Checklist Informatiebeveiliging voor praktijkhouder

Deze checklist is bedoeld voor alle in- en externe medewerkers en dient als hulpmiddel om met elkaar tot een betere informatiebeveiliging te komen. In de lege kolom kun je specifieke praktijkinformatie/ knelpunten noteren. Deze knelpunten kunnen dan in een plan van aanpak worden opgelost.

1 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 je apparaat waarop je werkt zou dan namelijk moeiteloos bij je gegevens kunnen komen en zich als jou kunnen voordoen in die internet applicatie.	
☐	Zorg ervoor dat je 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 zo mogelijk een toegangscode met printen.	
☐	Gebruik je praktijkwachtwoord niet voor niet-praktijk applicaties op internet. Een onbevoegde zou kennis kunnen nemen van je praktijk wachtwoord.	

2 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 patiënt 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 patiënt laten meekijken verhoogt de betrokkenheid bij de behandeling en de kwaliteit van de registratie. Bovendien heeft de patiënt inzagerecht in zijn dossier.	
☐	Wees terughoudend met het noemen van namen van patiënten in situaties waarin anderen je kunnen horen, zoals bij de balie, 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).	
☐	Telewerken: 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 patiëntgegevens, doorgeeft aan een datadief.	

3 E-mail en papieren post

☐	Verstuur naar een externe bestemming geen patiëntgegevens via de gewone e-mail (Outlook). Gegevens met vertrouwelijkheidsniveau 'Midden' mogen wel over de gewone e-mail worden verstuurd. Zie voor de vertrouwelijkheidsniveaus de tabel 'Classificatie van gegevens'.	
☐	Acceptabele middelen om veilig elektronisch te communiceren zijn: – Een communicatieplatform in een patiëntenportaal. Dit heeft de voorkeur, ook boven secure e-mail, omdat alle patiëntgegevens dan zoveel mogelijk bij elkaar blijven. – Secure e-mail.	

	– Fax. De verbinding is veilig, de uiteinden niet. De uiteinden (bron en bestemming) vergen extra controle zoals van tevoren bellen als je een faxbericht stuurt.	
☐	Stel dat je (beveiligd) mailt of berichten uitwisselt met patiënten en/of wettelijk vertegenwoordigers, spreek dan tevoren af via welk e-mail adres je je tot hen richt en houd je daaraan; gebruik dus niet 'reply' als de patiënt informatie vanaf een ander e-mail adres stuurt, bijvoorbeeld vanuit zijn werk. Maak duidelijk voor welke situaties de berichten-uitwisseling bedoeld is (niet voor noodgevallen) en vraag toestemming van de patiënt om naar hem/haar te mogen mailen. Leg deze toestemming vast in het HIS. Zie ook de KNMG richtlijn 'Online arts-patiënt contact'.	
☐	Berichtuitwisseling met de patiënt via een onveilig medium zoals onveilige mail of WhatsApp is niet toegestaan, ook al geeft de patiënt akkoord hierop.	
☐	Identificeer een patiënt waarover je elektronisch communiceert met een externe zorgaanbieder altijd met zijn burgerservicenummer (BSN). Dit is verplicht volgens de wet bsn-z. Ga verder spaarzaam om met identificerende patiëntgegevens 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 praktijk. Het risico op malware infectie zoals virussen is namelijk groot doordat de verbinding met je privé mail beveiligd is waardoor het netwerk van de praktijk binnenkomende bestanden niet inhoudelijk kan scannen op malware.	
☐	Open geen bijlage of link in verdachte mail. Verdacht is: onbekende afzender, vreemde teksten. Reageer niet maar verwijder deze mail.	
☐	Open alleen bestanden en links van een vertrouwde afzender	
☐	Het gebruik van de gewone mail voor het extern mailen van administratieve personeelsgegevens,	

	bedrijfsgegevens en andere vertrouwelijke niet-patiëntgegevens is toegestaan.	
☐	Intern mailen van patiëntgegevens via de gewone mail is toegestaan. Verwijder echter ontvangen en verstuurde mails met patiëntgegevens 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 patiëntgegevens thuis horen in het HIS.	
☐	Stuur geen gevoelige informatie door naar privé mail-accounts, ook niet naar de patiënt. 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.	

4 Fax

☐	Bel naar de geadresseerde voordat je een fax met vertrouwelijke informatie gaat versturen en/of vergewis je ervan dat het ontvangende fax apparaat in een afgeschermde ruimte staat. Dit doe je met name bij een 'vreemde' ontvanger en als de fax belangrijk is. Bij fax is de verbinding veilig, maar de uiteinden (plekken van zenden/ontvangen) zijn kwetsbaar. Vraag zonodig een ontvangstbevestiging.	
☐	Gebruik bij voorkeur voorgeprogrammeerde telefoonnummers van de ontvanger. Dit minimaliseert onjuiste adressering.	
☐	Laat geen vertrouwelijke gegevens liggen bij printer en fax.	

