Verwerkingsregister: checklist

Werkwijze, Aanvullingen en tips op het model verwerkingsregister

Over het verwerkingsregister

Vanuit Domus Medica hebben we een model verwerkingsregister opgesteld met een heel aantal mogelijke situaties van gegevensverwerking. Het is belangrijk om op te merken dat dit niet noodzakelijk een exhaustieve lijst is van alle situaties die zich voordoen, u dient voor de eigen praktijk of wachtpost dus te overlopen welke situaties van toepassing zijn, of u de voorgestelde maatregelen al dan niet neemt en of u mogelijk nog bijkomende stappen rond de veiligheid van persoonsgegevens kunt toevoegen. Het dient dus een gepersonaliseerd document te worden dat accuraat weergeeft welke gegevens worden verwerkt, om welke reden, en welke maatregelen er genomen worden om deze veilig te bewaren en verwerken.

Een verwerkingsregister is een werkdocument dat de processen op een bepaald moment weergeeft. Bij wijzigingen in de organisatie rond de manier waarop gegevens worden verwerkt, dient het register dus te worden aangepast.

Inleiding: gebruik van het verwerkingsregister

Indeling in verschillende tab-bladen

Het eerste tab-blad (Algemene informatie) omvat alle contactgegevens van de verwerkingsverantwoordelijke en eventuele functionaris gegevensbescherming. Dit algemene invulblad is weergegeven met blauw.

Voor elk verwerkingsdoel dient te worden weergegeven welke gegevens worden bewaard, hoe deze worden verwerkt, met welke rechtsgrond,…. In dit register wordt voor elk verschillend verwerkingsdoel een nieuw tab-blad voorzien, weergegeven in het groen.

Een algemeen overzicht van alle onderdelen van het register vindt u onder het tab-blad ‘Algemeen overzicht’. U kan van hieruit naar elk werkblad in het register springen door op de namen van de tab-bladen te klikken. Er wordt ook uitgelegd hoe u bij het toevoegen van bijkomende verwerkingsdoelen dit overzicht kan aanpassen.

Invullen van de velden bij de verwerkingsdoelen

Op elk tabblad zijn de verschillende elementen weergegeven die een register dienen te bevatten. Indien een kolom of rij in het lichtgeel is weergegeven, wil dit zeggen dat er een dropdown-menu beschikbaar is. Bijkomende uitleg over de elementen in de dropdown-menu’s kan u achteraan vinden onder het tab-blad ‘Informatie_Lijsten’ (grijze kleur).

Soms is een veld in het felgeel weergegeven. Dit wil zeggen dat de omschrijving in de velden niet gebaseerd zijn op specifieke wetgeving, maar een mogelijke afbakening van een bewaartermijn voorstellen. U dient dit dus aan te passen naar de geldende regels rond bewaartermijn binnen uw organisatie.

Deel 1: Invullen van het verwerkingsregister

In dit document willen we de elementen uit het verwerkingsregister overlopen, met nog bijkomende uitleg en tips voor het creëren van een veilige omgeving voor het verwerken van persoonsgegevens.

Stap 1: Verantwoordelijke voor de gegevensverwerking

De verwerkingsverantwoordelijke zal globaal genomen de huisartsenpraktijk, -kring of wachtpost zijn. Binnen de praktijk of wachtpost dient er een naam te worden opgegeven van wie als contactpersoon fungeert en voor de opvolging en implementatie van het verwerkingsregister zorgt. Let wel: deze persoon heeft niet de functie van functionaris gegevensbescherming of data protection officer (DPO)[1]. Het betreft louter de contactpersoon binnen de organisatie die zorgt voor het up-to-date houden van het verwerkingsregister en opvolgt of de genomen maatregelen rond gegevensbescherming effectief uitgevoerd worden. Binnen een solo-praktijk zal de verwerkingsverantwoordelijke veelal de huisarts zelf zijn, binnen een groepspraktijk kan de coördinerende rol aan één van de leden van de groepspraktijk worden toegewezen.

Indien er een functionaris gegevensbescherming is aangesteld, kunnen deze contactgegevens ook worden opgenomen.

