ZORG VOOR JE PATIËNTEN ÉN VOOR HUN GEGEVENS

© Wit-Gele Kruis

JOKE SAMYN, DATA PROTECTION OFFICER WIT-GELE KRUIS, EN USCHI DE COSTER, ADJUNCT DATA PROTECTION OFFICER WIT-GELE KRUIS VAN VLAANDEREN

Beschermen van gegevens en van privacy is niet alleen een zorg van je patiënten maar ook van jezelf

Als thuisverpleegkundige draag je zorg voor je patiënt. Dat betekent dat je ook zorgt voor zijn of haar privacy en gegevens. Met het oog op totaalzorg communiceren thuisverpleegkundigen met verschillende zorgpartners. Dat gebeurt uiteraard binnen de grenzen van het (gedeeld) beroepsgeheim, de therapeutische relatie met de patiënt en de *informed consent* voor gegevensdeling.

Onze maatschappij digitaliseert aan een snel tempo. Of het nu gaat om gezondheidszorg, bankieren of reizen, steeds vaker worden alledaagse handelingen digitaal verricht. Via deze digitale verrichtingen laten organisaties en individuen een digitaal spoor achter. Ook in de thuisverpleging zijn computers, tablets en smartphones vrijwel niet meer weg te denken.

De bescherming van gegevens en van privacy speelt een belangrijke rol zowel in het rechtstreeks contact met de patiënt en zijn omgeving als in de dagelijkse omgang met gezondheidsgegevens. Als verpleegkundige ben je bijvoorbeeld gebonden aan het beroepsgeheim, moet je persoonlijke documenten altijd veilig opbergen, discretie bewaren bij het telefoneren over of met een patiënt, observaties in een respectvolle schrijfstijl noteren ...

Enkele begrippen uitgelicht

Binnen de thuisverpleging komen we met heel wat persoonsgegevens in aanraking. Naast identificatiegegevens (bijvoorbeeld naam, adres, geboortedatum ...) gaat het vooral om **gevoelige persoonsgegevens**, meer bepaald gezondheidsgegevens. Deze gegevens krijgen vanuit de wetgeving[1] extra bescherming.

1. De GDPR (ook Algemene verordening gegevensbescherming of AVG genoemd) gaat over het beheer en de beveiliging van persoonsgegevens van Europese burgers.

© Marco Mertens

Privacy en **gegevensbescherming** zijn weliswaar twee afzonderlijke begrippen. We zijn allemaal vertrouwd met het recht op een persoonlijke levenssfeer en zaken die je in de privésfeer wenst te houden. Het recht op bescherming van je persoonsgegevens maakt daar deel van uit. Als organisatie en bijgevolg als medewerker van jouw organisatie, is het belangrijk daarrond een bewustzijn te creëren. De privacyverklaring van je organisatie vind je onder andere terug op de website. Het toont patiënten, zorgpartners, externen, medewerkers en andere stakeholders aan hoe de organisatie omgaat met hun rechten en met de inzage, de correctie en de verwijdering van informatie. Daarnaast geeft de privacyverklaring ook weer hoe de organisatie persoonsgegevens beveiligt, wat er met persoonsgegevens gebeurt en op welke gronden dit gedaan wordt.

Bewust omgaan met persoonsgegevens en privacy van patiënten

Louter verkondigen (of als organisatie documenteren) dat je veilig omgaat met de gegevens van je patiënten, van je collega's of van jezelf, is uiteraard niet voldoende. Het blijft een uitdaging om de goedbedoelde intenties – uitgeschreven in procedures en richtlijnen – duurzaam om te zetten in concrete acties op de werkvloer. Voorschriften die zichtbaar op het dashboard van de wagen liggen en het gebruik van onveilige of gedeelde wachtwoorden, kunnen natuurlijk niet. Er is een waslijst aan dergelijke incidenten. Ze gebeuren nog te vaak en kunnen eenvoudigweg vermeden worden door bewuster om te gaan met persoonsgegevens en privacy.

