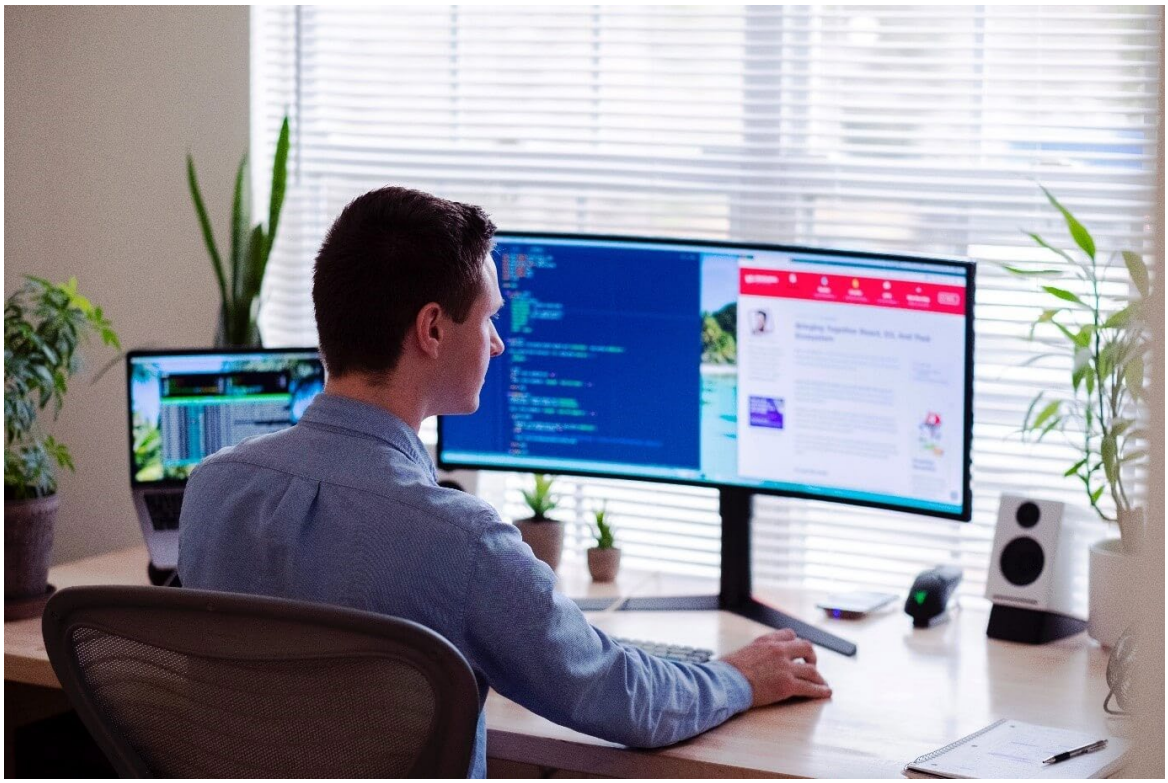

CHECKLIST INFORMATIEBEVEILIGING

AAN DE SLAG MET DIGITALE VAARDIGHEDEN
TRAINING: INFORMATIEBEVEILIGING EN PRIVACY

DIGIVAARDIG IN DE ZORG

CHECKLIST INFORMATIEBEVEILIGING VOOR MEDEWERKERS

Als zorgprofessional werk je met privacygevoelige persoonsgegevens. Veel van deze informatie is gedigitaliseerd. Waar je vroeger dossiers in kasten kon opbergen, moet je nu andere maatregelen nemen om persoonsgegevens te beschermen.

Onder de wet Algemene verordening gegevensbescherming (AVG) vallen regels die zorgprofessionals ook dwingen zorgvuldig om te gaan met privacygevoelige informatie. Deze checklist is bedoeld voor alle in- en externe medewerkers en dient als hulpmiddel om met elkaar tot een betere informatiebeveiliging te komen.

Deze checklist is gedeeltelijk overgenomen van www.onzehuisartsen.nl. Daar waar patiënt staat, kan ook cliënt worden gelezen.

