DEEL 2

GDPR in uw praktijk

Elfi Goesaert
Eef Dreesen

GDPR: Hoe starten?

- Awareness

- Concrete acties:
  - Verwerkingsregister opstellen
  - Contracten met verwerkers
  - Privacyverklaring opstellen
  - Procedures bij datalekken
  - …

- Hoe begin je daar nu aan?
  - Domus Medica en BV’s zorgen voor materiaal om geïnformeerd voor te bereiden op GDPR

- Casussen en tips

GDPR in uw praktijk

1. VERWERKINGSREGISTER

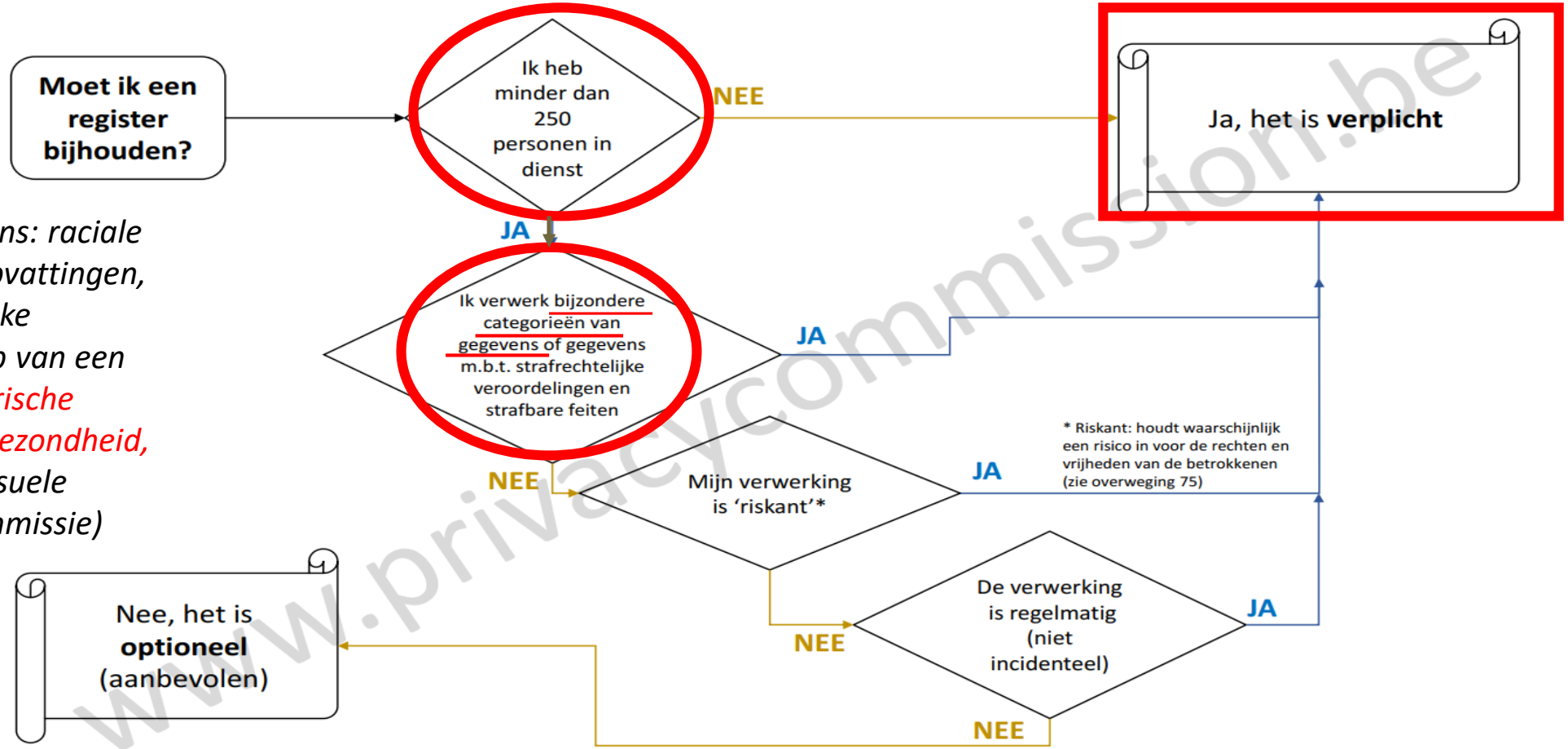
Wat?

- Overzicht van alle verwerkingen van persoonsgegevens
- Documentatieplicht en aantoonbaarheid
- Patiënten en medewerkers informeren over hoe de gegevens verwerkt worden en om welke redenen

Template vanwege Domus of BV’s

Verwerkingsregister = verplichting?

**dit wil zeggen persoonsgegevens: raciale of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, het lidmaatschap van een vakbond, of genetische, biometrische gegevens of gegevens over de gezondheid, iemands seksueel gedrag of seksuele gerichtheid (website Privacycommissie)*



Inhoud

A. Contactgegevens verwerkingsverantwoordelijke
   - *Verwerkingsverantwoordelijke: persoon of organisatie die het doel en de middelen voor de verwerking vaststelt*
B. Verwerkingsdoeleinden: **waarom** wordt de informatie verwerkt?
C. **Van wie** wordt informatie verwerkt?
D. **Welke persoonsgegevens** worden verwerkt/bijgehouden/…?
E. **Wettelijke basis en rechtsgronden** voor de verwerking van de gegevens
F. **Bewaartermijnen** van gegevens: hoe lang mag je de gegevens bijhouden?
G. **Met wie** worden de gegevens **gedeeld**?
H. **Beschermingsmaatregelen** (technisch en organisatorisch): wat doe je om de gegevens te beschermen?

Praktisch

- Huidige vorm: Excel file (Finalisatie uiterlijk mid mei)
- Kant en klare template
- Nog te doen: nakijken, aanvullen, schrappen

Casussen

Beheer (lokaal) farmaceutisch dossier

Beheer van medisch dossier

Inhoud

A. Contactgegevens verwerkingsverantwoordelijke
   - *Verwerkingsverantwoordelijke: persoon of organisatie die het doel en de middelen voor de verwerking vaststelt*

B. Verwerkingsdoeleinden: **waarom** wordt de informatie verwerkt?

C. **Van wie** wordt informatie verwerkt?

D. **Welke persoonsgegevens** worden verwerkt/bijgehouden/…?

E. **Wettelijke basis en rechtsgronden** voor de verwerking van de gegevens

F. **Bewaartermijnen** van gegevens: hoe lang mag je de gegevens bijhouden?

G. **Met wie** worden de gegevens **gedeeld**?

H. **Beschermingsmaatregelen** (technisch en organisatorisch): wat doe je om de gegevens te beschermen?

A. Verwerkingsverantwoordelijke

> Persoon of organisatie die doel en middelen voor de verwerking vaststelt

- Onder verantwoordelijkheid van apotheker-titularis
- Apotheek-eigenaar voor bepaalde verwerkingen (vb personeelsbeheer)

- Praktijk
- Best 1 ‘coördinator’ aanduiden die opvolgt en aanspreekpunt is

Inhoud

A. Contactgegevens verwerkingsverantwoordelijke
    - *Verwerkingsverantwoordelijke: persoon of organisatie die het doel en de middelen voor de verwerking vaststelt*
B. Verwerkingsdoeleinden: **waarom** wordt de informatie verwerkt?
C. **Van wie** wordt informatie verwerkt?
D. **Welke persoonsgegevens** worden verwerkt/bijgehouden/…?
E. **Wettelijke basis en rechtsgronden** voor de verwerking van de gegevens
F. **Bewaartermijnen** van gegevens: hoe lang mag je de gegevens bijhouden?
G. **Met wie** worden de gegevens **gedeeld**?
H. **Beschermingsmaatregelen** (technisch en organisatorisch): wat doe je om de gegevens te beschermen?

B. Verwerkingsdoel = waarom

> Redenen waarom de gegevens worden verwerkt = verantwoording

> Voorbeelden:
- Personeelsbeheer
- Boekhouding
- Patiëntenzorg
- Patiëntenadministratie
- Patiëntenregistratie
- Geneesmiddelenbeheer
- Direct marketing
- Beheer van verzekeringen
- …

B. Verwerkingsdoel = waarom

> Casus medisch/farmaceutisch dossier:

- Patiëntenzorg: het verstrekken van gezondheidszorg, behandeling patiënt
- Geneesmiddelenbeheer: verwerkingen mbt aflevering van geneesmiddelen, advies, gebruik

Inhoud

A. Contactgegevens verwerkingsverantwoordelijke
    - *Verwerkingsverantwoordelijke: persoon of organisatie die het doel en de middelen voor de verwerking vaststelt*
B. Verwerkingsdoeleinden: **waarom** wordt de informatie verwerkt?
C. **Van wie** wordt informatie verwerkt?
D. **Welke persoonsgegevens** worden verwerkt/bijgehouden/…?
E. **Wettelijke basis en rechtsgronden** voor de verwerking van de gegevens
F. **Bewaartermijnen** van gegevens: hoe lang mag je de gegevens bijhouden?
G. **Met wie** worden de gegevens **gedeeld**?
H. **Beschermingsmaatregelen** (technisch en organisatorisch): wat doe je om de gegevens te beschermen?

C. Betrokkenen = van wie wordt informatie verwerkt

> Casus medisch/farmaceutisch dossier:

- Patiënt
- Arts (wie is GMD-houder)
- Familieleden, mantelzorgers, indien die informatie relevantie heeft

Inhoud

A. Contactgegevens verwerkingsverantwoordelijke
   - *Verwerkingsverantwoordelijke: persoon of organisatie die het doel en de middelen voor de verwerking vaststelt*

B. Verwerkingsdoeleinden: **waarom** wordt de informatie verwerkt?

C. **Van wie** wordt informatie verwerkt?

D. **Welke persoonsgegevens** worden verwerkt/bijgehouden/…?

E. **Wettelijke basis en rechtsgronden** voor de verwerking van de gegevens

F. **Bewaartermijnen** van gegevens: hoe lang mag je de gegevens bijhouden?

G. **Met wie** worden de gegevens **gedeeld**?

H. **Beschermingsmaatregelen** (technisch en organisatorisch): wat doe je om de gegevens te beschermen?

D. Categorie van gegevens = welke

> **Persoonsgegevens**:
  - Identificatiegegevens (naam, voornaam), adresgegevens, lokalisatiegegevens (vb. GPS via GSM), beeldopnamen, fysieke gegevens (gewicht, haarkleur,…), samenstelling gezin, opleiding en vorming,…

> **Gevoelige gegevens** (!! Belang van rechtsgrond):

- Gerechtelijke gegevens
- Lichamelijke gezondheid
- Psychische gezondheid
- Risicosituaties en –gedragingen
- Genetische gegevens
- Gegevens met betrekking tot remediëring
- Raciale of etnische gegevens
- Gegevens over het seksuele leven
- Politieke opvattingen
- Lidmaatschap van een vakvereniging
- Filosofische of religieuze overtuiging

D. Categorie van gegevens = welke

> Casus medisch/farmaceutisch dossier:

- **Persoonsgegevens**: identificatiegegevens, rijksregisternummer, fysieke kenmerken, mantelzorger,…
- **Gevoelige gegevens**: gezondheid (lichamelijk en psychisch), seksuele leven, afkomst, risicogedragingen,…

Inhoud

A. Contactgegevens verwerkingsverantwoordelijke
   - *Verwerkingsverantwoordelijke: persoon of organisatie die het doel en de middelen voor de verwerking vaststelt*

B. Verwerkingsdoeleinden: **waarom** wordt de informatie verwerkt?

C. **Van wie** wordt informatie verwerkt?

D. **Welke persoonsgegevens** worden verwerkt/bijgehouden/…?

E. **Wettelijke basis en rechtsgronden** voor de verwerking van de gegevens

F. **Bewaartermijnen** van gegevens: hoe lang mag je de gegevens bijhouden?

G. **Met wie** worden de gegevens **gedeeld**?

H. **Beschermingsmaatregelen** (technisch en organisatorisch): wat doe je om de gegevens te beschermen?

E. Grond voor verwerking = rechtvaardiging

- Er moet kunnen aangetoond worden dat je de gegevens verwerkt omwille van gegronde, wettelijke redenen
- = rechtmatige verwerking van persoonsgegevens
- Zeker voor gevoelige gegevens is de wettelijke basis belangrijk, omdat die in principe niet verwerkt mogen worden
- In de GDPR/AVG staan enkele specifieke bepalingen rond wie dit wel kan en mag, voor zowel persoonsgegevens als gevoelige gegevens

E. Wettelijke grondslagen

Persoonsgegevens

- Toestemming
- Uitvoering overeenkomst
- Wettelijke verplichting
- Bescherming vitale belangen
- Algemeen belang of uitoefening openbaar gezag
- Gerechtvaardigde belangen

Gevoelige gegevens

- Toestemming
- Arbeidsrecht of sociale zekerheids- en sociale beschermingsrecht
- Bescherming vitale belangen
- Vereniging actief op politiek, levensbeschouwelijk, godsdienstig of vakbondsgebied
- Openbaar gemaakt door betrokkene
- Rechtsvordering
- Zwaarwegend algemeen belang
- Gezondheidszorg
- Algemeen belang volksgezondheid
- Archivering algemeen belang

E. Grond voor verwerking = rechtvaardiging

> Casus medisch/farmaceutisch dossier:

- **Persoonsgegevens** (identificatie, gezinssamenstelling, gewoontes, beroep,…)
  - ✓ Wettelijke verplichting
  - ✓ Gerechtvaardigd belang (vb. vastleggen van afspraken door secretariaat of online agenda)

- **Gevoelige gegevens** (gezondheidsgegevens, indien relevant: gegevens betreffende afkomst of seksuele leven)
  - ✓ Preventieve of arbeidsgeneeskunde
  - ✓ Gezondheidszorg
  - ✓ Door of onder verantwoordelijkheid van beroepsbeoefenaars gebonden aan het beroepsgeheim

Inhoud

A. Contactgegevens verwerkingsverantwoordelijke
   - *Verwerkingsverantwoordelijke: persoon of organisatie die het doel en de middelen voor de verwerking vaststelt*

B. Verwerkingsdoeleinden: **waarom** wordt de informatie verwerkt?

C. **Van wie** wordt informatie verwerkt?

D. **Welke persoonsgegevens** worden verwerkt/bijgehouden/…?

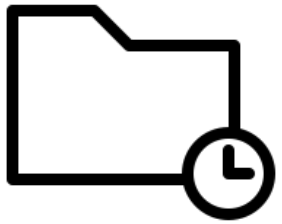
E. **Wettelijke basis en rechtsgronden** voor de verwerking van de gegevens

F. **Bewaartermijnen** van gegevens: hoe lang mag je de gegevens bijhouden?

G. **Met wie** worden de gegevens **gedeeld**?

H. **Beschermingsmaatregelen** (technisch en organisatorisch): wat doe je om de gegevens te beschermen?

F. Bewaartermijn = hoe lang



- Farmaceutisch dossier:
  - Min 10 max 30 jaar

- Medisch dossier:
  - 30 jaar (ook medische informatie op wachtpost)

Inhoud

A. Contactgegevens verwerkingsverantwoordelijke
   - *Verwerkingsverantwoordelijke: persoon of organisatie die het doel en de middelen voor de verwerking vaststelt*

B. Verwerkingsdoeleinden: **waarom** wordt de informatie verwerkt?

C. **Van wie** wordt informatie verwerkt?

D. **Welke persoonsgegevens** worden verwerkt/bijgehouden/…?

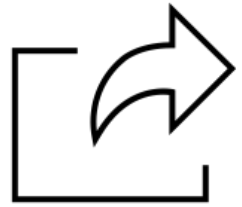
E. **Wettelijke basis en rechtsgronden** voor de verwerking van de gegevens

F. **Bewaartermijnen** van gegevens: hoe lang mag je de gegevens bijhouden?

G. **Met wie** worden de gegevens **gedeeld**?

H. **Beschermingsmaatregelen** (technisch en organisatorisch): wat doe je om de gegevens te beschermen?

G. Ontvanger/doorgifte = delen met



- Individu/patiënt

- Binnen de organisatie: zorgverleners of medewerkers (gebonden aan beroepsgeheim of geheimhoudingsplicht)

- Buiten de organisatie
  - Zorgverleners, medewerkers of organisaties gebonden aan beroepsgeheim
  - Privé-ondernemingen (vb verzekeringsmaatschappij ikv werkongeval)

Inhoud

A. Contactgegevens verwerkingsverantwoordelijke
   - *Verwerkingsverantwoordelijke: persoon of organisatie die het doel en de middelen voor de verwerking vaststelt*

B. Verwerkingsdoeleinden: **waarom** wordt de informatie verwerkt?

C. **Van wie** wordt informatie verwerkt?

D. **Welke persoonsgegevens** worden verwerkt/bijgehouden/…?

E. **Wettelijke basis en rechtsgronden** voor de verwerking van de gegevens

F. **Bewaartermijnen** van gegevens: hoe lang mag je de gegevens bijhouden?

G. **Met wie** worden de gegevens **gedeeld**?

H. **Beschermingsmaatregelen** (technisch en organisatorisch): wat doe je om de gegevens te beschermen?

H. Genomen maatregelen obv risico's

> Oplijsten of er op papier of elektronisch gewerkt wordt

> Maatregelen beschrijven om risico's te beperken:
  - Organisatorisch: papieren informatie in afgesloten ruimte, sleutelbeheer,…
  - Technisch: gebruik eHealthbox, instellen veilig paswoord,…

H. Genomen maatregelen obv risico's

> Patiëntenzorg en beheer medisch dossier
  - Voorbeeld: medisch dossier is elektronisch
    - ✓ Inloggen in dossier met eID
    - ✓ Paswoord op PC
    - ✓ Gebruik eHealth-diensten (dubbele encryptie)
    - ✓ Differentiële toegang dossiers arts/medewerkers
    - ✓ EMD afsluiten na consultatie
    - ✓ …

> (Lokaal elektronisch) Farmaceutisch dossier
    - ✓ Paswoord voor toegang PC
    - ✓ Gebruik eHealth-diensten
    - ✓ Scherm afsluiten/locken
    - ✓ …


ON YOUR MARK
GET READY
ANY TIME NOW
REALLY SOON...
GDPR

Verwerkingsregister domus

Template

domus medica

Verwerkingsregister

Verantwoordelijke voor de gegevensverwerking: _____

Verwerkende dienst: _____

Contactinformatie Verwerkingsverantwoordelijke

Adres _____

_____

Telefoonnummer _____

Ondernemingsnummer _____

Contactinformatie Functionaris Gegevensbescherming

Naam _____

Adres _____

_____

Telefoonnummer _____

Verwerkingsregister

Doel van de verwerking:	Patiëntenzorg	Dit omvat alle aspecten van patiëntenzorg: diagnose, preventie, remediëring,...
Bronnen:		
Binnen de organisatie	Alle patiëntinformatie bevindt zich in het patiëntendossier of wordt bij het dossier gevoegd	
Buiten de organisatie	Informatie aangeleverd door andere zorgverleners of instellingen wordt mee in het dossier opgenomen of via het dossier geraadpleegd	
Over wie wordt informatie bijgehouden?	De patiënt	
Welke gegevens worden bijgehouden?	Persoonsgegevens	Gevoelige gegevens
	Identificatiegegevens	Gegevens betreffende de lichamelijke gezondheid
	Samenstelling van het gezin	Gegevens betreffende de psychische gezondheid
	Rijksregisternummer	Gegevens betreffende risicosituaties en risicogedragingen
	Persoonlijke kenmerken	Genetische gegevens in het kader van bevolkingsonderzoek, erfelijkheidsonderzoek,...
	Leefgewoonten	Gegevens met betrekking tot de remediëring
	Fysieke gegevens	Gegevens over het seksuele leven
	Beeldopnamen	
Welke rechtsgrond?	Wettelijke verplichting	Preventieve of arbeidsgeneeskunde, gezondheidszorg
	Gerechtvaardigd belang	

Verduidelijk (welke wet, contract,...)	AVG artikel 6, 1.c en 1.f	AVG artikel 9, 2.h
		AVG artikel 9, 3
Met wie wordt de informatie gedeeld?		
Binnen onze organisatie	Zorgverleners en medewerkers gebonden aan beroepsgeheim	Zorgverleners en medewerkers gebonden aan beroepsgeheim
Buiten de organisatie	Zorgverleners en medewerkers gebonden aan beroepsgeheim	Zorgverleners en medewerkers gebonden aan beroepsgeheim
Bewaartermijn gegevens	30 jaar	30 jaar

Soorten toepassingen/databanken/platformen voor de verwerking van gegevens en risicoanalyse

Verwerking op papier	Verwerkingsvorm	Risico:	Kans op datalek	Beheersbaarheid/maatregelen
Medisch dossier	registreren, raadplegen	Inzage niet-gekwalificeerde personen	beperkt	**Organisatorisch:** * dossiers worden achter slot bewaard * arts heeft sleutel + veilige bewaring * kopie sleutel niet vrij toegankelijk voor personeel
Verwijsbrieven	verzenden, ontvangen	Inzage niet-gekwalificeerde personen	beperkt	**Organisatorisch:** * ontvangen brieven achter slot bewaard * brieven die verstuurd worden meteen in gesloten envelop * arts heeft sleutel + veilige bewaring * kopie sleutel niet vrij toegankelijk voor personeel of derden
Communicatie met patiënt	verzenden ,ontvangen	Inzage niet-gekwalificeerde personen	beperkt	**Organisatorisch:** * brieven die verstuurd worden meteen in gesloten envelop
Testresultaten	verzenden, ontvangen	Inzage niet-gekwalificeerde personen	beperkt	**Organisatorisch:** * ontvangen brieven achter slot bewaard * brieven die verstuurd worden meteen in gesloten envelop * arts heeft sleutel + veilige bewaring * kopie sleutel niet vrij toegankelijk voor personeel of derden

