KWALITEIT VEILIGHEID

90 dagen

INFORMATIE-VEILIGHEID

Bron: www.zorgzekeren.nl

Zorgvuldig omgaan met patiëntgegevens

TIP 1

Praat niet over patiënten bij het koffie-apparaat

Patiëntinformatie is privacygevoelige informatie. Bewaak de privacy van je patiënt of cliënt. Praat nooit over hem of haar in het openbaar en print vertrouwelijke informatie alleen, als je zeker weet dat alleen jij het geprinte document in handen krijgt.

TIP 2

Ga zorgvuldig om met documenten met patiëntgegevens

Zorg dat patiëntgegevens op papier of digitaal niet in verkeerde handen kunnen vallen. Gebruik geen onveilige usb-sticks, en plug deze nooit zomaar in je computer. Gooi papieren met patiëntgegevens niet in een gewone prullenbak, maar altijd in de daarvoor bestemde bakken of papierversnipperaar. Laat geen printje met patiëntgegevens op de printer of fax liggen. Als er toch een document met vertrouwelijke gegevens op de printer/ fax ligt, of als je een usb-stick of dvd met gegevens vindt, dan is dit een datalek. Een datalek moet je altijd melden.

TIP 3

Zwijg of vraag door

Deel je patiënt- of cliëntinformatie met anderen? Zorg er dan voor dat je er zeker van bent dat degene met wie je de informatie uitwisselt, een behandelrelatie heeft. Weet je het niet zeker, zeg dan niets of vraag door. Belt iemand bijv. van een andere zorginstelling vraag dan of hij of zij je een e-mail stuurt met daarin zijn contactgegevens.

TIP 4

Stel open vragen

Als iemand belt, moet je zeker weten dat je spreekt met diegene die hij/zij zegt dat hij is. Hiervoor stel je veiligheidsvragen. Stel altijd open vragen. In plaats van “Bent u geboren op 1 mei 1950?” vraag je “Wat is uw geboortedatum?”. Daarmee voorkom je dat je in je vraag privacygevoelige informatie aan de verkeerde persoon verstrekt.

TIP 5

Wees zeker van een behandelrelatie

Verzeker je ervan dat er een behandelrelatie is met de patiënt/ cliënt voordat je zijn of haar gegevens raadpleegt. Zonder behandelrelatie, of noodzakelijk voor je werk, mogen patiënt-/ cliëntgegevens niet bekeken worden. Er wordt vastgelegd wie in een dossier kijkt. Een patiënt heeft het recht op inzage in wie zijn dossier heeft ingekeken.

TIP 6

Check wie je toegang mag geven tot informatie uit het patiëntdossier

Een familielid of contactpersoon heeft niet vanzelfsprekend toegang tot informatie uit het patiëntdossier. Check de procedure van je instelling.

Voorkom datalekken

TIP 1

Herken een beveiligingsincident

Bij een beveiligingsincident bestaat de mogelijkheid dat de vertrouwelijkheid, integriteit of beschikbaarheid van informatie of systemen in gevaar is of kan komen. Voorbeelden zijn: besmettingen met virussen en malware, hacken, verlies van een usb-stick met persoonsgegevens, diefstal van data en hardware, het versturen van mail met verkeerde bijlage of gevoelige informatie naar het verkeerde e-mailadres. Maar ook bijvoorbeeld twee ontslagbrieven die per abuis in één envelop worden verstuurd. Meld een beveiligingsincident of een datalek altijd. Check hiervoor de procedure die geldt in jouw organisatie.

TIP 2

Vergrendel je computer

Vergrendel je scherm of sluit deze af, wanneer je (tijdelijk) je werkplek moet verlaten voor bijv. een toiletbezoek, een vergadering, lunch of afspraak. Hiermee voorkom je dat onbevoegden onder jouw naam toegang hebben tot gevoelige informatie waar jij verantwoordelijk voor bent. Zie je dat een collega zijn computer niet vergrendelt? Vergrendel de computer en spreek hem hierop aan. Een ingelogde computer mag niet onbeheerd worden achtergelaten. Ook niet voor een paar minuten.

TIP 3

Gebruik een veilig wachtwoord

Een goed wachtwoord bestaat uit minimaal acht tekens, met een combinatie van o.a. letters en cijfers. Kies een wachtwoord of wachtwoordzin die alleen jij kent, gebruik geen geboortedata of iets anders dat eenvoudig is te raden. Stel nooit één wachtwoord in voor al je toegang. Kijk op www.wachtwoordbewust.nl voor meer tips.

