

RadioWeb

Referrer Guide

Version 1.1.10, 2026-11-24

Contents

Overview 1
- The Chapters at a Glance 1

Signing In 2
- First Sign-In with an Access Code 2
- Setting Up a Permanent Login 2
- Signing Out 3

Sign-in & Security 4
- Setting up a second factor 4
- Backup codes 8
- Signing in with a second factor 8
- Managing factors 10
- Lost device 10

My Patients (PACS View) 11
- Searching 11
- Studies of a Patient 11
- Viewing, Downloading, Sharing 12

Sharing Examinations 14
- Types of Shares 14
- Creating an Access Link 14

Uploading Prior Examinations 15
- Portal Import (DLX) 15
- ZIP Upload 16
- Tracking progress 16

RadioWeb Bridge 18
- Downloading 18
- Installing 19
- Configuring 20
- Using 21

Frequently Asked Questions 22
- Privacy 22

Overview

This guide is intended for referring physicians who access the examinations of their patients through the Patient Portal of a radiology practice or clinic.

The referrer portal lets you

- search the examinations of your patients directly in the practice's archive (PACS),
- view images in the browser,
- download studies or transfer them into your own PACS with the desktop app **RadioWeb Bridge**,
- share examinations with patients or colleagues,
- send prior examinations from other institutions to the practice.

The Chapters at a Glance

Signing In

Signing in with an access code, permanent login with e-mail and password.

My Patients (PACS View)

Searching patients, showing studies, viewing and downloading images.

Sharing Examinations

Creating access links with QR code for patients or colleagues.

Uploading Prior Examinations

Sending studies from other portals (DLX) or as a ZIP archive to the practice.

RadioWeb Bridge

The desktop app for transferring studies into your local PACS.

Frequently Asked Questions

Answers to common questions and privacy notes.



Your access and the enabled features are defined by the radiology practice. Please contact the practice if you have any questions.

Signing In

First Sign-In with an Access Code

The radiology practice gives you a personal **access code** (token) in the format `XXXX-XXXX-XXXX`, usually as a printout with a QR code or as a link.

1. Open the link or scan the QR code – or open the portal, click **Login** and enter the code in the **Token Login** area.
2. Click **Next**. If the code is additionally protected, enter the agreed password.
3. You are taken directly to My Patients.

Setting Up a Permanent Login

So that you do not need the access code every time, you can set up a permanent login with e-mail address and password – provided the practice has enabled this feature.

1. Open the account menu (person icon) in the top right and click **Manage Login**.
2. Enter your e-mail address, choose a password that meets the displayed requirements and repeat it.
3. Click **Submit Registration**.
4. Confirm your e-mail address using the activation link you receive by e-mail.