Werkwijze

Voor een éénduidige werkwijze graag gebruik maken van volgende tekentjes:

☒ Afkruisen als jij of de organisatie hieraan voldoet.
? Als je het niet weet, geef dit aan met een vraagteken en plaats een opmerking onderaan het lege vak van het thema.
! Als jij of de organisatie niet aan dit punt voldoet of je bent van mening dat er risico's dreigen, plaats dan een opmerking onderaan het lege vak van het thema.
☐ Laat het vakje open indien dit niet van toepassing is voor jou in jouw functie.

Wachtwoord

☐	Houd het wachtwoord van je computer geheim. Geef nooit je inlogcode en wachtwoord aan een ander. Je bent namelijk aanspreekbaar op wat er onder je eigen account gebeurt en wat jouw account doet, wordt gelogd.
☐	Werk niet onder de inlogcode van een ander.
☐	Zeg altijd "NEE" als een internetapplicatie "Wachtwoord onthouden?" vraagt. Een onbevoegde met toegang tot het apparaat waarop je werkt zou dan namelijk moeiteloos bij je gegevens kunnen komen en zich als jou kunnen voordoen in die internetapplicatie.
☐	Zorg ervoor dat je werk- smartphone, tablet en laptop voorzien zijn van een wachtwoord. Gebruik dit wachtwoord ook, dus vergrendel het apparaat na gebruik, bijv. door het scherm van de laptop dicht te klappen.

☐	Gebruik je werkwachtwoord niet voor niet-werk gerelateerde applicaties op internet. Een onbevoegde zou kennis kunnen nemen van jouw werk- wachtwoord.

Notities:

Werkplek

☐	Berg vertrouwelijke informatie op in afgesloten kasten en laden. Laat nooit vertrouwelijke gegevens liggen op je bureau als je niet zelf aanwezig bent (clear desk).
☐	Gooi vertrouwelijke gegevens op papier na gebruik weg in een papierversnipperaar of afgesloten bak.
☐	Log uit of vergrendel je pc (Windowstoets + L) als je je werkplek verlaat (clear screen)
☐	Bij wat oudere pc's: Zet je pc uit aan het eind van de werkdag. Bij het opnieuw opstarten worden automatisch actuele antivirus updates op je pc geïnstalleerd.
☐	Denk na over hoe je informatie op je bureau hebt liggen terwijl je er mee werkt. Kunnen onbevoegden zomaar meekijken? Of meekijken op het scherm?
☐	Laat de cliënt juist wel of juist niet meekijken op het scherm, afhankelijk van wat je doet op de computer. Schaf desgewenst een zwenkarm of extra scherm aan. De cliënt laten meekijken verhoogt de betrokkenheid bij het zorgproces en de kwaliteit van de registratie. Bovendien heeft de cliënt inzagerecht in zijn dossier.
☐	Wees terughoudend met het noemen van namen van cliënten in situaties waarin anderen je kunnen horen, zoals in de huiskamer, in de gang of aan de telefoon. Hetzelfde geldt voor naamgeving van bestanden en voor de inhoud van losse documenten die zijn opgeslagen op een usb-stick, laptop of SD-kaartje (foto's, films).
☐	Thuiswerken: zorg ervoor dat je thuis-PC of thuis-laptop voldoende is beveiligd en niet wordt gebruikt voor m.n. gratis spelletjes. Het risico bestaat namelijk dat er een keylogger wordt geïnstalleerd die alles wat je intypt, bijv. wachtwoorden en cliëntgegevens, doorgeeft aan een datadief.

Notities:

E-mail, WhatsApp, andere elektronische communicatie en papieren post

☐	Verstuur naar een externe bestemming geen cliëntgegevens via de gewone e-mail (Outlook). Als de eigen zorgorganisatie TLS[1] aan heeft staan op de mailservers en de ontvanger van je mail dat ook heeft, is de verbinding veilig. Dan kunnen hoog-vertrouwelijke gegevens over de gewone mail worden verstuurd, mits de mailboxen aan beide kanten veilig zijn (toegang door anderen, geen synchronisatie naar onbeveiligde smartphone, geen autoforward naar onveilig mailadres).
☐	Acceptabele middelen om veilig elektronisch te communiceren zijn: – Een communicatieplatform in een cliëntenportaal. Dit heeft de voorkeur, ook boven secure e-mail, omdat alle cliëntgegevens dan zoveel mogelijk bij elkaar blijven. – Versleutelde e-mail.
☐	Stel dat je (beveiligd) mailt of berichten uitwisselt met cliënten en/of wettelijk vertegenwoordigers, spreek dan van tevoren af via welk e-mailadres je je tot hen richt en houd je daaraan. Gebruik dus niet 'reply' als de cliënt informatie vanaf een ander e-mailadres stuurt, bijvoorbeeld vanuit zijn werk. Maak duidelijk voor welke situaties de berichten-uitwisseling bedoeld is (niet voor noodgevallen) en vraag toestemming van de cliënt om naar hem/haar te mogen mailen. Leg deze toestemming vast in het ECD.
☐	Volg het WhatsApp beleid van de organisatie.[2]
☐	Identificeer een cliënt waarover je elektronisch communiceert met een externe zorgaanbieder altijd met zijn Burgerservicenummer (BSN). Dit is verplicht volgens de Wet gebruik Burgerservicenummer in de zorg (Wbsn-z). Ga verder spaarzaam om met identificerende cliëntgegevens en zet geen identificerende gegevens in de header (onderwerp) van een bericht.
☐	Download geen bestanden uit onbekende bron vanaf je inkomende privé mail op het netwerk van de organisatie. Het risico op malware infectie zoals virussen is namelijk groot doordat de verbinding met je privé mail beveiligd is waardoor het netwerk van de organisatie binnenkomende bestanden niet inhoudelijk kan scannen op malware.

[1] TLS = Transport layer security. Met een 'vinkje' op de mailserver zet een ICT beheerer TLS aan. Met Checktls.com controleer je of op het domein van de eigen zorgorganisatie en van de ontvangende organisatie TLS aan staat (domein = wat staat achter @ in het mailadres).

[2] Het bedrijf Whatsapp is eigendom van Facebook/META. Risico is dat Facebook je berichten kan inzien en elementen uit de inhoud toevoegt aan het 'profile' van jezelf en van de cliënt waarmee je Whatsappt. Ook geef je, als je Whatsapp installeert, toestemming voor toegang op je contactgegevens. Facebook heeft dus inzage in je contacten. Dit betekent dat je cliënt die in je contacten staat, bij Facebook bekend kan komen te staan als cliënt van jou, ook al Whatsapp je niet met die cliënt. Advies: gebruik Signal private messenger in plaats van Whatsapp en verwijder Whatsapp van je werktelefoon.

☐	Open geen bijlage of link in verdachte mails. Verdacht is: onbekende afzender, vreemde teksten. Reageer niet maar verwijder deze mail.
☐	Open alleen bestanden en links van een vertrouwde afzender. Wil je een link checken op veiligheid? https://checkjelinkje.nl/
☐	Het gebruik van de gewone mail voor het extern mailen van administratieve personeelsgegevens, bedrijfsgegevens en andere vertrouwelijke niet-cliëntgegevens is toegestaan.
☐	Intern mailen van cliëntgegevens via de gewone mail is toegestaan. Verwijder echter ontvangen en verstuurde mails met cliëntgegevens uit je mailbox na gebruik. Reden is dat het risico van datalekkage via smartphone bestaat, de autorisatie op de mailboxen te ruim kan zijn en cliëntgegevens thuis horen in het ECD.
☐	Stuur geen gevoelige informatie door naar privé mail-accounts, ook niet naar de cliënt. Je weet niet wie toegang heeft tot de mailbox.
☐	Zolang er geen goede elektronische alternatieven zijn, is de brief een acceptabel medium voor het versturen van hoog vertrouwelijke informatie. Papieren post geldt vanwege het briefgeheim als veilig voor het versturen van hoog vertrouwelijke informatie. In de praktijk is dat niet altijd zo, bijvoorbeeld omdat gezinsleden de brief kunnen openen. Het aangetekend versturen van papieren post is een maatregel om achteraf te kunnen nagaan of het poststuk de geadresseerde heeft bereikt. Het is geen maatregel tegen datalekkage.
Notities:	

Internet

☐	Wees voorzichtig met het binnenhalen van bestanden van internet, met name .exe bestanden.
☐	Zet geen vertrouwelijke gegevens op een ‘vreemde’ website, ook al zijn de gegevens beveiligd met een wachtwoord. Plaats dus géén vertrouwelijke gegevens in Dropbox, Google Drive of in privé mail.
☐	Gebruik je professionele e-mailadres niet voor privéaangelegenheden met een zakelijk karakter. De zorgorganisatie is daarin namelijk geen partij.

