6. De beveiliging van gegevens waarborgen

Hoe kan ik mijn technische veiligheid verbeteren?

Beveiliging omvat zowel de technische beveiliging die we in dit fiche zien als de organisatorische beveiliging waarover fiche 7 gaat.

Enerzijds dient het voorbestaan van de gegevens te worden gewaarborgd en anderzijds moet er een gezonde IT-omgeving en een goed beheer van de toegangen zijn.

Hieronder enkele tips:

1-Om ervoor te zorgen dat gegevens blijven voortbestaan en om het verliezen ervan te vermijden, moet:

- Er een **regelmatige back-up** van gegevens worden gemaakt
- **Deze back-up op een beveiligde plek worden bewaard**, buiten uw praktijk. *Voorbeeld: in geval van diefstal, brand of overstroming van uw praktijk, of in geval van vernietiging van uw systeem, moet uw back-up beschut zijn tegen schade/diefstal.*
- Er **een rampenplan** zijn in geval van stroomonderbreking of netwerkstoring.

2-Zorg voor een goed beheer van de toegangen:

- **Kies een individuele login en een individueel wachtwoord.**
  - Geef de voorkeur aan een **ingewikkeld wachtwoord:**geen geboortedatum of een gebruikelijk wachtwoord, zoals de voornaam van uw echtgeno(o)t(e) of kinderen, maar iets dat u zich makkelijk kunt herinneren (voorbeeld: naam van een plaats of een herinnering)
  - **Deel uw wachtwoord niet**: geef het aan niemand! *Opgelet: Hang of plak de wachtwoorden niet aan uw computer of onder uw toetsenbord.*
  - **Verander de wachtwoorden voor de toegangen regelmatig,** maar niet om de drie maanden om ervoor te zorgen dat u ze kunt onthouden.
  - Geef de voorkeur aan een **sterke** (twee-factor-) **authenticatie** om de risico's te verlagen. Applicaties kunnen helpen (vb. Itsme, myID.be,...)
- **Haal alle verouderde toegangen weg**: zorg ervoor dat alle toegangen van personen die uw organisatie hebben verlaten of er niet meer voor werken (werknemers, verwerkers, enz.), geblokkeerd en verwijderd worden.
- Gebruik **een automatisch vergrendelingssysteem** van uw sessie na bijvoorbeeld 5 minuten van inactiviteit.
- **Vergrendel uw computer** wanneer u uw bureau verlaat of wanneer u geen zicht meer op uw computer heeft en sta niemand toe om uw sessie te gebruiken die persoonlijk moet blijven. *Bijvoorbeeld, als u bent ingelogd op de eGezondheidsnetwerken, zijn alle toegangen getraceerd. Wanneer iemand anders toegang neemt tot gegevens via de sessie die op uw computer open is blijven staan, wordt u aansprakelijk gehouden aangezien uw inloggegevens zijn getraceerd (log van raadplegingstoegang).*

3-Beheer de IT-infrastructuur:

- Zorg ervoor dat u een performante **firewall** en **antivirus** heeft.
- Activeer de **automatische updates** van de computer (firewall, antivirus, software, Windows, …). U kunt deze taak delegeren aan uw verwerkers. Denk er in dit geval aan om een specifieke bepaling in uw overeenkomst op te nemen over het vernieuwen van softwarecontracten en het beheren van uw updates, zodat uw software en IT-infrastructuur performant blijven.
- Denk er voordat u een overeenkomst met een verwerker (software, programma, anders) ondertekent aan om **de systemen/software te testen zodat u er zeker van bent dat ze voldoen aan de behoeften** (in verband met het werkterrein in kwestie) en de prestaties op het vlak van gegevensbeveiliging.
- **Bescherm het wifinetwerk met een wachtwoord** (wijzig het oorspronkelijke wachtwoord). Als u wifi aan uw patiënten ter beschikking stelt, maak dan 2 afzonderlijke wifinetwerken aan:
    - een privénetwerk voor de activiteiten van de praktijk, beveiligd met een sterk wachtwoord dat alleen voor dit netwerk geldt (voor u en uw eventuele collega's)
    - een ander openbaar netwerk voor uw patiënten, met een gedeeld wachtwoord dat uitsluitend voor uw patiënten is bedoeld (denk eraan om een affiche in de wachtkamer op te hangen).
- **Als u twijfelt aan de veiligheid van een e-mail of website: controleer deze op** SafeOnWeb
- Gebruik van **IT-materiaal** (tablet/GSM/USB-stick/harde schijf, enz.):
    - **Beperk de opslag van gevoelige gegevens** op deze hulpmiddelen, aangezien ze vatbaar zijn voor verlies of diefstal.
    - Kies een **optimale beveiliging** voor uw IT-instrumenten door beveiliging met een wachtwoord of biometrische authenticatie (vingerafdruk, gezichtsherkenning).
- Een **beschadigd instrument:**
    - Vernietig alle gegevens van de harde schijf (boor gaten in de harde schijf) voordat u deze weggooit. Verkoop materiaal dat gebruikt is om al dan niet gevoelige persoonsgegevens op te slaan nooit tweedehands door.
    - Dank het (op deze manier vernietigde) materiaal af (Recupel-punten).
    - Andere optie: doe een beroep op een bedrijf dat IT-materiaal vernietigt.

OPGELET *: bepaalde instrumenten worden ondanks dat ze erg nuttig kunnen zijn toch afgeraden (matige beveiliging op heden), en de algemene voorwaarden zouden ook moeten worden gecontroleerd omdat deze kunnen veranderen (plaats van opslag van gegevens, naleving van AVG, enz.)*

Concreet gezien

Gegevens beschermen en gegevensverlies voorkomen

Goed toegangsbeheer

IT-infrastructuur beheren