeft dan de keuze: gaat men in het kader van wetenschappelijk onderzoek gaan werken met gecodeerde gegevens of gaat men werken met anonieme gegevens?

Het voordeel van anonieme gegevens is dat deze gegevens buiten de privacywet vallen en dat men aan de verplichte aangiftes en meldingen hierboven beschreven niet moet voldoen. Men moet de patiënt ook niks melden, dewelke veelal storend kunnen zijn voor de arts-patiënt relatie. Anonieme gegevens kan men echter niet linken intern (patiënt is meerdere keren langsgeweest, dus longitudinaal) of extern (kijken of patiënt ook zorg heef geconsumeerd in het nabijgelegen ziekenhuis).

Het voordel van gecodeerde gegevens is dat men de gegevens longitudinaal kan linken aan de hand van een code. Men kan dus zien of een patiënt verschillende keren is terugekomen. Men kan de gecodeerde gegevens ook gaan linken met externe databases aan de hand van het INSZ. Men kan dan zien of dezelfde patiënt zich die dag nog heeft aangemeld aan het ziekenhuis.

Indien men beslist de gegevens te gaan coderen, moet men volgende aangiftes doen aan de privacycommissie:

- aangifte van codering (art 13 uitvoeringsbesluiten)
- daarna aangifte dat men niet kan voldoen een art 14 wegens onmogelijkheid of onevenredigheid (art 16 uitvoeringsbesluiten). De privacycommissie zal dan binnen de 45 werkdagen een antwoord formuleren.

De codering mag gebeuren door:

- de verantwoordelijke van de primaire verwerking, dus in casu de kring (art. 8 uitvoeringsbesluiten)
- indien er externe bronnen worden gelinkt, moet men een TTP inschakelen (art. 10 uitvoeringsbesluiten). Alle data (vb kring en ziekenhuis) passeren eerst de TTP.

2.4.2. De medische gegevens worden geëxtraheerd uit het EMD van de huisartsen in het kader van wetenschappelijk onderzoek.

Meestal betreft dit een longitudinaal onderzoek en zal men dus werken moet gecodeerde gegevens. Aangezien er verschillende bronnen zijn (meerdere EMD's) moet er gewerkt worden met een TTP.

Praktisch zal er dus een aangifte van codering, alsook aangifte dat men niet kan voldoen aan art. 14 wegens onmogelijkheid of onevenredigheid.