Enkele handvaten voor de dagelijkse praktijk

- Het klinkt logisch, maar denk altijd en overal aan je beroepsgeheim en je discretieplicht.
- Werk met correcte en actuele gegevens. Voer tijdig voorschriften, observaties, parameters en dergelijke in. Link de juiste gegevens aan de juiste patiënt.
- Verwerk enkel gegevens in het kader van je job (bijvoorbeeld gegevens met betrekking tot patiëntenzorg en personeelsadministratie) en beperk je tot relevante informatie.
- Beperk de toegang tot persoonsgegevens. Kleef geen post-its met wachtwoorden op je werkmateriaal en vermijd dat 'vreemde ogen' meekijken wanneer je persoonsgegevens registreert. Leg dergelijke gegevens niet zichtbaar in de wagen of laat ze niet onbeheerd achter. Merk je vertrouwelijke informatie op op een bureau, op een pc waarvan het scherm niet vergrendeld is of in een open dossierkast? Spreek elkaar er dan op aan.

Hoe veilig gegevens delen?

Veilig omgaan met patiëntengegevens betekent dat alle communicatie over patiënten terug te vinden is in één centraal, beveiligd systeem. In vele gevallen is dit het elektronisch verpleegdossier. Dat is de centrale tool bij uitstek om patiëntengegevens veilig te verwerken. In communicatie met andere zorgverleners kan gebruik gemaakt worden van de beveiligde platformen, beschikbaar via eHealth, zoals de eHealth box, Vitalink, of andere, voor de zorgsector geschikte, veilige applicaties zoals Siilo. Het is belangrijk dat je de richtlijnen van je eigen organisatie kent en steeds nauwgezet opvolgt.

E-mails zijn niet het ideale middel om patiëntengegevens mee te delen. Toch kan deze communicatietool, weliswaar met de nodige maatregelen rond veilig mailen (bijvoorbeeld via versleuteling) en met een duidelijke e-mail etiquette, een goede aanvulling zijn.

Waar ben je aandachtig voor?

- Reageer niet met een reply, maar stel een nieuwe e-mail op met een geverifieerd adres.
- Gevoelige gegevens stuur je niet naar algemene groepen en bij het versturen gebruik je best geen info@-adressen.
- Zet de naam van de patiënt of andere gevoelige informatie niet in het onderwerp.
- Beperk de gevoelige informatie die je meegeeft tot een minimum. Gebruik bijvoorbeeld, indien mogelijk, het patiëntennummer in plaats van de naam van de patiënt.
- Indien meerdere patiënten besproken worden in een e-mail of indien er een lijst wordt meegestuurd, kan dit enkel via een beveiligde bijlage.
- Beveilig bijlages met een wachtwoord, maar gebruik niet steeds hetzelfde wachtwoord.
- Verifieer altijd het adres van de ontvanger, de inhoud en de bijlagen voor je op verzenden klikt.
- Wanneer het niet langer nodig is de informatie te bewaren, verwijder deze dan uit je mailbox.

Digitalisering biedt vele mogelijkheden. Door COVID-19 kwam de digitale gezondheidszorg in een stroomversnelling terecht. De talloze mogelijkheden om op afstand met elkaar in contact te blijven en zelfs zorg te verlenen – denk aan de teleconsultaties van diabeteseducatoren, diëtisten en

"De bescherming van gegevens en van privacy speelt een belangrijke rol zowel in het rechtstreeks contact met de patiënt en zijn omgeving als in de dagelijkse omgang met gezondheidsgegevens."

"Gedraag je professioneel op sociale media en respecteer het beroepsgeheim."

vroedkundigen – bieden heel wat voordelen. Het blijft evenwel belangrijk om de veilige tools van de onveilige tools te onderscheiden. Zo ga je best na of de applicatie voorziet in end-to-end encryptie[2], er geen gegevens op de applicatie worden opgeslagen en het mogelijk is om de contactpersoon te verifiëren. Daarnaast is het belangrijk om de juiste tool te gebruiken voor de juiste toepassing. Zo zijn Facebook, WhatsApp® of eender welke andere sociale media tools niet aangewezen om (gevoelige) persoonsgegevens in een zorgcontext mee te delen. Het zijn uiteraard wel ideale tools om in je privéleven met vrienden en familie te communiceren.