☐ **Verwerkingsverantwoordelijke toegevoegd aan verwerkingsregister**

☐ **Eventuele contactpersoon gegevensbeschermingsbeleid aangeduid en toegevoegd aan verwerkingsregister**

☐ **Indien functionaris gegevensbescherming of DPO: contactgegevens toegevoegd aan het register**

Stap 2: Doel van de verwerking

Er moet voor elk type van gegevens dat verwerkt wordt, aangegeven worden waarom deze verwerkt worden. Binnen de GDPR mag alleen die informatie verwerkt worden die noodzakelijk is voor het doel waarvoor gegevens werden verzameld. Binnen het voorbeeld-register zijn er verschillende doelcategorieën opgedeeld met elk een eigen pagina die ingevuld kan worden, zoals: patiëntenzorg, boekhouding, medewerkersbeheer (indien er met personeel wordt gewerkt of er meerdere leden in een praktijk werken), agenda en planning en wetenschappelijk onderzoek. Het is mogelijk dat u volgens uw eigen organisatie een aantal doelen in onderdelen wilt opsplitsen, of doelen wilt toevoegen. U kan hiervoor extra werkbladen toevoegen en volgens hetzelfde model verder aanvullen.

Voor elk doel van verwerking dient dus een pagina te worden aangevuld.

☐ **Selectie gemaakt van doelverwerkingen die van toepassing zijn op de praktijk- of wachtpostwerking**

☐ **Indien nodig: bijkomende bladen van doelverwerking toegevoegd die nog niet in het basismodel aanwezig waren.**

[1] Een functionaris gegevensbescherming of data protection officer (DPO) is een persoon die binnen de organisatie adviseert rond het gegevensbeschermingsbeleid. Dit is een persoon met een specifieke opleiding, en kan intern of extern aan de organisatie zijn. Een interne DPO heeft nooit een operationele verantwoordelijkheid binnen de organisatie (dus geen afdelingshoofden, directie,…) en dient zijn taken onafhankelijk te kunnen uitvoeren.

☐ **Indien nodig: Verwijzing naar bijkomende bladen van doelverwerking toegevoegd in het 'Algemeen overzicht'**

Opgelet: Het tab-blad rond patiëntenzorg is de meest uitgebreide pagina. Dit maakt immers de kern uit van de huisartsenpraktijk, en omdat er ook gevoelige gegevens (oa. gezondheidsgegevens) worden verwerkt, dient er duidelijk aangegeven te worden dat aan de wettelijke grondslagen voor het verwerken van gevoelige gegevens is voldaan. Het is immers in principe niet toegestaan om dit soort gegevens te verwerken, tenzij men onder bepaalde uitzonderingsbepalingen valt. Voor de huisartsenpraktijk en wachtpost is dit het geval, maar de wettelijke grondslagen moeten duidelijk vermeld worden, en er dient extra aandacht te zijn voor het veilig bewaren en verwerken van dit soort gegevens. De basisgrondslagen zijn al meegegeven in het model verwerkingsregister.

Stap 3: Bronnen: van waar komt de informatie?

Het is belangrijk aan te geven of uw praktijk of wachtpost zelf de persoonsgegevens verzameld heeft, en indien dit niet zo is, welke bronnen er buiten de organisatie juist zijn. Meestal, zeker in het geval van gegevens die de patiëntenzorg tot doel hebben, komt eventuele bijkomende informatie van andere zorgverleners of zorginstanties. Zo komen laboresultaten van een patiënt weer bij de huisarts terecht om opgenomen te worden in het dossier, kunnen er documenten van ziekenhuisopname bezorgd worden, enzovoort… Soms komen deze resultaten rechtstreeks in het medisch dossier van een patiënt terecht, andere keren worden deze via een applicatie in het medisch dossier geraadpleegd en kan de informatie soms ook in het medisch dossier van de patiënt worden opgenomen (bijvoorbeeld als er informatie via de Hubs wordt opgevraagd).

In het geval van boekhoudingsgegevens is in vele gevallen de persoonsinformatie die verwerkt wordt beperkt, aangezien betalingen van patiënten gepseudonimiseerd verwerkt worden. In het geval u met medewerkers werkt, zal hun contractinformatie en loongegevens wel persoonsgegevens bevatten. U dient dus voor elk verwerkingsdoel uit te maken of en welke persoonsgegevens worden verwerkt, en of deze informatie van interne bronnen komt (verzameld en verwerkt binnen de organisatie), of van externe bronnen (informatie afkomstig van buiten de organisatie, maar verwerkt of bewaard binnen de organisatie).

