

Veilig omgaan met patiëntgegevens



Bedoeld voor iedereen die in de huisartszorg werkt



Makkelijk toe te passen



Overzicht van werkwijze



Dosering: dagelijks toepassen



Veilig omgaan met patiëntgegevens is makkelijk en kost weinig tijd

Communiceren



Realiseer je dat mensen kunnen meeluisteren met gesprekken **aan de balie**. Beperk vragen naar persoonsgegevens.



Zorg dat niemand kan meeluisteren met **privacygevoelige gesprekken**. Sluit de deur van de kamer, een openstaand raam en voer telefoongesprekken in een afgesloten ruimte.



Gebruik een **veilig communicatiekanaal** voor gesprekken met patiënten en zorgprofessionals, zoals via een e-consult of beveiligde mail.



Controleer of je **gegevens mag delen** met de ontvanger.



Verstuur bestanden met **personeelsgegevens** via een beveiligde omgeving.



Zorg dat niemand ongewenst kan **meekijken** op je scherm.

Tip



Bespreek in je organisatie wie de werkprocessen aanpast.

Vernietigen



Haal **stickers** met patiëntgegevens overal vanaf en vernietig deze.



Scan **patiëntuitslagen** in, voeg ze toe aan het dossier en stop ze daarna in de versnipperaar of container voor vertrouwelijke documenten.



Stop **aantekeningenbriefjes** met patiëntgegevens in de versnipperaar of de container voor vertrouwelijke documenten.



Stel in dat je **computerprullenbak** dagelijks automatisch geleegd wordt.



Stel in dat de **downloadmap** op je computer elke dag wordt geleegd.



Verwijder **documenten** van de server nadat je ze in het juiste systeem hebt opgeslagen.

Tip



Probeer zoveel mogelijk papierloos te werken.

Opbergen



Lock je scherm bij het verlaten van je werkplek met een sneltoets.



Gebruik **twefactorauthenticatie (2FA)** voor extra beveiliging bij het inloggen.



Haal papieren direct op na **printen**.



Berg **medische en patiëntgegevens**, zowel digitaal als op papier, veilig op (zoals labuitslagen en verwijsbrieven).



Als je **buiten het HIS** opslaat, sla documenten dan ook in de juiste beveiligde mappen op.



Sluit kasten af met een sleutel die alleen personeel heeft.



Zorg dat iedereen een **eigen inlog** heeft voor computers en programma's.



Gebruik **beveiligde netwerken en programma's**, en deel nooit je wachtwoord.



Bewaar **personeelsgegevens** zoals salarisstroken en ziekmeldingen in een beveiligde map.

Tip



Bespreek in je organisatie wie het systeem veilig kan inrichten.



**Informatieveilig
gedrag in de zorg**