Secure documents containing patient data

Patient programs
Store patient data in a specially designed patient program that meets security requirements. The RadarOpus patient file meets all conditions.

Using Word files
There are also users who create an (unsecured) Word document for each patient. Patient data is classified as sensitive personal data (GDPR + medical confidentiality rules), so it is not permitted to store such unsecured files on a computer.

- You must ensure that files are encrypted and password protected as a minimum.
- You must also ensure that patient data is backed up regularly to at least one external medium (external disk or cloud drive) so that you cannot lose the data. This backup must be stored in a secure location.
- Ensure that your antivirus program is always up to date (the security included in Windows is also good, provided it is kept up to date).

Below is a practical and secure step-by-step plan for Word files.

For Windows

Encrypt the Word files individually
This is not recommended if there are many separate Word files.
Although it is possible to protect all files with the same password, it is not possible to change the password regularly for all those separate files, which is mandatory.
(In MS Word, password protection also encrypts the file.)

How to encrypt individual Word documents

In Microsoft Word:
- Select **File**, then **Info**, **Secure Document**, then: **Encrypt with password**.
- Choose a strong password with numbers and letters, upper and lower case letters, and a special character.
-

Advantage: secured per file. Useful if individual files remain separate.
Disadvantage: impractical for large numbers of files.
Please note: Keep this password safe, as without it you will never be able to open your documents again.

RECOMMENDED: Use patient codes instead of names in file names

A good solution for all individual files is to use patient codes for the file names and as the name at the top of the file.
Never use Name/Address/Email/Telephone number details in the files themselves. Only mention the patient code as the file name and at the top of the text itself.
This separate storage of N/A data is called pseudonymizations (GDPR best practice).

Store the patient codes with the corresponding N/A data separately:
- This can be done on paper.
- Or create a single Word file containing all this information and protect that document with a password.

In that document, you could list the names alphabetically, with the "surname – first name" as the first line.
Put that in a STYLE (e.g. Heading 1).
You can then create a Table of Contents at the top, which will list all the names in a concise list.
Use Ctrl+click on the table of contents to quickly jump to the data.
You can also use the search function, Ctrl+F, to quickly find the name.

You can also protect individual files (named with patient codes) with a password. You can use the same password for all files.
This password cannot be changed regularly for all those files, but it does provide an extra layer of security.

OneDrive – Secure vault

In **OneDrive**, it is possible to use an extra secure folder (vault) (personal vault).
This works, but in my experience, you always have to open it via Authenticator, because the vault closes automatically after a short time, and then you can no longer save the Word file unless you keep opening the vault.

Special software for use on Windows

There are also other ways, such as **Bitlocker**, which is included with Windows.
Or use a program such as **VeraCrypt**.
I recommend that this only be done by an experienced person.

For MAC

On an Apple Mac, you can secure patient Word files at least as securely as on Windows.
Below is the same type of practical step-by-step plan.

You can protect individual MS Word files as follows:
In Microsoft Word, from the menu bar:

- Select Check, then Secure, then: Secure Document
- Choose a strong password with numbers and letters, upper/lower case letters and a special character.

Advantage: secured per file. Useful if individual files remain separate.
Disadvantage: impractical for large numbers of files.
Please note: Keep this password safe, as without it you will never be able to open your documents again.

RECOMMENDED: Use patient codes instead of names in file names

A good solution for all individual files is to use patient codes. Never use

name/address/email/telephone number details in the files themselves but only state the patient code at the top.
This separate storage of N/A data is called pseudonymization (GDPR best practice).

Store patient codes with N/A data separately:
- This can be done in a **paper** list.
- Or create a single Word file containing all this information and protect the document with a password. You could list the names alphabetically, with the 'surname – first name' as the first line in a STYLE (e.g. Heading1).

In Word, you can automatically generate a table of contents from Style 1 at the beginning of the document.
With Cmd+click, you can jump to the data in the table of contents.
You can also quickly find the data using the search function, Cmd+F.

You can also password-protect these individual files (containing patient codes and N/A data).
Use the same password for all files.
Unfortunately, this password cannot be changed regularly for all these files, but it does provide an extra layer of security.

Disk encryption on Mac

Enable FileVault (highly recommended)
- Select System Preferences, then Privacy and Security, then FileVault
- Enable it, but be sure to store the recovery code securely!

What this does:
- Encrypts the entire Mac drive
- Please note: without the login, there is no access to files
- Protects against theft/loss

This is the most important measure on Mac.

You may also utilise "secure folders."
If you wish to insulate your files further:

On MAC, you can create a secure "safe":
- Open Disk Utility
- New Image, then Blank Image
- Select Encryption: AES-256
- Set password
- See, for example, this website for more information:
  Password Protect Files on a Mac: 4 Quick and Easy Ways

Access control start-up of the MAC
Ensure that only authorized people can log in.
Choose a strong Mac login password.
Via Settings: System Settings, then Passcode / Lock.

Backup (crucial for patient data): Encrypted Time Machine
Connecting an external drive
- Time Machine → encrypted backup
- This is Automatic + secure

Avoid:

- iCloud without policy (in healthcare context)
- Unencrypted USB

For both Windows and MAC

Cloud backup or a separate drive backup

If there is not at least one external backup of the patient data, there is a high risk of losing everything.

Select an external hard drive or other drive (SSD, memory stick) and store it securely.
It is best to also protect this external drive with a password/encryption.
On a Mac, choose a secure Time Machine backup.

Avoid:
• An unencrypted memory stick.
• It is also unsafe to store files on a cloud drive (Dropbox, Google Drive, OneDrive) without a password and encryption.

Sending Word files

Never send it unsecured.
Do not send the password later via the same channel but use a different channel or communicate it by telephone.

Summary

- Use a special patient program or use patient codes instead of names and store the codes separately in a secure file or on paper.
- When starting up the computer, use a strong password.
- Regularly make an encrypted backup on an external medium.
- Only send secure documents.

This complies with the basic GDPR level.

RadarOpus users tip: export analysis

From RadarOpus, it is possible to export the clipboards (the Analysis) and then send them to another user. The external file is encrypted and can only be opened by another RadarOpus user in RadarOpus.
It is best to choose a file name that cannot be traced back to a person; do not use full first and last names or dates of birth.

- **Right**-click on one of the clipboards
- Then select: **Save analysis**
- Then select: **Export analysis**

- Give the file a **name** and select a **location**.