<u>Binnen de organisatie, voorbeeld patiëntenzorg:</u> alle informatie van de patiënt wordt in of bij het medisch dossier bewaard. Het kan om een louter elektronisch of papieren dossier gaan, of er kunnen papieren documenten apart bewaard worden van het elektronisch dossier. Indien patiëntinformatie gespreid bewaard wordt, dient elke bewaarplaats voldoende afgeschermd te zijn, en dient dit onder deze rubriek gespecifieerd te worden.

<u>Buiten de organisatie, voorbeeld patiëntenzorg:</u> bijkomende informatie rond de patiënt komt van andere zorgverleners of klinische instellingen, die meestal een therapeutische relatie met de patiënt hebben, of die bijkomende onderzoeken hebben uitgevoerd (vb. labo-onderzoek). Hier dient aangegeven te worden welke externe bronnen er zijn, en waar de informatie terechtkomt. Probeer hier een algemene omschrijving te geven van de externe bronnen: zo valt te vermijden dat er onvolledigheden staan als men probeert een exhaustieve opsomming te geven. Belangrijk is om de omschrijving volledig en omvattend te houden.

☐ **Aangeven in het verwerkingsregister voor elk verwerkingsdoel of persoonsgegevens binnen de organisatie verzameld en verwerkt worden**

☐ **Aangeven of er ook externe bronnen zijn die persoonsgegevens aan de organisatie aanleveren, en zo ja, welke.**

Stap 4: Over wie wordt informatie bijgehouden?

Dit zal meestal gaan over de patiënt, medewerkers of zorgverleners binnen de praktijk of wachtpost. Geef de correcte omschrijving over wiens gegevens het gaat aan bij het juiste verwerkingsdoel. Let op: soms worden er ook persoonsgegevens van derden bijgehouden (vb. mantelzorgers, familieleden patiënt indien dit relevantie heeft voor de zorg).

☐ **Bij elk verwerkingsdoel wordt aangegeven over wie informatie wordt bijgehouden (patiënt, medewerker, zorgverlener,…)**

☐ **Binnen de organisatie wordt ook nagegaan of er andere lijsten worden bijgehouden vb. zorgverleners waarmee wordt samengewerkt, artsen uit de kring,…**

☐ **Indien deze lijsten worden bijgehouden, wordt gekeken naar de noodzaak om deze bij te houden, onder welk verwerkingsdoel deze worden bewaard, en of deze voldoende veilig worden bewaard**

Stap 5: Welke gegevens worden bijgehouden?

Onder het blad 'lijsten' in het voorbeeld-verwerkingsregister zijn er overzichten terug te vinden van alle soorten persoonsgegevens en gevoelige gegevens. In het register kan er met een drop-down menu een aantal soorten gegevens worden geselecteerd. Maak een goed onderscheid tussen persoonlijke en gevoelige gegevens, aangezien de rechtsgronden op basis waarvan ze verwerkt mogen worden, verschillen. Gevoelige gegevens zullen voornamelijk verwerkt worden onder het verwerkingsdoel 'patiëntenzorg'.

☐ **De lijst met soorten persoonsgegevens en gevoelige gegevens die worden bijgehouden in de organisatie wordt voor elk verwerkingsdoel aangevuld**

Stap 6: Welke rechtsgrond?

Zeer belangrijk in de nieuwe regelgeving is dat er correct kan aangegeven worden welke wettelijke basis er is om de persoonsgegevens te verwerken. De rechtsgronden die in de GDPR/AVG als correcte basis voor verwerking worden beschouwd, staan opgesomd in het blad 'lijsten', en kunnen geselecteerd worden in het voorbeeld-verwerkingsregister met een drop-down menu. Er is vervolgens een verduidelijking nodig, waar er naar een specifieke wettekst, overeenkomst, formulier van toestemming,… verwezen wordt.

