ALGEMENE VERORDENING GEGEVENSBESCHERMING

Een praktische handleiding voor actoren binnen het apothekersnetwerk

Deze praktische handleiding is tot stand gekomen in samenwerking met de Nederlands- en Franstalige tariferingsdiensten en beroepsverenigingen, BeMeSO en FarmaFlux.

De informatie in deze handleiding is uitsluitend bestemd voor actoren binnen het apothekersnetwerk. Verstrekking aan en gebruik door anderen dan de geadresseerde is zonder toestemming niet toegestaan. Er kunnen geen rechten worden ontleend aan de informatie in deze handleiding.

Huidige versie: 28 juni 2019

VOORWOORD

De doelstelling van dit document bestaat erin richting te geven en aanbevelingen te formuleren met betrekking tot de praktische invulling van de beveiliging van persoonsgegevens. Het document kwam tot stand door input van zowel apothekers, tariferingsdiensten, softwarehuizen als FarmaFlux. ***Waar u geen aanduiding ziet staan, geldt de aanbeveling voor alle partijen. Staat er wel een specifieke aanduiding, dan geldt de aanbeveling voor de partij(en) die vermeld is/zijn en is de tekst aangeduid door een cijfer gemarkeerd in groen:***

1 = apotheek; 2 = tariferingsdienst; 3 = FarmaFlux; 4 = softwarehuis.

De verplichting ligt steeds bij de partij die vermeld is. De aanbevelingen voor de andere partijen kunnen natuurlijk wel relevant zijn voor alle partijen. **Om apothekers in staat te stellen deze gids sneller te raadplegen, zijn de aanbevelingen die niet aan hen zijn gericht,** ***grijs*** **in de tekst aangegeven.**

Aanbevelingen, zeker op het vlak van technische ontwikkelingen, zijn voortdurend in evolutie. Het is dan ook de intentie om dit document op regelmatige tijdstippen te evalueren en te updaten indien dit nodig blijkt te zijn.

Voor zover mogelijk hebben we in het hoofdstuk rond IT en securitybeleid een onderscheid gemaakt tussen de minimale vereisten (die verplicht zijn) en de aanbevolen vereisten (*aangeduid in groen en schuingedrukt*). Afhankelijk van zowel de mate van maturiteit van de onderneming als van de (financiële) middelen waarover men beschikt, zal men de ene dan wel de andere vereisten nastreven.

Deze versie van het document is bijgewerkt tot en met **28 JUNI 2019**.

AANBEVELINGEN MET BETREKKING TOT DE ALGEMENE PRINCIPES

1. TOESTEMMING

"De toestemming dient te worden gegeven door middel van een duidelijke actieve handeling, bijvoorbeeld een schriftelijke verklaring, ook met elektronische middelen, of een mondelinge verklaring, waaruit blijkt dat de betrokkene vrijelijk, specifiek, geïnformeerd en ondubbelzinnig met de verwerking van zijn persoonsgegevens instemt.

Hiertoe zou kunnen behoren het klikken op een vakje bij een bezoek aan een internetwebsite, een andere verklaring of een andere handeling waaruit in dit verband duidelijk blijkt dat de betrokkene instemt met de voorgestelde verwerking van zijn persoonsgegevens. Stilzwijgen, het gebruik van reeds aangekruiste vakjes of inactiviteit mag derhalve niet als toestemming gelden.

De toestemming moet gelden voor alle verwerkingsactiviteiten die hetzelfde doel of dezelfde doeleinden dienen. Indien de verwerking meerdere doeleinden heeft, moet toestemming voor elk daarvan worden verleend. Indien de betrokkene zijn toestemming moet geven na een verzoek via elektronische middelen, dient dat verzoek duidelijk en beknopt te zijn en niet onnodig storend voor het gebruik van de dienst in kwestie." [1]

2. BEVEILIGING

Digitaal

Digitaliseer zoveel mogelijk, zodat het gebruik van papier vermeden wordt. Verander wachtwoorden op regelmatige basis en stel toegangen in.

Zorg voor een digitaal archief, zodat na een bepaalde termijn documenten eenvoudig verwijderd kunnen worden.

De gegevens dienen beveiligd te zijn in die zin dat ze enkel zichtbaar zijn voor de personen belast met de verwerking ervan. Werk met toegangbeheer en verdeel rollen binnen de onderneming. Logging door middel van een badgesysteem is hier bijvoorbeeld een idee.

Schakel steeds de computer uit op het einde van de werkdag. Draagbare toestellen zoals laptops en tablets die 's nachts in de apotheek/op kantoor blijven, moeten worden vastgemaakt/opgeborgen of de lokalen/gebouwen waar deze zich bevinden moeten afgesloten zijn.

Zorg voor encryptie en een beveiligde back-up. Vercijfering is de preventieve basismaatregel in geval van diefstal, misbruik of verlies van de informatiedrager en is een essentieel element in het bemoeilijken van het eventueel decoderen van de gegevens na het wissen van de drager.

Kritische apparatuur moet zo worden geplaatst en beschermd dat risico's van schade en storing van buitenaf en de gelegenheid voor onbevoegde toegang wordt verminderd. Deze apparatuur moet worden beschermd tegen stroomuitval en andere storingen door onderbreking van nutsvoorzieningen. Ten slotte moet de kritische apparatuur op correcte wijze worden onderhouden

[1] Overweging 32 van de AVG.

(steeds ook de laatste versie geïnstalleerd hebben), zodat deze voortdurend beschikbaar is en in goede staat verkeert.

Meer informatie over IT en securitybeleid is terug te vinden in Hoofdstuk 4.

Fysieke documenten

Vermijd papier en digitaliseer indien mogelijk.

Fysiek dienen de papieren documenten bewaard te worden in een afgesloten kast of niet-toegankelijke ruimte. Afhankelijk van het type documenten (al dan niet gevoelige gegevens) dient de kast of ruimte afgesloten te worden bij het verlaten van de werkplek. Op het einde van de werkdag gebeurt dit hoe dan ook.

De sleutels tot kasten dienen op aparte plaatsen bijgehouden te worden en dienen niet op het slot van de kast te blijven zitten. In geval er gewerkt wordt met een archief, dient de toegang tot het archief met gelijkaardige maatregelen afgeschermd te worden. De sleutels tot kasten of archief moeten op een aparte plaats bewaard worden en mogen niet op het slot blijven zitten.

Lokalen

Toegang tot de privaat toegankelijke zone van een gebouw en de beveiligde ruimten moet voorbehouden worden voor geautoriseerde personen. Werk met toegangbeheer en verdeel rollen binnen de onderneming. Logging door middel van een badgesysteem is hier bijvoorbeeld een idee.

De gebouwen of locaties waar zich kritieke en/of ICT voorzieningen bevinden moeten fysiek afdoende beveiligd zijn. Bezoekers van beveiligde kritieke ruimten moeten expliciete toestemming hebben om deze te betreden. Er mag alleen toegang verleend worden voor bepaalde geautoriseerde doeleinden.

Voor kritieke gebouwen, zones en ruimten moeten er anti-inbraaksystemen geïnstalleerd worden conform nationale, regionale en eventueel internationale normen. Onbemande kritieke ruimten moeten te allen tijde van een alarmsysteem voorzien zijn. De beveiligingssystemen moeten op regelmatige basis op effectieve werking getest worden.

(2, 3, 4) Niet-publieke gegevens moeten best beveiligd worden door een fysieke perimeter met toegangscontrole. Medische persoonsgegevens moeten best beveiligd worden door een dubbele fysieke perimeter met toegangscontrole. Er moet een nominatieve lijst bestaan van alle personen die toegang hebben tot de kleinste perimeter met vermelding van hun specifieke bevoegdheden. Deze toegang is bij voorkeur gekoppeld aan een badge. Op alle plaatsen waar originele documenten bewaard worden moeten adequate maatregelen genomen worden om verlies door omgevingsinvloeden tegen te gaan.

(2, 3, 4) Beveiligingsperimeters van het terrein, het openbaar toegankelijk gedeelte van een gebouw, de privaat toegankelijke zone van een gebouw en de beveiligde ruimten moeten geïdentificeerd en gedefinieerd worden.

(2, 3, 4) Privaat toegankelijke zones van een gebouw en de beveiligde ruimten moeten worden beschermd door geschikte toegangsbeveiliging, om te bewerkstelligen dat alleen bevoegd personeel wordt toegelaten.

(2, 3, 4) Er moeten toegangsbeveiligingen (barrières zoals muren, toegangspoorten met kaartsloten of een bemande receptie) worden aangebracht om ruimten te beschermen waar zich gevoelige of kritische informatie en ICT voorzieningen bevinden.

(2, 3, 4) Een bemande receptie of andere voorzieningen om de fysieke toegang tot kritieke gebouwen of locaties te beheren moeten aanwezig zijn. Bezoekers van de organisatie moeten geregistreerd worden, met bovendien aanduiding van datum en tijdstip van aankomst en vertrek.

3. BEWAARTERMIJNEN

"Persoonsgegevens moeten worden bewaard in een vorm die het mogelijk maakt de betrokkenen niet langer te identificeren dan voor de doeleinden waarvoor de persoonsgegevens worden verwerkt noodzakelijk is; persoonsgegevens mogen voor langere perioden worden opgeslagen voor zover de persoonsgegevens louter met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden worden verwerkt, mits de bij deze verordening vereiste passende technische en organisatorische maatregelen worden getroffen om de rechten en vrijheden van de betrokkene te beschermen ("opslagbeperking")."[2]

"Om ervoor te zorgen dat persoonsgegevens niet langer worden bewaard dan noodzakelijk is, dient de verwerkingsverantwoordelijke termijnen vast te stellen voor het wissen van gegevens of voor een periodieke toetsing ervan."[3]

Artikel 39 van het KB van 21 januari 2009 legt (wettelijke) bewaartermijnen op. De documenten opgesomd in dat artikel moeten gedurende minstens 10 jaar in de apotheek bewaard worden. Na verloop van 30 jaar moeten deze documenten of data op de informatiedragers vernietigd worden.

Meer informatie vindt u hier: link.

