Medrie

Veilig inloggen

Uitleg en advies op wachtwoordenkluizen en tweestapsverificatie

Versie: *21 augustus 2026*

Inleiding

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.

Bewustwording over de veiligheid is slechts een start, daarna komt veiliger werken dan voorheen. Dit hoeft niet altijd in te boeten op gebruiksvriendelijkheid wanneer dit goed georganiseerd wordt. Een wachtwoordenkluis biedt daarvoor een goede oplossing.

Dit document laat drie niveaus zien: onvoldoende, voldoende en goed. We schetsen praktijksituaties om dit verschil begrijpelijk te duiden. Ze lijken bewust veel op elkaar omdat het ontbreken van één onderdeel het verschil tussen twee niveaus kan maken.

Leeswijzer

Er komen twee soorten programma's en begrippen aan bod:

Programma's met patiëntgegevens

Bijvoorbeeld het HIS, dit zijn de kroonjuwelen van elke praktijk die goed beschermd moeten worden.

Programma's zonder patiëntgegevens

Bijvoorbeeld het portaal waar medicijnen of kantoorartikelen worden besteld.

Wachtwoordenkluis

Een programma dat voor elk account een uniek, sterk wachtwoord aanmaakt en veilig bewaart waardoor je geen wachtwoorden meer hoeft te onthouden. Het vult automatisch wachtwoorden in bij het benaderen van een site of programma en je kunt wachtwoorden delen die voor meerdere collega's relevant zijn.

Tweestapsverificatie (ook wel MFA of 2FA genoemd):

Naast je wachtwoord vraagt het systeem een tweede bewijs dat jij het echt bent. Een wachtwoord is 1 van de 3 verificatie mogelijkheden waarbij er minimaal een tweede nodig is om het 2FA te noemen.

- Iets wat je hebt (telefoon, UZI pas, smartcard)
- Iets wat je weet (wachtwoord, pincode)
- Wie je bent (vingerafdruk, gezichtsherkenning)

Inhoud

Inleiding 2
Leeswijzer 2
Niveau: Onvoldoende 4
Niveau: Voldoende (dit is het wettelijk minimum) 6
Niveau: Goed 8
Aanbevolen wachtwoordenkluizen 9
Waar we op hebben getoetst 9
De drie kluizen die we aanbevelen 10
Let op bij het aanmaken van het account 11
Verantwoording 11
Bijlage 1: Stem af met je ICT-beheerder 12
Bijlage 2: waarop is getoetst 13
Europese wetgeving 13
De eisen die we hebben gehanteerd 13
Uitgebreidere vergelijking 14

Niveau: Onvoldoende

Scenario programma's met patiëntgegevens

Als doktersassistent log 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 is goed onderweg, maar een wachtwoord dat iemand kan onthouden is vaak onvoldoende complex en/of wordt vaak op meerdere plekken gebruikt. Wat ontbreekt; 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 een wachtwoord ben je, ondanks alle andere goede maatregelen, nog steeds met één klap kwetsbaar: raakt dat ene wachtwoord bekend, dan ligt het hele dossier open.

Wat is er 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	✓

Scenario programma's zonder patiëntgegevens

Als huisarts heb 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 als mensen hem 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. 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 er 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: Voldoende (dit is het wettelijk minimum)

Scenario programma's met patiëntgegevens

> *Als doktersassistent log 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 er 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	✓ (informeel, meestal dezelfde dag)

Let op bij Medicom

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

1. *Door de UZI-pas verplicht in de lezer te steken om in te loggen, en dit ook zo af te dwingen in het systeem zodat dit de enige weg is,*
2. *Door ergens anders in de keten 2FA toe te passen. Dit kan door 2FA op in de wachtwoordenkluis in te stellen of op Windows, waarbij je alleen vanaf je eigen werkplek bij Medicom kunt.*

Scenario programma's zonder patiëntgegevens

Ik als huisarts heb voor elk leverancierssportaal 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 er 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: 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".

Wat is er 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 2 minuten)
Toegang wordt direct ingetrokken zodra iemand uit dienst gaat	✓ (vaste procedure)

Programma's zonder patiëntgegevens

Als praktijkmanager beheer 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 er 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	✓

Aanbevolen wachtwoordenkluizen

We hebben aan verschillende praktijken gevraagd welke wachtwoordenkluis ze gebruiken en getoetst. We hebben gekeken naar Europese wetgeving en belangrijke functies die in de praktijk het meest uitmaken. De drie die we hebben geselecteerd voldoen hieraan. De verschillen zitten in de prijs, het land waar het bedrijf gevestigd is, en hoe eenvoudig je later kunt overstappen.