Het is zeer belangrijk de juiste rechtsgrond te selecteren, er hangen vaak consequenties aan die keuze vast. Zo wordt het principe van 'toestemming' als rechtsgrond aanvaard bij zowel persoonsgegevens als gevoelige gegevens, maar zijn er bij deze rechtsgrond een aantal bijkomende beperkingen. Er zijn een aantal artikels in de GDPR die meer duiding en bijkomende bepalingen geven rond het geven van toestemming. De toestemming moet aantoonbaar zijn, en er moet duidelijk aangegeven worden op welk verwerkingsdoel deze toestemming betrekking heeft. Er moet helder gecommuniceerd worden met de betrokkene rond de toestemming, de toestemming moet actief worden gegeven, en de betrokkene heeft ook steeds het recht om de toestemming in te trekken. Voor kinderen moet er steeds toestemming zijn van de ouders, in België wordt de grens hier op 13 jaar gelegd. Er zijn heel wat bijkomende rechten van de betrokkenen als de verwerking gebeurd op basis van toestemming, zodra deze wordt ingetrokken valt de hele basis van verwerking weg, en kan de betrokkene vragen om alle gegevens te wissen. Bijkomend is het in een patiënt-arts relatie niet altijd een evidentie om te spreken van een vrijelijk gegeven toestemming.

Het is dus altijd aangeraden om **eerst te kijken of een andere rechtsgrond dan toestemming** kan gevonden worden waarop de verwerking kan gebaseerd worden. Zeker in het geval van persoonsgegevens in het kader van de gezondheidszorg is er een meer correcte grondslag te vinden: wettelijke verplichtingen van de verwerkers, vitale belangen en gezondheidszorg zijn de belangrijkste gronden waarop men zich daar baseert. Voor medewerkers zullen vaak contractuele bepalingen meespelen, er dient in dat geval naar de specifieke contracten verwezen te worden.

☐ **Voor de verwerking van persoonsgegevens is er aangegeven op welke rechtsgrond deze gebaseerd is.**

☐ **Indien er ook gevoelige gegevens verwerkt worden, wordt er binnen de specifieke rechtsgronden rond dit soort gegevens de correcte grond geselecteerd**

☐ **Voor elke rechtsgrond wordt ook meer in detail aangegeven om welke wettelijke bepalingen of contracten het gaat.**

Stap 7: Delen van informatie

Indien de informatie die verzameld en verwerkt wordt, ook met andere personen wordt gedeeld, dient dit verduidelijkt te worden in het verwerkingsregister. Voor zowel personen binnen de organisatie als personen buiten de organisatie dient dit verduidelijkt te worden. Er dient in het delen van informatie ook rekening gehouden te worden met de wettelijke basis waarop gegevens worden verwerkt, en de beperkingen die vb. aan gevoelige gegevens worden opgelegd.

Dit wil zeggen dat hoewel in het verwerkingsregister zelf louter gevraagd wordt met wie er wordt gedeeld, er een duidelijk beleid in de praktijk moet zijn rond de personen die toegang hebben tot persoonsgegevens.

In de GDPR staat proportionaliteit voorop, ook wel opgevat als ‘need to know’: enkel deze informatie mag verwerkt worden die nodig is om bepaalde taken te vervullen. Als een medisch secretaresse afspraken noteert en mogelijk ook reden tot contact (gevoelige informatie), kan dit gekaderd worden. In de verordening staat namelijk dat de verwerking van gevoelige persoonsgegevens enkel kan gebeuren door of onder verantwoordelijkheid van een beroepsbeoefenaar die aan het beroepsgeheim is gebonden. Deze verwerking kan ook noodzakelijk zijn om de toegang tot de gezondheidszorg van patiënten te waarborgen door de arts niet zelf met alle administratieve taken te belasten (gerechtvaardigd belang). Dit wil echter niet zeggen dat deze medewerker toegang dient te hebben tot het volledige medische dossier van een patiënt. Afhankelijk van het takenpakket van de medewerkers in de praktijk, dient de toegang afgebakend te worden. In elk geval dienen er ook vertrouwelijkheidsovereenkomsten afgesloten te worden met de medewerkers, om hen ook aan geheimhoudingsplicht ten opzichte van de informatie waartoe ze toegang hebben, te binden.

Voor multidisciplinaire praktijken waar ook andere zorgverleners deel van uitmaken, zijn deze gebonden aan het beroepsgeheim en kan hun rol makkelijker gekaderd worden binnen de rechtsgrond van de gezondheidszorg. Toch dient ook hier aandacht te zijn voor de ‘need to know’. Binnen de gegevensdeling op Vitalink zijn bijvoorbeeld regels vastgesteld voor de zorgberoepen en welk toegangs- of schrijfrecht deze hebben: een Sumehr, de samenvatting van het medisch dossier is enkel toegankelijk voor andere artsen. Zo moet het ook gaan met de toegang tot het medisch dossier in de praktijk: tot welke gegevens dient een zorgverlener toegang te hebben om zijn of haar functie correct uit te oefenen? Eens deze toegangsregels zijn bepaald, dient de toegang beperkt te worden tot enkel deze gegevens. De meeste EMD-pakketten voorzien al de mogelijkheid tot het instellen van een differentiële toegang tot de pakketten.

