hadoks

Handreiking

Veilig digitaal werken in de huisartsenpraktijk

Veilig digitaal werken in de huisartsenpraktijk is essentieel voor de bescherming van patiëntgegevens en de continuïteit van de zorg. In een omgeving waarin dagelijks wordt gewerkt met gevoelige informatie, digitale systemen en online toepassingen kunnen risico's ontstaan op het gebied van informatiebeveiliging en privacy.

In deze handreiking richten wij ons op de belangrijkste maatregelen die iedere huisartsenpraktijk zelf kan nemen om digitaal zo veilig mogelijk te werken in de huisartsenpraktijk. Het document is geen volledige uitwerking van NEN 7510 en vervangt geen risicoanalyse, juridisch advies of afspraken met uw ICT-leverancier. Beoordeel daarom periodiek welke aanvullende maatregelen nodig zijn voor uw praktijk, systemen en samenwerkingspartners.

Inhoud

ICT-beheer 3

Toegang en inlogbeveiliging 3

Veilige communicatie en informatie-uitwisseling 4

Opslag en back-up 4

Werken op afstand 5

Omgaan met datalekken 5

Praktijkwebsite en nieuwe patiënten 6

Bijlage I: optimalisatie veilig werken 7

Bijlage II: beheren van wachtwoorden 11

Werkplekbeveiliging 11

Wachtwoordmanager 12

Vergelijking wachtwoordmanagers 13

Bijlage III: Voorbeelden automatische antwoorden 15

ICT-beheer

Wanneer u een product of dienst afneemt bij een ICT-leverancier ontvangt u een service level agreement (SLA). Dit is een contract met afspraken over de kwaliteit van de te leveren diensten. Het gaat hierbij bijvoorbeeld om afspraken over de helpdesk, systeembeschikbaarheid, ontvangen van rapportages en een storingsplan.

- Belangrijke onderdelen rondom beveiliging en continuïteit waar in de SLA aandacht voor moet zijn: afspraken over beveiligingsupdates/patchmanagement, werkwijzen bij incident- en datalekmelding, back-up/herstel en toegangsbeheer.
- Zorg bij iedere computer, laptop en/of tablet voor een bijgewerkte virusscanner. Maak hierover duidelijke afspraken met uw ICT-leverancier, of zorg ervoor dat deze taak geborgd is bij een praktijkmedewerker.

Aandachtspunt: cyberverzekering

Het naleven van de AVG en de NEN 7510-norm is de belangrijkste basis voor het beperken van cyberrisico's.

Voor het ontvangen van directe bijstand of om beschermd te zijn tegen financiële schade bij bijvoorbeeld hacking, datadiefstal of gijzelsoftware, is het mogelijk om een cyberverzekering af te sluiten. Deze verzekering ondersteunt bij incidenten en is bedoeld als vangnet.

Houd er rekening mee dat verzekeraars vaak eisen stellen aan de beveiligingsmaatregelen waar u aan moet voldoen, wilt u in aanmerking komen voor eventuele uitkering.

Toegang en inlogbeveiliging

Toegangsbeveiliging is het geheel van maatregelen dat regelt wie, wanneer en onder welke voorwaarden toegang krijgt tot fysieke locaties of digitale systemen.

Toegangsbeveiliging is één van de belangrijkste onderdelen van informatiebeveiliging. Volgens de NEN 7510 en de AVG is de praktijkhouder verantwoordelijk voor het beschermen van de inloggegevens die toegang geven tot medische dossiers, het HIS, patiëntportalen en andere zorgapplicaties.

Figuur 1: U kunt uw pc gemakkelijk vergrendelen door deze toetsen tegelijkertijd in te drukken op uw toetsenbord.

- Om een goed beeld te krijgen bij welke elementen belangrijk zijn voor een goed beveiligde werkplek, hebben we voor u een overzicht gemaakt van verschillende scenario's in de praktijk en welke scenario's goed zijn, voldoende of nog niet voldoende. Deze vindt u in Bijlage I: elementen goed beveiligde werkplek.
- Om meerdere wachtwoorden veilig op te kunnen slaan adviseren wij gebruik te maken van een zakelijke wachtwoordmanager. Meer informatie hierover vindt u in dit document in Bijlage II: beheren van wachtwoorden.
- U kunt uw computer gemakkelijk vergrendelen door op uw toetsenbord de knoppen Windows+L tegelijkertijd in te toetsen. Zie ook figuur 1.