Elektronische verwerking				
Medisch dossier	registreren, raadplegen	Inzage niet-gekwalificeerde personen	beperkt	**Organisatorisch:** * differentiële toegang tot dossier voor arts en medewerkers praktijk * schermbeveiliging opzetten * EMD afsluiten aan einde consultatie **Technisch:** * paswoord op computer/tablet en aparte toegang tot medisch dossier * wijziging paswoord om de x maanden * ingebouwde complexiteit paswoord * toegang tot dossier met door eHealthplatform erkende authenticatieprocedure
Verwijsbrieven	verzenden, ontvangen	Inzage niet-gekwalificeerde personen	beperkt	**Technisch:** * verzending via eHealthbox - dubbele encryptie en door eHealthplatform erkende authenticatieprocedure
Communicatie met patiënt	verzenden, ontvangen	Inzage niet-gekwalificeerde personen	beperkt	**Technisch:** * verzending via eBox
Testresultaten	verzenden, ontvangen	Inzage niet-gekwalificeerde personen	beperkt	**Technisch:** * verzending via eHealthbox - dubbele encryptie en door eHealthplatform erkende authenticatieprocedure * raadpleging via Hub - dubbele encryptie en door eHealthplatform erkende authenticatieprocedure
Raadpleging van patiëntengegevens via externe bronnen	raadplegen, registreren	Inzage niet-gekwalificeerde personen	beperkt	**Technisch:** * raadpleging via dossier: dubbele encryptie en door eHealthplatform erkende authenticatieprocedure * raadpleging via Hub - dubbele encryptie en door eHealthplatform erkende authenticatieprocedure * raadpleging via kluis - dubbele encryptie en door eHealthplatform erkende authenticatieprocedure

ALGEMENE VERORDENING GEGEVENSBESCHERMING

BEREID JE VOOR IN 13 STAPPEN

1. BEWUSTMAKING

Informeer sleutelfiguren en beleidsmakers over de aankomende veranderingen. Zij moeten inschatten welke gevolgen de AVG zal teweegbrengen voor het bedrijf of de organisatie.

2. DATAREGISTER

Breng in kaart welke persoonsgegevens je bijhoudt, waar deze vandaan komen en met wie je deze hebt gedeeld. Registreer je verwerkingen. Mogelijks dien je hiervoor een informatie-audit te organiseren.

3. COMMUNICATIE

Evalueer je bestaande privacyverklaring en plan noodzakelijke wijzigingen hieraan in het licht van de AVG.

4. RECHTEN VAN DE BETROKKENE

Ga na of de huidige procedures in je bedrijf of organisatie alle rechten voorzien waarop de betrokkene zich kan beroepen, inclusief hoe persoonsgegevens kunnen worden verwijderd of hoe gegevens elektronisch zullen worden meegedeeld.

5. VERZOEK TOT TOEGANG

Update je bestaande toegangsprocedures en bedenk hoe je verzoeken tot toegang voortaan zal behandelen onder de nieuwe termijnen in de AVG.

6. WETTELIJKE GRONDSLAG VOOR HET VERWERKEN VAN PERSOONSGEGEVENS

Documenteer de verscheidene types van gegevensverwerkingen die je uitvoert en identificeer de wettelijke grondslag voor elk van hen.

7. TOESTEMMING

Evalueer de wijze waarop je toestemming vraagt, verkrijgt en registreert, en wijzig waar nodig.

8. KINDEREN

Ontwikkel systemen die de leeftijd van de betrokkene nagaan en die de ouder(s) of voogd(en) om toestemming vragen voor de gegevensverwerking van minderjarige kinderen.

9. DATALEKKEN

Voorzie adequate procedures om persoonlijke datalekken op te sporen, te rapporteren en te onderzoeken.

10. GEGEVENSBESCHERMING DOOR ONTWERP EN GEGEVENSBESCHERMINGSEFFECTBEOORDELING

Maak je vertrouwd met de begrippen "gegevensbescherming door ontwerp" en "gegevensbeschermingseffectbeoordeling" en ga na hoe je deze concepten in de werking van jouw bedrijf of organisatie kan implementeren.

11. FUNCTIONARIS VOOR GEGEVENSBESCHERMING

Duid, indien nodig, een functionaris voor gegevensbescherming aan, of iemand die de verantwoordelijkheid draagt voor het naleven van de databeschermingsregels. Beoordeel welke plaats deze inneemt binnen de structuur en het beleid van jouw bedrijf of organisatie.

12. INTERNATIONAAL

Bepaal onder welke toezichthoudende autoriteit je valt indien jouw bedrijf of organisatie internationaal actief is.

13. BESTAANDE CONTRACTEN

Beoordeel je bestaande contracten, hoofdzakelijk met verwerkers en onderaannemers, en breng tijdig de noodzakelijke veranderingen aan.

GDPR in uw praktijk

2. GEGEVENSLEKKEN

Gegevenslekken: wat?

- **Verlies, vernietiging, wijziging of ongeoorloofde toegang** tot persoonsgegevens
- Bewust en onrechtmatig of per ongeluk
- Het betreft **alle persoonsgegevens** die worden verwerkt binnen de organisatie:
  - patiënten
  - medewerkers
  - maar ook van zorgverleners of instanties waarmee wordt samengewerkt

Gegevenslekken: hoe hiermee omgaan?

> In eerste instantie: vermijden!

> Hoe:

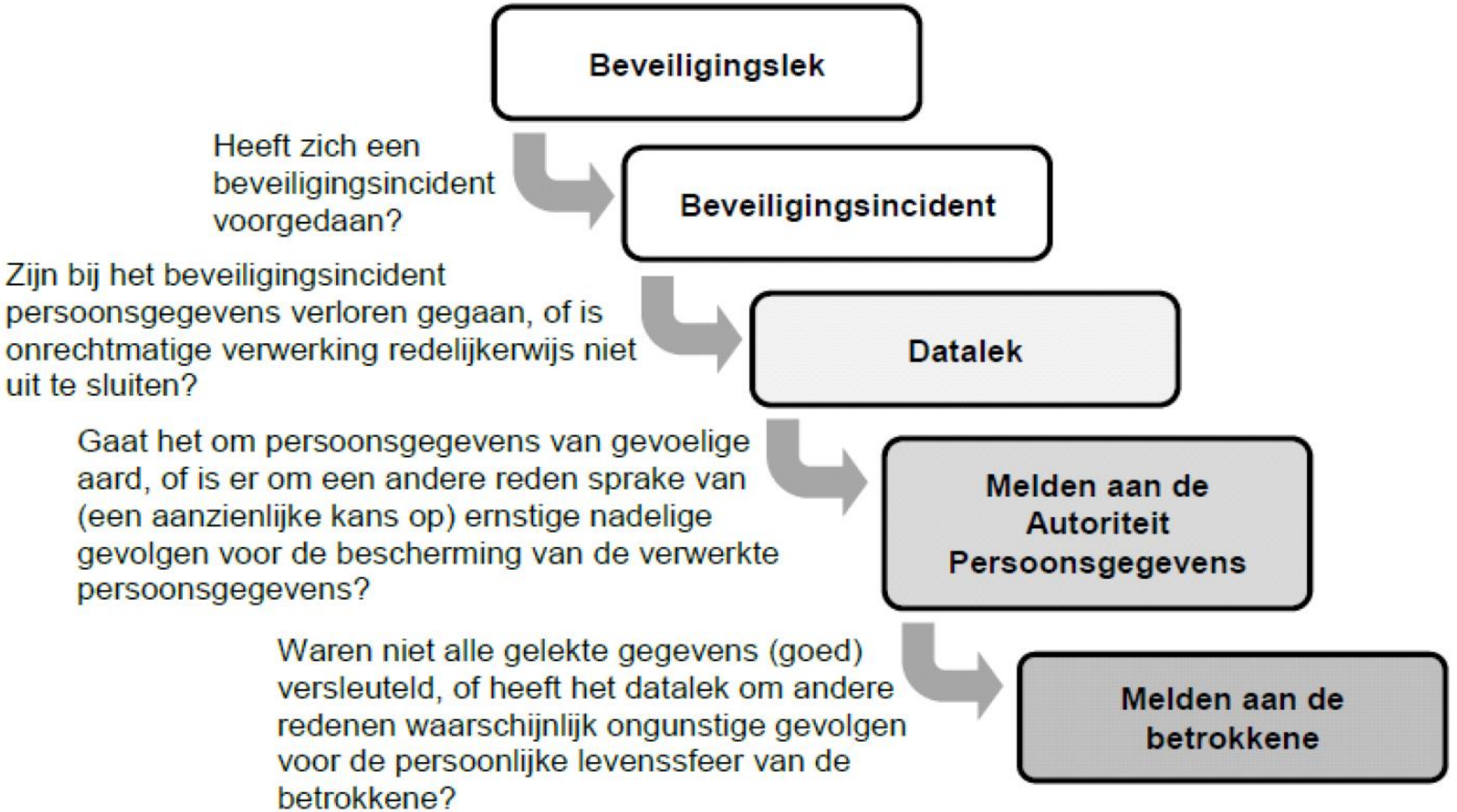
- Bewustmaking
- Verwerkingsregister
- Risicoanalyse
- Het nemen van voldoende beschermende maatregelen
- Procedures
- Afspraken en contracten met verwerkers

Gegevenslekken: hoe hiermee omgaan?

- Toch een lek?
  - Melding aan de Privacycommissie: indien risico op nadelige gevolgen voor betrokkene, en zeker in het geval van gevoelige gegevens
  - Melding aan de betrokkene: enkel indien ernstig risico