4. GEGEVENSBESCHERMINGSEFFECTBEOORDELING (3, 4)

Een gegevensbeschermingseffectbeoordeling (hierna: GEB) is een procedure om te evalueren of een verwerking van persoonsgegevens risico's inhoudt voor de rechten en vrijheden van de persoon wiens data wordt verwerkt en hoe men deze risico's kan beheersen.[4]

Het uitvoeren van een GEB is slechts verplicht wanneer de gegevensverwerking, gelet op de aard, de omvang, de context en de doeleinden daarvan een waarschijnlijk hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen.[5]

Een GEB moet minstens de volgende elementen bevatten:[6]

- een gedetailleerde en duidelijke beschrijving van de beoogde verwerkingen en de verwerkingsdoeleinden. Het register van verwerkingsactiviteiten kan hier richtinggevend zijn;
- een beoordeling van de noodzaak en de evenredigheid van de verwerkingen in functie van de doeleinden;
- een beoordeling van de risico's voor de rechten en vrijheden van betrokkenen;
- de beoogde maatregelen om de risico's aan te pakken.

[2] Artikel 5, 1, e) van de AVG.
[3] Extract uit overweging 39 van de AVG.
[4] Artikel 35, 1 van de AVG.
[5] Overweging 84 van de AVG.
[6] Artikel 35, 7 van de AVG.

HOOFDSTUK 1: DATA SUBJECT RECHTEN

Het betreft hier een algemene opsomming van de rechten van de betrokkene. Een specifieke opsomming van de verschillende rechten (van de patiënt) en de gevallen waarin deze van toepassing zijn, kan u terugvinden op de website van APB.

Bij het ontvangen van een verzoek van een betrokkene dient de verwerkingsverantwoordelijke:

- Te verifiëren of de betrokkene effectief de persoon is die hij/zij beweert te zijn (eID, paspoort, rijbewijs, GSM-nummer,…).
- Gevolg te geven aan het verzoek, tenzij kan aangetoond worden dat de verwerkingsverantwoordelijke niet in staat is om de betrokkene correct te identificeren.
- Binnen de 30 dagen na ontvangst van een verzoek, het verzoek te beantwoorden. Tenzij kan aangetoond worden dat het verzoek te complex is om binnen deze termijn correct af te handelen. In dat geval is er een verlenging mogelijk met maximaal 2 maanden, mits kennisgeving van de verlenging aan de betrokkene.
- Na het beantwoorden van het verzoek, dient de betrokkene hiervan op de hoogte te worden gebracht. Dit kan op elektronische wijze of via andere kanalen indien verzocht door de betrokkene zelf.
- De verzoeken tot uitoefening van de rechten dienen steeds geregistreerd te worden.

De betrokkene moet zijn rechten kosteloos kunnen uitoefenen. Indien hij om bijkomende kopieën verzoekt, kan de verwerkingsverantwoordelijke op basis van de administratieve kosten een redelijke vergoeding aanrekenen.

1. RECHT OP INFORMATIE

De verwerkingsverantwoordelijke heeft een informatieplicht ten opzichte van de betrokkene, ongeacht of de persoonsgegevens bij de betrokkene zelf worden verzameld of niet :

- De verwerkingsverantwoordelijke dient de betrokkene wiens persoonsgegevens verwerkt worden op de hoogte te brengen van de verwerking van zijn/haar persoonsgegevens. Dit dient te gebeuren:
    - Vóór de gegevensverzameling indien de gegevens rechtstreeks van de betrokkene verkregen worden.
    - Binnen 1 maand na het verkrijgen van de persoonsgegevens indien deze niet rechtstreeks van de betrokkene verkregen worden.
    - In duidelijke verstaanbare taal.
    - Op een beknopte, korte manier.
- Deze informatieplicht kan door middel van de verspreiding van een privacyverklaring.

In een aantal situaties hoeft u de betrokkene niet te informeren:

- de betrokkene is al op de hoogte
- de informatieplicht blijkt onmogelijk of vraagt een onevenredige inspanning van de verwerkingsverantwoordelijke.[7] De bewijslast ligt bij de verwerkingsverantwoordelijke.

[7] Enkel van toepassing wanneer de persoonsgegevens niet van de betrokkene zelf zijn verkregen.

- er geldt een ander zwaarwegend belang (bv. voorkoming, opsporing of vervolging van strafbare feiten)

2. RECHT OP INZAGE

Indien een betrokkene zijn recht tot inzage wenst uit te oefenen dient de verwerkingsverantwoordelijke:

- De betrokkene kosteloos een kopie te bezorgen van de persoonsgegevens die hij over hem/haar bezit of verwerkt.
- Het verzoek te beantwoorden op de wijze waarop de aanvraag ontvangen werd. Als het verzoek elektronisch ingediend wordt, dan wordt de informatie in een gangbare elektronische vorm gegeven.
- Een mogelijkheid hierbij is het online toegankelijk maken van de persoonsgegevens.
- Beperkingen op recht van inzage:
    - Indien identiteit niet kan gecontroleerd worden.
    - Indien rechten en vrijheden van een andere betrokkene niet kunnen gegarandeerd worden.

Als de verzoeken ongegrond of buitensporig zijn, kan de verwerkingsverantwoordelijke een redelijke vergoeding aanrekenen of mag hij het verzoek weigeren. De bewijslast ligt bij de verwerkingsverantwoordelijke.

3. RECHT OP RECTIFICATIE/VERBETERING

De betrokkene heeft het recht om zijn persoonsgegevens aan te passen indien deze onjuist of onvolledig zijn. De verwerkingsverantwoordelijke dient volgende zaken in acht te nemen:

- Deze wijziging dient kosteloos en zonder uitstel uitgevoerd te worden.
- De vraag tot aanpassing dient door de verwerkingsverantwoordelijke doorgegeven te worden aan derden die mee instaan voor de verwerkingen van persoonsgegevens in het kader van de farmaceutische zorg.
- Rectificatie kan door (her)inlezing van de eID kaart. Dit kan een verificatie en correcte wijziging van de persoonlijke identificatiegegevens in één klap bewerkstelligen.

Een verzoek tot rectificatie/verbetering kan worden geweigerd als het verzoek kennelijk ongegrond of buitensporig is, rekening houdend met de vraag of het verzoek repetitief van aard is. De bewijslast ligt bij de verwerkingsverantwoordelijke.

4. RECHT OP GEGEVENSUITWISSING/RECHT OM VERGETEN TE WORDEN

De betrokkene heeft het recht om te vragen zijn persoonsgegevens te laten verwijderen. De verwerkingsverantwoordelijke dient echter niet in alle gevallen gevolg te geven aan het verzoek van de betrokkene, er gelden enkele uitzonderingen:

- Er is een wettelijke verplichting voorhanden op basis waarvan de verwerkingsverantwoordelijke de persoonsgegevens dient te bewaren.
- De persoonsgegevens zijn nog steeds noodzakelijk in het kader van de (voortgezette) farmaceutische zorg of in het kader van wetenschappelijk of historisch onderzoek of statistische doeleinden, en het belang van de verwerkingsverantwoordelijke primeert boven het belang van de betrokkene.
- Wanneer de verwerking van persoonsgegevens door de verwerkingsverantwoordelijke gerechtvaardigd is om redenen van openbaar belang op het gebied van de volksgezondheid.

De AVG geeft aan dat gegevens wél gewist dienen te worden in het geval dat:

- De persoonsgegevens niet langer relevant/noodzakelijk zijn.
- De betrokkene zijn/haar toestemming heeft ingetrokken en er geen andere verwerkingsgrond voorhanden is.
- De persoonsgegevens niet op een rechtmatige verwerkingsgrond gestoeld zijn.
- De persoonsgegevens niet langer mogen bijgehouden worden op basis van een wettelijke verplichting.

5. RECHT OP BEPERKING VAN DE VERWERKING

Indien de betrokkene dit wenst, kan hij/zij steeds aan de verwerkingsverantwoordelijke vragen om een recht van beperking van verwerking. Dit houdt in dat de verwerkingsverantwoordelijke:

- De reeds verzamelde persoonsgegevens van de betrokkene niet langer verder mag verwerken.
- De verwerkingsverantwoordelijke dient dit zonder onredelijke vertraging en verplicht uit te voeren indien:
    - De juistheid wordt betwist, waardoor de verdere verwerking wordt beperkt tot wanneer de gegevens werden geverifieerd. De persoonsgegevens die als juist werden aangegeven door de betrokkene kunnen intussen verwerkt worden.
    - De verwerking is onrechtmatig, maar de betrokkene wil niet dat zijn gegevens gewist worden.
    - De persoonsgegevens zijn niet langer nodig voor de doeleinden, maar zijn wel nog nodig in het kader van een rechtsvordering.
    - De betrokkene heeft bezwaar gemaakt tegen verdere verwerking van de persoonsgegevens.
- De verwerking van persoonsgegevens kan enkel verder gezet worden indien een van volgende voorwaarden voldaan is:
    - De betrokkene heeft toestemming gegeven.
    - De persoonsgegevens zijn nodig voor het uitoefenen van een rechtsvordering.
    - De verwerking is nodig voor de bescherming van de rechten van een andere persoon.
    - Er een algemeen belang is voor de verwerking.
- De verwerkingsverantwoordelijke dient alle derden die de persoonsgegevens ontvangen op de hoogte te stellen van de beperking van de verdere verwerking.

6. RECHT OP OVERDRAAGBAARHEID

De betrokkene heeft het recht om zijn persoonsgegevens over te dragen naar een andere verwerkingsverantwoordelijke.

- Dit dient te gebeuren in een gestructureerde, gangbare en machine leesbare vorm.
- De verwerkingsverantwoordelijke dient gevolg te geven aan het recht op overdraagbaarheid indien:
    - De verwerking berust op toestemming, of op een overeenkomst tussen de verwerkingsverantwoordelijke en de betrokkene, en
    - De verwerking wordt verricht via geautomatiseerde procedés.
- Alle verzamelde persoonsgegevens dienen overgedragen te worden naar de gekozen verwerkingsverantwoordelijke.

7. RECHT VAN BEZWAAR

Elke betrokkene heeft het recht om bezwaar te maken tegen de verwerking van zijn persoonsgegevens gestoeld op de rechtmatige verwerkingsgronden toestemming en gerechtvaardigd belang.

- De verwerkingsverantwoordelijke dient de verwerking te staken, tenzij er dwingende gerechtvaardigde gronden kunnen aangevoerd worden waarbij de belangen van de verwerkingsverantwoordelijke zwaarder zijn dan de belangen, rechten en vrijheden van de betrokkene.
- De verwerkingsverantwoordelijke dient de gegevens evenwel niet automatisch te verwijderen.