Veilige communicatie en informatie-uitwisseling

Binnen de patiëntenzorg wordt privacygevoelige informatie uitgewisseld zoals naam, geboortedatum en BSN. Als zorgverlener bent u verantwoordelijk voor het veilig uitwisselen van deze gegevens, bijvoorbeeld met andere zorgverleners of met de patiënt zelf. Binnen de huisartsenpraktijk kunnen verschillende communicatiemiddelen worden gebruikt.

- **Patiëntportaal:** Gebruik voor patiëntcommunicatie een beveiligd patiëntportaal. Dit waarborgt de veiligheid van de communicatie en zorgt voor een directe koppeling met het patiëntdossier.
- **E-mail:** Gebruik een gespecialiseerde en veilige dienst zoals ZorgMail in plaats van gratis diensten zoals Gmail of Hotmail. Wij adviseren u om het algemene praktijkmailadres van de website te verwijderen en deze niet meer te verstrekken aan patiënten. U kunt een automatische reply instellen met uitleg hoe zij u kunnen bereiken, en u kunt een disclaimer plaatsen onderaan de e-mailhandtekening. Voorbeeldteksten van automatische antwoorden vindt u verderop in dit document in Bijlage III: Voorbeelden automatische antwoorden.
- **Siilo:** voor communicatie tussen zorgverleners kunt u Siilo gebruiken. Dit is een veilige berichten-app die speciaal is ontworpen voor professionals in de gezondheidszorg. Het voldoet aan de NTA 7516-norm.

Aandachtspunt communicatie

Gebruik voor communicatie met patiënten en andere zorgverleners géén WhatsApp, Telegram of een andere berichtenservice, vanwege het risico op vermenging met privébestanden en onvoldoende beveiliging.

Aandachtspunt uitwisseling

Maak voor het uitwisselen van medische gegevens géén gebruik van de fax of e-fax. Het risico op verkeerd geadresseerde of onvolledige berichten is groot en voldoet niet aan de huidige AVG- en informatiebeveiligingsnormen.

Opslag en back-up

- Sla patiëntgegevens uitsluitend op in het HIS.
- Vermijd lokale opslag op laptops, USB-sticks of privé apparaten.
- Niet-HIS documenten: Documenten zoals arbeidscontracten slaat u bij voorkeur op in een zakelijke (betaalde), Europese cloud-omgeving. Opslag op NAS-systemen, externe harde schijven of papier wordt afgeraden vanwege risico op diefstal, verlies of schade.
- Beperk toegang tot documenten op basis van rol (autorisatie). U dient ervoor zorg te dragen dat privacygevoelige documenten niet voor iedereen toegankelijk zijn. Zorg ervoor dat privacygevoelige documenten van uw medewerkers alleen toegankelijk zijn voor de persoon die verantwoordelijk is voor deze gegevens (praktijkhouder en/of praktijkmanager). Dit kan in een beveiligde map of door te zorgen dat geautoriseerde personen een persoonlijke inlog hebben met bijbehorende rechten.

- Back-ups: Zorg ervoor dat er automatische back-ups worden gemaakt van belangrijke documenten. Ook moeten back-ups beschermd zijn tegen ransomware en moet periodiek gecontroleerd worden of gegevens daadwerkelijk kunnen worden hersteld.
    - » Vraag hierbij ondersteuning of advies van uw ICT-leverancier om een betrouwbare oplossing te implementeren.

Werken op afstand

- Apparatuur: Gebruik bij voorkeur een zakelijk beheerde laptop met een bijgewerkte virusscanner. Indien een privé-PC wordt gebruikt, sla dan geen wachtwoorden op in de browser, log uit na gebruik, zorg dat niemand meekijkt en verwijder gedownloade bestanden na gebruik.
- Verbinding: Gebruik een beveiligde verbinding en de door de organisatie/ICT-leverancier voorgeschreven toegangsvoorziening. Zorg ervoor dat software en de virusscanner altijd up-to-date zijn.
    - » In verband met beveiliging raden wij af om gebruik te maken van openbare WIFI-verbindingen.