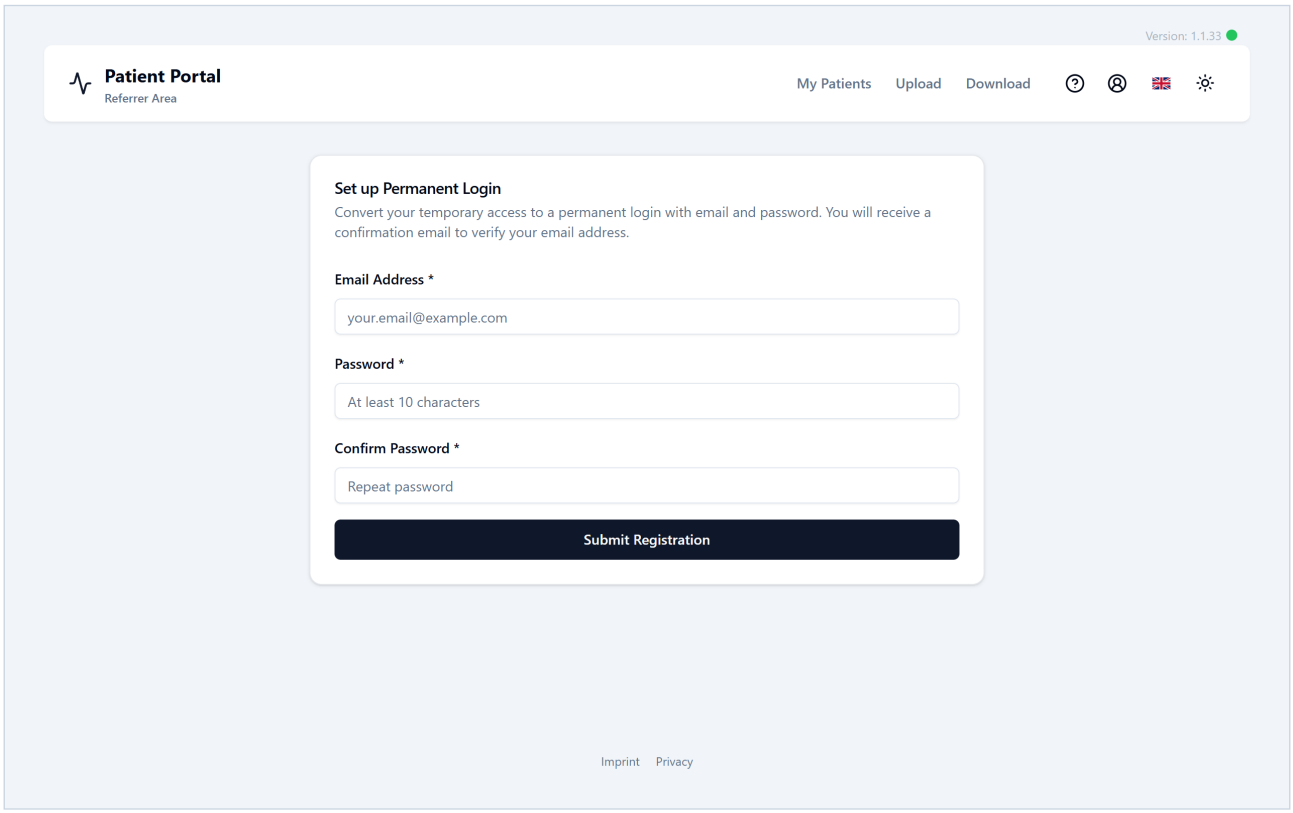

Figure 1. Setting up a permanent login

Afterwards you sign in in the **Login** area of the login page with e-mail address and password. At the first sign-in you set up a second factor (passkey or authenticator app), see Sign-in & Security. Under **Manage Login** you can later change the password, request the activation link again or delete the login.



If **Manage Login** shows the notice "Account creation is currently disabled by the administrator", the feature is not enabled for your practice.

Signing Out

Open the account menu (person icon) in the top right and click **Logout**. After a longer period of inactivity you are signed out automatically; shortly before, a notice with a countdown appears.

Sign-in & Security

This chapter applies to your permanent login with email address and password (see Signing In). Signing in with an access code does not need a second factor.

To protect health data, the password alone is not enough for signing in with **e-mail and password**: every account needs a **second factor**. Someone who knows your password still cannot sign in with it.

> Signing in with an **access code** (share code, token) is not affected and works as before.

You can choose between:

Passkey (recommended)

The sign-in is confirmed with your fingerprint, face recognition or your device PIN – no code to type and no additional app. Passkeys work with current smartphones, tablets and computers (Windows Hello, Apple Touch ID/Face ID, Android) and with security keys. You can add several passkeys, for example for your smartphone and your workplace PC.

Passkeys are considered particularly secure because they are protected against phishing: a passkey only works on the real address of the portal and therefore cannot be stolen through a fake website – unlike a password or a typed-in code. Your fingerprint and face are only used to unlock the passkey on your device; they never leave the device and are not sent to the portal.

Authenticator app

A free app on your smartphone generates a new 6-digit code every 30 seconds, which you enter when signing in. The portal recommends **Microsoft Authenticator** and **Google Authenticator**; any other app following the common standard (TOTP) works as well.

With the first factor you also receive ten **backup codes** for emergencies.

Setting up a second factor

When you first sign in with e-mail and password, the portal automatically opens the page **Sign-in & security** with the notice **Please set up a second sign-in factor**. It briefly explains why this is necessary and introduces the two options. As long as no second factor is set up, all other areas are locked. Later you can always reach the page via the account menu (person icon in the top right) under **Sign-in & security**.

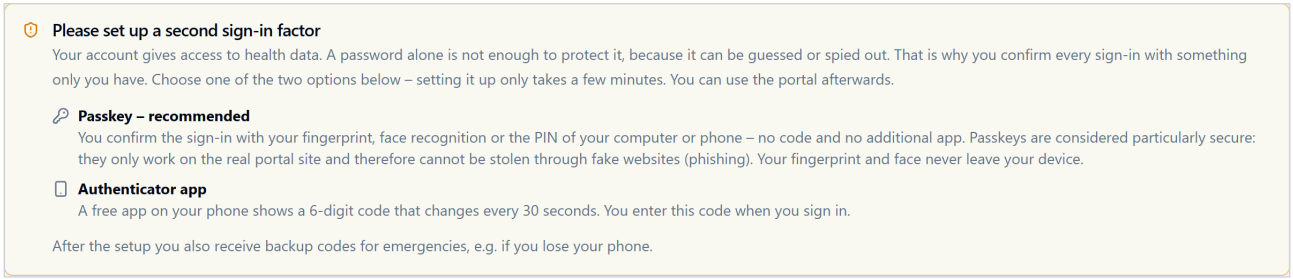

Figure 2. Notice at the first sign-in

Set up one of the two factors – or both, then you have a fallback.