5 Voicemail

☐	Als je een patiënt de mogelijkheid geeft je voicemail in te spreken, luister deze dan af en reageer er op. (Dit voorkomt verlies van de ingesproken informatie). Spreek tevoren je beschikbaarheid en reactietijd met de patiënt af.	
☐	Wees voorzichtig met het inspreken van een voicemail bericht aan de patiënt. Een ander kan kennis nemen van de inhoud.	

6 Internet

☐	Wees voorzichtig met het binnenhalen van bestanden van internet, met name .exe bestanden.	
☐	Zet geen vertrouwelijke gegevens op een 'vreemde' internet site, 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 praktijk 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.	

7 Wifi

☐	Telewerken op het HIS via openbaar wifi, bijvoorbeeld in de trein, is toegestaan mits er allereerst een beveiligde verbinding wordt gelegd en daarna pas wachtwoorden etc. over de lijn gaan. Als je niet zeker weet dat het veilig is: niet doen. Zorg er sowieso 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.	
☐	3G/4G is altijd veilig. De verbinding van 3G/4G loopt niet via internet	

	maar via het telefoonsignaal. Technisch wordt dit gerealiseerd door een sim kaart in je laptop of tablet, door een dongel (usb stick met sim kaart), 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.	

8 Social media[1]

☐	Wees voorzichtig met wat je plaatst op social media. Noem nooit de naam van een patiënt of collega en houd het blazoen van de praktijk rein.	
☐	Bescherm je inlogcode en wachtwoord op social media heel goed; iemand die zich als jou voordoet, kan je identiteit misbruiken, bijvoorbeeld richting een patiënt.	
☐	Nodigt een patiënt je – in je hoedanigheid als professional - uit als 'vriend' op een sociale netwerksite? Weiger de uitnodiging, het is verboden vriendschappen met patiënten aan te knopen op sociale media. Je kunt die patiënt het beste vriendelijk laten weten dat het vanuit je beroepsgroep aanbevolen wordt om geen social media vriendschappen met patiënten aan te gaan.	
☐	Scherm je profiel voldoende af op je social media.	
☐	Wees alert op het vrijgeven van privé informatie op internet. Privé informatie over de hulpverlener is niet altijd wenselijk in de behandelrelatie.	

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

☐	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.	

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

☐	Alleen in het HIS worden patiëntgegevens permanent opgeslagen. Praktische uitzonderingen zijn: – Het papieren archief met patiëntdossiers; – De back-up, voor zover je die zelf maakt; – Het patiëntportaal, voor zover je de berichten daarin ziet als onderdeel van het medisch dossier. Het is aan de praktijk om te bepalen in hoeverre informatie in het portaal al dan niet tot het HIS behoort. Dit is m.n. van belang voor de bewaartermijn (15 jaar). Als je de inhoud van het patiëntportaal 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 patiëntgegevens en hoog-vertrouwelijke gegevens van medewerkers. Zie de tabel Classificatie van gegevens. Voor het beveiligen van een bestand is 7-zip een optie. Het 7-zip programma geeft via het opgeven van een wachtwoord een sterke versleuteling.	
☐	Sla bij voorkeur geen telefoonnummer van de patiënt op in je mobiele telefoon, zeker niet met naam en toenaam. Gebruik in plaats daarvan het telefoonnummer dat is vastgelegd in het HIS. Risico is dat als de telefoon wordt gestolen en onvoldoende is beveiligd, deze gegevens 'op straat liggen'. Ook kan de dief richting patiënten net doen of hij de arts is, bijv. via sms of WhatsApp (identiteits-fraude).	

	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 aanspreekpunt van de praktijk naar de leverancier toe om je SIM kaart te laten blokkeren. Dit vermindert het risico dat je contactgegevens in verkeerde handen vallen (als die alleen op de SIM kaart 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.	

10 Foto's

☐	Gebruik voor het maken van foto's en films van cliënten een smartphone of tablet, geen gewone camera. Smartphones en tablets zijn beveiligd, een gewone camera niet.	
☐	Verwijder foto's en films als ze niet meer nodig zijn. Verplaats foto's en films desgewenst naar een map op het praktijknetwerk die voorzien is van de juiste autorisatie.	
☐	Maak alleen met toestemming van de patiënt foto's van de patiënt en leg deze toestemming vast in het HIS.	