☐	Bezoek geen sites die een verhoogd risico op malware infectie met zich meebrengen, zoals het geval is bij spelletjes en porno.
Notities:	

Wifi

☐	Thuiswerken op het ECD via openbaar wifi, bijvoorbeeld in de trein, is toegestaan mits er allereerst een beveiligde verbinding (VPN) wordt gelegd en daarna pas wachtwoorden etc. over de lijn gaan. Als je niet zeker weet dat het veilig is: niet doen. Zorg er voor dat je via openbaar wifi geen minder goed beveiligde applicaties benadert, zoals Facebook. Gegevens en wachtwoorden kunnen worden onderschept en je laptop kan worden overgenomen, ook zonder dat je dat merkt. Het risico dat je laptop wordt gehackt, is groter als je software, zoals Windows, niet is bijgewerkt naar de nieuwste versie.
☐	4G/5G is altijd veilig. De verbinding van 4G/5G loopt niet via internet maar via het telefoonsignaal. Technisch wordt dit gerealiseerd door een simkaart in je laptop of tablet, door een dongel (USB-stick met simkaart), door mifi (werkt als een dongel) of door tethering via een kabeltje (doe dit niet via wifi in openbaar gebied!) waarbij je smartphone werkt als dongel.
☐	Laat je laptop, tablet of telefoon niet automatisch verbinding maken met wifi. Een hacker kan net doen of hij je 'thuis' router is ook al ben je in een openbare ruimte, en maakt verbinding met je device.
☐	Kies zorgvuldig je wifi verbinding, niet een naam die er op lijkt. Dit kan een hacker zijn.
Notities:	

Social media[3]

☐	Wees voorzichtig met wat je plaatst op social media. Noem nooit de naam van een cliënt of collega en beschadig de reputatie van de zorgorganisatie niet.

[3] Zie ook de KNMG handreiking Arts en social media https://www.knmg.nl/advies-richtlijnen/dossiers/sociale-media.htm

☐	Bescherm je inlogcode en wachtwoord op social media heel goed; iemand die zich als jou voordoet, kan je identiteit misbruiken, bijvoorbeeld richting een cliënt.
☐	Scherm je profiel voldoende af op je social media.
☐	Wees alert op het vrijgeven van privé informatie op internet. Privé informatie over de begeleider is niet altijd wenselijk in de zorgrelatie.
☐	Nodigt een cliënt je – in je hoedanigheid als professional - uit als 'vriend' op een sociale netwerksite? Accepteer de uitnodiging niet blindelings. Check of er binnen de zorgorganisatie een social media protocol bestaat die richtlijn kan geven op dit punt.
☐	Als je elektronisch communiceert met de cliënt, check dan of de cliënt een wachtwoord of pincode (dit is minder sterk) heeft staan op zijn smartphone of tablet. Je wil niet dat jouw communicatie op straat ligt als de cliënt zijn smartphone heeft verloren.
☐	Communiceer met de cliënt via een cliëntenportaal of e-health applicatie als die er is.
☐	Houd er rekening mee dat communicatie die in e-mail, WhatsApp etc. is vastgelegd, op een social medium zoals Facebook kan worden gepubliceerd. Met één druk op de knop kan een hele berichtenwisseling uit WhatsApp worden gemaild.
Notities:	

USB stick, camera, SD kaartje, telefoon, DVD, laptop en andere externe opslag

☐	Alleen in het ECD worden cliëntgegevens permanent opgeslagen. Praktische uitzonderingen zijn: – Het papieren archief met cliëntdossiers; – De back-up, voor zover je die zelf maakt; – Het cliëntportaal, voor zover je de berichten daarin ziet als onderdeel van het (medisch) dossier. Het is aan de zorgorganisatie om te bepalen in hoeverre informatie in het portaal al dan niet tot het ECD behoort. Dit is m.n. van belang voor de bewaartermijn (15 jaar). Als je de inhoud van het cliëntportaal niet ziet als deel van het dossier, mag je deze inhoud verwijderen als het dossier is bijgewerkt.