HOOFDSTUK 2: VERWERKINGEN MET BETREKKING TOT DIENSTVERLENING AAN DE PATIËNT

1. ZORGVERLENING

1.1 FARMACEUTISCHE ZORG (1)

Bij het verlenen van farmaceutische zorg, dienen volgende principes in acht genomen te worden:

- Minimale gegevensverwerking:
    - Geneesmiddelen op voorschrift:
        - Wettelijk verplichte minimum (én bijkomend de gegevens die op het voorschrift staan):
            - Identificatie- en contactgegevens van de voorschrijver (naam, voornaam, werkadres, telefoonnummer en/of mailadres);
            - Persoonlijke identificatiegegevens van de patiënt (naam, voornaam);
            - Identificatienummer van de sociale zekerheid (INSZ-nummer)
            - Geboortedatum (als onderdeel INSZ)
            - Verzekerbaarheidsgegevens
        - Bijkomende gegevens van de patiënt worden geregistreerd uit gerechtvaardigd belang (bv. adres, telefoonnummer) of uit noodzakelijkheid voor het verstrekken van gezondheidszorg (bv. gezondheidsgegevens zoals allergie of intoleranties).
    - Geneesmiddelen zonder voorschrift:
        - Registratie persoonlijke identificatiegegevens van de patiënt uit gerechtvaardigd belang of uit noodzakelijkheid voor het verstrekken van gezondheidszorg.
- Bewaartermijn: zie link.
- In het kader van de juistheid en gegevenskwaliteit kan de inlezing van de eID of de regelmatige consultatie van *MyCareNet* gegevens naar aanleiding van de aflevering op basis van een voorschrift of het ophalen van een elektronisch voorschrift dienen om de gegevens van de patiënt up to date te houden.
- De apotheker vergewist zich van de identiteit van de persoon voor wie en aan wie afgeleverd wordt en de correcte registratie.
- Voorgeschreven geneesmiddelen mogen aan derden (de gemachtigde) afgeleverd worden indien:
    - genoteerd in het Lokaal Farmaceutisch Dossier dat de derde voor de patiënt geneesmiddelen mag komen afhalen, of
    - de derde beschikt over een schriftelijk mandaat, of
    - ofwel verschijnt de derde met een voorschrift of een bewijs van elektronisch voorschrift op naam van deze patiënt in de apotheek ofwel ontvangt de apotheker een door hem afgeleverde afhaalbon voor de aflevering van de geneesmiddelen.

1.2 VOORTGEZETTE FARMACEUTISCHE ZORG (1)

De toestemmingsformulieren dienen:

- Beveiligd te zijn: zie hier.
- Bewaard te worden: zie link.

1.3 LEVERING VAN MEDICATIE AAN GEMEENSCHAPPEN (WOONZORGCENTRA, ETC.) (1)

Voor het leveren van medicatie aan gemeenschappen moet er een aantoonbare toestemming/mandaat van de patiënt voorgelegd kunnen worden, alvorens de geneesmiddelen te bezorgen aan de verantwoordelijke/verpleegkundige van de gemeenschap.

Met betrekking tot deze documenten geldt:

- Beveiliging van de formulieren/medicatieschema's: zie hier.
- Bewaartermijn: zie link.

1.4 ONLINE DIENSTEN EN PRODUCTEN

Bij het opzetten/onderhouden van een website waar online diensten of producten worden aangeboden dienen volgende principes in acht genomen te worden:

- Beveiliging: de website dient steeds te beschikken over een beveiligde verbinding (https://).
- Minimale gegevensverwerking: verzamel enkel die gegevens die nodig zijn voor het aanleveren van de gekochte diensten of producten (contactgegevens, adresgegevens). Sla andere gegevens (bv. gegevens met betrekking tot de gezondheid) niet op zonder rechtmatige verwerkingsgrond.
- Informeren:
  - De website dient te beschikken over een privacyverklaring en een cookie verklaring. Zie de templates hier.
  - Indien persoonsgegevens doorgegeven worden aan derde partijen, zoals de betalingsprovider of pakketservice, dient de klant hiervan op de hoogte te zijn. Dit kan door opname in de privacyverklaring.
- Rechtmatige verwerkingsgronden:
  - Zorg voor actieve toestemming/opt-in door middel van een checkbox voor marketingactiviteiten. Stilzwijgende toestemming of aangevinkte checkboxen zijn niet toegestaan.
  - Het is niet toegestaan om zonder expliciete toestemming persoonsgegevens door te geven aan derden indien dat niet noodzakelijk is voor de uitvoering van de overeenkomst. Denk bijvoorbeeld aan het doorverkopen van e-mailadressen aan derde partijen voor marketingdoeleinden.
- Rechten van data subjecten:
  - Klanten moeten op een makkelijke manier zowel hun persoonsgegevens kunnen/laten bewerken, zoals hun account, als ook informatie volledig uit een systeem kunnen/laten verwijderen.
  - Indien een klant zijn account verwijdert, dienen de persoonsgegevens uit alle systemen verwijderd te worden voor zover deze niet bijgehouden moeten worden op basis van een andere verplichting.

- Klanten moeten de gegeven toestemming voor marketingactiviteiten op een makkelijke manier kunnen intrekken. Dit kan door opt-out of door hen de mogelijkheid te geven zelf de voorkeuren in hun account te wijzigen.
- Bewaartermijn: zie link.

2. ADMINISTRATIE

2.1 BEHANDELING VAN PAPIEREN DOCUMENTEN

De volgende beveiliging dient in acht genomen te worden met betrekking tot fysieke documenten die persoonsgegevens bevatten (bv. voorschriften, medicatieschema's, contracten, BVAC-attesten, mandaten, etc.): zie hier.

2.2 FYSIEK TRANSPORT

Voor transport van gegevens tussen de lokalen van de onderneming binnen eenzelfde gebouw moeten geen specifieke beveiligingsmaatregelen genomen worden voor zover het transport steeds onder toezicht is van een bevoegde persoon.

Het fysiek transport van persoonsgegevens (en al dan niet gezondheidsgegevens) buiten de lokalen van de onderneming dient te gebeuren door een bevoegde persoon. Dit kan iemand intern binnen de onderneming zijn of hiervoor kan beroep gedaan worden op een externe koerierdienst.

Voor elk transport van medische persoonsgegevens buiten de onderneming moeten transportgegevens (wie, wat, wanneer) geregistreerd worden.

- Beveiliging:
  - Zorg voor een veilige ophaling/aflevering. Er kan gewerkt worden met een interne/externe koerier en/of traceerbare zending (in geval van een externe koerier).
  - Zorg ervoor dat de persoonsgegevens niet zichtbaar zijn voor onbevoegden. Voor geneesmiddelen betekent dit dat het geneesmiddel verzonden wordt in een verzegelde verpakking die de naam en het adres van de patiënt draagt.
  - Verstuur zendingen steeds naar de specifieke dienst/persoon voor wie de documenten bedoeld zijn.
- Verwerkersovereenkomst: indien er gewerkt wordt met een interne/externe koerier is het belangrijk dat de veiligheid gegarandeerd kan worden door middel van een overeenkomst (met inbegrip van een vertrouwelijkheidsverklaring).

2.3 TARIFICATIE EN ARCHIVERING VAN ELEKTRONISCHE VOORSCHRIFTEN (1, 2)

De TD moet zich verzekeren een getekend mandaat te hebben van de apotheker alvorens over te gaan tot de verwerking van deze bestanden.

Beveiliging: er dient steeds gewerkt te worden met een beveiligde verbinding (https://).

2.4 FARMAFLUX

- Verwerkersovereenkomst: Farmaflux treedt op als verwerker ten aanzien van de apotheker. Alvorens over te gaan tot de doorgifte van gegevens, dient een verwerkersovereenkomst afgesloten te worden.
- Informeren van de patiënt: voorafgaandelijk aan het geven van de *eHealth* toestemming moet de patiënt geïnformeerd worden over de doeleinden waarvoor hij deze toestemming geeft. Meer informatie kan de patiënt hier terugvinden.
- Er moet een contractuele relatie bestaan tussen de patiënt en de/zijn verzekeraar. Het is op basis van dit contract dat de apotheker met toestemming van de patiënt bijvoorbeeld digitale BVAC-attesten kan versturen naar de verzekeraar.

De uitrol van kaliumjodide is onderworpen aan volgende voorwaarden:

- Gegevens in het kader van kaliumjodide worden door de apotheker naar Farmaflux verstuurd en door Farmaflux geanonimiseerd.
- Farmaflux stuurt maandelijks de statistieken van de afgeleverde jodiumtabletten naar de FOD Binnenlandse Zaken. Deze rapportering omvat geaggregeerde gegevens waarbij per regio aangegeven wordt hoeveel kaliumjodide afgeleverd werd.

2.5 BOEKHOUDING / FACTURATIE

Voor boekhouding/facturatie dient er rekening gehouden te worden met verschillende richtlijnen:

- Minimale gegevensverwerking: documenten met gezondheidsgegevens worden in principe niet meegestuurd met facturen. Indien er toch een basis zou bestaan om deze gegevens mee te versturen, dan dienen deze als aparte bijlage bij de factuur te worden verstuurd.
- Bewaartermijn: wettelijke bewaartermijn van boekhoudkundige stukken is 7 jaar.

2.6 INFORMATIEMAILS (NIEUWSBRIEVEN) EN MARKETINGMAILS

- Informatiemails mogen verstuurd worden naar de betrokkene voor zover de betrokkene verwacht dat zijn mailadres hiervoor gebruikt wordt en voor zover de informatiemail in het belang van de betrokkene is.
- Voor mails die een commercieel doel nastreven (of niet vallen onder de noemer 'informatiemails') dient er vooraf toestemming verzameld te worden. Dit kan onder andere via:
    - Inschrijving op de website, of
    - Het aanvinken voor akkoord gekoppeld aan een andere handeling (bv.: aangaan klantenkaart), of
    - Een link in een informatiemail waarbij de data subjecten zich kunnen aanmelden op de marketingmails.
- De betrokkene moet zich op elk moment – gemakkelijk – kunnen uitschrijven voor deze mails.
- Verwerkersovereenkomst: stel een verwerkersovereenkomst op indien er gewerkt wordt met een extern mailplatform (bv. *MailChimp*).