☐	Maak foto's en films als professional niet op je privé telefoon. Dit voorkomt dat foto's en films van patiënten tussen de familiefoto's terechtkomen.	
☐	Toon foto's van een patiënt niet aan anderen tenzij de patiënt of wettelijk vertegenwoordiger uitdrukkelijk daarvoor toestemming heeft gegeven en je die toestemming ook hebt vastgelegd in het dossier.	

11 Dossiervoering

☐	Registreer zorgvuldig, volgens de geldende richtlijnen zoals ADEPD. Iemand die het later terugleest, op een andere tijd, andere plaats en in een andere context, moet het kunnen begrijpen.	
☐	Uw dossiers zijn actueel en qua inhoud geschikt voor inzage door de patiënt.	
☐	Noteer geen vermoedens in het dossier maar maak feiten van vermoedens door een check bij de patiënt. Noteer dus niet 'Ik vermoed dat de patiënt ….' maar 'patiënt vertelde …'.	
☐	Houd bij voorkeur geen eigen administratie (werkaantekeningen) bij naast het dossier. Relevante informatie hoort thuis in het dossier en werkaantekeningen zouden ter inzage kunnen komen van onbevoegden.	
☐	Beperk de registratie tot het minimum dat nodig is. Irrelevante informatie versluiert andere informatie, kan lekken en kan een eigen leven gaan leiden.	
☐	Bij voorkeur geen vertrouwelijke gegevens printen. Geprinte informatie kan zoekraken en kan verouderd zijn tijdens het gebruik.	

12 Delen van patiëntgegevens

☐	Geef nooit patiëntinformatie aan iemand die niet rechtstreeks betrokken is bij de patiënt. Zorg ervoor dat je eerst checkt of deze persoon bevoegd is de informatie in te zien.	

☐	Bedenk dat je zelf alleen kennis mag nemen van informatie over de patiënt als je rechtstreeks betrokken bent bij de actuele behandeling van de patiënt. Het feit dat je informatie kunt zien, betekent niet dat je deze informatie ook mag zien.	
☐	Houd er bij het delen van patiëntgegevens rekening mee dat kinderen van 12 tot 16 jaar medeverantwoordelijk zijn voor hun dossier. Houd rekening met de zorg van een goed hulpverlener m.n. bij kinderen jonger dan 12. Dit betekent dat de verantwoordelijkheid van de ouders in bijzondere situaties kan worden overruled.	
☐	Wees je bewust van welke informatie je geeft aan derden, beperk je tot het noodzakelijke. Een teveel aan informatie kan oneigenlijk worden gebruikt.	
☐	Verstuur geen patiëntgegevens aan een organisatie waarvan je weet dat die zijn informatiebeveiliging, bijvoorbeeld de autorisatie, niet op orde heeft. Kom je in een moeilijke situatie wat dit betreft, bespreek dit dan in je team bijv. bij de koffie of escaleer het dilemma aan de verantwoordelijke arts.	
☐	Geef géén patiëntinformatie door als iemand belt (incl. verzekeraar, politie of Raad voor Kinderbescherming), maar noteer de vraag met de gegevens van de beller en stem af met de verantwoordelijke behandelaar, eventueel met de patiënt/ouder. Als je de gevraagde informatie met toestemming mag geven of als de patiënt zelf belt: zorg ervoor dat je ervan verzekerd bent dat je de juiste persoon aan de lijn hebt. Dit doe je bijvoorbeeld door terugbellen via een nummer dat al eerder in je bezit was.	
☐	Let op als een gescheiden ouder belt omdat dit een ouder kan zijn zonder gezag over het kind of omdat de informatie die je geeft oneigenlijk kan worden gebruikt in een conflict tussen de twee echtelieden.	
☐	Laat patiënten tevoren toestemming geven als je patiëntinformatie wilt delen met andere partijen.	