Informatie delen met externe zorgverleners of medewerkers van medische instellingen kan ook gekaderd worden binnen de verordening. Het betreft onder andere het delen van gezondheidsgegevens via verwijsbrieven, opvragen van testen bij labo's, doorsturen van derde betalers naar de ziekenfondsen, persoonsgegevens die doorgestuurd of verwerkt worden door een sociaal secretariaat,…

Wat betreft het delen van gezondheidsgegevens kan dit enkel met personen gebonden aan het beroepsgeheim, of onder verantwoordelijkheid van een persoon gebonden aan het beroepsgeheim, of wie wettelijk tot geheimhouding is verplicht, en kan dit ook enkel indien dit kadert binnen het beoefenen van preventieve of arbeidsgeneeskunde of het verstrekken van gezondheidszorg, of in het geval van toestemming.

Ook voor andere verwerkingsdoelen moet toegang tot bepaalde sets van persoonsgegevens ingeperkt worden in functie van het takenpakket. Denk hier bijvoorbeeld aan een HR-verantwoordelijke, die wel inzicht heeft in loonadministratie, en een onthaalmedewerker die deze toegang niet dient te hebben.

☐ **Er is binnen de organisatie nagegaan wie, met het oog op de specifieke functie en takenpakket, toegang kan hebben tot welke sets van gegevens**

☐ **Er worden binnen de organisatie maatregelen genomen om de toegang van gegevens te beperken tot wie recht heeft op deze toegang**

☐ **Informatie buiten de organisatie wordt enkel gedeeld conform de rechtsgronden waarop de verwerking is gebaseerd**

☐ **Er is binnen de organisatie opgelijst met welke externe instanties informatie wordt gedeeld**

Stap 8: Bewaartermijn gegevens

Tip rond bewaartermijnen in het verwerkingsregister

U kan er voor opteren om een apart overzicht op te stellen rond de verschillende bewaartermijnen van de bewaarde persoonsgegevens. U kan dan in het vak rond de bewaartermijnen verwijzen naar dit document, in plaats van voor alle verwerkingsdoelen apart de verschillende bewaartermijnen te noteren.

Persoonsgegevens mogen niet langer bewaard worden dan noodzakelijk voor de uitvoering van de grond waarop de verwerking van deze gegevens is gebaseerd. Voor de verwerking van bepaalde gegevens zijn er wel wettelijke termijnen vastgesteld die gevolgd dienen te worden. Zo moet een patiëntendossier 30 jaar bewaard worden (dit geldt ook voor dossiers die op de wachtpost worden bijgehouden), en geldt voor de bewaartermijn van getuigschriften en boekhoudkundige gegevens een bewaartermijn van 7 jaar.

Indien er geen wettelijke indicaties zijn rond bewaartermijnen, dient u te bepalen hoe lang deze gegevens bewaard dienen te worden. Dit mag niet langer dan noodzakelijk zijn voor een bepaald doel, maar er kunnen bijkomende redenen zijn om gegevens toch iets langer te bewaren. Dit dient dan geduid te worden. Bijvoorbeeld: gegevens van sollicitanten zijn slechts geldig zolang de procedure loopt. Eens een persoon is geselecteerd, is het doel bereikt. Toch kan het aangewezen zijn om de gegevens te bewaren tot de persoon effectief in dienst is gekomen, of een periode te voorzien in het geval van betwistingen. Indien u gegevens van sollicitanten wil bewaren in het kader van het

aanleggen van een werfreserve, kan deze periode nog verlengd worden (mits toestemming van de sollicitant om opgenomen te worden in de werfreserve).

☐ **Voor elk verwerkingsdoel wordt voor de persoonsgegevens die verwerkt worden de bewaartermijnen genoteerd.**

☐ **Voor bewaartermijnen die verlopen zijn, worden de dossiers of bewijsstukken vernietigd met aandacht voor de bescherming van persoonsgegevens**

Deel 2: Risico's en beschermende maatregelen

In het verwerkingsregister wordt eveneens opgenomen welke toepassingen, databanken en platformen er gebruikt worden voor de verwerking van gegevens, en of deze op gepaste manier wordt afgeschermd. Dit dient zowel voor papieren als digitale toepassingen te gebeuren.