2.7 KLANTENKAARTEN

Indien gewerkt wordt met klantenkaarten, dienen volgende principes in acht genomen te worden:

- Minimale gegevensverwerking: beperk de persoonsgegevens op de fysieke klantenkaart (vermeld bijvoorbeeld louter de naam van de patiënt).
- Informeer voorafgaand aan het opzetten van de klantenrelatie de patiënt via de privacyverklaring (hier te vinden).

2.8 CAMERABEWAKING

- Meld de bewakingscamera in uw apotheek aan via het e-loket (http://aangiftecamera.be). Voor huidige reeds aangemelde camera's moeten dit opnieuw gebeuren **tegen 25 mei 2020**.
- De gegevens betreffende de bewakingscamera moeten opgenomen worden in het verwerkingsregister (zie het hoofdstuk GPDR in het *Kwaliteitshandboek*.
- Informeren: hang het verplichte pictogram zichtbaar uit.
- Bewaartermijn: camerabeelden dienen na 30 dagen verwijderd te worden. Uitzonderlijk mogen ze in het kader van een misdrijf bewaard blijven.
- Beveiliging: encryptie en back-up encryptie van de beelden die geregistreerd worden.
- Verwerkersovereenkomst: stel een verwerkersovereenkomst op indien er gewerkt wordt met externe softwareleverancier of een extern bewakingsbedrijf (hier te vinden).

Zie ook hier wat betreft het toezicht op de werknemers.

3. GEGEVENSUITWISSELING MET ANDERE ZORGVERLENERS

3.1 GEDEELD FARMACEUTISCH DOSSIER (GFD)

- Registratie in GFD (zonder deling) gebeurt omwille van de noodzakelijkheid voor het verstrekken van gezondheidszorg.
- Het delen van gegevens via het GFD, kan mits aan volgende voorwaarden voldaan is:
  - Er bestaat een (verwerkers)overeenkomst tussen Farmaflux en de apotheek
  - De patiënt is geïnformeerd (via brochure Farmaflux/privacyverklaring)
  - De patiënt heeft via *eHealth* zijn toestemming gegeven
  - Er bestaat een therapeutische relatie met de apotheker.

Uitzonderlijk kunnen persoonsgegevens gedeeld worden zonder de toestemming van de patiënt, doch dit kan enkel als er sprake is van een kwestie van leven of dood (vitale belangen), waarbij de apotheker nood heeft aan de gegevens met betrekking tot medicatie, die zich in het GFD bevinden en waarbij de toestemming van de patiënt niet bekomen kan worden. Dit kan dus alleen in zéér uitzonderlijke omstandigheden.

3.2 DELEN VAN MEDICATIESCHEMA

Het digitaal delen van medicatieschema's met zorgverleners dient bij voorkeur via een beveiligd platform (VITALINK/BRUSAFE+/INTER-MED) te gebeuren.

3.3 GEGEVENSUITWISSELING ZORGVERSTREKKERS

Het uitwisselen van informatie over patiënten en het delen van medicatieschema's gebeurt:

- Bij voorkeur via de *eHealthBox*.
- Het gebruik van mail om gegevens uit te wisselen wordt niet uitgesloten, maar in dat geval dienen de nodige voorzorgmaatregelen genomen te worden: zie hier.
- Vermijd het gebruik van *WhatsApp*. Ten eerste gaan de uitgewisselde gegevens via deze app naar de Verenigde Staten. Vervolgens worden deze gegevens ook onbeveiligd op uw smartphone opgeslagen. Vaak wordt bovendien gewerkt met groepen van verschillende zorgverstrekkers. Het kan gebeuren dat de uitgewisselde gegevens van een patiënt niet elke zorgverstekker aanbelangen.
  Een alternatieve app die u hiervoor kan gebruiken, is *Siilo*. Deze werd ontwikkeld met gezondheidszorgverstrekkers in het achterhoofd.

4. ZORGONDERZOEK EN VERBETERING

4.1 KLACHTEN

- Rechtmatige verwerkingsgrond: toestemming van de betrokkene.
- Bewaartermijn: maximaal 5 jaar, tenzij de inhoud langere bewaring vereist.

4.2 WETENSCHAPPELIJKE STUDIES

Bij het participeren in het mobiliseren van patiënten voor wetenschappelijke studies, dient de apotheker, volgende principes in acht te nemen:

- Rechtmatige verwerkingsgrond: de patiënt moet een toestemming gegeven hebben, tenzij het gaat om geanonimiseerde gegevens of de wetenschappelijke studie kadert in het algemeen belang
- Informeren: de patiënt dient geïnformeerd te worden indien er sprake is van niet-anonieme doorgifte. Dit kan door opname in het toestemmingsformulier of in een afzonderlijke Privacy Verklaring.
- Beveiliging: de apotheker dient de gegevens te pseudonimiseren alvorens deze door te geven aan derde partijen.
- Er dient een overeenkomst te worden opgesteld met de onderzoekspartij die de nodige waarborgen formaliseert.
- Bewaartermijn: in principe 1 jaar, tenzij de context langere bewaring vereist.

4.3 MARKTONDERZOEKEN

Bij het participeren in marktonderzoekprogramma's (denk maar aan bijvoorbeeld IQVIA of REDPHARMA) dient de apotheker volgende principes in acht te nemen:

- De doorgifte van statistieken over verkoop van producten dient steeds geanonimiseerd te zijn, wat wil zeggen dat er geen elementen mogen inzitten die terug leiden naar een individu, zoals:
  - Naam
  - Adres
  - INSZ-nummer
  - (Productnaam, voor zover op basis van de naam van het product het individu te identificeren is, bv. wanneer slechts enkele patiënten in België dit product nemen)
- Er dient steeds een overeenkomst te zijn met de apotheker.

HOOFDSTUK 3: VERWERKINGEN VAN PERSONEELSGEGEVENS

1. AANWERVING

1.1 SOLLICITATIE

- Rechtmatige verwerkingsgrond: noodzakelijk in het kader van de overeenkomst (precontractueel).
- Informeren: informeer de sollicitant over de verwerkingen die plaatsvinden (via de privacyverklaring of "*just-in-time notice*" bij het verkrijgen van het CV).
- Sociale media:
  - Raadpleeg in het kader van een aanwerving/recrutering enkel sociale media bedoeld voor professioneel gebruik, zoals *LinkedIn*.
  - Andere (sociale) media mogen enkel geraadpleegd worden indien de betreffende informatie door de betrokkene publiekelijk werd gemaakt.
  - Deze gegevens mogen louter geraadpleegd worden en mogen niet bijgehouden (of verder verwerkt) worden.
- Bewaartermijnen:
  - CV: van zodra duidelijk is dat de persoon niet aangenomen wordt, dient het CV verwijderd te worden binnen de 4 weken, tenzij er toestemming van de betrokkene voor handen is om dit langer te bewaren. In dit laatste geval geldt een maximum bewaartermijn van 5 jaar.
  - Wervingsreserve: beperkte opname van gegevens uit het CV in de wervingsreserve kan gezien worden als "gerechtvaardigd belang", doch enkel indien de sollicitant hierover geïnformeerd werd. De wervingsreserve dient zich te beperken tot de strikt noodzakelijke elementen (naam, functie en onderscheidende factor zoals bv. woonplaats/geboortejaar, motivering).
  - Evaluaties van sollicitatiegesprekken van personen die niet werden aangenomen, mogen bijgehouden worden tot 1 jaar na het gesprek.
  - Uitzondering: in het geval er een vermoeden is dat zich een betwisting zou voordoen met betrekking tot de motieven, kan de werkgever besluiten om bepaalde informatie een langere termijn te bewaren. Deze redenering dient geval per geval bekeken te worden en gedocumenteerd te worden.
- Verwerkersovereenkomst: stel een verwerkersovereenkomst op indien er gewerkt wordt met een extern recruteringsbureau.

1.2 DIMONA-AANGIFTE

- Rechtmatige verwerkingsgrond: wettelijke verplichting.
- Bewaartermijnen:
  - DMFA: 5 jaar vanaf ontvangst van het Dimonabericht.
  - Dimonabericht aan RSZ: 6 maand vanaf de ontvangst van het Dimonabericht.
  - Documenten tewerkstelling: 5 jaar vanaf ontvangst van het Dimonabericht.
- Beveiliging: zie hier.

2. PERSONEELSADMINISTRATIE

2.1 PERSONEELSDOSSIER

- Rechtmatige verwerkingsgrond: wettelijke verplichting en noodzakelijk in het kader van de overeenkomst.
- Bewaartermijn: 5 jaar na beëindiging van de arbeidsovereenkomst (wettelijk).
- Beveiliging van het personeelsdossier en de personeelsadministratie: zie hier.

2.2 ARBEIDSONGEVALLEN

- Rechtmatige verwerkingsgrond: noodzakelijk voor de uitvoering van de overeenkomst.
- Bewaartermijn: minimaal 10 jaar na datum arbeidsongeval (wettelijk).
- Beveiliging van het personeelsdossier en de personeelsadministratie: zie hier.

2.3 VACCINS

- Rechtmatige verwerkingsgrond: gerechtvaardigd belang van de verwerkingsverantwoordelijke.
- Bewaartermijn: één jaar na het laatste vaccin.
- Doorgifte van gegevens aan de derde partij die vaccins uitvoert dient beperkt te worden tot een nominatieve lijst waarop de naam en de voornaam zijn vermeld van de personen voor wie de vaccins bestemd zijn.
- Beveiliging van het overzicht: zie hier.

2.4 MEDISCH ONDERZOEK

- Rechtmatige verwerkingsgrond: wettelijke verplichting en gerechtvaardigd belang van de verwerkingsverantwoordelijke.
- Bewaartermijn: zie 2.1 personeelsdossier.
- Doorgifte van gegevens aan een derde partij wordt beperkt tot minimale persoonlijke identificatiegegevens. Overige gegevens worden verzameld door de arbeidsgeneesheer/externe dienst voor preventie en bescherming op het werk (EDPBW).
- Er dient géén verwerkersovereenkomst opgesteld te worden, aangezien de arbeidsgeneesheer/EDPBW optreedt als verwerkingsverantwoordelijke omwille van het feit dat zij de finaliteit van de te verzamelen gegevens bepalen.
- Beveiliging van het overzicht: zie hier.

2.5 EVALUATIE

Evaluatie houdt in de ruimste zin ook verzuimgesprekken en functioneringsgesprekken in.

- Rechtmatige verwerkingsgrond: noodzakelijk in het kader van de overeenkomst.
- Bewaartermijn: zie 2.1 personeelsdossier.
- Beveiliging van het personeelsdossier en de personeelsadministratie: zie hier.