	Registreer in het HIS dat toestemming is verleend.	
☐	De patiënt heeft recht op inzage in zijn dossier en op afschriften hiervan. NB: Toon geen informatie die afkomstig is van gezinsleden of andere bekenden en spreek zo nodig, bijv. in een gespannen gezinssituatie, af dat de patiënt alléén komt.	
☐	Patiënten die ter plekke onder het account van een praktijkmedewerker het dossier bestuderen, blijven tijdens die actie onder toezicht van de praktijk-medewerker. Geef deze patiënt desgewenst een kopie van het dossier mee. Hiertoe mag een wettelijk bepaald geldbedrag in rekening worden gebracht.	
☐	Adresseer vertrouwelijke informatie altijd aan een persoon – niet aan een commissie o.i.d. - of laat als dat verantwoord is de patiënt zijn eigen gegevens meenemen in een niet dichtgeplakte brief. Een verwijsbrief kan wel onpersoonlijk, bijv. naar de poli, worden geadresseerd.	
☐	Informeer een nieuwe patiënt bij aanmelding over hoe er met zijn gegevens wordt omgegaan, met name over wie er inzage zal hebben. Verwijs naar wat er hierover op de website staat.	
☐	Bij dossieroverdracht naar een andere praktijk: Geef het dossier niet mee aan de patiënt zelf omdat het dan niet zeker is dat het dossier (geheel) aankomt bij de nieuwe huisarts[2]. Stuur het dossier op over een beveiligde verbinding, breng het zelf of verstuur het aangetekend.	
☐	Patiëntgegevens worden uitsluitend verwerkt in het verlengde van de behandelrelatie. Patiëntgegevens worden dus niet oneigenlijk gebruikt zoals voor het promoten van een goed doel.	
☐	Wees duidelijk naar je patiënt toe in wat er met zijn gebeurd.	
☐	Het welzijn van de cliënt staat voorop. Dit betekent dat de vertrouwelijkheid van cliëntgegevens kan worden overruled in bijvoorbeeld een crisissituatie of vanuit 'de zorg van	

[2] Zie ook de KNMG richtlijn 'Advies voor overdracht patiëntendossier bij verandering van huisarts, een actualisering'

	een goed hulpverlener'.	

13 Wat kun jij samen met je collega's doen?

☐	Maak afspraken met elkaar over privacy en informatiebeveiliging.	
☐	Spreek elkaar aan op onvoldoende informatiebeveiliging.	
☐	Meld een datalek direct bij de verantwoordelijke arts. Een datalek is 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'.[3] Leg het datalek vast in het meldingssysteem voor VIM meldingen van de praktijk (VIM = veilig incidenten melden).	
☐	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 VIM meldingen-systeem.	
☐	Als een patiënt of wettelijk vertegenwoordiger je opmerkzaam maakt op een informatiebeveiligingsrisico of -incident, bespreek dit dan in het team of met de verantwoordelijke arts en maak er melding van in het VIM systeem. Informeer de patiënt over wat er gebeurt met de melding of laat de verantwoordelijke arts dat doen.	
☐	Denk na over wat je doet, hoe je praat, hoe je handelt. Kijk eens kritisch naar je eigen handelen.	

14 Aanbevelingen voor het management

☐	Wees duidelijk in wie verantwoordelijk is voor welke gegevens c.q. werkprocessen.	

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

☐	Koffie: Neem informatiebeveiliging periodiek op als onderwerp in het werkoverleg en, als dat van toepassing is, het managementoverleg. Vijf minuten per maand is minimaal. Leg de resultaten vast in een 'issue-list'. Ook als er niets significants uit het overleg komt, verdient het aanbeveling om dit feit vast te leggen als bewijsstuk bij audits dat informatiebeveiliging is besproken in de praktijk.	
☐	Maak iemand in de praktijk aanspreekpunt voor informatiebeveiliging. Hij of zij is meldpunt voor informatiebeveiligingsincidenten en –risico's, zorgt voor een periodieke check op de werkvloer, houdt de registratie bij van informatiebeveiliging-issues, zorgt er voor dat informatiebeveiliging in het werkoverleg en - als dat er is - managementoverleg wordt behandeld en ziet er op toe dat informatiebeveiliging-issues weloverwogen vertaald worden naar de bedrijfsvoering (protocollen, techniek, deze checklist).	
☐	Wees duidelijk naar nieuwe medewerkers toe wat er van hen verwacht wordt.	
☐	Voer periodiek een risicoafweging uit.	
☐	Spreek elkaar aan op onvoldoende informatiebeveiliging.	
☐	Wees duidelijk in missie, informatiebeveiligingsbeleid, werkafspraken, protocollen etc.	
☐	Check periodiek of werkafspraken, protocollen etc. worden nageleefd. Dit kan door onderwerpen in het werkoverleg te behandelen, in individuele gesprekken, audits of door middel van een door medewerkers in te vullen enquête.	
☐	Houd een registratie bij van informatiebeveiliging-issues. Dat zijn bevindingen uit de genoemde check of uit meldingen van datalekken, incidenten en risico's.	
☐	Behandel informatiebeveiliging als een gewoon kwaliteitsonderwerp; neem informatiebeveiliging bijvoorbeeld op in intervisiegesprekken met collega's van andere praktijken of in jaargesprekken.	