Adding a passkey

1. Open **Sign-in & security** on the device you want to sign in with from now on (computer, smartphone or tablet).
2. Under **Passkeys**, click **Add passkey**.
3. Keep or change the suggested name (for example "office laptop") – it helps you tell the passkeys apart later. Enter your current password and click **Create passkey**.

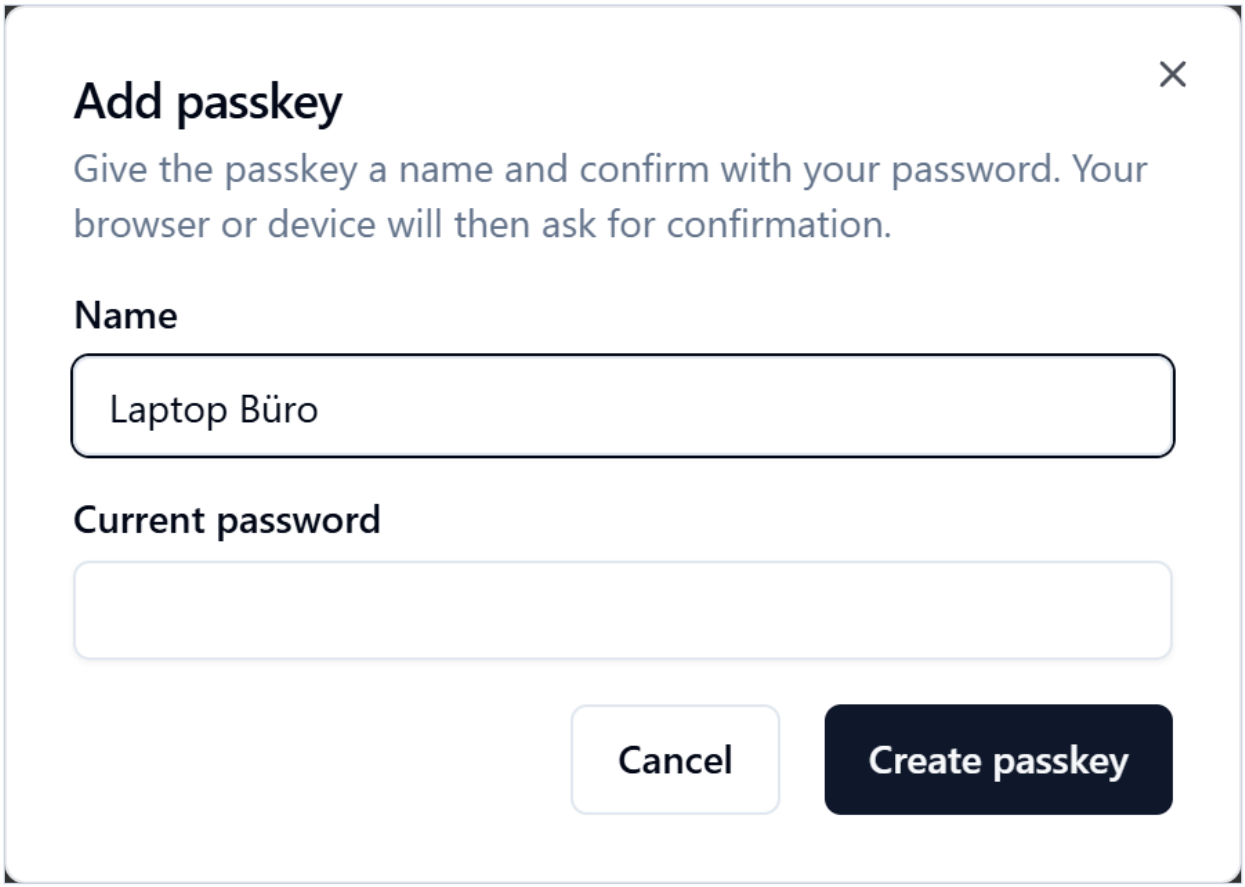

Figure 3. Adding a passkey

4. Your browser or operating system now opens its own window. Depending on the device:
   - **Windows:** confirm with Windows Hello (face, fingerprint or Windows PIN).
   - **Mac, iPhone, iPad:** confirm with Touch ID, Face ID or the device passcode. The passkey is stored in the iCloud Keychain.
   - **Android:** confirm with fingerprint, face or screen lock. The passkey is stored in Google Password Manager.
   - **Storing the passkey on your phone while working at the computer:** choose "Use another device" or "Phone or tablet" in the window and scan the QR code shown with your phone.
5. The new passkey appears in the list. The label **synced** means it is also available on your other devices via your Apple or Google account.