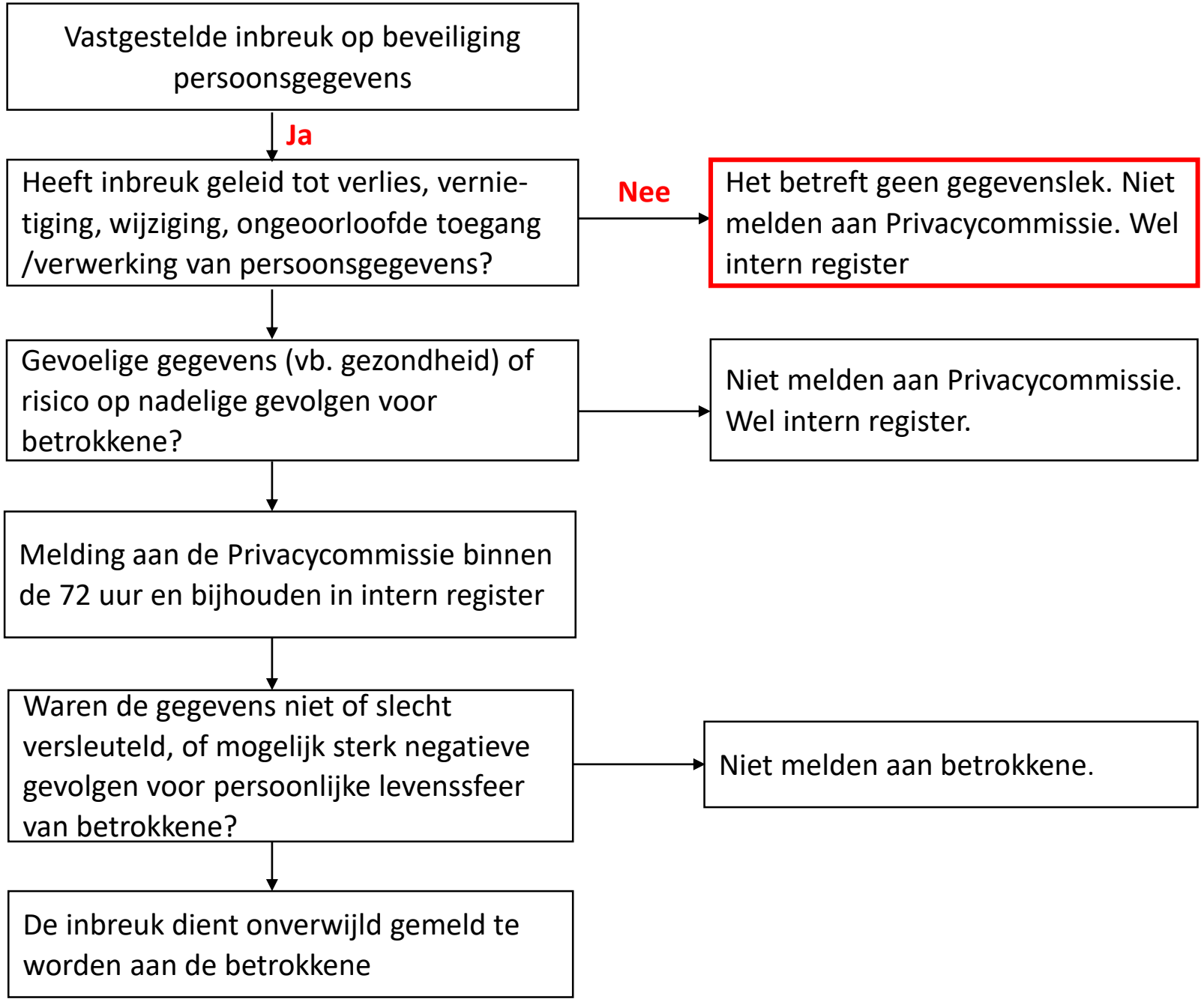
- Hou binnen je organisatie een register bij van datalekken:
  - Welke en wanneer
  - Oplossing en maatregelen

Beslisboom datalekken



Gegevenslekken: voorbeeld

Brief met patiëntengegevens wordt naar het verkeerde adres gestuurd. De brief wordt ongeopend teruggestuurd.

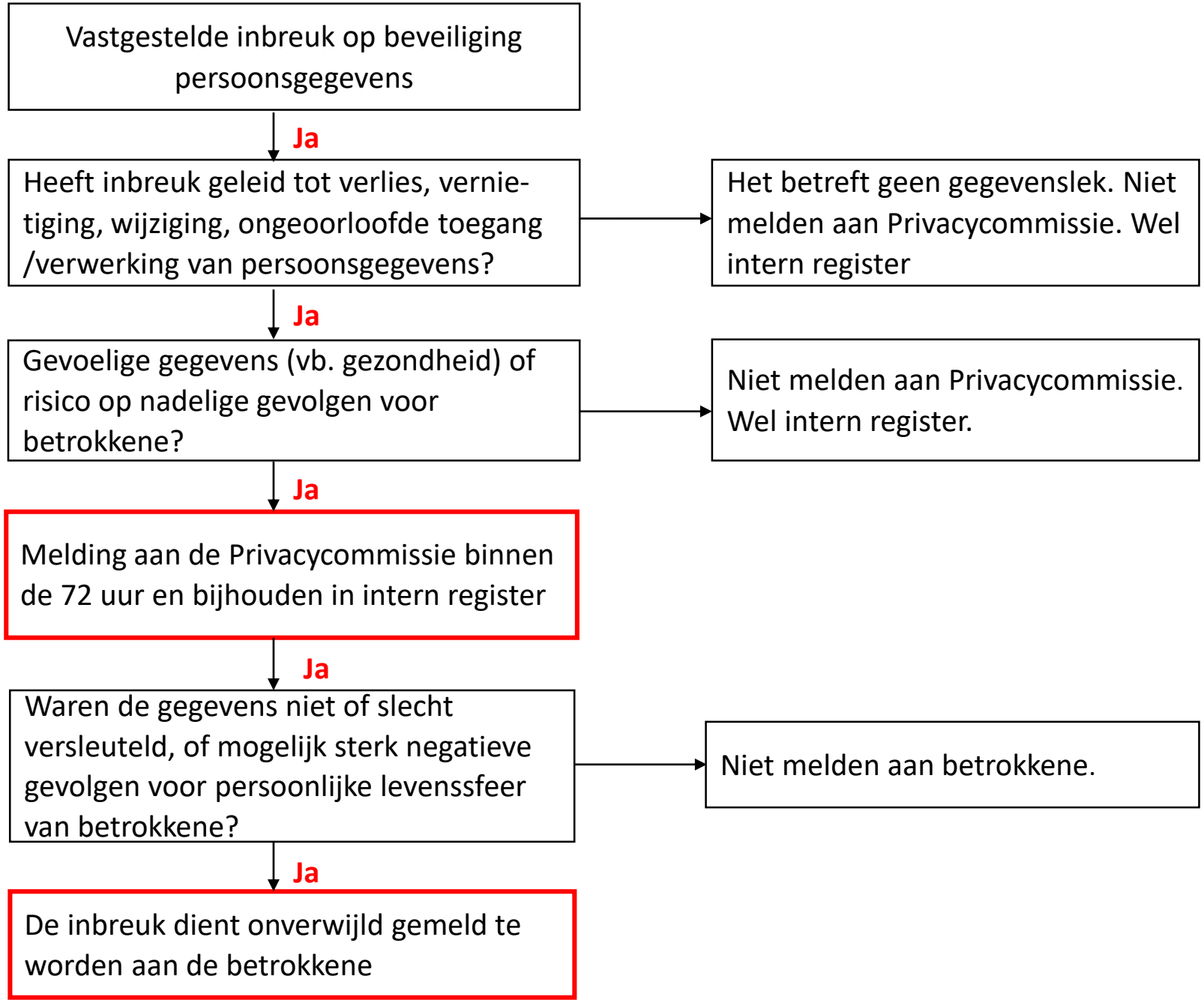


Voorbeeld: Brief met patiëntengegevens wordt naar het verkeerde adres gestuurd. De brief wordt ongeopend teruggestuurd.

Gegevenslekken: voorbeeld

Fout bij een handeling in het softwarepakket.

Zorgverlener neemt print screen van het dossier en stuurt dit door naar de helpdesk via mail. De print screen bevat patiënt- en gezondheidsgegevens.



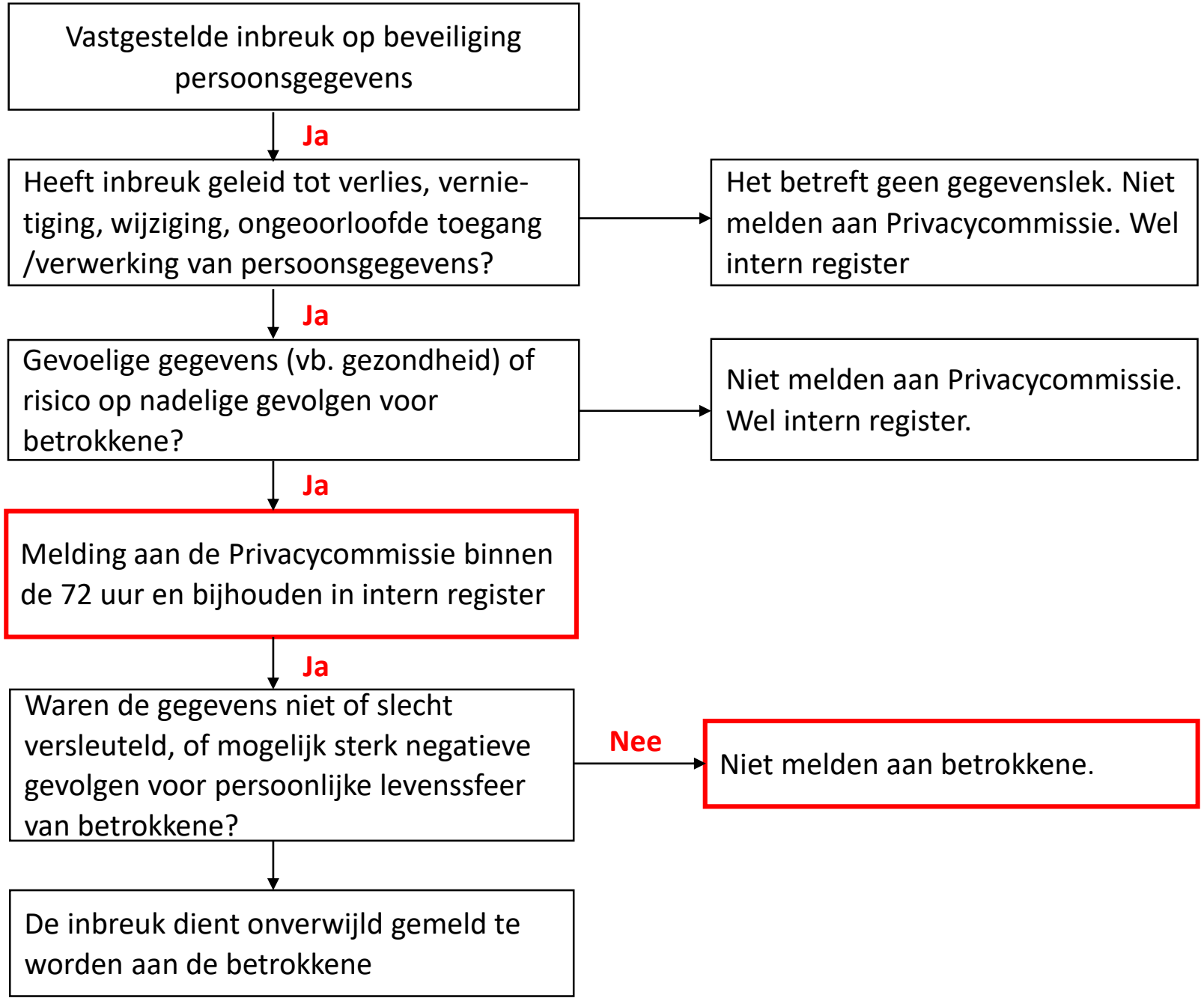
Voorbeeld: Fout bij een handeling in het softwarepakket. Zorgverlener neemt print screen van het dossier en stuurt dit via mail door naar de helpdesk. De print screen bevat patiënt- en gezondheidsgegevens.

Gegevenslekken: voorbeeld

Laptop van arts of USB-stick met back-up van apotheekdata wordt gestolen.

Toegang tot de laptop of USB is beveiligd.

Toegang tot de medische dossiers kan enkel via eID.



Voorbeeld: Laptop van arts of USB-stick met backup van apotheekdata wordt gestolen. Toegang tot de laptop of USB is beveiligd, en toegang tot de medische dossiers kan enkel via eID.

Gegevenslekken: voorbeeld

Ziekenhuis stuurt ontslagbrief van een patiënt naar de verkeerde huisarts.