2.6 INSCHRIJVEN EN VOLGEN OPLEIDINGEN / VORMING

- Rechtmatige verwerkingsgrond: noodzakelijk in het kader van de overeenkomst.
- Bewaartermijn: zie 2.1 personeelsdossier.
- Doorgifte van gegevens aan een derde partij is enkel mogelijk indien de tewerkgestelde een externe opleiding volgt. Binnen de onderneming mag een lijst bijgehouden worden van wie welke opleiding (intern/extern) heeft gevolgd.
- Beveiliging van de gegevens: zie hier.

3. LOONADMINISTRATIE

3.1 LOONADMINISTRATIE

- Rechtmatige verwerkingsgrond: noodzakelijk in het kader van de overeenkomst met de tewerkgestelde.
- Bewaartermijn: zie 2.1 personeelsdossier.
- Beveiliging van de loonsadministratie (in de brede zin van het woord): zie hier.
- Indien de loonsadministratie uitbesteed wordt aan een sociaal secretariaat of een andere partij, dient met die partij een verwerkersovereenkomst te worden opgesteld (zie model hier).

3.2 BEDRIJFSWAGENS

- Rechtmatige verwerkingsgrond: noodzakelijk in het kader van de overeenkomst met de tewerkgestelde.
- Bewaartermijn: zie 2.1 personeelsdossier.
- Beveiliging van de loonsadministratie (in de brede zin van het woord): zie hier.
- Doorgifte van gegevens aan een derde partij:
  - Indien gewerkt wordt met de aankoop van wagens, dient bij de aankoop de registratie voldaan te worden op naam van de tewerksteller (niet de bestuurder).
  - Indien gewerkt wordt met een leasingmaatschappij, dienen de gegevens die doorgegeven worden op een beveiligde wijze doorgegeven te worden (zie hier) én dienen deze beperkt te worden tot het minimum.
- Indien gewerkt wordt met een leasingmaatschappij dient bovendien een verwerkersovereenkomst opgesteld te worden (zie model hier).

3.3 GROEPSVERZEKERING / HOSPITALISATIE VERZEKERING

- Rechtmatige verwerkingsgrond: noodzakelijk in het kader van de overeenkomst met de tewerkgestelde.
- Bewaartermijn: zie 2.1 personeelsdossier.
- Beveiliging van de loonsadministratie (in de brede zin van het woord): zie hier.
- Er dient met de externe verzekeringspartij een verwerkersovereenkomst opgemaakt te worden (zie model hier). Echter, in bepaalde gevallen heeft de verzekeringsmaatschappij een dergelijke overeenkomst onderdeel gemaakt van de algemene voorwaarden. In dit geval is het aan de verzekeringnemer (de werkgever/tewerksteller) om na te gaan of de uiteengezette voorwaarden/garanties afdoende zijn.

4. TOEZICHT OP WERKNEMERS

4.1 CAMERABEWAKING

- Rechtmatige verwerkingsgrond: gerechtvaardigd belang van de verwerkingsverantwoordelijke.
- Voorafgaand aan het instellen van camerabewaking dient een Gegevensbeschermingseffectbeoordeling te worden uitgevoerd.
- Informeren: informeer de werknemers over alle aspecten van de camerabewaking.

Zie ook hier wat de camerabewaking betreft.

4.2 TOEZICHT OP GEBRUIK VAN COMPUTERS / INTERNET

Computers/internet wordt in de eerste plaats ter beschikking gesteld voor professionele doeleinden. Het verkennen van internet voor persoonlijke vorming en ontwikkeling wordt aanvaard mits het in beperkte mate gebeurt.

Regels met betrekking tot het instellen van toezicht op gebruik van computers/internet:

- Informeer de werknemer over de toezichtsmaatregelen en de reikwijdte ervan.
- Neem in het arbeidsreglement op dat privé-gegevens niet mogen worden opgeslagen op computers die gebruikt worden voor professionele doeleinden.

4.3 TOEZICHT OP COMMUNICATIE / MAILGEBRUIK

Regels met betrekking tot het instellen van toezicht op communicatie/mailgebruik:

- Informeer de werknemer over de toezichtsmaatregelen en de reikwijdte ervan.
- Hanteer volgende preventieve principes:
  - Werknemers dienen gebruik te maken van privé-mailboxen voor privé-berichten.
  - Bij langdurige afwezigheid van een medewerker (meerdere dagen) dient een automatisch antwoord ingesteld te worden zodat correspondenten op de hoogte zijn van de langdurige

afwezigheid ("*out of office*"), waarbij verwezen wordt naar een mailadres waar men tijdens de afwezigheid terecht kan.
    - Aanbeveling om te werken met generieke mailadressen per dienst/afdeling (bv. afdeling@onderneming.be) in geval van externe communicatie.
- Indien de preventieve maatregelen niet volstaan, kunnen volgende stappen gezet worden, doch mits documentering van redenering en belangen van de tewerksteller die primeren boven die van de werknemer:
    - Gebruik zoekfuncties om op zoek te gaan naar een bepaalde communicatie, zonder alle communicaties te overlopen;
    - Beperk de vaststelling tot het feit dat een dergelijke communicatie (op basis van titel) bestaat, zonder de inhoud te bekijken;
    - Indien de inhoud bekeken dient te worden, dient grondig gedocumenteerd te worden waarom het belang van de tewerksteller primeert;
    - Bij onverwachte afwezigheid wordt in overleg met de tewerksteller en de verantwoordelijke voor de bescherming van persoonsgegevens een persoon aangeduid die toegang verkrijgt tot de mailbox. Mails en documenten die als privé gemarkeerd zijn, of factoren erop wijzen dat het over privé communicatie/documenten gaat, mogen niet geopend worden;
    - Bij vertrek van de werknemer uit de onderneming dient de toegang tot de mailbox onmiddellijk afgesloten te worden.

4.4 TELEWERKEN

Elke organisatie moet de gepaste maatregelen treffen, in functie van het toegangsmedium (vb. internet, privaat netwerk, draadloos), voor de informatieveiligheid van de online-toegang van buiten de organisatie tot de professionele, vertrouwelijke en gevoelige gegevens van de organisatie.

Indien de telewerker een telewerk-apparaat van de organisatie ter beschikking heeft, kan de organisatie autonoom bepalen welke veiligheidsmaatregelen van toepassing zijn. Daarmee kan een organisatie de risico's grotendeels afdekken.

De werkgever kan de volgende gepaste maatregelen treffen:

- Wat betreft de locatie:
    - Vastleggen op welke locatie de telewerker mag telewerken. De organisatie kan verbieden om vanuit een internetcafé of via een onbeveiligde draadloze verbinding te telewerken.
    - *Clean desk*-beleid invoeren (zie meer info hier).
- Wat betreft het apparaat:
    - De telewerker moet inloggen met een gebruikersnaam en wachtwoord/wachtzin, eventueel ondersteund door een certificaat. Bescherm de toegang tot organisatie systemen door twee-factor authenticatie (met het telewerk-apparaat alleen kan geen toegang worden verkregen).
    - De werkgever gebruikt tools waarmee op alle telewerk-apparaten, zowel van de organisatie of privé, met gegevens van de organisatie, het veiligheidsbeleid technisch kan afgedwongen worden.
    - Schermbeveiliging (screensaver) maakt na een periode van maximaal 15 minuten inactiviteit alle informatie op het scherm ontoegankelijk.

    - Gebruiksvoorwaarden voor telewerken vastleggen, valideren, communiceren en onderhouden.
- Wat betreft de verbinding:
    - Het telewerk-apparaat dat een verbinding met de ICT-infrastructuur van de organisatie wil opzetten wordt gecontroleerd of deze voorzien is van een up-to-date virusscanner en een firewall.

HOOFDSTUK 4: IT EN SECURITY

De informatie in dit hoofdstuk is gekoppeld aan de software/het softwarepakket dat u gebruikt. **Voor meer informatie omtrent deze aanbevelingen kan u terecht bij uw softwareleverancier. Zij zullen u kunnen antwoorden in welke mate de voorgestelde aanbevelingen technisch geïmplementeerd zijn/kunnen worden in uw systeem.**

Dezelfde technische aanbevelingen kunnen niet voor alle partijen gegeven worden. In dit hoofdstuk zal u dan ook algemene aanbevelingen terugvinden die aangevuld worden met aanbevelingen die verder gaan (*aangeduid in groen en schuingedrukt*) dan wat minimaal vereist is. In functie van de mate van materniteit van de onderneming en de mogelijke (financiële) middelen, zal deze aan alle verplichtingen of enkel aan de minimale verplichtingen moeten voldoen.

1. WACHTWOORDBELEID

Volgende principes – of sterker – dienen in acht genomen te worden bij het instellen en gebruik van accounts en paswoorden:

- Het is verplicht een gebruikersnaam en wachtwoord te gebruiken voor het opstarten van softwaresystemen en computers om te voorkomen dat onbevoegden toegang tot het systeem bekomen.
- Het is aanbevolen om voor iedereen een individuele gebruikersnaam/account en bijhorend wachtwoord te gebruiken om traceerbaarheid te kunnen garanderen. Dit kan evenzeer bereikt worden door middel van een badgesysteem.
- De gekozen wachtwoorden moeten sterk zijn. Gebruik geen standaard leverancierswachtwoorden. Wijzig deze steeds in een zelfgekozen wachtwoord. Kies geen gemakkelijk te raden wachtwoorden, zoals wachtwoorden die je naam, geboortedatum, huisdier, etc. bevatten.
    - Tip: gebruik wachtwoordzinnen in plaats van simpele wachtwoorden.
- *Maak indien mogelijk gebruik van 2-factor authentication.*
- Wachtwoorden worden best op regelmatige basis (bijvoorbeeld na 90 dagen) gewijzigd.
- Zorg dat eerder gekozen wachtwoorden niet opnieuw kunnen ingesteld worden.
- Een wachtwoord is persoonlijk, deel het dus nooit met anderen, ook niet met iemand van bijv. de technische dienst (IT) of een leidinggevende. Schrijf nooit wachtwoorden op en bewaar ze nergens in het kantoor.
- Noteer nooit een wachtwoord in een e-mailbericht en sla nooit wachtwoorden op in een bestand zonder dat het versleuteld is.