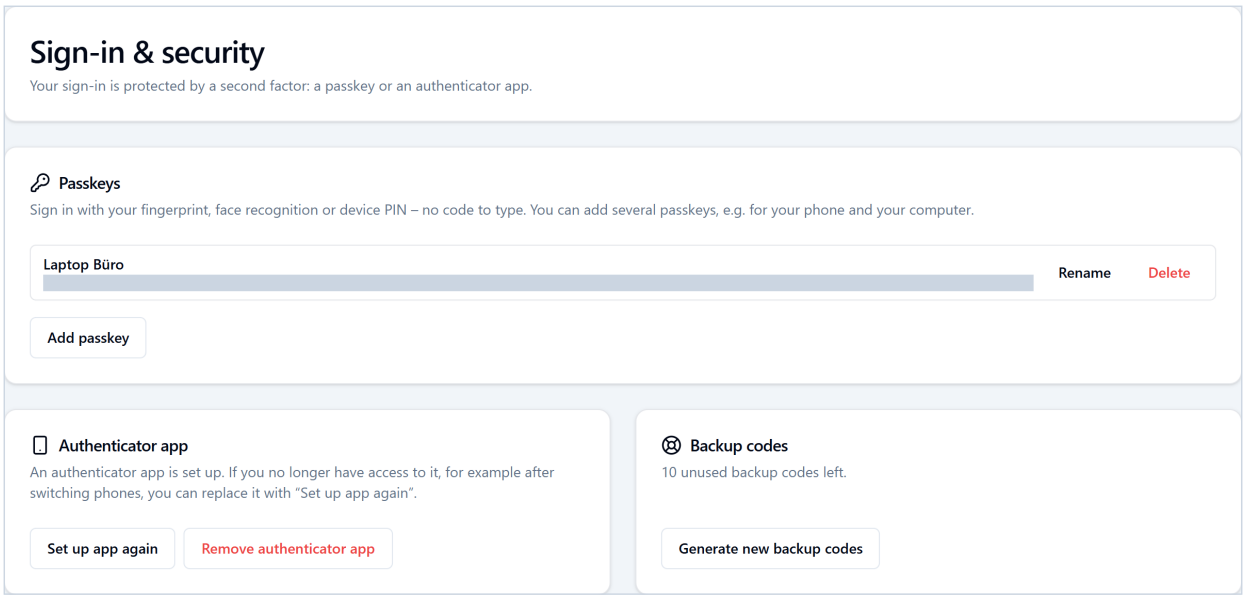

Figure 4. Passkeys, authenticator app and backup codes on the page Sign-in & security

Add a passkey for each device you regularly sign in with – or use a synced passkey. If the browser asks where to store it, your device's password manager is the easiest choice for most users.

Setting up an authenticator app

1. Under **Authenticator app**, click **Set up authenticator app** and enter your current password. The setup guides you through three steps.