In het eerste deel werden al een aantal stappen ondernomen om in kaart te brengen welk soort informatie wordt verwerkt, met welk doel en op basis van welke rechtsgronden. Deze basis wordt nu verder uitgewerkt om aan te geven welke beschermende maatregelen werden genomen.

> ### Tip rond beschermende maatregelen in het verwerkingsregister
> Indien uw organisatie over een gegevensbeschermingsbeleid beschikt, kan u naar dit document verwijzen in het register in plaats van een opsomming van de genomen maatregelen.

Algemeen: alles start met 'need to know' en toegangsbeheer

In een huisartsenpraktijk met meerdere zorgverleners, of waar medewerkers aanwezig zijn, moet er goed worden toegekeken op wie toegang heeft tot de informatie. Voor elke functie en lid van de praktijk dient te worden afgebakend welke informatie strikt noodzakelijk is voor het uitoefenen van diens functie, en bijkomend dienen er maatregelen genomen te worden die garanderen dat er slechts tot deze informatie toegang is. Zodra een persoon toegang krijgt tot gegevens waar men geen recht op heeft, is er al sprake van een datalek. Zeker binnen de eigen organisatie is dit dus de eerste stap om de veiligheid van persoonsgegevens te waarborgen.

De genomen beschermingsmaatregelen voor de verschillende soorten persoonsgegevens dienen passend en proportioneel te zijn: voor bijzondere categorieën van persoonsgegevens zoals gezondheidsgegevens, zal een hoger niveau van veiligheidsmaatregelen vereist worden. Er zijn verschillende tools beschikbaar die helpen om risico's in te schatten. Dit houdt steeds een afweging in tussen de impact bij een lek of inbreuk en de waarschijnlijkheid dat deze zal plaatsvinden (of reeds plaatsvindt), met inachtneming van de reeds genomen beschermende maatregelen. Achteraan in het register is een voorbeeld opgenomen van een matrix voor het inschatten van risico's (tab-blad 'Voorbeeld inschatten risico').

Papieren verwerking van persoonsgegevens

De maatregelen die hier genomen kunnen worden, zijn voornamelijk organisatorisch van aard.

Mogelijke manieren om papieren dossiers, documenten,… veilig te bewaren (let op: dit is een voorbeeldlijst van maatregelen, zorg voor die maatregelen die passend en proportioneel zijn voor de specifieke soort gegevens en verwerkingsdoelen in uw eigen organisatie):

- Achter slot bewaren van dossiers (persooneelsgegevens, medische dossiers,…)

- Als er verschillende machtigingen zijn op het vlak van toegang tot de bewaarde gegevens, dienen deze uiteraard op verschillende plaatsen bewaard te worden (bijvoorbeeld: persooneelsgegevens of boekhouding niet op dezelfde plaats bewaren als de medische dossiers)
- Veilig beheren van sleutel en reservesleutel. Afsluiten van gegevens terwijl de sleutel of reservesleutel vrij toegankelijk zijn is uiteraard niet de bedoeling. Voor medische dossiers dient de arts of dienen de artsen die de dossiers beheren toegang te hebben, de reservesleutel dient veilig te worden bewaard.
- Na consultatie/wijziging van de papieren dossiers moeten deze veilig worden opgeborgen: vermijd dat er bijvoorbeeld medische dossiers van andere patiënten open op uw bureau liggen bij een volgend consult.
- Leg geen brieven die niet afgesloten zijn in het postvakje, sluit deze altijd onmiddellijk af. Zorg ook dat het postvak goed beheerd wordt, en niet vrij toegankelijk is voor derden.
- Gebruik een papierversnipperaar voor het vernietigen van gevoelige documenten of documenten die persoonsgegevens bevatten.