Omgaan met datalekken

Om datalekken te kunnen opsporen en melden is het van belang dat praktijkmedewerkers deze herkennen en weten wat ze moeten doen. Een datalek omvat incidenten zoals phishing, een verkeerd geadresseerde e-mail, een verloren USB-stick, onbedoelde inzage in dossiers maar ook een leesbaar briefje op de balie met naam en geboortedatum van een patiënt.

- **Herkenning**: Het is belangrijk dat alle medewerkers weten wat een datalek is en waarom het melden ervan essentieel is.
- **Melden**: Zorg voor een duidelijke procedure voor het melden van (mogelijke) datalekken. Kijk voor tips op https://www.informatieveiliggedragzorg.nl/toolkit/melden-datalek/ Medewerkers melden een (vermoedelijk) datalek zo snel mogelijk bij de binnen de praktijk aangewezen verantwoordelijke. Deze beoordeelt het incident en bepaalt welke vervolgstappen nodig zijn. Indien sprake is van een **meldplichtige datalek**, moet dit binnen 72 uur na ontdekking worden gemeld bij de Autoriteit Persoonsgegevens. Zie de website van de Autoriteit Persoonsgegevens wanneer u wel of niet moet melden. Leg de gemaakte

Acties bij (mogelijke) datalek of hack

Heeft u het vermoeden dat uw praktijk, mailbox of systemen zijn gehackt of misbruikt? Neem dan direct contact op met uw eigen IT-leverancier. Snel handelen kan verdere schade beperken.

Daarnaast kunt u terecht bij **Z-CERT**, het expertisecentrum voor cybersecurity in de zorg. Z-CERT ondersteunt zorgorganisaties bij dreigingsinformatie, waarschuwingen en advies bij cyberincidenten. Ook helpt Z-CERT zorginstellingen om hun digitale weerbaarheid te vergroten. Meer informatie vindt u op deze pagina van Z-CERT: Incident melden bij Z-CERT.

beoordeling en eventuele vervolgstappen vast. Een voorbeeld van hoe u dit kunt vastleggen staat in het voorbeeld van een verwerkingsregister, opgesteld door de LHV.

- Het is waardevol om binnen de praktijk regelmatig aandacht te besteden aan privacy risico's. Laat iemand bijvoorbeeld periodiek inventariseren welke privacygevoelige informatie onbedoeld zichtbaar is op werkplekken of in openbare ruimtes. Bespreek (mogelijke) datalekken tijdens een werkoverleg en stel daarbij steeds de vragen: *Hoe kon dit gebeuren?* en *Wat kunnen we aanpassen om herhaling te voorkomen?* Door dit structureel bespreekbaar te maken, wordt privacy-bewust werken een vanzelfsprekend onderdeel van de praktijkcultuur.
- Leren en verbeteren: Documenteer elk incident en evalueer de oorzaak om de kwaliteit van de zorg en de informatiebeveiliging continu te verbeteren.

Trainingen, informatie en toolkits

Op de website van de LHV vindt u informatie over veilig werken in de praktijk. Ook kunt u terecht op de website van Informatieveilig gedrag in de zorg.

Praktijkwebsite en nieuwe patiënten

- **Websitebeveiliging**: Zorg dat de website beveiligd is, zeker wanneer via webformulieren persoonsgegevens worden uitgewisseld. Gebruik een HTTPS-verbinding (deze verbinding is te herkennen wanneer u in de adresbalk van de website het slotje ziet staan) voor versleutelde communicatie en bescherming tegen meekijkers of hackers. Laat het SSL-certificaat automatisch verlengen, zodat de beveiliging niet onverwacht verloopt.
- **Identificatie**: Wanneer een nieuwe patiënt zich meldt, moet de identiteit van de patiënt worden vastgesteld. Dit vaststellen mag ook digitaal, bijvoorbeeld door het legitimatiebewijs te tonen tijdens een beeldbelverbinding. Ook moet het soort identiteitsbewijs en het documentnummer worden vastgelegd in de administratie.
    - » Er mag geen scan of kopie worden gemaakt en het ID-bewijs mag niet bewaard worden.

