Tips om een datalek te voorkomen

1. **Mogen medewerkers zelf software downloaden en installeren op bedrijfsapparatuur?**
   Als medewerkers op eigen houtje software mogen installeren, zorgt dit voor kwetsbaarheden in de databeveiliging. Zorg er daarom voor dat dit op apparaten die toegang hebben tot persoonsgegevens niet is toegestaan. Vraag aan je ICT leverancier hierop toe te zien

2. **Worden bij afgeschreven hardware alle persoonsgegevens daarop vernietigd?**
   Het is aan te raden om bij het verkopen of vernietigen van hardware te zorgen dat persoonsgegevens onleesbaar zijn gemaakt. Bestanden verwijderen betekent niet dat deze niet meer terug te vinden zijn op de harde schijf. Zorg dat de data overschreven worden of maak de gegevensdragers in zijn geheel onbruikbaar. En vergeet vooral ook de printer niet - die hebben vaak nog duizenden print- en scanopdrachten in het geheugen staan.

3. **Wissen alle medewerkers bestanden met persoonsgegevens na gebruik van lokale apparatuur en externe gegevensdragers?**
   Soms is het noodzakelijk om een kopie van een patiënt bestand te maken. Het is dan aan te raden medewerkers te instrueren de kopie te verwijderen, zowel van lokale apparatuur als eventuele externe gegevensdragers als USB-sticks etc. Het is belangrijk dat iedereen zich ervan bewust is dat ze zorgvuldig met dit soort bestanden moeten omgaan, zodat onbevoegden er niet bij kunnen.

4. **Verzend je bestanden met persoonsgegevens via mail of gebruik je een beveiligde SFTP-server?**
   Als je organisatie gegevens uitwisselt per e-mail of fysieke gegevensdragers zoals USB-sticks, adviseert de Autoriteit Persoonsgegevens deze gegevens goed te versleutelen. Gebruik Zorgmail voor het veilig versturen van bestanden.

   Daar komt nog bij dat het onwenselijk is dat er bestanden met persoonsgegevens rondzweven in mailboxen, omdat deze data volledig van de radar zijn. Daardoor is deze niet in beeld bij een ‘recht om vergeten te worden’-verzoek van een klant of bij een potentieel datalek.

5. **Slaat je organisatie persoonsgegevens op in de cloud, bijvoorbeeld via Dropbox, Google Drive of Microsoft Azure?**
   Voorkeur is om deze middelen niet te gebruiken As je ze wel gebruikt let er dan op waar deze gegevens opgeslagen worden. Wanneer persoonsgegevens opgeslagen worden buiten de EU, zijn er specifieke regels om de bescherming van die gegevens te garanderen. Voordat je organisatie deze diensten gaat gebruiken, is het van belang na te gaan of deze aan privacy- en beveiligingsvoorschriften voldoen. Veel aanbieders van clouddiensten zijn gevestigd in de VS, waardoor de Amerikaanse overheid zich op basis van de Patriot Act toegang kan verschaffen tot je gegevens.

Bonustips

- Beveilig al je online webformulieren met een gratis SSL-encryptie. Als de formulieren door derden worden gehost, check dan of zij dit in orde hebben.
- Zorg voor dagelijkse back-ups van gegevens, inclusief databases en configuratiebestanden, op een externe locatie.
- Als u gasten internettoegang wilt geven, gebruik hier dan een apart draadloos netwerk voor, waarbij zij geen toegang hebben tot het hoofdnetwerk van de router.