☐ **In het verwerkingsregister worden voor de digitale verwerking van persoonsgegevens aangegeven om welke verwerkingen het gaat**

☐ **In het verwerkingsregister worden voor de papieren verwerking van persoonsgegevens de genomen organisatorische maatregelen vermeld**

☐ **Er wordt toegezien op de implementatie van deze maatregelen**

Digitale verwerking van persoonsgegevens

Er kunnen zowel organisatorische als technische maatregelen genomen worden. Een aantal maatregelen gaan vervat moeten zitten in de software, controle van de contracten of de gebruikte software voldoende voorzorgsmaatregelen voorziet voor het veilig bewaren van gegevens is bijgevolg nodig. Zo is het loggen van wie toegang tot persoonsgegevens heeft en wat er is gewijzigd belangrijk: wie had toegang, tot welke gegevens, op welk moment en via welke weg? Dit biedt een bijkomende garantie op het toegangsbeheer en laat controle toe bij misbruik.

☐ **In het verwerkingsregister worden voor de digitale verwerking van persoonsgegevens aangegeven om welke verwerkingen het gaat**

☐ **Voor de digitale verwerking worden de genomen organisatorische maatregelen vermeld**

☐ **Voor de digitale verwerking worden de genomen technische maatregelen vermeld**

☐ **Er wordt toegezien op de implementatie van deze maatregelen**

Mogelijke maatregelen (let op: dit is een voorbeeldlijst van maatregelen, zorg voor die maatregelen die passend en proportioneel zijn voor de specifieke soort gegevens en de verwerkingsdoelen in uw eigen organisatie):

- Paswoordbeveiliging op computer
- Zorg voor voldoende complexiteit bij de paswoorden, dit kan ingebouwd worden in de toegang tot het systeem
- Voorzie verschillende manieren van toegang tot bestanden die persoonsgegevens bevatten (voorbeeld: paswoord en eID-toegang tot PC en dossier).
- Vermijd dat er één wachtwoord wordt gehanteerd voor alle systemen

- Zorg dat de PC na een bepaalde periode van inactiviteit in slaapstand gaat en enkel ontgrendeld kan worden met het paswoord
- Geen persoonsgegevens bewaren op niet-geëncrypteerde losse dragers zoals USB-stick, externe harde schijf of CD-rom
- Zorg bij gebruik van tablets of smartphone voor toegang tot persoonsgegevens voor verschillende beveiligingselementen, zoals encryptie, wachtwoord- of vingerafdruk-toegang en toegang tot de bestanden of applicaties met persoonsgegevens via een veilige weg (vb. 2-factor authenticatie, Itsme,…)
- Printer instellen met toegangscontrole (papieren enkel afgedrukt na ingeven code op toestel), of aparte printers voorzien voor algemene zaken vs persoons- of gevoelige persoonsgegevens
- Bij gebruik van websites waar persoonsgegevens worden opgevraagd of verwerkt, moet het om een beveiligde website gaan. Kijk of er in de adresbalk 'https' staat in plaats van 'http'
- Gebruik geen onbeveiligde e-mail om persoonsgegevens uit te wisselen. In het geval van de gezondheidszorg is de eHealthbox beschikbaar, waar er via verschillende maatregelen de veiligheid van de verzonden boodschappen wordt gegarandeerd. Zo wordt er gebruik gemaakt van een authenticatieprocedure (voorlopig eID, wordt nog uitgebreid met bijkomende procedures) en geëncrypteerde informatie die enkel ontcijferbaar is voor de bestemmeling aan wie deze bestemd is (zie ook https://www.ehealth.fgov.be/ehealthplatform/nl/beveiligde-elektronische-brievenbus). Ook het intranet van de Orde (www.ordomedic.be) biedt de kans op veilige uitwisseling van gegevens en documenten.
- Er zijn mailprogramma's beschikbaar die de mogelijkheid geven om geëncrypteerde of versleutelde mails te versturen[2].
- Bij het versturen van mails waar geen persoonsgegevens in vervat zitten, dient ook vermeden te worden een boodschap te forwarden of door te sturen aan grote groepen mensen.
    - Voor interne communicatie binnen de organisatie kan u wel de medewerkers in Cc plaatsen
    - Bij externe communicatie dient Bcc gebruikt te worden: zo worden geen contactgegevens verspreid van wie hier geen expliciete toestemming voor heeft gegeven

[2] Voor meer info zie vb. https://www.smarthealth.nl/2016/07/07/hoe-mail-veilig-patienten/

- Gebruik van de eHealthdiensten biedt bijkomende garanties op het veilig uitwisselen van informatie. Het eHealthplatform zorgt voor de veilige uitwisseling van persoonsgegevens, maar slaat zelf geen data op. In de basisdiensten van het eHealth platform worden een aantal beveiligde tools aangeboden aan zorgverleners zodat gegevensdeling op een veilige manier kan verlopen. Ook worden er door het eHealthplatform specificaties en aanbevelingen uitgewerkt waaraan nieuwe diensten dienen te voldoen om de veiligheid van de gegevens te waarborgen.