Waar we op hebben getoetst

- **Wachtwoorden delen met collega's.** De kluis werkt met gedeelde mappen per onderwerp of functie. De assistentes kunnen bij de bestelportalen, en niemand krijgt toegang tot meer dan nodig is.
- **Toegang eenvoudig kunnen intrekken.** Gaat een collega uit dienst, dan haal je die persoon met één handeling uit de kluis.
- **Noodtoegang tot de kluis.** Vertrekt iemand zonder overdracht, of vergeet iemand het hoofdwachtwoord, dan kan een beheerder van de praktijk er alsnog bij. Zonder die mogelijkheid raak je de toegang tot bijvoorbeeld het portaal van de zorgverzekeraar definitief kwijt.

De drie kluizen die we aanbevelen

	1Password Business	Proton Pass Business	Bitwarden Enterprise
Wachtwoorden delen met collega's	Ja, gedeelde kluizen met rechten per persoon of groep	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	Ja, in één handeling via het beheerscherm
Noodtoegang door een beheerder van de praktijk	Ja	Ja	Ja, alleen in de Enterprise-versie
Opslag binnen Europa	Ja, mits je het account aanmaakt via 1password.eu	Zwitserland en de EU	Ja, mits je bij aanmelden de EU-server kiest
Land van het bedrijf	Canada	Zwitserland	Verenigde Staten
Opslaglocatie	Keuze uit VS, Canada of EU	Zwitserland en de EU	Keuze uit VS of EU
Indicatie prijs per gebruiker per maand	Circa €8	Vanaf circa €2, met logboek en SSO circa €4,50	Circa €6
Actuele prijs	1password.com/pricing	proton.me/business/pass/pricing	bitwarden.com/pricing
Past het beste bij een praktijk die	De meest uitgewerkte oplossing wil en een ICT-partij heeft die de Microsoft-omgeving beheert	Let op de kosten en de sterkste privacybescherming wil	Later zonder gedoe wil kunnen overstappen naar een andere partij of naar eigen beheer

Let op bij het aanmaken van het account

Bij 1Password en Bitwarden bepaal je op het moment van aanmelden waar de wachtwoorden worden opgeslagen. Meld je je aan via de gewone website, dan staan ze in de Verenigde Staten. Achteraf wisselen kan alleen door een nieuw account aan te maken en alles handmatig over te zetten. Laat je ICT-partij dus vooraf de Europese variant kiezen: 1password.eu bij 1Password, en de EU-server in het aanmeldscherm bij Bitwarden.

In de bijlage staat waarop we verder hebben getoetst en welke vragen je aan een leverancier kunt stellen voordat je tekent.

Verantwoording

De gegevens in dit advies zijn op 28 juli 2026 ontleend aan openbare documentatie van de leveranciers. Certificeringen, opslaglocaties en prijzen wijzigen regelmatig. Laat de praktijk of de ICT-partij de punten over opslaglocatie en noodtoegang schriftelijk bevestigen voordat een contract wordt getekend.

Bijlage 1: Stem af met je ICT-beheerder

- Staan alle andere wachtwoordmanagers uit zoals bijvoorbeeld Chrome, Edge en Firefox? Deze webbrowers hebben vaak een account waarmee browsergeschiedenis, cookies, favorieten én wachtwoorden worden onthouden. Het biedt automatisch aan om ingevulde wachtwoorden (uit de organisatiekluis) op te slaan, maar deze zijn hier niet veilig opgeslagen. Hierdoor komen gevoelige wachtwoorden op plekken te staan die je niet kunt intrekken als iemand uit dienst gaat.
- Is de wachtwoordenkluis geïnstalleerd op ieder apparaat (laptop, desktop, mobiel apparaat) inclusief de plug-in voor de webbrowser? Dit bevordert de gebruiksvriendelijkheid en daarmee ook de implementatie.
- Op wiens naam staat het abonnement van de wachtwoordenkluis? De ICT-partij richt de kluis vaak in en beheert hem, 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 de praktijkmanager. Als alleen de ICT-partij beheerder is, kan de praktijk bij een storing of een meningsverschil niets zelf oplossen. Twee beheerders is ook prettig bij vakantie en ziekte.
- Wie mag noodtoegang gebruiken en wie controleert dat achteraf? Noodtoegang is bedoeld voor het geval een medewerker vertrekt zonder overdracht of het hoofdwachtwoord vergeet. Diezelfde mogelijkheid betekent dat een beheerder in principe bij opgeslagen wachtwoorden kan. Leg daarom vast wie dit mag inzetten en spreek af dat de praktijk het logboek periodiek bekijkt. Test de procedure een keer voordat je hem echt nodig hebt.
- Binnen hoeveel tijd wordt een vertrokken medewerker uit de kluis gehaald, en wie meldt dat iemand vertrekt? Het intrekken van toegang werkt alleen als de beheerder weet dat het moet gebeuren. Denk hierbij ook aan het aantal licenties dat je kunt afschalen wanneer het aantal medewerkers verkleint.
- 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.
- Loopt de beheerder jaarlijks door wie er toegang heeft tot welke gedeelde kluis? Zo houd je 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 2: Waarop is getoetst

