

Beveilig documenten met patiëntengegevens

Patiëntenprogramma's

Bewaar patiëntgegevens bijvoorbeeld in een speciaal daarvoor geschikt patiënten-programma voldoet een de veiligheidseisen. De patientfile van RadarOpus voldoet aan alle voorwaarden.

Word bestanden gebruiken

Er zijn ook users die voor elke patient een (onbeveiligd) Word document aanmaken. Patiëntgegevens vallen onder **gevoelige persoonsgegevens** (AVG/GDPR + medische beroepsgeheim-regels) en het is dus niet toegestaan zulke onbeveiligde bestanden op een computer te hebben staan.

- Je moet minimaal zorgen voor **encryptie en wachtwoordbeveiliging van de bestanden**.
- Zorg ook voor een regelmatige **backup** van de patiëntgegevens minimaal op één **extern medium** (externe disk of een clouddrive), zodat je de gegevens niet kwijt kan raken. En deze backup moet op een veilig plaats worden bewaard.
- Zorg ook voor een steeds bijgewerkt antivirusprogramma (in Window is de inbegrepen beveiliging ook goed, indien steeds 'up to date' gehouden).

Hieronder een praktisch en veilig stappenplan voor Word-bestanden.

Voor Windows

Versleutel de Word bestanden (encryptie) individueel

Dit is **niet** aan te raden als er veel losse Word bestanden zijn. Men kan dan wel alle bestanden met hetzelfde wachtwoord beveiligen, maar het is dan niet mogelijk om regelmatig het wachtwoord te veranderen voor al die losse bestanden, wat verplicht is.

In MS-Word wordt bij wachtwoord-beveiliging het bestand ook encrypted (versleuteld).

Hoe individuele Word-documenten versleutelen

In Microsoft Word:

1. Kies **Bestand**, dan **Info**, **Document beveiligen**, dan: **Versleutelen met wachtwoord**
2. Kies een sterk wachtwoord met cijfers en letters, een hoofdletters/kleine letters en een apart teken.

Voordeel: per bestand beveiligd. Handig als individuele dossiers apart blijven.

Nadeel: onpraktisch bij veel bestanden.

Let op: Bewaar dit wachtwoord goed, want zonder zijn documenten nooit meer te openen.

AANBEVOLEN: Gebruik patiëntcodes i.p.v. namen in bestandsnaam

Een goede oplossing voor alle individuele bestanden is het gebruik van patiëntcodes.

En gebruik in de bestanden zelf nooit Naam/Adres/Email/Telnr gegevens. Vermeld dus slechts de patiëntcode als bestandsnaam en in de tekst zelf.

Dit apart opslaan van de N/A gegevens heet **pseudonimisering** (AVG-best practice).

Bewaar de N/A gegevens apart.

- Dit kan in een **papieren lijst**

- Of maak slechts **één Word bestand** aan met al deze gegevens, en beveilig dat document goed. Je zou de namen er alfabetisch in kunnen noteren, met de “achternaam – voornaam” als eerste regel in een STIJL (bijvoorbeeld Kop1).

Word kan automatisch een inhoudsopgave maken van de Stijl aan het begin van het document. Met Ctrl+klik spring dan naar de gegevens. Met zoeken, Ctrl+F, is ook bij een lange lijst namen het nog snel te vinden.

Men kan eventueel ook nog deze individuele bestanden (met patiënten codes als naam) met een wachtwoord beveiligen, en dan voor alle bestanden hetzelfde wachtwoord gebruiken.

Dit wachtwoord kan dan niet regelmatig veranderd worden, maar het is wel een extra beveiligingstap.

Onedrive – Beveiligde kluis

In **Onedrive** is het mogelijk een extra beveiligde map (kluis) te gebruiken (personal vault).

Dit werkt wel, maar mijn ervaring is dat je steeds via de Authenticater moet openen, want de kluis sluit automatische snel weer, en dan krijg je het Word bestand niet meer bewaard, tenzij je steeds weer de kluis opent.

Speciale software voor gebruik op Windows

Er zijn ook andere manieren, zoals meegeleverd bij Windows **Bitlocker**. Of gebruik een programma zoals **VeraCrypt**.

Ik raad aan dit alleen door een ervaren persoon te laten toepassen.

Voor een MAC

Op een **Apple Mac** kun je patiënten Word-bestanden minstens zo veilig beveiligen als op Windows. Hieronder hetzelfde soort praktisch stappenplan.

Je kan individuele MS-Word bestanden beveiligen als volgt:

In Microsoft Word vanuit de menubalk:

1. Kies **Controleren**, dan **Beveiligen**, dan: **beveilig document**
2. Kies een sterk wachtwoord met cijfers en letters, een hoofdletters/kleine letters en een apart teken.

Voordeel: per bestand beveiligd. Handig als individuele dossiers apart blijven.

Nadeel: onpraktisch bij veel bestanden

Let op: Bewaar dit wachtwoord goed, want zonder zijn documenten nooit meer te openen.