De mutualiteit stuurt een document met patiëntgegevens in verband met een facturatie naar de verkeerde apotheek.

Voorbeeld: Ziekenhuis stuurt ontslagbrief van een patiënt naar de verkeerde huisarts.
De mutualiteit stuurt een document met patiëntgegevens ivm een facturatie naar de verkeerde apotheek.

!!! Actie zorgverlener die foutieve brief ontvangt: verzender (verwerkingsverantwoordelijke) informeren. Daar stopt de actie voor de zorgverlener.
Verdere acties door verwerkingsverantwoordelijke.

Gegevenslekken: voorbeeld

Een wachtverslag wordt per mail naar de GMD-houdende huisarts gestuurd. Of de apotheker stuurt per mail een voorschrift door naar een andere partij (RVT, TD, arts, …)

Voorbeeld: Een wachtverslag wordt per mail naar de GMD-houdende huisarts gestuurd. Of de apotheker stuurt per mail een voorschrift door naar een andere partij (RVT, TD, arts,…)

*Na onderzoek als niet uitgesloten kan worden dat persoonsgegevens onrechtmatig zijn verwerkt

To leak or…

- Verdere informatie vanwege de Privacycommissie noodzakelijk

- Nog verduidelijking en bijsturing nodig en mogelijk
  - *? niet verplicht is om te melden ‘Als de verwerkingsverantwoordelijke achteraf maatregelen heeft genomen om ervoor te zorgen dat het hoge risico voor de rechten en vrijheden van betrokkenen zich waarschijnlijk niet meer zal voordoen’*

- Meldpunt?

ALGEMENE VERORDENING GEGEVENSBESCHERMING

BEREID JE VOOR IN 13 STAPPEN

1. BEWUSTMAKING

Informeer sleutelfiguren en beleidsmakers over de aankomende veranderingen. Zij moeten inschatten welke gevolgen de AVG zal teweegbrengen voor het bedrijf of de organisatie.

2. DATAREGISTER

Breng in kaart welke persoonsgegevens je bijhoudt, waar deze vandaan komen en met wie je deze hebt gedeeld. Registreer je verwerkingen. Mogelijks dien je hiervoor een informatie-audit te organiseren.

3. COMMUNICATIE

Evalueer je bestaande privacyverklaring en plan noodzakelijke wijzigingen hieraan in het licht van de AVG.

4. RECHTEN VAN DE BETROKKENE

Ga na of de huidige procedures in je bedrijf of organisatie alle rechten voorzien waarop de betrokkene zich kan beroepen, inclusief hoe persoonsgegevens kunnen worden verwijderd of hoe gegevens elektronisch zullen worden meegedeeld.

5. VERZOEK TOT TOEGANG

Update je bestaande toegangsprocedures en bedenk hoe je verzoeken tot toegang voortaan zal behandelen onder de nieuwe termijnen in de AVG.

6. WETTELIJKE GRONDSLAG VOOR HET VERWERKEN VAN PERSOONSGEGEVENS

Documenteer de verscheidene types van gegevensverwerkingen die je uitvoert en identificeer de wettelijke grondslag voor elk van hen.

7. TOESTEMMING

Evalueer de wijze waarop je toestemming vraagt, verkrijgt en registreert, en wijzig waar nodig.

8. KINDEREN

Ontwikkel systemen die de leeftijd van de betrokkene nagaan en die de ouder(s) of voogd(en) om toestemming vragen voor de gegevensverwerking van minderjarige kinderen.

9. DATALEKKEN

Voorzie adequate procedures om persoonlijke datalekken op te sporen, te rapporteren en te onderzoeken.

10. GEGEVENSBESCHERMING DOOR ONTWERP EN GEGEVENSBESCHERMINGSEFFECTBEOORDELING

Maak je vertrouwd met de begrippen "gegevensbescherming door ontwerp" en "gegevensbeschermingseffectbeoordeling" en ga na hoe je deze concepten in de werking van jouw bedrijf of organisatie kan implementeren.

11. FUNCTIONARIS VOOR GEGEVENSBESCHERMING

Duid, indien nodig, een functionaris voor gegevensbescherming aan, of iemand die de verantwoordelijkheid draagt voor het naleven van de databeschermingsregels. Beoordeel welke plaats deze inneemt binnen de structuur en het beleid van jouw bedrijf of organisatie.

12. INTERNATIONAAL

Bepaal onder welke toezichthoudende autoriteit je valt indien jouw bedrijf of organisatie internationaal actief is.

13. BESTAANDE CONTRACTEN

Beoordeel je bestaande contracten, hoofdzakelijk met verwerkers en onderaannemers, en breng tijdig de noodzakelijke veranderingen aan.

GDPR in uw praktijk

3. BIJKOMENDE ACTIES & AANDACHTSPUNTEN

Privacyverklaring

> Informeren van betrokkenen
> Een privacyverklaring maakt duidelijk hoe er op een verantwoorde wijze met persoonsgegevens van patiënten wordt omgegaan
> In de praktijkruimte of op de website

Template volgt

Privacyverklaring

Algemeen

De AVG is de nieuwe wet ter bescherming van privacy en persoonsgegevens. Op grond van deze wet heeft een organisatie die met persoonsgegevens werkt bepaalde plichten en heeft degene van wie de gegevens zijn bepaalde rechten. Naast deze algemene wet gelden specifieke regels voor de privacy in de gezondheidszorg. Deze regels staan onder andere vermeld in de Wet geneeskundige behandelingsovereenkomst (WGBO). Dit privacyreglement is bedoeld om u te informeren over uw rechten en onze plichten die gelden op grond van de AVG en de WGBO.

Huisartsenpraktijk

In onze huisartsenpraktijk kunnen diverse persoonsgegevens van u verwerkt worden. Dit is noodzakelijk om u medisch goed te kunnen behandelen en nodig voor het financieel afhandelen van de behandeling. Daarnaast kan verwerking noodzakelijk zijn voor, bijvoorbeeld, de bestrijding van ernstig gevaar voor uw gezondheid of ter voldoening aan een wettelijke verplichting (bijvoorbeeld het verplicht melden van een besmettelijke ziekte op grond van de Wet Publieke Gezondheid).

De plichten van de huisartsenpraktijk

Huisartsenpraktijk Verijdt is volgens de AVG de verantwoordelijke voor de verwerking van persoonsgegevens die in de praktijk plaatsvindt. Aan de plichten die daaruit voortkomen, voldoet de praktijk als volgt:

• Uw gegevens worden voor specifieke doeleinden verzameld:
o voor zorgverlening;
o voor doelmatig beheer en beleid;
o voor ondersteuning van wetenschappelijk onderzoek, onderwijs en voorlichting.
• Er vindt in beginsel geen verwerking plaats voor andere doeleinden.
• U wordt op de hoogte gesteld van het feit dat er persoonsgegevens van u verwerkt worden. Dit kan gebeuren door uw zorgverlener, maar ook via een folder of via onze website.

Privacyverklaring

Menu

- Zo werkt het
- Belangrijke gegevens
- Informatie voor de arts
- Privacyverklaring
- Algemene Voorwaarden
- Prijslijst

Privacyverklaring nationale-apotheek.nl

Voor ons is een zorgvuldige omgang met uw persoonsgegevens van groot belang. Uw persoonlijke gegevens worden zorgvuldig verwerkt en beveiligd. Hierbij houden wij ons aan de eisen die de Wet Bescherming Persoonsgegevens en andere toepasselijke wet- en regelgeving stellen. De Nationale Apotheek B.V. is de verantwoordelijke voor de gegevensverwerking. De Nationale Apotheek B.V. is aangemeld bij het College Bescherming Persoonsgegevens onder meldingsnummer 1409189. In deze privacyverklaring leggen wij uit welke persoonsgegevens wij verzamelen en gebruiken en met welk doel.

Deze privacyverklaring is voor het laatst aangepast op 9 oktober 2010.

Vastleggen en verwerking van gegevens

Wij bewaren en gebruiken uitsluitend die persoonsgegevens die rechtstreeks door u worden opgegeven of waarvan bij opgave duidelijk is dat ze aan ons worden verstrekt. Gegevens die niet langer nodig zijn worden verwijderd. U kunt ook zelf vragen om inzage, wijziging of verwijdering van gegevens. Zie hiervoor de contactgegevens onderaan.

Als klant van nationale-apotheek.nl wordt u gevraagd om medische informatie aan ons te verstrekken, voor zover deze noodzakelijk is voor nationale-apotheek.nl om de gevraagde dienstverlening aan u op een medisch- en farmaceutisch verantwoorde manier uit te voeren. Alleen die medewerkers, die de gegevens noodzakelijkerwijs moeten inzien in het kader van de uitoefening van hun functie, hebben toegang tot deze gegevens. De medewerkers van De Nationale Apotheek B.V. hebben allen geheimhoudingsplicht om uw privacy te waarborgen.

Door gebruik te maken van onze diensten geeft u automatisch toestemming aan de medewerkers van De Nationale Apotheek B.V. om de gegevens in te zien.

Indien uw behandelend arts daarom verzoekt, kan hij inzage krijgen in de voorgeschreven recepten. Dit is wettelijk geregeld.

Registratiesysteem

Bij bepaalde onderdelen van deze website moet u zich eerst inschrijven. Na het inschrijven bewaren wij via de door u gekozen inlognaam (het e-mailadres) de door u opgegeven persoonsgegevens, zoals naam, adres, woonplaats, geboortedatum, e-mailadres en de gegevens van eerder door u gedane bestellingen. Wij bewaren deze gegevens zodat u deze niet elke keer opnieuw hoeft in te vullen, zodat wij u kunnen contacteren in het kader van uitvoering van de bestelling en betaling.

Wij zullen de aan uw inlognaam gekoppelde gegevens in beginsel niet aan derden verstrekken, tenzij dat noodzakelijk is in het kader van een overeenkomst die u met ons sluit, u daarvoor toestemming heeft gegeven, of wanneer dit wettelijk verplicht is. In geval van een vermoeden van fraude of misbruik van onze website kunnen wij persoonsgegevens aan de bevoegde autoriteiten overhandigen.

Inlognaam en wachtwoord

Uw inlognaam is gekoppeld aan een wachtwoord. U bent zelf verantwoordelijk voor het zorgvuldig omgaan met het

ALGEMENE VERORDENING GEGEVENSBESCHERMING

BEREID JE VOOR IN 13 STAPPEN

1. BEWUSTMAKING

Informeer sleutelfiguren en beleidsmakers over de aankomende veranderingen. Zij moeten inschatten welke gevolgen de AVG zal teweegbrengen voor het bedrijf of de organisatie.

2. DATAREGISTER

Breng in kaart welke persoonsgegevens je bijhoudt, waar deze vandaan komen en met wie je deze hebt gedeeld. Registreer je verwerkingen. Mogelijks dien je hiervoor een informatie-audit te organiseren.

3. COMMUNICATIE

Evalueer je bestaande privacyverklaring en plan noodzakelijke wijzigingen hieraan in het licht van de AVG.

4. RECHTEN VAN DE BETROKKENE

Ga na of de huidige procedures in je bedrijf of organisatie alle rechten voorzien waarop de betrokkene zich kan beroepen, inclusief hoe persoonsgegevens kunnen worden verwijderd of hoe gegevens elektronisch zullen worden meegedeeld.