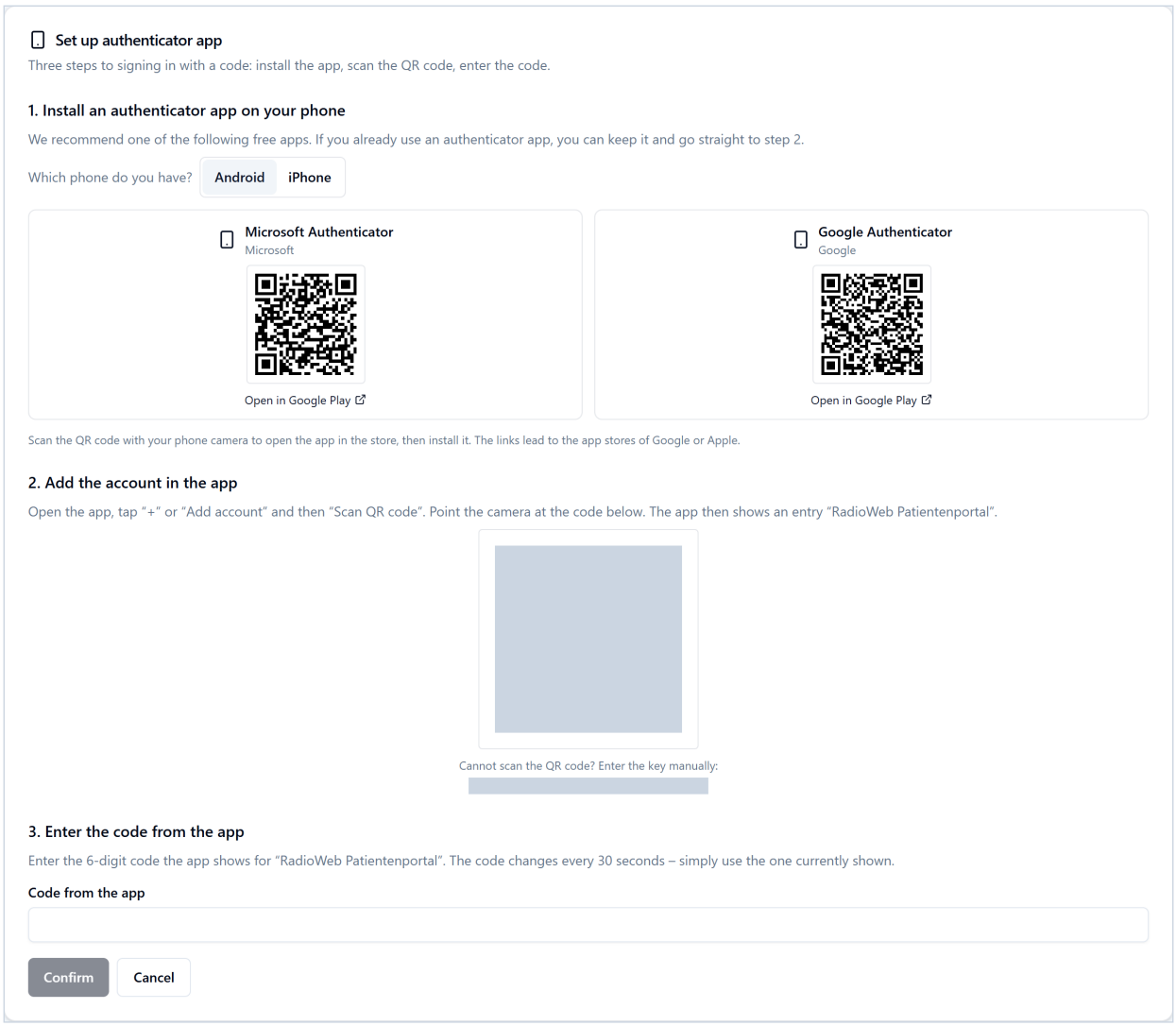

Figure 5. Setting up the authenticator app (QR code and key are hidden here)

2. **Install the app:** the portal recommends two free apps available for Android and iPhone: **Microsoft Authenticator** and **Google Authenticator**. Choose your phone (Android or iPhone) and scan the QR code of the app you want with your phone camera – it opens the app in Google Play or the App Store. If you open the portal on the phone itself, the links lead to the store directly. You can keep using an authenticator app you already have.
3. **Add the account:** in the app, tap "+" or "Add account" and scan the QR code in the portal. If the code cannot be scanned, enter the key shown below it manually in the app. On a phone, **Open directly in the authenticator app** opens the app without scanning. The app then shows the entry "RadioWeb Patientenportal".
4. **Enter the code:** enter the 6-digit code currently shown in the app and click **Confirm**. The code changes every 30 seconds – simply use the current one.



Choose an app with a backup function (with Microsoft and Google via your account) so the entries are kept when you get a new phone.

Backup codes

After the first factor, the portal shows ten backup codes once (format `XXXXX-XXXXX`). With a backup code you can sign in when you cannot use your passkey or app – for example after losing your smartphone.