Bijlage I:

Elementen goed beveiligde werkplek

Het kan van kleine nuances afhangen of de werkplekken in uw praktijk voldoende of juist onvoldoende beveiligd zijn.

In deze bijlage schetsen we praktijksituaties ingedeeld op drie niveaus: onvoldoende, voldoende en goed, en hebben dit opgesplitst in scenario's voor programma's met en zonder patiëntgegevens. De scenario's lijken bewust veel op elkaar, zodat duidelijk wordt dat het ontbreken van één onderdeel het verschil kan maken tussen twee niveaus.

Niveau: Onvoldoende

Scenario | programma's met patiëntgegevens

Als doktersassistent log ik in op het HIS met mijn eigen account. Ik heb een sterk en uniek wachtwoord bedacht dat voldoet aan de eisen van het HIS. Mijn werkplek vergrendelt na 15 minuten vanzelf, en als een collega uit dienst gaat, wordt diens toegang direct ingetrokken. Bij het inloggen typ ik alleen mijn wachtwoord in, er wordt verder niets gevraagd.

Waarom dit toch onvoldoende is: de praktijk in dit scenario is goed op weg, maar een wachtwoord dat iemand kan onthouden is vaak onvoldoende complex en/of wordt vaak op meerdere plekken gebruikt. Wat ontbreekt is een tweede controle bij het inloggen. En juist dit punt is wettelijk verplicht (NEN 7510, de norm voor informatiebeveiliging in de zorg) zodra een systeem patiëntgegevens toont. Met alleen één wachtwoord ben je, ondanks alle andere goede maatregelen, nog steeds kwetsbaar: raakt dat ene wachtwoord bekend, dan ligt het hele dossier open.

Wat is nodig?	**In deze situatie**
Eigen account per medewerker	✓
Uniek wachtwoord, bewaard in een wachtwoordenkluis	x
Tweestapsverificatie bij programma's met patiëntgegevens	x
Scherm vergrendelt vanzelf na korte tijd	✓ (na 15 minuten)
Toegang wordt direct ingetrokken zodra iemand uit dienst gaat	✓

Scenario | programma's zonder patiëntgegevens

Als huisarts heb ik voor elk leveranciersportaal een account met een wachtwoord dat bekend is bij mijn assistenten, zij moeten namelijk ook materialen kunnen bestellen. Dit soort wachtwoorden wordt jaarlijks aangepast en houden we bij in een Excel-bestand voor iemand het wachtwoord is vergeten. Mijn werkplek vergrendelt na 15 minuten vanzelf en de portalen loggen vanzelf uit als ze een tijd niet worden gebruikt.

Waarom dit onvoldoende is: hoewel er voor programma's zonder patiëntgegevens minder strenge eisen gelden dan programma's met patiëntgegevens, is een sterk wachtwoord een belangrijke basis voor informatiebeveiliging. Wachtwoorden die meerdere collega's kunnen onthouden zijn (meestal) onvoldoende complex. Als hier toch zeer complexe wachtwoorden worden gebruikt, betekent dit dat de werknemers het niet kunnen onthouden en men moet kopiëren-plakken vanuit het Excel-bestand. Naast een onveilige opslag van het wachtwoord, is het vooral onhandig voor de werknemers.

Wat is nodig?	**In deze situatie**
Uniek en complex wachtwoord, bewaard in een wachtwoordenkluis	x
Scherm vergrendelt vanzelf na korte tijd	✓
Toegang wordt direct ingetrokken zodra iemand uit dienst gaat	x

Niveau: Voldoende (dit is het wettelijk minimum)

Scenario | programma's met patiëntgegevens

Als doktersassistent log ik in op het HIS met mijn eigen account. Mijn wachtwoord is uniek, complex en wordt bewaard in de wachtwoordenkluis van de praktijk. Bij het inloggen vraagt het systeem ook een code uit de authenticator-app op mijn telefoon. Na 15 minuten dat ik niets doe, vergrendelt mijn werkplek vanzelf. Gaat een collega uit dienst, dan wordt de toegang ingetrokken zodra iemand daar tijd voor heeft, meestal dezelfde dag.