Europese wetgeving

Een verwerkersovereenkomst is altijd nodig. Ook als er geen patiëntgegevens in de kluis staan, verwerkt de leverancier persoonsgegevens van medewerkers, zoals e-mailadressen en inlogmomenten. Dat maakt een verwerkersovereenkomst verplicht op grond van artikel 28 AVG. Alle drie de aanbevolen leveranciers stellen die standaard beschikbaar.

Daarnaast is gekeken naar de opslaglocatie, het vestigingsland van het bedrijf en de vraag of buitenlandse autoriteiten toegang zouden kunnen afdwingen. Als toets op de interne beveiliging van de leverancier is ISO 27001 gebruikt, de internationale norm voor informatiebeveiliging. Vraag daarbij de scope van het certificaat op, omdat een bedrijfsbreed certificaat niet automatisch het product dekt dat je afneemt.

De eisen die we hebben gehanteerd

- **Toegang en delen.** Gedeelde kluizen per onderwerp of functie. Rechten per gedeelde kluis, minimaal lezen, bewerken en beheren. Scheiding tussen persoonlijke en zakelijke items. Toegang van een gebruiker binnen enkele minuten in te trekken. Rechten toe te kennen aan een groep in plaats van per persoon. Opslag van codes voor tweestapsverificatie van gedeelde accounts. Apps voor Windows, iOS en Android plus een browserextensie.
- **Beheer en continuïteit.** Centrale beheerdersomgeving. Herstel van een account door een beheerder. Minimaal twee beheerders mogelijk. Logboek van beheerhandelingen. Tweestapsverificatie verplicht te stellen voor alle gebruikers. Rapportage over zwakke, hergebruikte en gelekte wachtwoorden. Koppeling met Microsoft Entra ID is een wens.
- **Soevereiniteit en overstapvrijheid.** Opslag binnen Nederland of de EU, en anders expliciet vastgelegd waar dan wel. Bekend vestigingsland en toepasselijk recht. Inzicht in blootstelling aan buitenlandse wetgeving zoals de Amerikaanse CLOUD Act. Volledige export in een open formaat, uit te voeren door de praktijk zelf. Gedocumenteerde procedure voor beëindiging en verwijdering. Zelf hosten is een wens.

Uitgebreidere vergelijking

Criterium	1Password Business	Proton Pass Business	Bitwarden Teams / Enterprise
Bedrijf en vestiging	1Password, Canada	Proton AG, Zwitserland	Bitwarden, Verenigde Staten
Opslaglocatie	Keuze uit VS, Canada of EU	Zwitserland en de EU	Keuze uit VS of EU
Opslag buiten Europa	Nee bij keuze voor de EU-regio	Zwitserland ligt buiten de EU, met adequaatheidsbesluit	Nee bij keuze voor de EU-regio
Regio achteraf te wijzigen	Nee	Te verifiëren	Nee
Gedeelde kluizen	Ja	Ja	Ja
Rechten per rol of groep	Ja	Ja	Ja
Centrale beheerdersomgeving	Ja	Ja	Ja
Noodtoegang door beheerder	Ja	Ja, procedure verifiëren	Ja, alleen in Enterprise
Logboek	Ja	Ja, vanaf Pass Professional	Ja
Koppeling met Entra ID	Ja	Ja, vanaf Pass Professional	Ja, in Enterprise
Versleuteling op het apparaat	Ja	Ja	Ja
ISO 27001	Ja, plus 27017, 27018 en 27701	Ja, sinds mei 2024	Ja, ISO 27001:2022
Onafhankelijke audit	Jaarlijkse externe audits	Cure53 en Recurity Labs, publiek	Jaarlijkse audits plus ETH Zürich
Broncode openbaar	Nee	Ja	Ja
Zelf hosten mogelijk, dus opslag in eigen beheer	Nee	Nee	Ja, in Enterprise
Export van alle gegevens	Ja	Ja	Ja
Buitenlands recht van invloed	Canadees recht	Zwitsers recht	Amerikaans recht, CLOUD Act
Indicatie prijs per gebruiker per maand	circa €8	€2 tot €4,50	€4 (Teams) of €6 (Enterprise)