2. AUTORISATIE

Alle medewerkers werken op basis van minimale autorisatie voor de uitvoering van hun taak. Om te bepalen wie wat kan binnen een applicatie, dient er een rechten- en rollensysteem uitgewerkt te worden volgens het principe van de minste privileges:

- Beperk toegang tot de verschillende modules in het softwaresysteem tot die personen die het nodig hebben voor het uitoefenen van hun job. Dit kan door toegangen te koppelen aan een account of door het gebruik van een badgesysteem waarbij de toegangen gekoppeld zijn aan een badge die behoort aan een persoon.
- Maak steeds een onderscheid tussen administrator accounts en gewone (gebruikers)accounts.
- Stel een op rollen gebaseerd toegangsbeleid op: bepaal een aantal rollen en koppel daaraan welke toegangen ze nodig hebben tot welke modules en welke rechten ze in deze modules dienen te hebben.

3. TRACIBILITY / MONITORING

Zorg dat het op elke moment duidelijk is wie welke handeling gedaan heeft met welk document/gegevens. Zoveel als mogelijk wordt systeemgebruik automatisch gelogd.

- Iedere werknemer dient bij voorkeur zijn eigen account te hebben. Het gebruik van gedeelde accounts dient vermeden te worden.
- Iedere werknemer dient met zijn eigen account in te loggen wanneer gedeelde software of gedeelde computers worden gebruikt.
- **(3)** *Voorzie in applicatieve auditing die het toelaat om loggevens te bekijken op dataniveau:*
    - *Pas logging toe om alle mogelijke software-, beveiliging- of systeemmeldingen te kunnen opvolgen en zorg ervoor dat de logbestanden niet kunnen aangepast worden.*
        - *Aanbeveling: voorzien in SSL/TLS encrypted syslog (Cisco).*
    - *Schrijf logbestanden weg naar een locatie die enkel toegankelijk is voor bevoegden en analyseer regelmatig de gelogde gebeurtenissen.*
        - *Aanbeveling: implementatie Security and Information Event Management (SIEM) – Rapid7.*
- **(3)** *Bewaartermijn:*
    - *Technical / infrastructurele logs :*
      Logs aangemaakt voor het technische analyseren en het technisch herstellen van ICT assets.
      Wenselijke retentietijd 6 maanden tenzij er andere wettelijke bepalingen zijn die een langere bewaartermijn voorzien.
    - *Business logs (transactionele logs) :*
      Logs aangemaakt voor het analyseren en het herstellen van business transactionale systemen.
      Wenselijke retentietijd 2 jaar tenzij er andere wettelijke bepalingen zijn die een langere bewaartermijn voorzien.
    - *Veiligheidslogs :*
      Logs aangemaakt met als doel om beveiligingsgebeurtenissen en -incidenten te detecteren en/of te analyseren.
      Wenselijke retentietijd 1 jaar tenzij er andere wettelijke bepalingen zijn die een langere bewaartermijn voorzien.

(3) *Logbestanden dienen beschermd te worden tegen inzage door onbevoegden, wijzigingen en verwijderingen. De raadpleging van logbestanden is altijd het voorwerp van een georganiseerde procedure binnen de organisatie met een historiek van de verzoeken die werden goedgekeurd/uitgevoerd of die werden afgekeurd.*

4. INCIDENTEN

Elke medewerker (zowel vast of tijdelijk, intern of extern) is verplicht melding te maken van ongeautoriseerde toegang, gebruik, verandering, openbaring, verlies of vernietiging van informatie en informatiesystemen.

Binnen elke onderneming bestaan er richtlijnen rond incidentenbeheer. Deze richtlijnen betreffen de volgende punten:

- Pro-actief opstellen van procedures en verantwoordelijkheden
- Identificeren en rapporteren van gebeurtenissen
- Meldingen bij incidenten rond persoonsgegevens
- Beoordelen van/beslissen over gebeurtenissen
- Rapporteren van zwakheden in informatiesystemen of diensten
- Verzamelen en veilig stellen van bewijsmateriaal
- Reageren op en herstellen van incidenten
- Leren uit incidenten via rapport en evaluatie

5. *CLEAN DESK / CLEAR SCREEN POLICY*

Elke medewerker speelt een belangrijke rol in het vermijden van ongeoorloofde toegang tot gevoelige informatie. Dit geldt zowel voor de toegangen tot de informatiesystemen en toepassingen als voor de fysieke toegang tot lokalen/kasten of tot documenten. De medewerking van alle medewerkers is van essentieel belang voor de informatieveiligheid en de privacy.

Zorg er bij voorkeur voor dat op het einde van de werkdag alle documenten die persoonsgegevens of vertrouwelijke informatie bevatten veilig opgeborgen zijn in een afgesloten kast.

- “Clean desk”-richtlijnen promoten de toepassing van drie basisregels:
    - Wanneer de medewerker in de apotheek/op kantoor aanwezig is: de medewerker probeert enkel de documenten die hij die dag nodig heeft op zijn bureau te laten liggen.
    - Wanneer de medewerker tijdelijk zijn bureau verlaat: de medewerker moet controleren of er geen vertrouwelijke informatie aanwezig is op zijn bureau die onbewaakt mag worden achtergelaten. Indien dit wel het geval is, moet hij/zij deze informatie veilig opbergen. Bovendien moet hij/zij minimaal de computer in slaaptoestand zetten (windows + L toets) en beveiligen aan de hand van een paswoord. Schermbeveiliging (screensaver) maakt na een periode van maximaal 15 minuten inactiviteit alle informatie op het scherm ontoegankelijk.
    - Wanneer de medewerker zijn bureau verlaat: het is de taak van de medewerker om ervoor te zorgen dat alle gevoelige informatie op een veilige plaats wordt opgeborgen zoals een kast die op slot kan en dat zijn bureau is opgeruimd alvorens de organisatie te verlaten. Het behoort tot de verantwoordelijkheid van de medewerkers om de nodige veiligheidsmaatregelen te nemen in hun bureau.
- Verwerkingsverantwoordelijken moeten nagaan of hun medewerkers dit beleid in acht nemen. Voer hiertoe periodieke controles uit om te garanderen dat er toegekeken wordt op de naleving van het beleid.

6. MOBIELE TOESTELLEN / '*BRING YOUR OWN DEVICE*' (BYOD)

De organisatie heeft voldoende garanties dat de private mobiele toestellen over een gelijkaardig informatieveiligheid- en privacy-niveau beschikken als dat van de mobiele toestellen (bv. gsm, laptop) die door de organisatie ter beschikking worden gesteld. De organisatie is bevoegd om veiligheidsinstellingen af te dwingen als privé-apparaten zakelijk gebruikt worden. Dit gaat dan onder meer over controle op wachtwoord/wachtzin, encryptie, aanwezigheid van anti-*malware* software.

De organisatie zal de eigen mobiele toestellen duidelijk identificeren, veilig configureren (met de nodige anti-*malware* software en met software die alle data op het toestel vanop afstand kunnen wissen) en de identificatie bijhouden in een centraal register.

De organisatie zal steeds de mogelijkheid hebben om de toegang tot de informatie van de organisatie (gegevens of toepassingen aanwezig op het mobiele toestel) direct te blokkeren en de gegevens te wissen.

In geval van verlies of diefstal verwittigt de gebruiker onmiddellijk de bevoegde dienst/persoon binnen de organisatie, ook voor een privaat mobiele toestel dat voor beroepsdoeleinden wordt gebruikt.

7. EXTERNE APPARATEN VOOR OPSLAG

Onder deze apparaten vallen zowel digitale opslagmedia als apparaten waarin dergelijke opslagmedia geïntegreerd zijn of gebruikt kunnen worden (bijvoorbeeld CD, DVD, verwisselbare harddisk, memory stick, flash geheugens, backup-media, externe harde schijven, cloud storage).

Mobiele apparaten vallen onder strengere veiligheidsvereisten dan apparaten op het vaste netwerk. Slechts mits autorisatie door de bevoegde dienst/persoon mogen externe apparaten voor opslag gebruikt en aangesloten worden.

Het aansluiten van mobiele opslagmedia op apparatuur of op het netwerk van de organisatie geeft de organisatie het recht om alle nodig geachte veiligheidsmaatregelen te nemen, inclusief het testen op virussen, het nemen van kopieën en onderzoek naar naleving van het interne reglement. Het gebruik van opslagmedia of apparatuur die niet aan de veiligheidsregels beantwoorden is niet toegelaten.

Indien externe apparaten voor de opslag van vertrouwelijke gegevens gebruikt worden, dan moeten de gegevens steeds beveiligd zijn (zie hier). Bovendien moet van alle gegevens die op mobiele opslagmedia opgeslagen worden regelmatig een backup gemaakt worden. Indien de externe apparaten voor opslag louter gebruikt worden om gegevens over te zetten, dan moeten de gegevens na de overzetting verwijderd worden. In alle andere gevallen van online verwerking moet de verbinding steeds verlopen via het extranet van de organisatie.

Apparaten voor massaopslag, zoals cd's, dvd's, USB-drives of externe harde schijven die persoonsgegevens bevatten dienen eveneens te worden opgeborgen in afgesloten kasten indien ze niet worden gebruikt. Informatie rond het verwijderen van (digitale) persoonsgegevens vindt u hier.

8. (*CLOUD*) STORAGE BELEID

Alvorens storage-diensten in te voeren, maak je een analyse van alle mogelijke oplossingen.

- Het gebruik van storage-diensten voor werkdoeleinden moet formeel worden goedgekeurd door de persoon verantwoordelijk voor IT (bv. de IT Manager), na advies ingewonnen te hebben van de *Data Protection Officer* (indien deze er binnen de onderneming is). Het is noodzakelijk om het geschikte type storage voor de beoogde verwerking te identificeren in functie van het huidige aanbod inzake storage-diensten.
- Met elke goedgekeurde provider van storage-diensten dient een verwerkersovereenkomst te worden afgesloten.
- In geval van opslag in de *cloud* mogen de accounts voor toegang tot deze clouddiensten nooit gedeeld worden.
- Persoonlijke clouddiensten accounts mogen niet gebruikt worden voor opslag, bewerking of uitwisseling van werk gerelateerde gegevens.
- *Verhinder waar mogelijk het bewaren van documenten op clouddiensten die niet toegelaten zijn door upload van documenten te blokkeren op firewall-niveau.*

Bij gebruik van een clouddienst, dienen de fysieke locaties van de datacentra van een cloudprovider binnen de Europese Economische Ruimte (EER) te liggen of het land moet door de Gegevensbeschermingsautoriteit goedgekeurd zijn (op basis van een adequaatheidsbesluit).