Waarom dit voldoende is, en wat het net niet 'goed' maakt: alle wettelijk verplichte onderdelen zijn aanwezig, met als kern de tweede controle bij het inloggen. Wat nog kan verbeteren: de vergrendeling duurt met 15 minuten relatief lang en het intrekken van toegang gaat nu nog op gevoel ("zodra iemand eraan denkt") in plaats van via een vast, direct proces.

Wat is nodig?	In deze situatie
Eigen account per medewerker	✓
Uniek wachtwoord, bewaard in een wachtwoordenkluis	✓
Tweestapsverificatie bij programma's met patiëntgegevens	✓
Scherm vergrendelt vanzelf na korte tijd	✓ (na 15 minuten)
Toegang wordt direct ingetrokken zodra iemand uit dienst gaat	✓ (meestal dezelfde dag)

Aanvulling voor Medicom
Het registreren van de persoonlijke UZI-pas maakt het mogelijk om in te loggen op Medicom, maar daarmee voldoet u nog niet aan de wettelijke eis. Alleen toegang tot patiëntgegevens met een tweede controle (2FA) is wettelijk toegestaan. Dat kan op twee manieren:

1. Steek voordat u inlogt de UZI-pas in de kaartlezer. Op deze manier dwingt u af om via dit systeem in te loggen.
2. U kunt op een ander moment in de keten de 2FA toepassen. Dit kan door 2FA in te stellen in de wachtwoordenkluis, of u kunt dit doen op Windows, waarbij je alleen vanaf je eigen werkplek bij Medicom kunt.

Scenario | programma's zonder patiëntgegevens

Als huisarts heb ik voor elk leveranciersportaal een account met een uniek en complex wachtwoord uit de wachtwoordenkluis van de praktijk. Gaat een collega uit dienst, dan trekken we de toegang meteen in. Twee van onze portalen bieden tweestapsverificatie aan, maar die hebben we nooit aangezet, want "het werkte al zo prima". Het scherm vergrendelt automatisch na 15 minuten.

Waarom dit voldoende is: Dit programma bevat geen patiëntgegevens, dus de harde 2FA plicht uit NEN 7510 is hier niet van toepassing. Toch is er een belangrijk overweging vanuit de AVG: aan het account zitten bankgegevens gekoppeld waarmee bestellingen geplaatst kunnen worden. De AVG vraagt om maatregelen passend bij het risico, en dat risico is hier hoger dan "geen patiëntgegevens" doet vermoeden. Tweestapsverificatie is daarom de passende maatregel, ook al is ze niet wettelijk verplicht. Een tussenvorm is het regelmatig aanpassen van het wachtwoord in de kluis.

Wat is nodig?	In deze situatie
Uniek en complex wachtwoord, bewaard in een wachtwoordenkluis	✓
Scherm vergrendelt vanzelf na korte tijd	✓
Toegang wordt direct ingetrokken zodra iemand uit dienst gaat	✓

Niveau: Goed

Scenario | programma's met patiëntgegevens

Als doktersassistent log in op het HIS met mijn eigen account. Mijn wachtwoord komt (automatisch) uit de wachtwoordenkluis van de praktijk. Bij het inloggen vraagt het systeem een code uit mijn authenticator app, en dat geeft mij toegang tot zowel de eigen patiënten als, met toestemming, dossiers via het LSP. Na 2 minuten waarin ik niets doe, vergrendelt mijn scherm automatisch. Ga ik uit dienst, dan wordt mijn toegang meteen ingetrokken via een vaste procedure, zowel in het HIS als in de wachtwoordenkluis en andere werkaccounts.

Wat dit toevoegt aan het *minimum* in het vorige scenario: dit niveau is dezelfde basis als "voldoende" (eigen account, kluis, tweestapsverificatie), aangevuld met de twee punten die daar nog op gevoel gingen: het scherm vergrendelt nu sneller (2 in plaats van 15 minuten), en het intrekken van toegang gebeurt via een vaste procedure in plaats van "zodra iemand eraan denkt".

