Praktische privacytips

voor zorgprofessionals

Nedap healthcare

Parallelweg 2
7141 DC Groenlo

healthcare@nedap.com

+31 (0) 544 471 677

Praktische privacytips voor zorgprofessionals

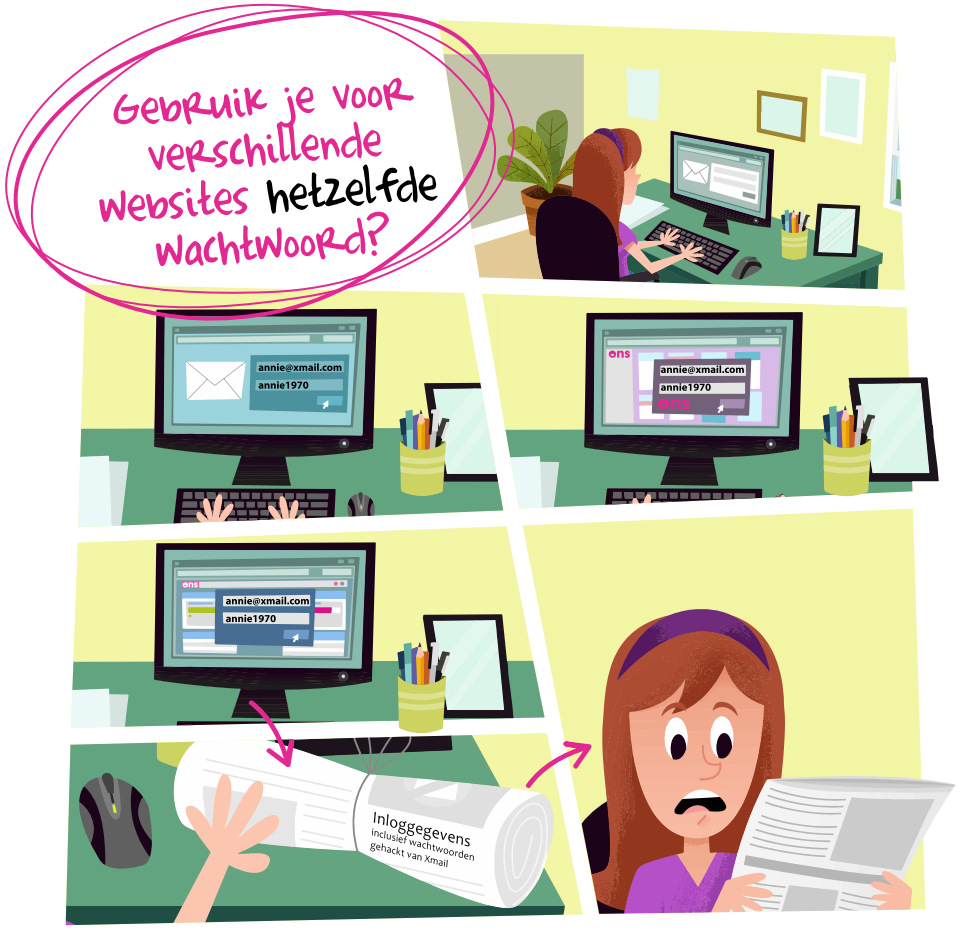
nedap

Praktische privacytips voor zorgprofessionals

Tijdens je werk als zorgprofessional kunnen alledaagse situaties je zomaar in een gelegenheid brengen waarin onbewust de privacy van cliënten of collega's wordt geschonden. Gelukkig zijn er met wat eenvoudige tips al veel verbeteringen te behalen. Sommige tips lijken erg vanzelfsprekend en overdreven, maar zonder naleving en bewustwording van deze situaties kun je de privacywetten al snel overtreden. Het zit soms al in de meest simpele situaties. Na het lezen van deze praktische tips zijn jij en je collega's op de hoogte van wat privacywetgeving voor de zorg op hoofdlijnen betekent.

Herken je de volgende situaties?

Inhoud



Hetzelfde wachtwoord voor meerdere websites gebruiken is soortgelijk aan dezelfde sleutel gebruiken voor ieder slot.

Als een hacker jouw wachtwoord van een website in handen krijgt, kijkt hij vaak meteen even na of het wachtwoord ook op andere websites te gebruiken is. Dit kan ook een zorgapplicatie zijn, waarin alle cliëntgegevens staan.

Het is daarom van belang om verschillende wachtwoorden voor je accounts te gebruiken. Want naast je eigen gegevens uit bijvoorbeeld je privé e-mail, kunnen ook de gegevens van cliënten uit de applicaties op straat komen te liggen.

TIP!

Een wachtwoord-manager is een handig hulpmiddel om verschillende, moeilijke wachtwoorden aan te maken en te helpen onthouden.
Het voordeel hiervan is dat je maar één goed wachtwoord hoeft te onthouden. Als je op internet zoekt naar wachtwoordmanagers, komen er allerlei gratis en betaalde wachtwoordmanagers naar voren.

Via je computer heb je toegang tot veel vertrouwelijke informatie. Denk hierbij aan medische (dossier)gegevens, salarisgegevens, vertrouwelijke documenten en/of cliëntgegevens.

Je wilt natuurlijk voorkomen dat anderen deze gegevens kunnen inzien terwijl ze hier geen toegang toe mogen hebben.

Als je bijvoorbeeld wegloopt van je computer - ook al is het maar even om bijvoorbeeld een kopje koffie te halen - dan kan er al iemand per ongeluk op je computerscherm gegevens zien of raadplegen. Dit is ook al een datalek! Ook is in het geval van misbruik achteraf niet meer te achterhalen of jij of iemand anders achter de computer heeft gezeten.