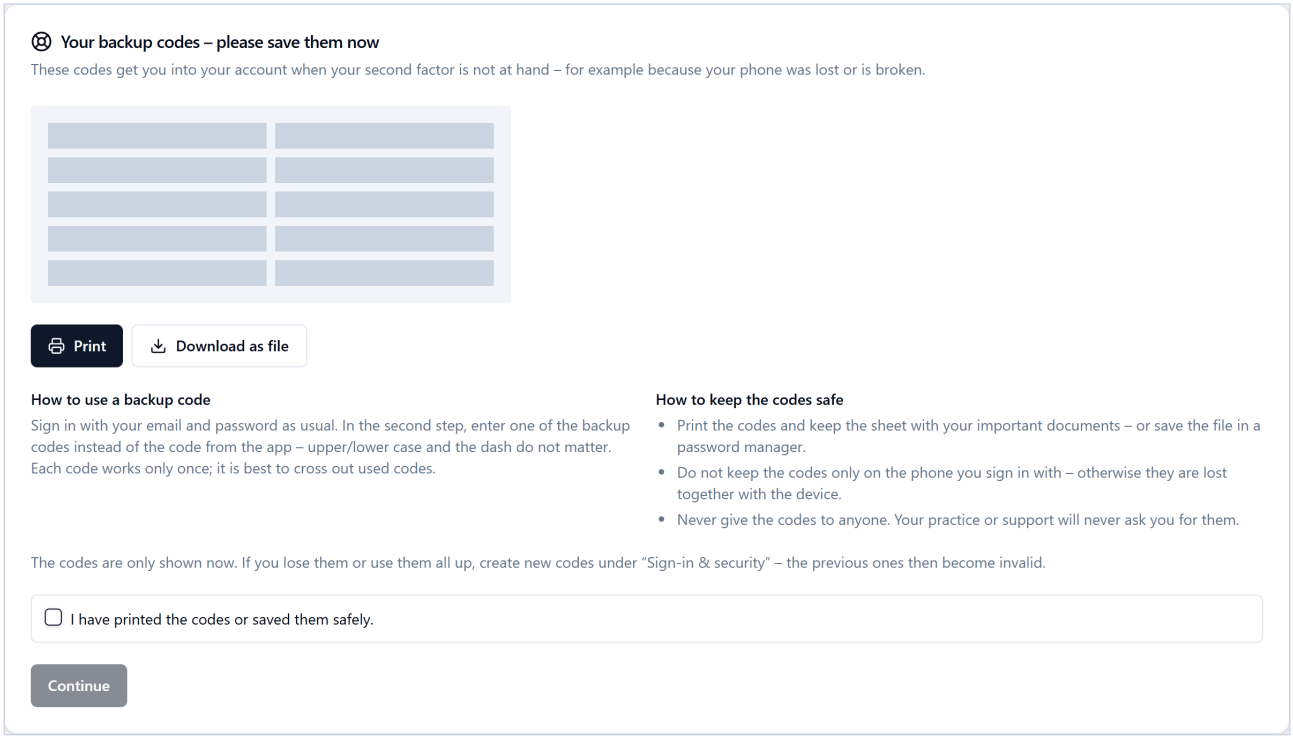

Figure 6. Backup codes after the setup (codes hidden here)

Using a backup code

Sign in with e-mail and password as usual and, in the second step, enter a backup code instead of the app code. Upper/lower case and the dash do not matter. Each code works exactly once – it is best to cross out used codes.

Keeping backup codes safe

- Click **Print** and keep the sheet with your important documents – or download the codes with **Download as file** and save the file in a password manager. The printout and the file also contain short instructions.
- Do not keep the codes only on the phone you sign in with – otherwise they are lost together with the device.
- Never give the codes to anyone. Your practice or support will never ask for your backup codes.

Only after you confirm that you have printed or safely saved the codes does **Continue** take you back to the overview. The page then shows how many unused codes you have left. **Generate new backup codes** gives you a new set; the previous codes become invalid.

Signing in with a second factor

1. Enter your e-mail address and password as usual and click **Sign in**.
2. In the step **Confirmation required**, click **Use passkey** and confirm the prompt of your device – or

enter the code from the authenticator app or a backup code and click **Confirm**.