9. BACK-UPS

- Beveilig de back-ups waarbij bij voorkeur zowel de back-up zelf versleuteld wordt alsook een strikt toegangebeheer tot de back-up gewaarborgd wordt.
- De backupbestanden die bewaard worden op externe schijven (SD drive, CD, DVD, USB-sleutel, externe harde schijf, etc.), moeten fysiek beveiligd worden door deze te bewaren in een afgesloten kast, een niet-toegankelijke ruimte of in de cloud.
- De sleutels tot ofwel de kasten of de niet-toegankelijke ruimte moeten op een aparte plaats bewaard worden en mogen niet op het slot blijven zitten.
- Bewaartermijn: backupbestanden dienen na een periode van 30 dagen tot maximaal 90 dagen overschreven te worden.

10. GEBRUIK VAN TELEFOON

Persoonsgegevens mogen alleen via de telefoon worden uitgewisseld als enerzijds de persoon die de informatie ontvangt het recht heeft om de informatie te ontvangen, en anderzijds de identiteit van de persoon die de informatie wenst te ontvangen geverifieerd werd.

Bellers hebben alleen het recht om persoonsgegevens te ontvangen als:
- de beller de patiënt is die het onderwerp van de informatie betreft;
- de beller een geautoriseerde wettelijke vertegenwoordiger is van de persoon die het onderwerp vormt van de informatie;

- de patiënt specifiek toestemming heeft gegeven voor het vrijgeven van de informatie aan de persoon die telefonisch contact opneemt met de apotheek en de apotheek bijgevolg is geautoriseerd om de informatie aan deze persoon vrij te geven.

Voor de verificatie van de identiteit van de beller vraagt men best de gegevens op die waarover men reeds beschikt, in plaats van bijkomend nieuwe gegevens te vragen aan de beller. Dit betekent dat men moet proberen de kennis van de betrokkene te verifiëren (bijvoorbeeld door enkele vragen te stellen) met betrekking tot dergelijke gegevens die onder het verzoek vallen of die men voor de gerelateerde doeleinden heeft.

Men kan geen persoonsgegevens doorgeven aan een beller zonder eerst van hem de volledige naam van de patiënt te hebben verkregen, aangevuld met een ander stuk informatie dat in het systeem/dossier van de patiënt opgenomen is, zoals:

1) geboortedatum patiënt
2) naam van het afgeleverde product (indien van toepassing)
3) INSZ-nummer

Eventuele verzoeken om toegang tot persoonsgegevens door onbevoegde personen kunnen resulteren in een datalek. Indien de beller onvoldoende geïdentificeerd kan worden, moet geweigerd worden persoonsgegevens telefonisch door te geven.

De communicatie moet in alle vertrouwelijkheid en veiligheid kunnen plaatsvinden. Bij de gegevensuitwisseling tussen de betrokken partijen mag het medisch beroepsgeheim niet uit het oog worden verloren: de communicatie mag bijgevolg alleen betrekking hebben op de gegevens die nodig zijn voor de continuïteit van de zorg voor de patiënt.

11. GEBRUIK VAN E-MAIL

Beperk het gebruik van e-mail voor het versturen van vertrouwelijke gegevens in het kader van farmaceutische zorg. Gebruik indien mogelijk hiervoor de beveiligde platformen zoals *Vitalink*/BRUSAFE+/INTER-MED en *eHealth*.

Gebruik altijd het professionele e-mailadres. Privé-mailadressen mogen niet gebruikt worden voor beroepsmatig mailverkeer.

Let op het onderwerp en de inhoud van de mail. Vermijd het gebruik van namen en andere persoonsgegevens in het onderwerp van de e-mail. Zorg ervoor dat je nakijkt of het e-mailadres van de ontvanger juist is en correct geschreven. Zet ook enkel ontvangers in kopie waarvan er een noodzaak is dat zij deze informatie ontvangen.

Indien je communiceert over een patiënt, probeer de gegevens dan te beperken tot die specifieke patiënt, bv. niet meerdere zorgverleners met één e-mail aanschrijven. Gebruik indien mogelijk zoveel mogelijk gepseudonimiseerde gegevens, zoals bv. patiëntennummer.

Verwijder e-mails zoveel mogelijk. Na het verwerken van een e-mail met (gevoelige) persoonsgegevens kan je deze best verwijderen uit je mailbox. Vergeet ook verzonden en verwijderde items niet leeg te maken.

Geen enkel medisch gegeven mag via e-mail worden overgemaakt in zichtbare vorm. Zorg ervoor dat persoonsgegevens beveiligd/versleuteld zijn. Neem bijvoorbeeld gevoelige informatie op in een Word-document, beveilig dit document (ga naar: *Bestand > Info > Document beveiligen > Versleutelen met wachtwoord*) en voeg dit document vervolgens toe als bijlage bij de mail. Het wachtwoord van het document kan telefonisch gecommuniceerd worden aan de ontvanger. Andere methoden zijn bijvoorbeeld het gebruik van *Own Cloud*.

Digitaal dienen documenten zo verstuurd te worden dat het mogelijk is om het document met gezondheidsgegevens apart te verwerken ten opzichte van documenten met persoonsgegevens.

In het geval clouddiensten worden gebruikt om het mailen van persoonsgegevens te vermijden, dan kan men zich beperken tot het doormailen van de link naar de serverlocatie (bijvoorbeeld een gedeelde Dropbox). Op die manier vermijdt men in de eerste plaats dat persoonsgegevens doorgemaild moeten worden en vervolgens schermt men ook de persoonsgegevens af, daar men enkel toegang heeft tot de serverlocatie indien de ontvanger bevoegd is.

Elektronische uitwisseling van gegevens/documenten (bv. medicatieschema's) dient te gebeuren op een manier waarbij verzekerd wordt dat de bestemmeling bevoegd is om de gegevens te verwerken. Als een document verstuurd wordt naar een grote groep bestemmelingen, voeg deze dan allemaal toe in BCC ('*Blind Carbon Copy*') zodat deze niet kunnen zien wie de mail allemaal gekregen heeft.

- *Pas "Secure e-mail" toe om mails te encrypteren. (Indien gebruik gemaakt wordt van Office 365, kan via de gratis extensie "Azure information Protection" gebruikt worden.)*
- *Beperk Outlook WebAccess voor gebruikers die vanop afstand aan hun mailbox willen.*
- *Stel Data Loss Prevention (DLP)-regels in, door toevoeging van een DLP-functie/extensie aan de gebruikte beveiligingssoftware.*

12. GEBRUIK FAX

- Vermijd het uitwisselen van confidentiële of geheime informatie via fax.
- Externe faxnummers en emailadressen mogen enkel overgenomen worden van officiële lijsten of rechtstreeks via de bestemmeling.
- Alvorens men een fax met confidentiële gegevens uitstuurt, moet men de bestemmeling hiervan op de hoogte brengen.
- Na de transmissie moet de ontvangst van de fax telefonisch bevestigd worden.
- Inkomende faxen dienen onmiddellijk van de fax verwijderd te worden.
- Zorg ervoor dat de fax in een ruimte staat die niet toegankelijk is voor onbevoegden.
- De verzender dient ervoor te zorgen dat het ontvangstbewijs verwijderd wordt van het faxtoestel.

13. LOKALE COMPUTERS

Om laptops en desktops te voorzien van een passend beveiligingsniveau om gegevens te beschermen dienen volgende maatregelen te worden toegepast:

- Voorzie elk toestel van de laatste security en software patches.

- Voorzie elk toestel van antivirus en -malware beschermingsoftware en werk de virusdefinities continu bij.
- Zorg ervoor dat enkel toegang tot een toestel kan verkregen worden door in te loggen met gebruikersnaam en wachtwoord. *Indien mogelijk past u 2-factor authentication toe.*
- Vermijd diefstal van laptops door deze op te bergen in een afgesloten kast wanneer niet in gebruik of deze vast te maken met een Kensington slot.
- *Zorg ervoor dat voor het uitvoeren van administratortaken zoals het installeren van programma's, er automatisch gevraagd wordt om in te loggen met een gebruiker die administratorrechten heeft.*
- *Elk toestel heeft ook verschillende mogelijkheden om externe media te gebruiken. Een beperking van USB-gebruik wordt aangeraden. Hierbij kan een beperking opgelegd worden op het gebruik van media voor massaopslag zonder de functionaliteit van een muis of toetsenbord af te blokken.*
- *Encrypteer de harde schijf zodat gegevens niet leesbaar zijn wanneer het toestel in onrechtmatige handen komt.*
- *Extern gebruik van de toestellen dient te gebeuren over een beveiligd kanaal waardoor deze niet onderschept kan worden (VPN).*

14. NETWERK

Draadloze netwerken voor intern gebruik geven rechtstreeks toegang tot de interne systemen van de organisatie. Authenticatiemethoden voor toegang tot draadloze netwerken moet bestaan uit sterke authenticatie (bijvoorbeeld 2-factor).

Draadloze netwerken voor bezoekers moeten enkel toegang geven tot internet en internetdiensten van de organisatie. Rechtstreekse toegang tot interne systemen van de organisatie is niet toegestaan. Zorg ervoor dat onbeheerde of onbeveiligde toestellen geen toegang krijgen tot het netwerk en de daarop opgeslagen gegevens:

- Voorzie in een firewall oplossing ter bescherming van alle trafiek van en naar het internet.
- Beveilig draadloze verbindingen.
- *Segmenteer of isoleer de computers met persoonsgegevens.*
- *Laat geen onveilige verbindingen toe. Gebruik enkel versleutelde verbindingen HTTPS, SFTP, SSL.*
- *Gebruik Data Loss Prevention (DLP) regels om datalekken te voorkomen.*

15. DIGITALE GEGEVENSOPSLAG / SERVERS (2, 3, 4)

Niet-publieke persoonsgegevens mogen niet op de vaste werkpost opgeslagen worden, tenzij voor de duur van een toepassingssessie. De systemen voor opslag van niet-publieke persoonsgegevens moeten minstens beveiligd zijn door een dubbele fysieke perimeter met toegangscontrole. Er moet een nominatieve lijst bestaan van alle personen die toegang hebben tot de kleinste perimeter met vermelding van hun specifieke bevoegdheden. Deze toegang is bij voorkeur gekoppeld aan een badge.