TIP!

Maak er een gewoonte van om je scherm te vergrendelen zodra je wegloopt van je computer, ook al ben je maar even weg.

Wanneer je met anderen overlegt kan het zomaar gebeuren dat er iemand meeluistert.

Dit is ook al een datalek! En in de zorg gaat het al gauw over cliënten met privacygevoelige informatie. Om te voorkomen dat buitenstaanders deze informatie opvangen is het van belang dat je in een afgesloten ruimte zit, zeker tijdens een cliëntoverleg.

Datalek?

Definitie: het opzettelijk of onopzettelijk vrijgeven van (beveiligde) informatie aan een onvertrouwd publiek.

Wist je dat het in beginsel verboden is om een ID-kaart, rijbewijs of paspoort te kopiëren?

In de praktijk zien we echter dat bijvoorbeeld tijdens een cliëntintake om een kopie wordt gevraagd. Voor de zorg zijn deze gegevens van belang:

- het soort identiteitsbewijs (paspoort, rijbewijs of ID-kaart);
- het documentnummer.

Voorbeeld "Paspoort, NWLFR3706".

Tevens moet het BSN worden vastgelegd, maar dit nummer mag nooit met een identiteitsbewijs mee worden gekopieerd. Deze moet je daarom ergens anders opschrijven.

De belangrijkste reden voor dit verbod is om identiteitsfraude te voorkomen. Identiteitsfraude betekent dat iemand anders misbruik maakt van jouw identiteitsgegevens; bijvoorbeeld door een abonnement op jouw naam af te sluiten.

TIP!

Is het toch noodzakelijk om een kopie te maken? Gebruik dan een ID-cover. Nedap heeft speciale covers voor de zorg gemaakt, die alleen het documenttype, documentnummer en de voor- en achternaam laten zien.

Meer informatie over dit onderwerp staat op www.rijksoverheid.nl/onderwerpen/identiteitsfraude

In de praktijk zien we dat er in de zorg vaak gebruik wordt gemaakt van een 'groepsapp' of privé e-mail om te overleggen of om elkaar te informeren.

Het is volgens toezichthouders niet toegestaan om via privé e-mail te communiceren over cliënten. Bij verschillende gratis berichtenapps of sociale media is het bovendien vaak onbekend of zij de privacyrichtlijnen naleven en wat er met alle gesprekken (en daarmee mogelijke cliëntgegevens) wordt gedaan. Het is daarom van belang dat je samen met je team een veilige communicatietool gebruikt als het over cliëntgegevens gaat.

TIP!

De Nedap Ons app is een voorbeeld van een veilige communicatietool, speciaal ontwikkeld voor de (thuis)zorg. Deze applicatie houdt rekening met de privacywetgeving en veiligheid. Met de app kun je ook foto's maken en versturen; de foto's blijven niet op de telefoon of app opgeslagen, maar komen in het ECD terecht. Download de app gratis via: **www.nedapons.nl**

Soms ontkom je er niet aan om documenten te printen.

Maar als iemand door jouw toedoen een document in handen krijgt met daarop bijvoorbeeld cliëntgegevens of andere privacygevoelige informatie, dan overtreed je daarmee de wet.

Helaas zijn er genoeg praktijkvoorbeelden. Zo is het weleens voorgekomen dat er een uitgeprinte cliëntroute met sleutelgegevens in een gehuurde auto is teruggevonden. Dit is natuurlijk per ongeluk gebeurd, maar het had grote gevolgen voor de betrokkenen.

Vraag jezelf daarom in het kader van de privacy van cliënten altijd af of het écht nodig is om een printje te maken. En als je dat toch doet, vergeet dan niet om na gebruik het printje te vernietigen in een papierversnipperaar.

AVG?

De **Algemene Verordening Gegevensbescherming (AVG)**, geeft richtlijnen en regels ter bescherming van de privacy van personen. De wet is van toepassing op alle vormen van het verwerken van persoonsgegevens. Dit omvat het gehele proces van verkrijgen, combineren, bewerken, opslaan en doorgeven tot vernietigen van gegevens. Op de naleving van de AVG wordt toezicht gehouden door de Autoriteit Persoonsgegevens (AP).

Om te voorkomen dat anderen met jouw gegevens kunnen inloggen, bieden veel websites zogenaamde tweefactor authenticatie aan.

Naast het invoeren van je gebruikersnaam en wachtwoord, ontvang je een eenmalige code bij het inloggen, bijvoorbeeld via SMS. Zo is zeker dat jij zelf degene bent die probeert in te loggen en niet iemand anders. De bekendste voorbeelden van websites die tweefactor authenticatie gebruiken zijn internetbankieren en DigID.

Veel websites bieden deze extra beveiliging bij het inloggen, maar je moet het vaak nog wel apart inschakelen. Websites zoals Facebook, Gmail en Hotmail ondersteunen tweefactor authenticatie, alleen staat dit niet standaard aan.

Tweefactor wat?

Tweefactor authenticatie heet zo, omdat er twee factoren nodig zijn voor het inloggen. Iets wat je weet (gebruikersnaam, wachtwoord) en iets wat je bezit (telefoon, digipass).

Heb je de bijbehorende filmpjes al gezien?

Deel de filmpjes en de tips met je collega's zodat zij ook op de hoogte zijn van de privacywetgeving. De filmpjes vind je op het Nedap Ons YouTube kanaal.

www.youtube.com/user/**nedaphealthcare/videos**

nedap