Nodig voor niveau 'goed'	**In deze situatie**
Eigen account per medewerker	✓
Uniek wachtwoord, bewaard in een wachtwoordenkluis	✓
Tweestapsverificatie bij programma's met patiëntgegevens	✓
Scherm vergrendelt vanzelf na korte tijd (na 2 minuten)	✓
Toegang wordt direct ingetrokken zodra iemand uit dienst gaat (vaste procedure)	✓
Programma's zonder patiëntgegevens	✓

Scenario | programma's zonder patiëntgegevens

Als praktijkmanager beheer ik via de zakelijke wachtwoordenkluis wie toegang heeft tot welk portaal. Dat beheer doe ik op rolbasis wat mij helpt met overzicht houden. Zodra iemand uit dienst gaat, trek ik die toegang gemakkelijk in. Om bij de wachtwoorden te komen, moet iedereen minimaal 1 keer per dag 2FA gebruiken.

Wat dit toevoegt aan het minimum: Door 2FA op de gehele wachtwoordenkluis af te dwingen, is de beveiliging voor elk portaal nog wat sterker, ook de portalen met een gedeeld wachtwoord. Het verlenen van toegang op rolbasis, maakt het makkelijker om dit te managen en behoudt het overzicht.

Wat is nodig?	**In deze situatie**
Uniek en complex wachtwoord, bewaard in een wachtwoordenkluis	✓
Scherm vergrendelt vanzelf na korte tijd	✓
Toegang wordt direct ingetrokken zodra iemand uit dienst gaat	✓

Bijlage II

Beheren van wachtwoorden

Op een werkdag wordt er door verschillende collega's met regelmaat ingelogd op allerlei soorten systemen. Dit gaat vaak routinematig en bij voorkeur zo gebruiksvriendelijk mogelijk. Bewustzijn van digitale veiligheid is daarbij een belangrijke eerste stap, maar uiteindelijk draait het om daadwerkelijk veilig(er) werken. Dat hoeft niet ten koste te gaan van het gebruiksgemak, mits dit goed is ingericht.

Werkplekbeveiliging

Iedere computer op de praktijk dient beveiligd te worden met een wachtwoord. Wanneer u uw werkplek verlaat, of even kort van uw plek bent, kunt u de computer gemakkelijk handmatig vergrendelen (zie figuur 1). Stel ook een automatische vergrendeling in zodat de computer automatisch vergrendelt, mocht u dat zelf vergeten.

Figuur 2: U kunt uw pc gemakkelijk vergrendelen door deze toetsen tegelijkertijd in te drukken op uw toetsenbord.

HIS-toegang » UZI en Dezi

- Een veilige en gecontroleerde toegang tot het HIS is essentieel voor het beschermen van patiëntgegevens. Gebruik voor iedere werknemer een aparte UZI-pas op naam of een andere vorm van 2-factor authenticatie.
- Het Dezi-register wordt onderdeel van het nieuwe inlogstelsel in de zorg en vervangt op termijn het UZI-register én de uitgegeven UZI-middelen. Ook nadat het Dezi-stelsel in werking is getreden, blijven de UZI-middelen geldig tot de einddatum die op het middel is vermeld. Te zijner tijd wordt het huidige UZI-stelsel uitgefaseerd waarbij ook de uitgifte van middelen stopt. Klik hier voor informatie voor zorgaanbieders ZORG-ID VZVZ.

Autorisatiebeheer

- Breng autorisatiebeheer onder bij één of twee personen in de praktijk. Leg in een protocol vast voor welke diensten nieuwe medewerkers aangemeld worden en hoe medewerkers bij uitdiensttreding worden afgemeld.

Wachtwoordmanager

Om uw programma's zo goed mogelijk te beveiligen is het belangrijk dat te doen met sterke wachtwoorden die veelal bestaan uit een reeks tekens. Hierdoor, en door de groei van het aantal accounts waar u een wachtwoord voor nodig heeft, is het niet haalbaar om al deze wachtwoorden te onthouden. Een wachtwoordmanager biedt uitkomst.