TIP 4

Bescherm je werkmobiel of -tablet

Heb je een telefoon of tablet voor het werk? Zorg dan dat anderen, bijvoorbeeld je familieleden, hier geen gebruik van kunnen maken. Vergrendel je device met een pincode en/of vingerafdruk. Maak ook geen gebruik van openbare wifi-netwerken.

TIP 5

Spreek mensen aan

Spreek mensen vriendelijk aan, als ze zich op een plek bevinden waar ze waarschijnlijk niet mogen komen of waar ze niet zouden moeten zijn.

TIP 6

Bespreek informatieveiligheid

Het is belangrijk incidenten en zwakheden rondom informatiebeveiliging en privacy te signaleren en te bespreken tijdens een afdelings- of werkoverleg. Neem informatieveiligheid structureel op in het jaarplan van de afdeling. Stimuleer collega’s om fouten te melden en bespreek incidenten. Pas als fouten zichtbaar zijn, kunnen mensen ervan leren en kan een werkproces worden verbeterd.

Veilig mailen

TIP 1

Communiceer op veilige wijze

Voorkom dat gevoelige gegevens op straat komen te liggen. Zorg er daarom voor dat je er zeker van bent dat de ontvanger van de gegevens daadwerkelijk de beoogde ontvanger is. Communiceer gevoelige gegevens enkel via veilige communicatiemiddelen, zoals secure e-mail.

TIP 2

Check je link

Ontvang je een mail met een link erin? Controleer dan vóórdat je op de link klikt, of deze verwijst naar een vertrouwde site. Dit doe je door eerst met de muis over de hyperlink te zweven (‘hoveren’). Je ziet dan het werkelijke webadres. Controleer of dit webadres juist is. Wanneer je twijfelt over een link, neem dan contact op met ICT of de verantwoordelijke voor informatieveiligheid. Op die manier voorkom je mogelijke beveiligingsincidenten.

TIP 3

Wees alert op phishingmails

De verzender van nepmails zijn erop uit om je persoonlijke gegevens of geld te ontfutselen. Helaas zijn ze steeds lastiger te herkennen. Let op de volgende signalen:

- Vreemd taalgebruik.
- De naam van de afzender klopt niet.

Goed voorbeeld helpt

TIP 1

Medewerker en leidinggevende samen verantwoordelijk

Informatieveiligheid is een gedeelde verantwoordelijkheid. Als leidinggevende kun je daarnaast veilig gedrag stimuleren door het goede voorbeeld te geven, medewerkers aan te spreken of een compliment te geven.

TIP 2

Wees bewust van de risico’s

Bewustwording onder alle medewerkers mag niet onderschat worden. Vaak gaat het om onwetendheid of het niet kunnen inschatten van de gevolgen van bepaalde acties van medewerkers. Een fout met privacygevoelige informatie is snel gemaakt. Breng risico’s op het gebied van informatieveiligheid in kaart, tref maatregelen en stel continuïteitsplannen (noodprocedures) op. Raadpleeg zo nodig voor ondersteuning de verantwoordelijke voor Informatieveiligheid.

TIP 3

Geef het goede voorbeeld

Draag het belang van informatiebeveiliging uit binnen je afdeling. Geef het goede voorbeeld aan collega’s door zelf beveiligingsbewust te werken.

TIP 4

Stuur en beloon veilig gedrag

Instrueer en motiveer medewerkers op veilig gedrag conform het interne beleid en wet- en regelgeving. Onderneem actie bij onveilige situaties en incidenten. Neem veilige omgang met informatie mee in de beoordeling van je medewerkers.

KWALITEIT VEILIGHEID

90 dagen

INFORMATIE-VEILIGHEID

Doe de test!

- ✓ Je weet hoe te handelen bij een datalek
- ✓ Tips voor het voorkomen van datalekken
- ✓ Je weet hoe je moet omgaan met Veilig mailen
- ✓ Je weet hoe je een veilig wachtwoord kunt maken
- ✓ Test je kennis op www.zorgzekeren.nl
- ✓ Meer informatie of vragen?

zgt

Topzorg voor uw levenskwaliteit