Privacy is ook mijn zorg!

Ik ga integer en zorgvuldig om met (persoons)gegevens

Help elkaar om samen integer en zorgvuldig om te gaan met (persoons)gegevens:

Geef elkaar tips!

Plak een post-it op een situatie die niet helemaal in orde is. Schrijf jouw tip erop.

Neem voor meer informatie binnen uw organisatie contact op met:

.....

JOUW ACCOUNT IS ALLEEN VOOR JOU

Privacy en informatieveiligheid

In de praktijk blijkt dat accountgegevens met elkaar gedeeld worden. Door het gebruik van andermans 'identiteit' krijg je toegang tot vertrouwelijke of gevoelige informatie waarvoor je geen toegang had. Geef anderen geen toegang tot jouw account. Is dit toch wel gebeurd? Verander dan meteen je inloggegevens.

Alleen personen met een behandelrelatie met de patiënt/cliënt mogen toegang hebben tot patiënt/cliëntgegevens. Maar ook dan mag je geen inloggegevens van iemand anders gebruiken om de gegevens te bekijken.
Jammer genoeg zijn er praktijkvoorbeelden waarbij op onrechtmatige wijze in dossiers van patiënten/cliënten is gekeken. Naast dat dit erg vervelend is voor een patiënt/cliënt, levert dit een organisatie een fikse boete op: soms zelfs van bijna een half miljoen euro!
Stel dat jij jouw accountgegevens had gedeeld met collega's, maar niet zelf in het dossier had gekeken? Hoe bewijs je dan dat jij het niet bent geweest?

Hoe zorg je dat jij de enige bent die jouw account gebruikt?

Een wachtwoord in combinatie met een token/ UZI-pas of gebruikersnaam is een middel om toegang te krijgen tot netwerken, e-mail, databases, websites, etc. Met deze toegang kan een ander onder jouw naam activiteiten uitvoeren. Als die ander per ongeluk of expres onverantwoordelijk omgaat met jouw gegevens, kan dit schade toebrengen aan een cliënt/patiënt of de organisatie. Jij kan hierdoor in de problemen komen.

Het delen van accountgegevens veroorzaakt mogelijk onbedoeld een datalek: iemand kan zonder toestemming inzicht hebben in gegevens die hij of zij eigenlijk niet mag zien.

- ➔ Deel jouw inloggegevens niet.
- ➔ Schrijf je inloggegevens ook niet op. Iemand kan dit vinden en misbruiken.

Tip: Beveilig jouw account door twee-factor-authenticatie te gebruiken. Je hebt dan meer informatie nodig om in je account te komen: een code of wachtwoord én specifieke lichamelijke kenmerken (bijv. je vingerafdruk of gezicht). Op de meeste telefoons, tablets en laptops is dit tegenwoordig mogelijk.

Autorisatie: wat mag je met jouw account zien en doen?

Om gevoelige gegevens over personen of over de eigen organisatie te beveiligen kent jouw organisatie bepaalde rechten toe voor het gebruik van systemen en applicaties. Je krijgt zo alleen toegang tot de gegevens die je nodig hebt om je werk goed uit te voeren. Als jij vermoedt dat je te veel kan zien of doen in een systeem geef je dit door aan je leidinggevende.

Ben jij op de hoogte wat het autorisatiebeleid is van jouw organisatie? Of weet jij wie er in jouw organisatie de autorisatie bepaalt?

"Ik laat niemand met mijn gegevens inloggen en ik log zelf ook niet in met gegevens van anderen!"

Waarom werk jij alleen op jouw account?

Via jouw account kan jij alleen gegevens zien en wijzigen waar jij toegang toe hebt. Veel patiënt/cliënt informatiesystemen houden een logboek bij van inzagen en wijzigingen van dossiers. Je kunt in het systeem achterhalen wie op welke datum wat heeft aangepast. Organisaties controleren of dossiers zijn ingezien.

Als je jouw accountgegevens hebt gedeeld, is het moeilijk te achterhalen wie nu precies de aanpassing heeft gemaakt. Er zijn voorbeelden van organisaties die medewerkers hiervoor op staande voet hebben ontslagen.