7. De beveiliging van gegevens waarborgen

Hoe kan ik mijn organisatorische veiligheid verbeteren?

Elke Verwerkingsverantwoordelijke moet alle gegevens die hij verwerkt beschermen en dit door alle voorzorgsmaatregelen te treffen op het gebied van organisatorische en technische beveiliging (fiche 6. Technische beveiliging).

Wat de organisatorische beveiliging betreft, moet de Verwerkingsverantwoordelijke:

Basisbeginsel:

- Elke persoon die werkzaam is in de praktijk en persoonsgegevens verwerkt **bewustmaken van de verwerking van persoonsgegevens**
- **Bewustmaken van het beroepsgeheim**
- **Het hele personeel regelmatig** (bijvoorbeeld: een keer per jaar) bewustmaken
- **Een individuele login** en een **individueel wachtwoord** kiezen:
    - Kies voor een wachtwoord dat ingewikkeld en niet aan anderen communiceerbaar is (cf. fiche 6).
      Opgelet: Hang of plak de wachtwoorden niet aan uw computer
    - Wijzig alle wachtwoorden van uw toegangen (+/- elk jaar) (cf. fiche 6)
- **Plaats van de printer**: deze moet niet op een plek staan die toegankelijk is voor de patiënten
  Voorbeeld: in de wachtkamer, gang naar de toiletten
- **Afgedrukte documenten moeten meteen na het afdrukken worden opgehaald**. *Bijvoorbeeld, kies een printer met toegang per gebruikersnaam en wachtwoord per gebruiker of badge*
- **Verouderde documenten**: vernietig documenten die gevoelige gegevens bevatten met een **papierversnipperaar**
- Ongebruikte computers (of elk ander IT-instrument): vergeet niet om de harde schijf te vernietigen (cf. fiche 6)
- **De werkplek beveiligen**: sluiten van deuren, ramen en kasten bij het verlaten van het kantoor. Geen dossiers laten liggen op plaatsen waar iedereen erbij kan
- **Regelmatig een back-up maken** en deze op een andere plaats bewaren dan de werkplek: want in geval van brand of overstroming van de praktijk, of in geval van vernietiging van het systeem, moet uw back-up beschut zijn tegen schade (cf. fiche 6)

Een professioneel en beveiligd communicatiekanaal kiezen

- **De ontvanger controleren**
- **Zich afvragen of de informatie die zal worden meegedeeld belangrijk/noodzakelijk is of niet**
- **Kies voor een end-to-end** vercijfering bij het versturen van informatie via een informatiekanaal (bijvoorbeeld het gebruik van de eHealthBox, het Brusselse Gezondheidsnetwerk)

Wanneer een patiënt vraagt om met hem te communiceren via een middel waarvan de beveiliging niet is gegarandeerd, vermeld de aanvraag dan in zijn lokale medische dossier door het document ‘Communicatiemiddel’ in te vullen.

Opletten met de doorgifte van informatie

- **Bepaal de gegevens van de ontvanger**
- **Controleer deze vóór het versturen** (let op met het automatisch invullen van het e-mailadres van de ontvanger). *Opgelet met doorgifte van gegevens buiten de EU.*

Elk incident vermelden in zijn register van incidenten

- De verwerkingsverantwoordelijke heeft de verplichting om een register van incidenten bij te houden waarin hij elke inbreuk moet vermelden (zie fiche 8). *Ter herinnering: inbreuk op gegevens is het verlies, de diefstal, de verstrekking of de vernietiging van persoonsgegevens, op opzettelijke of onopzettelijke wijze, maar ook de onbeschikbaarheid van de gegevens. Als de inbreuk op persoonsgegevens een risico inhoudt voor de persoonlijke levenssfeer van de patiënt moet de inbreuk, in voorkomend geval, worden gemeld bij de Gegevensbeschermingsautoriteit (GBA), binnen een termijn van 72 kalenderuren.*

Alle gegevens moeten gedurende minimaal 30 jaar worden gearchiveerd (maximaal 50 jaar)

- Deze gegevens moeten op beveiligde wijze worden gearchiveerd en indien nodig toegankelijk zijn (zie fiche 9).

Overeenkomsten afsluiten met verwerkers

- deze overeenkomsten moeten waarborgen bieden op het vlak van beveiliging ten aanzien van de AVG (zie fiche 3)

Concreet gezien

Respecteer de bovenstaande basisprincipes

Kies een professioneel en veilig communicatiekanaal

Wees voorzichtig bij het overbrengen van gegevens

Verplichting om alle incidenten te melden in een register

Gegevens minimaal 30 jaar en maximaal 50 jaar archiveren

Contracten ondertekenen met alle verwerkers