5. VERZOEK TOT TOEGANG

Update je bestaande toegangsprocedures en bedenk hoe je verzoeken tot toegang voortaan zal behandelen onder de nieuwe termijnen in de AVG.

6. WETTELIJKE GRONDSLAG VOOR HET VERWERKEN VAN PERSOONSGEGEVENS

Documenteer de verscheidene types van gegevensverwerkingen die je uitvoert en identificeer de wettelijke grondslag voor elk van hen.

7. TOESTEMMING

Evalueer de wijze waarop je toestemming vraagt, verkrijgt en registreert, en wijzig waar nodig.

8. KINDEREN

Ontwikkel systemen die de leeftijd van de betrokkene nagaan en die de ouder(s) of voogd(en) om toestemming vragen voor de gegevensverwerking van minderjarige kinderen.

9. DATALEKKEN

Voorzie adequate procedures om persoonlijke datalekken op te sporen, te rapporteren en te onderzoeken.

10. GEGEVENSBESCHERMING DOOR ONTWERP EN GEGEVENSBESCHERMINGSEFFECTBEOORDELING

Maak je vertrouwd met de begrippen "gegevensbescherming door ontwerp" en "gegevensbeschermingseffectbeoordeling" en ga na hoe je deze concepten in de werking van jouw bedrijf of organisatie kan implementeren.

11. FUNCTIONARIS VOOR GEGEVENSBESCHERMING

Duid, indien nodig, een functionaris voor gegevensbescherming aan, of iemand die de verantwoordelijkheid draagt voor het naleven van de databeschermingsregels. Beoordeel welke plaats deze inneemt binnen de structuur en het beleid van jouw bedrijf of organisatie.

12. INTERNATIONAAL

Bepaal onder welke toezichthoudende autoriteit je valt indien jouw bedrijf of organisatie internationaal actief is.

13. BESTAANDE CONTRACTEN

Beoordeel je bestaande contracten, hoofdzakelijk met verwerkers en onderaannemers, en breng tijdig de noodzakelijke veranderingen aan.

Functionaris gegevensbescherming of DPO

- Kennis wetgeving en deskundigheid op het vlak van gegevensbescherming
- Adviserende en opleidende rol
- Verplichting als o.a. grootschalige verwerking gevoelige gegevens
  - *In principe niet voor individuele zorgverleners*
  - *Na te gaan in welke mate 'grootschalig' van toepassing is op groepspraktijk, wijkgezondheidscentrum of wachtpost, (grote/groepen van) apotheken*

- Aanpak:
  - Indien verplicht: organisatie op overkoepelend niveau
  - Sowieso aan te raden bij twijfel of concrete vragen

ALGEMENE VERORDENING GEGEVENSBESCHERMING

BEREID JE VOOR IN 13 STAPPEN

1. BEWUSTMAKING

Informeer sleutelfiguren en beleidsmakers over de aankomende veranderingen. Zij moeten inschatten welke gevolgen de AVG zal teweegbrengen voor het bedrijf of de organisatie.

2. DATAREGISTER

Breng in kaart welke persoonsgegevens je bijhoudt, waar deze vandaan komen en met wie je deze hebt gedeeld. Registreer je verwerkingen. Mogelijks dien je hiervoor een informatie-audit te organiseren.

3. COMMUNICATIE

Evalueer je bestaande privacyverklaring en plan noodzakelijke wijzigingen hieraan in het licht van de AVG.

4. RECHTEN VAN DE BETROKKENE

Ga na of de huidige procedures in je bedrijf of organisatie alle rechten voorzien waarop de betrokkene zich kan beroepen, inclusief hoe persoonsgegevens kunnen worden verwijderd of hoe gegevens elektronisch zullen worden meegedeeld.

5. VERZOEK TOT TOEGANG

Update je bestaande toegangsprocedures en bedenk hoe je verzoeken tot toegang voortaan zal behandelen onder de nieuwe termijnen in de AVG.

6. WETTELIJKE GRONDSLAG VOOR HET VERWERKEN VAN PERSOONSGEGEVENS

Documenteer de verscheidene types van gegevensverwerkingen die je uitvoert en identificeer de wettelijke grondslag voor elk van hen.

7. TOESTEMMING

Evalueer de wijze waarop je toestemming vraagt, verkrijgt en registreert, en wijzig waar nodig.

8. KINDEREN

Ontwikkel systemen die de leeftijd van de betrokkene nagaan en die de ouder(s) of voogd(en) om toestemming vragen voor de gegevensverwerking van minderjarige kinderen.

9. DATALEKKEN

Voorzie adequate procedures om persoonlijke datalekken op te sporen, te rapporteren en te onderzoeken.

10. GEGEVENSBESCHERMING DOOR ONTWERP EN GEGEVENSBESCHERMINGSEFFECTBEOORDELING

Maak je vertrouwd met de begrippen "gegevensbescherming door ontwerp" en "gegevensbeschermingseffectbeoordeling" en ga na hoe je deze concepten in de werking van jouw bedrijf of organisatie kan implementeren.

11. FUNCTIONARIS VOOR GEGEVENSBESCHERMING

Duid, indien nodig, een functionaris voor gegevensbescherming aan, of iemand die de verantwoordelijkheid draagt voor het naleven van de databeschermingsregels. Beoordeel welke plaats deze inneemt binnen de structuur en het beleid van jouw bedrijf of organisatie.

12. INTERNATIONAAL

Bepaal onder welke toezichthoudende autoriteit je valt indien jouw bedrijf of organisatie internationaal actief is.

13. BESTAANDE CONTRACTEN

Beoordeel je bestaande contracten, hoofdzakelijk met verwerkers en onderaannemers, en breng tijdig de noodzakelijke veranderingen aan.

To BeContinued

Rechten patiënt

- Gelijkaardig aan huidige privacywetgeving en wet patiënten rechten
- **Recht op inzage**:
  - Doorverwijzing naar federale patiënt-portalen (als informed consent)
  - Afdruk eigen dossier → na te vragen bij softwarepakket
- **Recht op overdracht**:
  - Toegang tot eigen gegevens in gestructureerde en elektronische vorm → na te vragen bij softwarepakket

Rechten patiënt

- Data protection by design

- => ontwerp van de databank moet afgestemd zijn op de rechten van de betrokkenen
    - ✓ Informatie (metadata)
    - ✓ Inzage
    - ✓ Correctie
    - ✓ Vergetelheid
    - ✓ Dataportabiliteit

ALGEMENE VERORDENING GEGEVENSBESCHERMING

BEREID JE VOOR IN 13 STAPPEN

1. BEWUSTMAKING

Informeer sleutelfiguren en beleidsmakers over de aankomende veranderingen. Zij moeten inschatten welke gevolgen de AVG zal teweegbrengen voor het bedrijf of de organisatie.

2. DATAREGISTER

Breng in kaart welke persoonsgegevens je bijhoudt, waar deze vandaan komen en met wie je deze hebt gedeeld. Registreer je verwerkingen. Mogelijks dien je hiervoor een informatie-audit te organiseren.

3. COMMUNICATIE

Evalueer je bestaande privacyverklaring en plan noodzakelijke wijzigingen hieraan in het licht van de AVG.

4. RECHTEN VAN DE BETROKKENE

Ga na of de huidige procedures in je bedrijf of organisatie alle rechten voorzien waarop de betrokkene zich kan beroepen, inclusief hoe persoonsgegevens kunnen worden verwijderd of hoe gegevens elektronisch zullen worden meegedeeld.

5. VERZOEK TOT TOEGANG

Update je bestaande toegangsprocedures en bedenk hoe je verzoeken tot toegang voortaan zal behandelen onder de nieuwe termijnen in de AVG.

6. WETTELIJKE GRONDSLAG VOOR HET VERWERKEN VAN PERSOONSGEGEVENS

Documenteer de verscheidene types van gegevensverwerkingen die je uitvoert en identificeer de wettelijke grondslag voor elk van hen.

7. TOESTEMMING

Evalueer de wijze waarop je toestemming vraagt, verkrijgt en registreert, en wijzig waar nodig.

8. KINDEREN

Ontwikkel systemen die de leeftijd van de betrokkene nagaan en die de ouder(s) of voogd(en) om toestemming vragen voor de gegevensverwerking van minderjarige kinderen.

9. DATALEKKEN

Voorzie adequate procedures om persoonlijke datalekken op te sporen, te rapporteren en te onderzoeken.

10. GEGEVENSBESCHERMING DOOR ONTWERP EN GEGEVENSBESCHERMINGSEFFECTBEOORDELING

Maak je vertrouwd met de begrippen "gegevensbescherming door ontwerp" en "gegevensbeschermingseffectbeoordeling" en ga na hoe je deze concepten in de werking van jouw bedrijf of organisatie kan implementeren.

11. FUNCTIONARIS VOOR GEGEVENSBESCHERMING

Duid, indien nodig, een functionaris voor gegevensbescherming aan, of iemand die de verantwoordelijkheid draagt voor het naleven van de databeschermingsregels. Beoordeel welke plaats deze inneemt binnen de structuur en het beleid van jouw bedrijf of organisatie.

12. INTERNATIONAAL

Bepaal onder welke toezichthoudende autoriteit je valt indien jouw bedrijf of organisatie internationaal actief is.

13. BESTAANDE CONTRACTEN

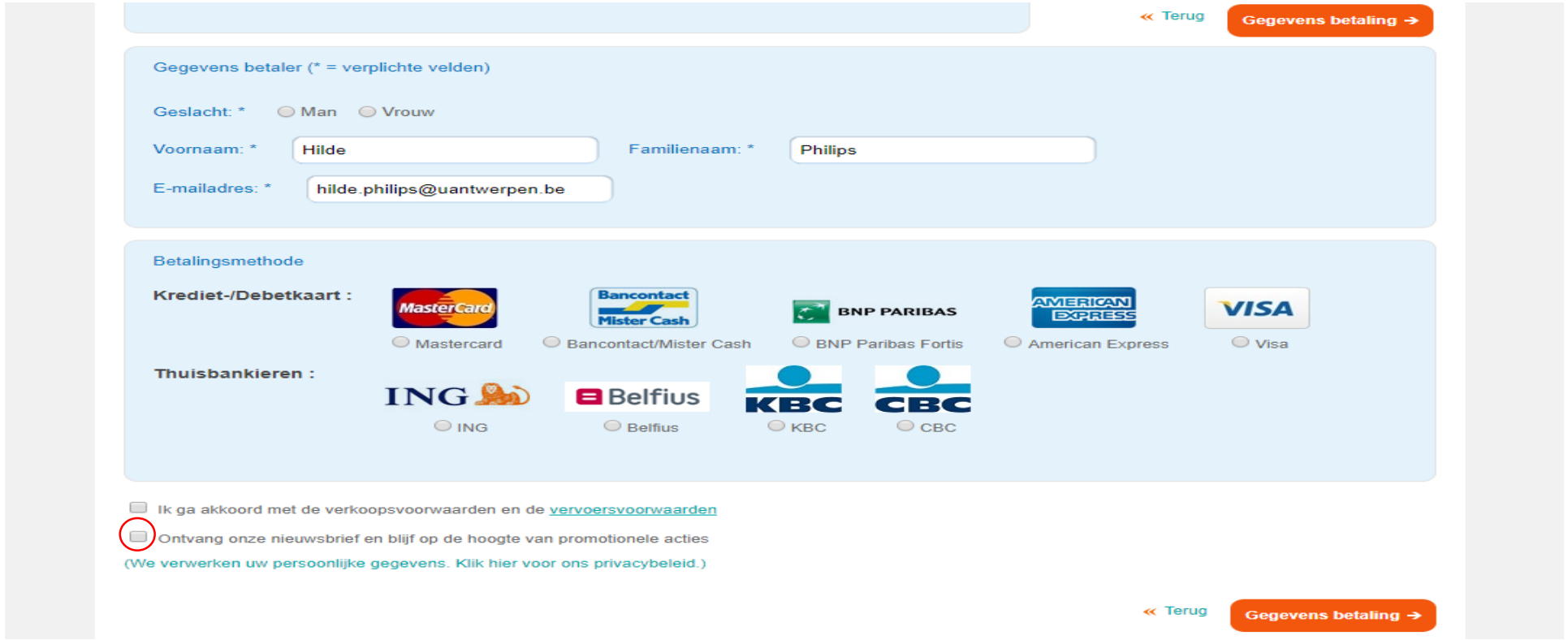
Beoordeel je bestaande contracten, hoofdzakelijk met verwerkers en onderaannemers, en breng tijdig de noodzakelijke veranderingen aan.