Een wachtwoordmanager is een beveiligde digitale 'kluis' waarin uw wachtwoorden worden opgeslagen. Om toegang te krijgen tot deze kluis hoeft u slechts één sterke wachtzin te onthouden. Een wachtwoordmanager kan ook sterke wachtwoorden voor u genereren wanneer u een nieuw wachtwoord moet instellen.

- Eén hoofdwachtwoord: U onthoudt slechts één sterke wachtzin.
- Geen onveilige lijstjes: Wachtwoorden worden niet langer opgeschreven of in onveilige browserlijsten (zoals Chrome) bewaard.
- Veilig delen: U deelt inloggegevens voor gedeelde portalen (bijv. ZorgDomein of Lab-uitslagen) veilig met assistenten of waarnemers zonder dat het wachtwoord zichtbaar hoeft te zijn.

Licenties

Kies voor een zakelijke licentie, en geen gratis versie. Een gratis versie van een passwordmanager lijkt aantrekkelijk, maar is voor een huisartsenpraktijk onveilig en niet geschikt. Daarvoor zijn drie belangrijke redenen:

- **AVG-Logging:** Volgens de AVG en NEN 7510 moet u kunnen aantonen wie wanneer toegang heeft gehad tot medische systemen. Alleen zakelijke versies bieden het noodzakelijke logboek die dit bijhoudt.
- **Eigendom en continuïteit:** Bij een zakelijke licentie blijft de praktijk altijd eigenaar van de data. Bij een gratis account daarentegen, is de medewerker die de kluis aanmaakt de eigenaar. Als een medewerker de organisatie verlaat, verliest de praktijk de toegang.
- **Veilig delen:** Zakelijke versies maken 'gedeelde kluizen' mogelijk, waardoor teamleden veilig bij gezamenlijke accounts kunnen, zonder wachtwoorden naar elkaar te hoeven sturen.

Voor systemen als VECOZO en ZorgDomein kunt u wel een persoonlijk account kiezen. Het voordeel hiervan is dat duidelijk blijft wie welke handelingen uitvoert.

Vergelijking wachtwoordmanagers (indicatie 2026, excl. BTW)

Er zijn verschillende wachtwoordmanagers beschikbaar. Op basis van verschillende criteria, adviseren wij *1Password* of *Bitwarden*. Beide voldoen aan de strengste eisen voor de zorg.

Kenmerk	1Password	Bitwarden
Wachtwoorden delen met collega's	Ja, gedeelde kluizen met rechten per persoon of groep	Ja, gedeelde mappen met rechten per persoon of groep
Toegang intrekken bij uitdiensttreding	Ja, in één handeling via het beheerscherm	Ja, in één handeling via het beheerscherm
Noodtoegang door een beheerder van de praktijk	Ja	Ja, alleen in de Enterprise-versie
Opslag binnen Europa	Ja, mits je het account aanmaakt via 1password.eu	Ja, mits je bij aanmelden de EU-server kiest
Land van het bedrijf	Canada	Verenigde Staten
Opslaglocatie	Keuze uit VS, Canada of EU	Keuze uit VS of EU
Kosten Teams[1]	€ 19,00 per maand (vast tarief tot 10 gebruikers).	€ 3,75 per gebruiker per maand (flexibel per persoon).
Kosten Business[2]	€ 7,50 per gebruiker per maand	€ 5,60 per gebruiker per maand
Extra voordeel	Gratis privé-account voor medewerkers.	Mogelijkheid tot eigen hosting (lokale server).
Gebruiksgemak	Zeer intuïtief	Functioneel; iets technischer in het gebruik.
Past het beste bij een praktijk die…	…de meest uitgewerkte oplossing wil en een ICT-partij heeft die de Microsoft-omgeving beheert	…later zonder gedoe wil kunnen overstappen naar een andere partij of naar eigen beheer.

[1] *Teams* is geschikt voor kleinere praktijken (tot ±10-15 medewerkers). Biedt de basis voor veilig delen en beheer.

[2] *Business* is bedoeld voor grotere organisaties of als u wilt inloggen met uw bestaande Microsoft 365-account (SSO) en uitgebreidere beveiligingsrapportages wilt.