Aanbevolen: Gebruik patiëntcodes i.p.v. namen in bestandsnaam

Een goede oplossing voor alle individuele bestanden is het gebruik van patiëntcodes. In de bestanden zelf gebruik nooit Naam/Adres/Email/Telnr gegevens. Vermeld slechts de patiëntcode bovenaan.

Dit apart opslaan van de N/A gegevens heet **pseudonimisering** (AVG-best practice).

Bewaar de N/A gegevens apart.

- Dit kan in een **papieren lijst**

- Of maak slechts **één Word bestand** aan met al deze gegevens, en beveilig dat document goed. Je zou de namen er alfabetisch in kunnen noteren, met de “achternaam – voornaam” als eerste regel in een STIJL (bijvoorbeeld Kop1).

Word kan automatisch een inhoudsopgave maken van de Stijl aan het begin van het document. Met Cmd+klik spring naar de gegevens. Met zoeken, Cmd+F, is ook bij een lange lijst namen het nog snel te vinden.

Men kan eventueel ook nog deze individuele bestanden (met patiënten codes als naam) met een wachtwoord beveiligen, en dan voor alle bestanden hetzelfde wachtwoord gebruiken.

Dit wachtwoord kan dan niet regelmatig veranderd worden, maar het is wel een extra beveiligingstap.

Schijfversleuteling op Mac

FileVault inschakelen (sterk aanbevolen)

- Kies Systeeminstellingen, dan Privacy en beveiliging, dan **FileVault**
- Zet aan, let op, de herstelcode veilig opslaan !!

Wat dit doet:

- Hele Mac-schijf versleuteld
- Let op, zonder de login is er geen toegang tot bestanden
- Beschermt bij diefstal/verlies

Dit is de belangrijkste maatregel op Mac.

Je kunt ook “veilig mappen” gebruiken.

Als je dossiers extra wilt isoleren:

Op MAC kan je een beveiligde “kluis” maken:

1. Schijfhulpprogramma openen
2. Nieuwe afbeelding (Image), dan Lege afbeelding (Image)
3. Kies, Encryptie: **AES-256**
4. Wachtwoord instellen
5. Zie bijvoorbeeld deze website voor meer uitleg:

[Hoe bestanden en mappen op Mac te vergrendelen en met een wachtwoord te beveiligen](#)

Toegangscontrole opstarten van de MAC

Zorg dat alleen bevoegden kunnen inloggen.

Kies een sterk Mac-loginwachtwoord

Via Instellingen: Systeeminstellingen, dan Toegangscode / Vergrendeling

Back-up (cruciaal voor patiëntdata): Versleutelde Time Machine

- Externe schijf aansluiten
- Time Machine → versleutelde back-up
- Dit is Automatisch + veilig

Vermijd:

- iCloud zonder beleid (in zorgcontext)
- Onversleutelde USB

Voor zowel Windows & MAC

Cloud-backup of een aparte drive back-up

Als er niet minimaal één externe backup is van de patiëntengegevens, dan loopt men ook een groot risico om alles eens te verliezen.

Kies een externe harddisk of andere drive (SSD, Memory stick), en berg die veilig op.

Het beste is om deze externe disk ook te beveiligen met wachtwoord/encryptie.

Op MAC kies voor een beveiligde Time machine backup

Vermijd:

- Een onversleutelde Memory stick.
- Onveilig is ook om bestanden op een Clouddrive (Dropbox, Google Drive, Onedrive) te bewaren zonder wachtwoord en encryptie.

Verzenden van Word-dossiers

Verstuur deze nooit onbeveiligd.

Verstuur het wachtwoord niet later via hetzelfde kanaal, maar gebruik een ander kanaal, of geef door per telefoon.

Samenvatting

- Gebruik een speciaal patiëntenprogramma of, gebruik Patiëntcodes i.p.v. namen en sla de codes apart op in een beveiligd bestand of op papier.
- Opstarten van de computer: gebruik een sterk wachtwoord.
- Maak regelmatig een (versleutelde) back-up op een extern medium.
- Alleen beveiligde documenten verzenden.

Dit voldoet aan het AVG-basisniveau.

Tip: Bekijk ook de website van de Landelijke Huisartsen Vereniging: [Veilig omgaan met gegevens in de praktijk - LHV](#)

RadarOpus users tip: exporteer analyses

Vanuit RadarOpus is het mogelijk om de klemborden (de Analyse) te exporteren en dan naar een andere user te sturen. Het externe bestandje is encrypted en kan alleen door een andere RadarOpus user in RadarOpus worden geopend.

Het beste is om een bestandsnaam te kiezen die niet herleid kan worden naar een persoon, gebruik geen volledige voor en achternaam en geboortedatum.

- Klik met **Rechts** op een van de klemborden
- Kies dan: **Analyse opslaan**
- Kies dan: **Exporteer** analyse
- Geef een naam aan het bestand, en kies een locatie.