Zorg ervoor dat de opslag van gegevens passend beveiligd wordt door middel van volgende maatregelen:

- Maak gebruik van centrale opslag zodat enkel deze bron beveiligd dient te worden.

- Beperk het bewaren van informatie op onveilige opslag door middel van een Data Loss Prevention oplossing of technische beperkingen.
- Gebruik encryptie om de bron te beveiligen.
- Onderzoek of bestands- en database encryptie kan toegepast worden om ongeoorloofde verspreiding te vermijden.
- *Onderzoek of bestanden verder kunnen beveiligd worden door het implementeren van een Digital Rights Managementoplossing die ongeoorloofde verwerking van gegevens kan beperken door middel van gebruiksbeperkingen (gebruik, opslag, doorsturen, printen).*
- Voorzie in een veilige opslagmogelijkheid in functie van het delen van bestanden.

16. ENCRYPTIE

Wanneer cryptografie vereist is, moet de organisatie een overzicht bijgehouden waarin terug te vinden is waar cryptografische maatregelen worden toegepast, welke cryptografische maatregelen worden toegepast en wie hiervoor verantwoordelijk is.

De toepassing en gepastheid van cryptografische oplossingen en maatregelen moet periodiek beoordeeld worden. Versleutelde data van derden die binnenkomen op het netwerk van de organisatie moeten eerst gedecrypteerd worden om gescand te worden op virussen en andere *malware*.

De organisatie is verantwoordelijk voor effectief sleutelbeheer. Specifieke processen en procedures gerelateerd aan sleutelbeheer moeten opgesteld, gevalideerd, gecommuniceerd worden aan alle betrokken actoren en ook regelmatig onderhouden worden.

Voor elke sleutel moet een interne medewerker verantwoordelijk zijn. Er moet een overzicht bijgehouden worden van alle verantwoordelijken voor sleutels. Er moeten maatregelen toegepast worden om ongeautoriseerde pogingen tot verspreiding, ontcijfering, toegang, gebruik, wijziging of vervanging van sleutels of versleutelde data te detecteren. In overeenkomsten met leveranciers van cryptografische diensten of producten moeten deze richtlijnen ingesloten zijn.

17. PRINTERS

- Vermijd papier en digitaliseer documenten waar mogelijk.
  Print zo weinig mogelijk documenten af, documenten dienen waar mogelijk elektronisch te worden bekeken, gedeeld en bewerkt.
- Geprinte documenten met persoonlijke gegevens moeten onmiddellijk na het afdrukken van de printer worden verwijderd door degene die het document geprint heeft.
- *Implementeer Secure Printing indien mogelijk. De documenten met gevoelige gegevens worden bij voorkeur afgedrukt na het intypen van een code waardoor ze niet direct uit een printer komen en onbewaakt achterblijven. Medewerkers kunnen dan aan de printer alsnog beslissen om documenten niet af te drukken (ook goed voor lager tonerverbruik en voor het milieu).*
- *Scherm de toegang tot de printerinstellingen af voor onbevoegden en wijzig het standaard wachtwoord van een netwerkprinter.*

- *Laat het vernietigen van afgeschreven toestellen uitvoeren door een hierin gespecialiseerde partij zodat er geen gegevens kunnen gevonden worden in het geheugen.*

18. SUPPORT / REMOTE ACCESS

Bij het aanstellen van derde partijen die mogelijks (van op afstand) toegang kunnen krijgen tot de persoonsgegevens die verwerkt worden, moet er enerzijds voldaan worden aan de wettelijke vereisten, anderzijds moet ervoor gezorgd worden dat ondersteuning op afstand op een zo veilig mogelijke manier gebeurt. Hieronder volgen enkele aanbevelingen:

- Voorzie in een verwerkersovereenkomst (zie model hier).
- Voorzie in een vertrouwelijkheidsverklaring. Dit kan onderdeel zijn van de verwerkersovereenkomst. Zorg ervoor dat alle werknemers die in aanraking komen met persoonsgegevens eveneens zo'n verklaring ondertekend hebben.
- Vraag steeds toestemming vooraleer een scherm over te nemen. Een bijkomend advies hierbij is dat de gegeven toestemming bijgehouden wordt zodat deze achteraf kan worden voorgelegd.
- *Zorg ervoor dat het inloggen op toestellen van op afstand gebeurt over een beveiligd kanaal zodat deze niet onderschept kan worden.*
- *In geval laptops/computers moeten worden overgenomen, kies dan voor een software waarbij de sessie's integraal opgenomen worden. Dit om interventies achteraf te kunnen analyseren.*
- *Indien er voor de analyse van een bepaald probleem een export van gegevens nodig is, moeten hierbij strikte maatregelen genomen worden.*

19. VEILIG VERWIJDEREN / VERNIETIGEN VAN (DIGITALE) PERSOONSGEGEVENS

Binnen de 30 dagen na het verstrijken van de toepasselijke bewaartermijn moeten de gegevens verwijderd worden. Documenteer – bij voorkeur in uw verwerkingsregister – hoe dit proces verloopt.

- Op analoge drager (bv. papier):

De vernietiging van documenten die persoonsgegevens bevatten moet op een gecontroleerde manier gebeuren. Documenten die persoonsgegevens bevatten dienen vernietigd te worden door gebruik te maken van papierversnipperaars of afgesloten papiermanden (*destrabox*).

De inhoud van deze containers wordt door een gespecialiseerde firma vernietigd. Vernietiging van originele gegevens kan uitsluitend met medeweten van de verwerkingsverantwoordelijke en rekening houdend met de wettelijke bepalingen die erop van toepassing zijn. De actie van de vernietiging moet het voorwerp uitmaken van een autorisatie.

- Op digitale dragers:

Behalve de fysieke vernietiging garandeert geen enkele technische oplossing dat de gegevens volledig gewist zullen worden op een magnetische of andersoortige drager.

  - Fysiek vernietigen

"Het fysiek vernietiging van informatiedragers dient altijd te worden toegepast bij defecte en WORM ("write once, read many") media. Dit kan gebeuren door gespecialiseerde firma's. In dat geval dient na vernietiging een 'attest van gewaarborgde vernietiging' worden opgevraagd of dient de vernietiging minstens geregistreerd te worden. Bewaartijd van de registratie is minstens 2 jaar."[8]

De fysische vernietiging kan op verschillende manieren gebeuren: vervormen, versnipperen, desintegratie, fijnmalen, verbranden of chemisch vernietigen.

Persoonsgegevens op gegevensdragers dienen op een veilige manier vernietigd te worden. Denk hierbij onder andere aan computers, laptops, servers, kopieerapparaten, printers, faxapparaten, telefoons, smartphones, tablets, USB-sticks, externe harde schijven en digitale camera's.

- Investeer in software om gegevens onherroepelijk te vernietigen.
- Apparatuur dat niet langer in gebruik is dient ofwel te worden weggeven, te worden verkocht of te worden vernietigd en gerecycleerd.
- Het wel of niet hergebruiken en het al of niet defect zijn van de gegevensdrager bepaalt mee de keuze van de te gebruiken wismethode (overschrijven, softwarematig wissen of demagnetiseren).
    - Indien apparatuur wordt weggegeven of verkocht, dienen de gegevens softwarematig te worden gewist of te worden gedemagnetiseerd.
    - Indien apparatuur wordt vernietigd volstaat overschrijven van de gegevens.
- Indien de gegevensdrager hergebruikt wordt door derden, moet je echt zeker zijn dat alle data echt vernietigd werd.
- Zorg voor bewijs dat de gegevens echt vernietigd werden.

- *Vercijfering/encryptie*

"De voorafgaande encryptie van de gegevens vermindert aanzienlijk het risico op het compromitteren van professionele, vertrouwelijke en gevoelige gegevens zelfs al is niet alle informatie op de informatiedrager volledig verwijderd."[9]

De overschrijving op het einde van de levenscyclus wordt altijd aanbevolen.

- *Overschrijven*

Via het overschrijven van de informatiedrager, kan informatie verwijderd worden.

"De efficiëntie van deze methode hangt af van het aantal overschrijfcycli (om de remanentie in de randen te beperken), van de competenties en de kennis van de persoon die het proces uitvoert, en van de verificatiefuncties van de overschrijvingssoftware. Deze helpen garanderen dat de gehele toegankelijke opslagruimte van de informatiedrager overschreven wordt."

"Een drievoudige overschrijving is algemeen aanvaardbaar als methode om alle professionele en vertrouwelijke gegevens te vernietigen. Het drievoudig overschrijven van gegevens volstaat niet als vernietigingsmethode van gegevens op magnetische informatiedragers die gevoelige informatie bevatten. Indien het drievoudig overschrijven echter gecombineerd wordt met andere vernietigingsmethodes zoals de desintegratie of de versnippering van gegevens, biedt deze werkwijze

[8] Bron: *Beleidslijn beveiliging van informatie en privéleven : vernietiging van elektronische informatiedragers*, Versie 2017, Sociale zekerheid.be, pagina 7, 2.4 Fysieke vernietiging

[9] Bron: *Beleidslijn beveiliging van informatie en privéleven : vernietiging van elektronische informatiedragers*, Versie 2017, Sociale zekerheid.be, pagina 5, 2.1 Encryptie

een aanvullende garantie op vernietiging van de gegevens. In dat geval is er geen redelijke mogelijkheid meer om de gegevens te achterhalen."

"Wat niet-magnetische informatiedragers betreft, zoals USB-sticks, geheugenkaarten, FLASH-geheugens, bestaan er specifieke schrijfalgoritmes om degradatie tegen te gaan. Dit leidt tot meerdere kopieën zodat de kans op het achterhalen van gegevens na het wissen vergroot. Voor dit type informatiedrager is, voor een maximale beveiliging, niet alleen de encryptie van gegevens essentieel maar ook de fysieke vernietiging van de informatiedrager."

- *Demagnetisatie*

"Demagnetisatie bestaat erin aan de hand van een voldoende krachtig magnetisch veld alle gegevens te wissen op een specifieke magnetische informatiedrager. De efficiëntie van de methode is gekoppeld aan de intensiteit van het magnetische veld dat opgewekt wordt door het demagnetisatie-apparaat en aan de magnetische eigenschappen van de informatiedrager."[10]

[10] Bron: *Beleidslijn beveiliging van informatie en privéleven : vernietiging van elektronische informatiedragers*, Versie 2017, Sociale zekerheid.be, pagina 6, 2.2 Overschrijven en 2.3 Demagnetisatie