☐	Wil je hoog-vertrouwelijke gegevens mee naar buiten nemen op een onbeveiligd medium zoals DVD, SD kaart of onbeveiligde USB stick, beveilig dan het bestand dat je verstuurt en/of het medium (encryptie). Hoog-vertrouwelijke gegevens zijn cliëntgegevens en hoog-vertrouwelijke gegevens van medewerkers.
☐	Sla bij voorkeur geen telefoonnummer van de cliënt op in je mobiele telefoon, zeker niet met naam en toenaam. Gebruik in plaats daarvan het telefoonnummer dat is vastgelegd in het ECD. Risico is dat als de telefoon wordt gestolen en onvoldoende is beveiligd, deze gegevens 'op straat liggen'. Ook kan de dief richting cliënten net doen of hij de begeleider is, bijv. via sms of WhatsApp (identiteitsfraude).
☐	Noem geen naam en toenaam van de cliënt in je Outlook agenda en in de (interne) mail. Beperk je bijv. tot intialen en een cliëntnummer. Agenda en mail worden gesynchroniseerd naar je smartphone. Als je smartphone wordt gestolen, liggen deze gegevens 'op straat'. Als de smartphones wel beschermd is met een wachtwoord maar de gegevens die er op staan, niet zijn versleuteld, dan kan een hacker daar met weinig inspanning bij komen.
☐	Als je telefoon wordt gestolen, neem dan direct contact op met de leverancier of met het aandachtfunctionaris AVG om je simkaart te laten blokkeren. Dit vermindert het risico dat je contactgegevens in verkeerde handen vallen (als die alleen op de simkaart staan) en er kan niet meer vanuit jouw nummer worden gebeld (identiteitsfraude en financiële schade).
☐	Vind je een USB-stick, CD-ROM of DVD van onbekende herkomst, schuif hem dan nooit in je pc. Er kan een zelf-startend programma op staan dat spyware installeert of de macht over je pc overneemt. Vind je een onbekende USB-stick, geef deze aan je leidinggevende of aan je aanspreekpunt voor informatiebeveiliging.
Notities:	

Wat kun jij samen met je collega's doen?

☐	Maak afspraken met elkaar over privacy en informatiebeveiliging.
☐	Spreek elkaar aan op onvoldoende informatiebeveiliging.
☐	Vraag het als je iets niet weet.

☐	Meld een datalek direct bij de aandachtfunctionaris AVG. Een datalek betekent dat er daadwerkelijk vertrouwelijke persoonsgegevens in handen van onbevoegden zijn gekomen of 'op straat liggen'. Ook onherstelbaar verlies of verminking van gegevens valt onder een 'datalek'.[4] Leg de datalek vast in het meldingssysteem voor MIC-meldingen van de organisatie (MIC = Melding Incident Cliënt)
☐	Signaleer je dat informatie onvoldoende beschikbaar is, onvoldoende betrouwbaar is of onvoldoende is afgeschermd, meld dit dan in het team 'bij de koffie', bij je lokale aanspreekpunt voor de informatiebeveiliging, bij de verantwoordelijke arts of in het MIC-meldingssysteem.
☐	Als een cliënt of wettelijk vertegenwoordiger je opmerkzaam maakt op een informatiebeveiligingsrisico of -incident, bespreek dit dan in het team of met de aandachtfunctionaris AVG en maak er melding van in het MIC-systeem. Informeer de cliënt of wettelijk vertegenwoordiger over wat er gebeurt met de melding of laat de verantwoordelijke begeleider dat doen.
☐	Denk na over wat je doet, hoe je praat, hoe je handelt. Kijk eens kritisch naar je eigen handelen.
Notities:	

Bron: https://www.onzehuisartsen.nl/zorgprofessionals/diensten/informatiebeveiliging/checklist-informatiebeveiliging/

Deze module is gemaakt door Xiomara Vado Soto voor Digivaardig in de Zorg in samenwerking met Daan Brinkhuis van 's Heeren loo.

Heb je opmerkingen of vragen over dit lesmateriaal? Mail dan naar info@digivaardigindezorg.nl

[4] Zie ook de website van KNMG over Datalekken https://www.knmg.nl/actualiteit-opinie/nieuws/nieuwsbericht/handreiking-voor-naleving-meldplicht-datalekken.htm