Sociale media en privacy

Hoewel je vaak zou denken dat een profiel of een account privé is, is het internet een heel open gebeuren. Zelfs wanneer je een bericht, een foto of een filmpje enkel met vrienden deelt, kan dit via verschillende kanalen toch online de wereld in worden gestuurd.

TIPS

- Gedraag je professioneel op sociale media en respecteer ook hier het beroepsgeheim. Verspreid dus geen namen of foto's van patiënten en deel geen gegevens uit het patiëntendossier.
- Controleer je privacy-instellingen. Zijn berichten op je profiel enkel zichtbaar voor vrienden of zijn ze publiek te bekijken? Vakantiefoto's aan het zwembad of andere foto's vanuit je privésfeer zijn misschien leuk om te delen met vrienden, maar het is minder leuk wanneer patiënten ze vinden.
- Krijg je vriendschapsverzoeken van patiënten? Wijs hen dan beleefd af en maak duidelijk dat dit voortvloeit uit respect voor elkaars privacy.

Opgelet voor fraude

Naast de vele voordelen, hangen er ook risico's vast aan de digitalisering. Doordat we veelvuldig gebruik maken van een smartphone en van talloze applicaties, zijn we een gemakkelijk doelwit voor **phishing-technieken**. Dat zijn technieken waarbij een oplichter via valse e-mails en nepberichten – op het eerste zicht afkomstig van een betrouwbare organisatie – vertrouwelijke informatie (gebruikersnamen, wachtwoorden, kredietkaartnummers ....) probeert te verkrijgen om later te misbruiken. Oplichters maken ook steeds vaker gebruik van sms'en of van social media-accounts zoals WhatsApp of Messenger om deze informatie te verkrijgen.

TIPS OM EEN VERDACHTE MAIL OF EEN VERDACHT BERICHT TE ONDERSCHEPPEN

- Een phishing-mail krijg je meestal onverwacht en zonder reden.
- Wees op je hoede als men 'onmiddellijke actie' van jou verwacht. Betrouwbare organisaties vragen je niet zomaar om persoonlijke informatie.
- De phishing-mail bevat vaak taalfouten of is op een vreemde manier geschreven.
- Meestal heeft het bericht ook een vage aanspreektitel of staat jouw volledig e-mailadres in de aanspreektitel.
- De e-mail bevat een link die niet naar een veilige website leidt.
- Wees op je hoede. Wanneer je dergelijke e-mails van een gekend iemand ontvangt, wil dat niet altijd zeggen dat hij of zij het ook werkelijk naar jou heeft verstuurd. Klik dus enkel op de e-mails of op de informatie die je van die persoon verwacht.

Ook patiënten zijn vaak nietsvermoedende slachtoffers van frauduleuze praktijken of van oplichters die de naam van de zorgorganisatie misbruiken. Wees dus alert wanneer patiënten vreemde oproepen of bezoeken signaleren. Leg uit dat de organisatie hen enkel zal opbellen voor zorggerelateerde zaken. Een zorgorganisatie zal nooit naar bankgegevens vragen of vragen om een overschrijving te doen zonder verwijzing naar een concrete factuur. Wanneer je langsgaat bij patiënten thuis, maak je dan steeds kenbaar met je werkbadge.

De toevloed aan gegevens waarmee we elke dag werken en de middelen die we daarvoor gebruiken, dragen bij aan een efficiënte zorgverlening. Dat mag uiteraard niet ten koste gaan van de privacy en de gegevensbescherming van de betrokkenen. Jouw organisatie voert hierrond best een transparant beleid om medewerkers vertrouwd te maken met de procedures en richtlijnen die zij verder in de praktijk kunnen brengen. Bewust en verantwoord omgaan met vertrouwelijke informatie van patiënten, van collega's, maar ook van jezelf, kan het risico op inbreuken en misbruiken heel wat inperken. Tenslotte heeft niemand graag dat zijn of haar gegevens op straat komen te liggen.

2 Dit is het versleuteld versturen van gegevens naar een ontvanger. Alleen de zender en de ontvanger kunnen de versleutelde gegevens lezen.