To BeContinued

Privacy by default

> = inbouwen van gegevensbescherming in de gebruikte pakketten/tools

> Voornamelijk een opdracht voor leveranciers (vb softwarefirma) = contract!



Privacy Impact Assesment (PIA) of gegevensbeschermingseffectbeoordeling

- Beschrijving van verwerkingen, doeleinden, noodzaak van verwerking, risicoanalyse op rechten en vrijheden betrokkenen en beschermende maatregelen

- Nodig bij grootschalige verwerking van persoonsgegevens of gevoelige gegevens
  - *In principe niet voor individuele zorgverleners*
  - *Na te gaan in welke mate 'grootschalig' van toepassing is op groepspraktijk, wijkgezondheidscentrum of wachtpost, (grote/groepen van) apotheken*

ALGEMENE VERORDENING GEGEVENSBESCHERMING

BEREID JE VOOR IN 13 STAPPEN

1. BEWUSTMAKING

Informeer sleutelfiguren en beleidsmakers over de aankomende veranderingen. Zij moeten inschatten welke gevolgen de AVG zal teweegbrengen voor het bedrijf of de organisatie.

2. DATAREGISTER

Breng in kaart welke persoonsgegevens je bijhoudt, waar deze vandaan komen en met wie je deze hebt gedeeld. Registreer je verwerkingen. Mogelijks dien je hiervoor een informatie-audit te organiseren.

3. COMMUNICATIE

Evalueer je bestaande privacyverklaring en plan noodzakelijke wijzigingen hieraan in het licht van de AVG.

4. RECHTEN VAN DE BETROKKENE

Ga na of de huidige procedures in je bedrijf of organisatie alle rechten voorzien waarop de betrokkene zich kan beroepen, inclusief hoe persoonsgegevens kunnen worden verwijderd of hoe gegevens elektronisch zullen worden meegedeeld.

5. VERZOEK TOT TOEGANG

Update je bestaande toegangsprocedures en bedenk hoe je verzoeken tot toegang voortaan zal behandelen onder de nieuwe termijnen in de AVG.

6. WETTELIJKE GRONDSLAG VOOR HET VERWERKEN VAN PERSOONSGEGEVENS

Documenteer de verscheidene types van gegevensverwerkingen die je uitvoert en identificeer de wettelijke grondslag voor elk van hen.

7. TOESTEMMING

Evalueer de wijze waarop je toestemming vraagt, verkrijgt en registreert, en wijzig waar nodig.

8. KINDEREN

Ontwikkel systemen die de leeftijd van de betrokkene nagaan en die de ouder(s) of voogd(en) om toestemming vragen voor de gegevensverwerking van minderjarige kinderen.

9. DATALEKKEN

Voorzie adequate procedures om persoonlijke datalekken op te sporen, te rapporteren en te onderzoeken.

10. GEGEVENSBESCHERMING DOOR ONTWERP EN GEGEVENSBESCHERMINGSEFFECTBEOORDELING

Maak je vertrouwd met de begrippen "gegevensbescherming door ontwerp" en "gegevensbeschermingseffectbeoordeling" en ga na hoe je deze concepten in de werking van jouw bedrijf of organisatie kan implementeren.

To BeContinued

11. FUNCTIONARIS VOOR GEGEVENSBESCHERMING

Duid, indien nodig, een functionaris voor gegevensbescherming aan, of iemand die de verantwoordelijkheid draagt voor het naleven van de databeschermingsregels. Beoordeel welke plaats deze inneemt binnen de structuur en het beleid van jouw bedrijf of organisatie.

To BeContinued

12. INTERNATIONAAL

Bepaal onder welke toezichthoudende autoriteit je valt indien jouw bedrijf of organisatie internationaal actief is.

13. BESTAANDE CONTRACTEN

Beoordeel je bestaande contracten, hoofdzakelijk met verwerkers en onderaannemers, en breng tijdig de noodzakelijke veranderingen aan.

Contracten met verwerkers

- Afspraken met verwerkers van persoonsgegevens. Wat mag die wel en niet doen?
- Op initiatief verwerkingsverantwoordelijke
- Met wie: dienstverleners/leveranciers die persoonsgegevens verwerken
  - Softwarepakketten
  - Sociaal secretariaat
  - …

Template volgt

ALGEMENE VERORDENING GEGEVENSBESCHERMING

BEREID JE VOOR IN 13 STAPPEN

1. BEWUSTMAKING

Informeer sleutelfiguren en beleidsmakers over de aankomende veranderingen. Zij moeten inschatten welke gevolgen de AVG zal teweegbrengen voor het bedrijf of de organisatie.

2. DATAREGISTER

Breng in kaart welke persoonsgegevens je bijhoudt, waar deze vandaan komen en met wie je deze hebt gedeeld. Registreer je verwerkingen. Mogelijks dien je hiervoor een informatie-audit te organiseren.

3. COMMUNICATIE

Evalueer je bestaande privacyverklaring en plan noodzakelijke wijzigingen hieraan in het licht van de AVG.

4. RECHTEN VAN DE BETROKKENE

Ga na of de huidige procedures in je bedrijf of organisatie alle rechten voorzien waarop de betrokkene zich kan beroepen, inclusief hoe persoonsgegevens kunnen worden verwijderd of hoe gegevens elektronisch zullen worden meegedeeld.

5. VERZOEK TOT TOEGANG

Update je bestaande toegangsprocedures en bedenk hoe je verzoeken tot toegang voortaan zal behandelen onder de nieuwe termijnen in de AVG.

6. WETTELIJKE GRONDSLAG VOOR HET VERWERKEN VAN PERSOONSGEGEVENS

Documenteer de verscheidene types van gegevensverwerkingen die je uitvoert en identificeer de wettelijke grondslag voor elk van hen.

7. TOESTEMMING

Evalueer de wijze waarop je toestemming vraagt, verkrijgt en registreert, en wijzig waar nodig.

8. KINDEREN

Ontwikkel systemen die de leeftijd van de betrokkene nagaan en die de ouder(s) of voogd(en) om toestemming vragen voor de gegevensverwerking van minderjarige kinderen.

9. DATALEKKEN

Voorzie adequate procedures om persoonlijke datalekken op te sporen, te rapporteren en te onderzoeken.

10. GEGEVENSBESCHERMING DOOR ONTWERP EN GEGEVENSBESCHERMINGSEFFECTBEOORDELING

Maak je vertrouwd met de begrippen "gegevensbescherming door ontwerp" en "gegevensbeschermingseffectbeoordeling" en ga na hoe je deze concepten in de werking van jouw bedrijf of organisatie kan implementeren.

To BeContinued

11. FUNCTIONARIS VOOR GEGEVENSBESCHERMING

Duid, indien nodig, een functionaris voor gegevensbescherming aan, of iemand die de verantwoordelijkheid draagt voor het naleven van de databeschermingsregels. Beoordeel welke plaats deze inneemt binnen de structuur en het beleid van jouw bedrijf of organisatie.

To BeContinued

12. INTERNATIONAAL

Bepaal onder welke toezichthoudende autoriteit je valt indien jouw bedrijf of organisatie internationaal actief is.

13. BESTAANDE CONTRACTEN

Beoordeel je bestaande contracten, hoofdzakelijk met verwerkers en onderaannemers, en breng tijdig de noodzakelijke veranderingen aan.

GDPR in uw praktijk

4. NUTTIGE INFO, TIPS & FAQ

Gegevens delen met andere zorgverleners buiten de organisatie: mag dat nog?

> Absoluut!

> Heb aandacht voor het verwerkingsdoel en de gerechtigde verwerkingsgrond

Een patiënt trekt zijn geïnformeerde toestemming in. Mag nu niets meer gedeeld worden?

> Informed consent = toestemming voor delen met zorgverleners via eHealth-netwerk, Vb. Sumehr voor andere artsen of medicatieschema op Vitalink

> Ja, andere informatie delen is noodzakelijk en blijft mogelijk
  - ander soort informatie
  - via andere weg gedeeld
  - naar een specifieke bestemmeling
  - met medeweten patiënt

Beveiliging door het eHealth-platform

- eHealthbox en e-box
- Gratis voor elke zorgverlener
- Dubbele encryptie en authenticatie van zender en ontvanger
- Maar:
  - nog onvoldoende geïmplementeerd in de softwarepakketten - gebruiksvriendelijkheid
  - Niet toereikend qua capaciteit
  - Wordt aan gewerkt

Secretariaatsmedewerker die afspraken vast-legt en klachten noteert: mag dat nog?

> Ja, gerechtvaardigd belang

> Goede praktijkvoering en toegankelijke medische zorg

> ! Wil niet zeggen dat vrije toegang tot medische dossiers toegelaten is

- Alleen die informatie die nodig is om taken uit te voeren
- Mogelijke maatregelen:
  - ✓ Toegangsbeheer via pakket regelen
  - ✓ Logging van gegevens: controle van wie wanneer toegang had

Geheimhoudingsplicht in medewerkerscontract

Chauffeur WP die patiëntengegevens in GPS ingeeft + info over ernst klacht. Kan dat nog?

> Ja, gerechtvaardigd belang rond goede praktijkvoering en toegankelijke medische zorg
  - ! Wil niet zeggen dat toegang tot medische dossiers toegelaten is

Geheimhoudingsplicht wordt opgenomen in contract met de chauffeur

Bewaringstermijn: GPS-gegevens enkel nodig om bij patiënt te geraken – kunnen dus kort daarna gewist worden

Is een softwarefirma een verwerker?