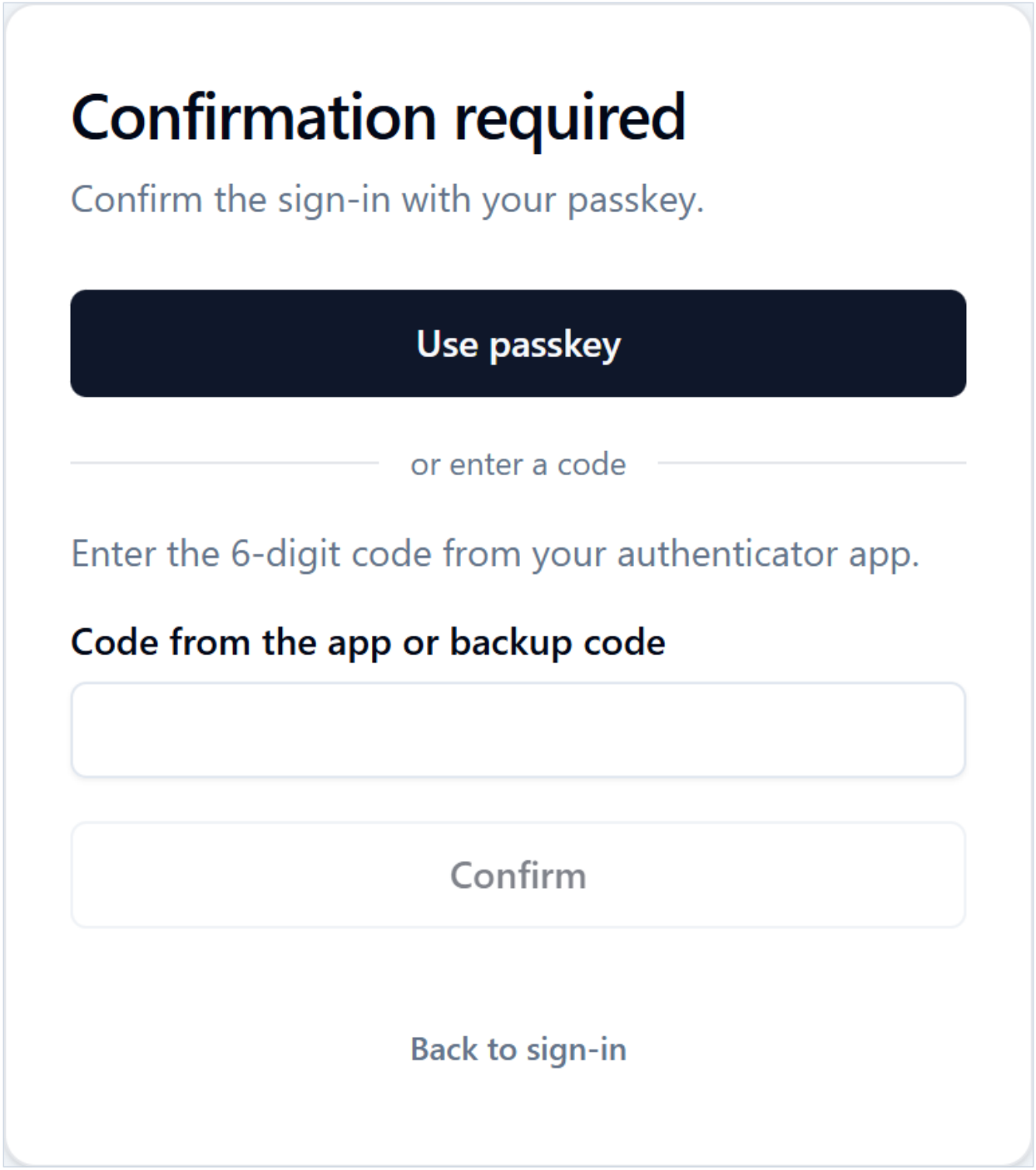

Figure 7. Second step of the sign-in

With a passkey you can also sign in without a password: click **Sign in with a passkey** on the login page or pick the passkey directly from the suggestion of the e-mail field. If the passkey is on your phone but you sign in at the computer, choose "Use another device" in the browser window and scan the QR code with your phone.

After five failed attempts (wrong password or wrong code), the account is locked temporarily: first for 15 minutes, longer after further failed attempts (at most 4 hours).

Managing factors

- **Rename** and **Delete** for individual passkeys and **Remove authenticator app** are on the page **Sign-in & security**.
- The last remaining factor cannot be removed – set up another one first. This way your account is never protected by the password alone.
- **Set up app again** replaces the authenticator app, for example after switching phones. The setup works as the first time; the previous app stays valid until you have confirmed the code of the new app. After that, only codes of the new app are accepted and your sign-ins on other devices are ended.
- Changes to the factors require your password. If your last confirmation was more than ten minutes ago, the portal also asks for a passkey or code (**Confirm your identity**).
- When a factor is removed, all other sessions of your account are ended.
- You receive an e-mail about every change – in the language of your last sign-in. If you did not make the change yourself, contact your practice or the administrator immediately.

Lost device

1. Sign in with e-mail, password and a **backup code**.
2. Open **Sign-in & security** and replace the lost factor:
    - **Authenticator app:** under **Authenticator app**, click **Set up app again** and set up the app on the new phone. Codes of the lost phone are no longer valid afterwards.
    - **Passkey:** first add a new passkey (or set up an authenticator app), then delete the passkey of the lost device.
3. Check how many backup codes you have left and generate new ones if needed.