Implementatie wachtwoordmanager

1. Pakketkeuze: Kies de Business- of Teamsvariant. Richt hiermee een centrale organisatieomgeving voor de praktijk in. Wanneer een medewerker uit dienst gaat kan de beheerder diens toegang intrekken. De gedeelde wachtwoorden blijven beschikbaar voor de praktijk.

2. Hoofdwachtwoord: Bedenk één sterke wachtzin zonder spaties (bijv: DeKoffieInDePraktijkIsLekker!). » *Schrijf deze nergens op.*

3. Activeer 2FA: Schakel tweefactor-authenticatie in voor de toegang tot de manager zelf.

4. Kluizen inrichten: Maak binnen de zakelijke omgeving gedeelde kluizen aan voor praktijkportalen en andere gezamenlijke accounts. Iedere medewerker krijgt een individueel zakelijk account en alleen toegang tot de kluizen die nodig zijn voor diens werkzaamheden. Let op; de ICT-partij richt de kluis vaak in en beheert het, maar de praktijk blijft eigenaar van de gegevens. Staat het contract op naam van de beheerder, dan ben je bij een wisseling van ICT-partij afhankelijk van hun medewerking om bij je eigen wachtwoorden te komen.

- Heeft de praktijk zelf ook iemand met beheerdersrechten in de kluis? Bijvoorbeeld een praktijkmanager. Als alleen de ICT-partij beheerder is, kan de praktijk bij een storing of een meningsverschil niets zelf oplossen.
- Wie mag noodtoegang gebruiken en wie controleert dat achteraf? Noodtoegang is bedoeld voor het geval een medewerker vertrekt zonder overdracht of het hoofdwachtwoord vergeet.

5. Opschonen: verwijder alle wachtwoorden uit webbrowsers en vernietig papieren lijstjes in de versnipperaar. Hoe u dit doet per browser is te vinden via de zoekterm ‘wachtwoorden verwijderen + naam browser’.

6. Verwerkersovereenkomst: is er een verwerkersovereenkomst met de ICT-partij zelf? De praktijk is verwerkingsverantwoordelijke voor de gegevens in de kluis. Zowel de leverancier van de kluis als de ICT-partij die erin beheert, is verwerker. Voor beide is een verwerkersovereenkomst nodig.

7. Toegangsbeheer: wij adviseren de beheerder van de praktijk om jaarlijks na te lopen wie er toegang heeft tot welke gedeelde kluis. Zo houdt u zicht op rechten die na een functiewissel zijn blijven staan. Bewaar de uitkomst want dit is bruikbaar bewijs dat de praktijk haar autorisaties beheert.

Bijlage III

Voorbeelden automatische antwoorden

Voorbeeld automatisch antwoord mail:

Beste lezer,
Hartelijk dank voor uw bericht. Wij proberen uw mail binnen 2 werkdagen te beantwoorden. Dit e-mailadres is niet bedoeld om privacygevoelige informatie te sturen.

Bent u patiënt: gebruik het patiëntportaal voor het herhalen van medicatie, maken van afspraken (en chats met de praktijk).

Bent u collega; wij ontvangen patiëntinformatie graag via EDI-fact of ZorgMail.

Vriendelijke groet,

Voorbeeld standaard reactie bij krijgen privacygevoelige informatie:

Beste lezer,
U heeft ons een bericht gestuurd met privacygevoelige informatie. Dit e-mailadres is niet geschikt om deze informatie naartoe te sturen.

Wij nemen uw vraag daarom niet in behandeling.

Bent u patiënt: gebruik het patiëntportaal voor het herhalen van medicatie, maken van afspraken en het stellen van een korte medische vraag (en chats met de praktijk).

Bent u collega; wij ontvangen patiëntinformatie graag via EDI-fact of ZorgMail.

Vriendelijke groet,

Disclaimer onderaan onbeveiligde mail vanuit de praktijk:
Disclaimer:
Dit mailadres is niet geschikt om privacygevoelige informatie naar te sturen. Gebruik hiervoor alleen het patiëntportaal of de Medgemak app.