Encryptie?

Voor bijkomende veiligheid van uw elektronische systemen kan er gebruik gemaakt worden van encryptie, dit wil zeggen dat de informatie vergrendeld wordt en niet zonder de juiste authenticatie toegankelijk is. Zoals al vaak aangehaald is de standaard-email geen veilig medium voor het versturen van informatie van persoonsgegevens, maar bestaan er naast de eHealth-box ook andere geëncrypteerde mailsystemen. Verder kan ook een bestand in een bericht versleuteld worden.

Naast berichten kunnen dus ook bestanden versleuteld worden, en op de pc of smartphone zelf kan deze bijkomende beveiliging eveneens worden toegepast (bijvoorbeeld het versleutelen van de harde schijf met Bitlocker).

Let op dat er systemen worden gebruikt die voldoende garanties bieden. Zo is er binnen Gmail een gratis encryptie-optie, maar houden ze wel het recht op toegang tot de berichten. Ga na welke garanties een dienst biedt op de beveiliging van persoonsgegevens, en consulteer bij twijfel een IT-deskundige.

Algemene bijkomende tips

- Vermijd bij telefoongesprekken het vermelden van de naam. Beantwoordt u bijvoorbeeld een vraag van een patiënt, kan zo vermeden worden dat derden informatie horen die niet voor hen bestemd is.

Datalekken en risico's

Dit stuk wordt uitgebreider behandeld in het dossier datalekken, belangrijk is wel dat alle datalekken gemeld worden binnen 72 uur aan de Privacycommissie, en dat in sommige gevallen ook de betrokkenen op de hoogte moeten worden gesteld. Hou ook intern bij welke beveiligingsincidenten en datalekken er zijn geweest, en welke maatregelen zijn genomen om deze in de toekomst te vermijden

☐ **Register voor datalekken en inbreuken wordt opgesteld en bijgehouden**

☐ **Beveiligende maatregelen na een datalek worden in dit register opgenomen**

☐ **Indien er aanpassingen gebeuren aan de beschermingsmaatregelen, wordt ook het verwerkingsregister aangepast**

<u>Kans op datalekken:</u>

In het register kan u aangeven of u binnen uw organisatie al voldoende maatregelen genomen heeft om de persoonsgegevens te beschermen (beperkte kans op datalekken), of er nog verbeterpunten

zijn (gemiddelde kans op datalekken), of dat er nog te weinig of geen maatregelen zijn genomen en deze prioritair dienen opgenomen te worden (hoge kans op datalekken).

☐ **Er wordt in het register aangegeven wat de kans op een datalek is, gezien de genomen beschermende maatregelen.**

Verwerkers

Voor sommige verwerkingen van persoonsgegevens doet u mogelijk beroep op externe partijen. Bijvoorbeeld het bijhouden van patiëntengegevens in een elektronisch medisch dossier, het bijhouden van een personeelsbestand via een website van het Sociaal secretariaat,…. Voor veilig gebruik van deze diensten, moeten deze verwerkers ook voldoende garanties op de veiligheid van deze gegevens kunnen bieden. Dit moet worden geregeld in een verwerkersovereenkomst (zie voorbeeld op de website en extra informatie rond verwerkers). Indien u bij een bepaalde verwerking van gegevens beroep doet op een verwerker, kan u dat aangeven, en eveneens of de nodige contractuele afspraken hierrond zijn vastgelegd. Naast het bestaande contract dient er dus een specifieke verwerkersovereenkomst te worden opgesteld. Deze kan aan het bestaande contract worden toegevoegd als addendum. Een aantal voorbeelden van verwerkersovereenkomsten zijn reeds beschikbaar.

☐ **Controle van de overeenkomsten met externe partners voor het verwerken van persoonsgegevens: zijn de bijkomende verwerkersovereenkomsten afgesloten?**

☐ **Bijzonder aandachtspunt: is een vertrouwelijkheidsclausule opgenomen in deze verwerkersovereenkomsten?**