- Software-leveranciers verwerken in principe geen persoonsgegevens
- Het product dat ze aanleveren, verwerkt wel persoonsgegevens (vb opslag van data in de cloud)
- In geval van softwarematige ingrepen of problemen, kan en zal het softwarehuis toegang hebben tot de persoonsgegevens
- Daarnaast zullen ze ook wel op andere manieren de persoonsgegevens verwerken (aangezien de definitie van ‘verwerken’ heel breed is)

Ja! → extra clausules overeenkomst

Mag ik foto van wonde of vragen over patiënt via WhatsApp doorsturen naar collega?

> In sé niet herleidbaar tot de persoon als de patiënt niet herkenbaar is
> Wel opgelet met ‘aanvullende informatie’ waaruit er toch afleiding mogelijk is (context, meta-data zoals locatie, tijdstip, IP adres van de instelling)

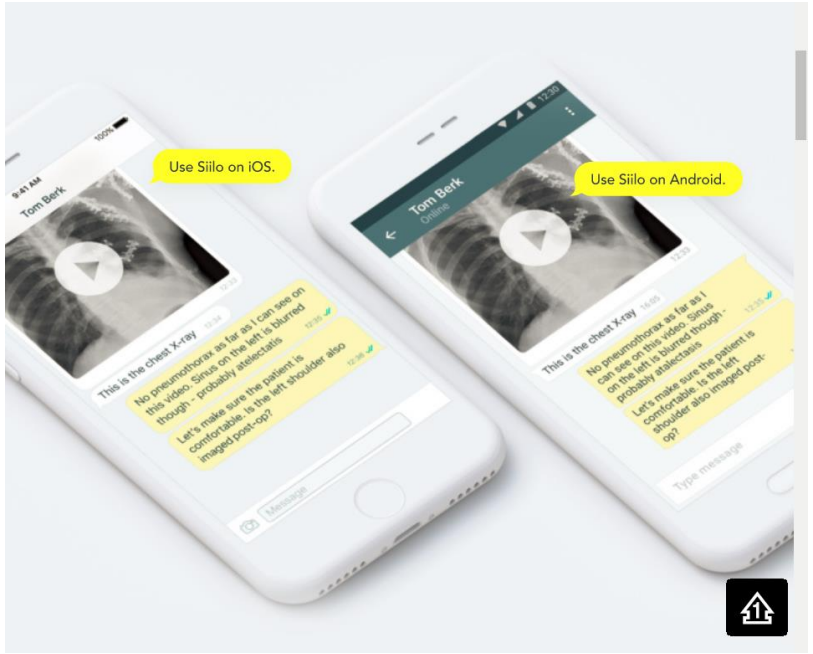
> Transport is versleuteld
> Maar: onduidelijkheid over opslag

> In NL verbod!

Zeker niet aan te raden voor foto’s owv opslag van foto’s tussen je persoonlijke foto’s

Siilo

- Beveiligde ‘whatsapp’ voor zorgverleners (ook voor desktop)
- In NL al in gebruik – samenwerking met KNMP
- Eigenschappen:
  - Controle identiteit - zorgverlener
  - End-to-end encryptie
  - Gescheiden locatie voor informatie
  - Automatisch gewist na 30 dagen
- *In testfase*



Een patiënt geeft zijn akkoord om laboresultaten of een voorschrift per mail te versturen. Dan mag dat toch?

- E-mail dient absoluut vermeden te worden
- Niet-versleutelde gegevens die verstuurd worden en gegevenslekken kunnen zo niet vermeden worden.
- Zelfs als er een akkoord van de patiënt is, neem je niet de nodige maatregelen om de beveiliging van persoonsgegevens te waarborgen.

- Dus: nee!

Hoe dan wel?

- Portalen of beveiligde websites om info te delen met derden
  - Veel labo's of ziekenhuizen stellen al informatie beschikbaar aan de patiënt via patiëntenportalen.

- Patiëntenportalen: vanaf nu publiekscampagne en makkelijker toegankelijk (ovv informed consent)

Mijngezondheid

Patient
HealthViewer

Mijngezondheid

WAT IS MIJN GEZONDHEID?

Mijngezondheid is een online portaal, ook wel "Personal Health Viewer" genoemd. Dit portaal geeft u een zicht op uw gezondheidsgegevens via één enkele toegangspoort. Het gaat om:

- medische informatie die zorgverleners (uw huisarts, uw artsen in het ziekenhuis, uw apotheker ...) elektronisch bewaren en delen
- informatie van uw ziekenfonds (bijv. over terugbetalingen) en van overheidsinstellingen (bijv. registratie van orgaandonatie)
- informatie over patiëntenverenigingen via de website van het Vlaams Patiëntenplatform (VPP).

Heeft u vragen over het portaal? Dan kan u de FAQ-pagina raadplegen of uw vraag stellen via het contactformulier.

Beveiligde Toegang

Aanmelden

federale overheidsdienst
VOLKSGEZONDHEID,
VEILIGHEID VAN DE VOEDSELKETEN
EN LEEFMILIEU

RECIP-e

eHealth

abrumet

CoZo
Collaboratief Zorgplatform

Réseau Santé Wallon

vitalink

VZN Vlaams Ziekenhuisnetwerk KU Leuven

IMA-AIM

Vlaams Patiëntenplatform

LUSS
LIGUE DES USAGERS DES SERVICES DE SANTÉ

https!

Voorbeeld van toepassing: SSL

Data Protection Institute

- HTTPS: Hyper Text Transfer Protocol Secure
- HTTP verkeer dat verloopt over een beveiligde verbinding
- Verkeer dat via HTTPS is versleuteld en kan niet worden gelezen als het wordt onderschept
- Hoe herken je https?

Mag ik mailadressen van patiënten opslaan en gebruiken?

- Ja, maar informeer patiënt dat je het doet en over doelstelling
  - voor informatieve mails (verlof,…) = gerechtvaardigd belang
  - voor nieuwsbrieven = ? toestemming nodig

- !! Opgelet voor gezondheidsinformatie
- Patiëntgegevens verwijderen

Opgelet met keuze mailprovider/tool
→ !! opslag data buiten de EU

Elke patiënt heeft recht op ‘vergeten’ te worden. Geldt dat ook voor medische gegevens?

Elke patiënt heeft recht op ‘vergeten’ te worden. Geldt dat ook voor medische gegevens?

- De patiënt heeft het recht om dit te vragen
- Wijs hem in elk geval op de gevolgen en gevaren
- **Maar** uiteraard geldt voor bepaalde gegevens een wettelijke bewaarplicht
- Die verplichting van bewaringstermijn voor specifieke gegevens gaat in tegen het recht op vergeten te worden

- Het antwoord is afhankelijk van welke data gewist moeten worden:
  - Nee, als het gaat om gegevens van medisch dossier of afleveringen van voorschriften
  - Ja, als de patiënt bijv. vraagt om zijn mailadres te wissen

Vertrouwelijke gesprekken of vermelding van persoonsgegevens in ‘openbare’ ruimte of in aanwezigheid van derden?

> Wet Patiëntenrechten: *De patiënt heeft recht op respect voor zijn intimiteit*

> GDPR: passende technische en organisatorische maatregelen

Gesprek elders voeren
Markeren waar volgende patiënt dient te wachten
! Opgelet met noemen van namen in aanwezigheid van derden

Chauffeur pikt bloedstalen op aan buitendeur.
Voorschriften ter afhaling op prikbord.
Pak vsn voor TD ligt klaar aan buitendeur

> Lek!!

> Opgelet met de verpakking, plaatsing en uitwisseling van persoonsgegevens

vb. voorschriften, verslagen, bloedstalen, (tarificatie)bestanden

Gebruik afgesloten en veilige verpakkingen
Beveiligde manier voor uitwisseling van bestanden of verslagen (niet per mail, fax,…)

Ik bewaar mijn papieren archief in een overbodige slaapkamer thuis. Dat mag toch?

> ! Need to know principe = toegang tot ‘bevoegden’
> Maatregelen nemen voor afgesloten bewaarplaats

Ik stel bij de aflevering vast dat patiënt een ‘medische shopper’ is. Mag ik dit melden aan collega-artsen en apothekers?

- Ja, op voorwaarde dat de patiënt zijn toestemming gaf om dit te melden

- Zonder toestemming van de patiënt: apotheker mag de informatie van het voorschrift alleen overmaken aan de voorschrijver
- Bij bevestiging van misbruik van de voorschrijver:

  apotheker dient de inspecteur te informeren

Mag ik medicatie of documenten of informatie meegeven aan partner/kind/mantelzorger/vpk?

- Doorgifte aan derden blijft mogelijk bij GDPR
- Betrokkene moet op de hoogte zijn – toestemming geven

Het papierafval van mijn praktijk verzamel ik voor ophaling door de jeugdbeweging.

> Documenten met persoonsgegevens ‘vrij’ terug te vinden = lek
> Vb afgedrukt medicatieschema, kassaticketjes die niet meegenomen worden, laboverslag

Vernietig vertrouwelijk papier
– gebruik een papierversnipperaar

Tot slot nog enkele tips

Tips – organisatorische maatregelen

- Spreek er regelmatig over met collega's, partners = bewustzijn
- Gebruik je gezond verstand
- Vermeld (telefonisch) geen persoonsgegevens wanneer derden kunnen meeluisteren
- Check je bronnen (kijk uit met telefoon!)
- Zorg dat patiënten je niet via mail, social media edm contacteren met gezondheidsvragen
- Sluit dossiers van patiënten die vertrokken zijn meteen af
- Wis gegevens als je ze niet meer nodig hebt (en niet moet bewaren)

Tips – organisatorische maatregelen

- Laat deuren niet openstaan
- Bewaar geen data in kasten/locaties die toegankelijk zijn
- Maak afspraken rond toegang (sleutels, alarmcode,…)
- Vernietig documenten met persoonsgegevens als je ze niet meer nodig hebt → papierversnipperaar
- Vermijd persoonsgegevens via mail of losse dragers (CD, USB, papier)
- Print geen gevoelige gegevens af op een printer die centraal staat en toegankelijk is voor onbevoegden

Tips – technische maatregelen

- Stel screensaver snel genoeg in: poetsdienst of patiënt die rap meekijkt terwijl scherm nog openstaat is snel gebeurd
- Zorg voor anti-virus, anti-malware,…
- Zorg voor geüpdatet systeem (geen windows XP)
- Zorg voor toegangsbeveiliging en veilige paswoorden (geen gedeelde accounts)
- Gebruik ‘geijkte’ kanalen voor gegevensuitwisseling (eHealth, Vitalink, veilige portalen, Zivver,…)
- Zorg dat er geen persoonsgegevens, gevoelige gegevens via (onbeveiligde) websites uitgewisseld worden
- Zorg dat je de harde schijf ‘gecleand’ wordt bij wissel van PC

Domus Medica en de BV's helpen

- Nog verduidelijking nodig op een aantal vlakken (PIA, DPO, meldpunt)
- Praktisch:
  - Communicatie en artikels
  - Voorbeeld verwerkingsregister
  - Begeleidende checklist
  - Document gegevenslekken
  - Voorbeeld privacyverklaring (via eHealth)
  - Voorbeeld contracten leveranciers (via eHealth)
- Aanvullende ondersteuning


KEEP
CALM
AND
PREPARE FOR
GDPR


VRAGEN?

B E D A N K T V O O R U W A A N D A C H T !