If you have no backup code left, the portal administrator can reset your sign-in factors. At the next sign-in you then set up a new second factor.

If someone else changes your factors, you receive an e-mail – contact your practice or the administrator immediately.

My Patients (PACS View)

My Patients lets you search the archive (PACS) of the radiology practice for examinations in which you are registered as the referring physician. You only see your own patients.

Searching

1. Choose the **Time Period** of the examinations: *Today & Yesterday*, *Last Week*, *Last Month* (default), *Last 6 Months*, *Last Year*, *Last 2 Years* or *All*.
2. Optionally narrow the search by **Patient Name** and **Birth Date**.
3. Click **Search** (or press Enter in the name field).

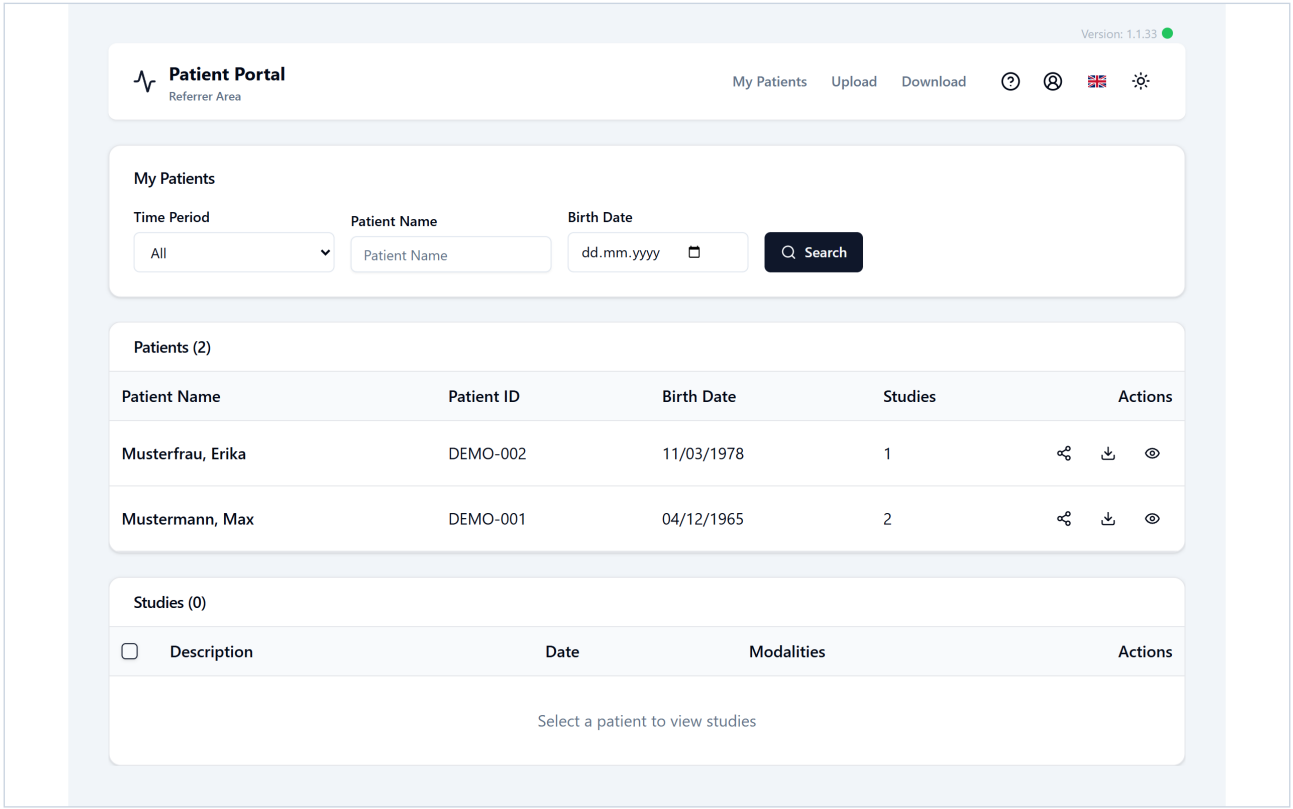

Figure 8. Search and result list

The **Patients** list shows name, patient ID, date of birth and the number of studies found. Depending on the practice's settings there is additionally

- a search field above the list that filters the results by name, patient ID, description or modality,
- a **Refresh** button with the time of the last update – search results are cached, **Refresh** queries the archive again.

Studies of a Patient

Click a row in the patient list. Below it, **Studies** shows all examinations of this patient with description, date and modality.

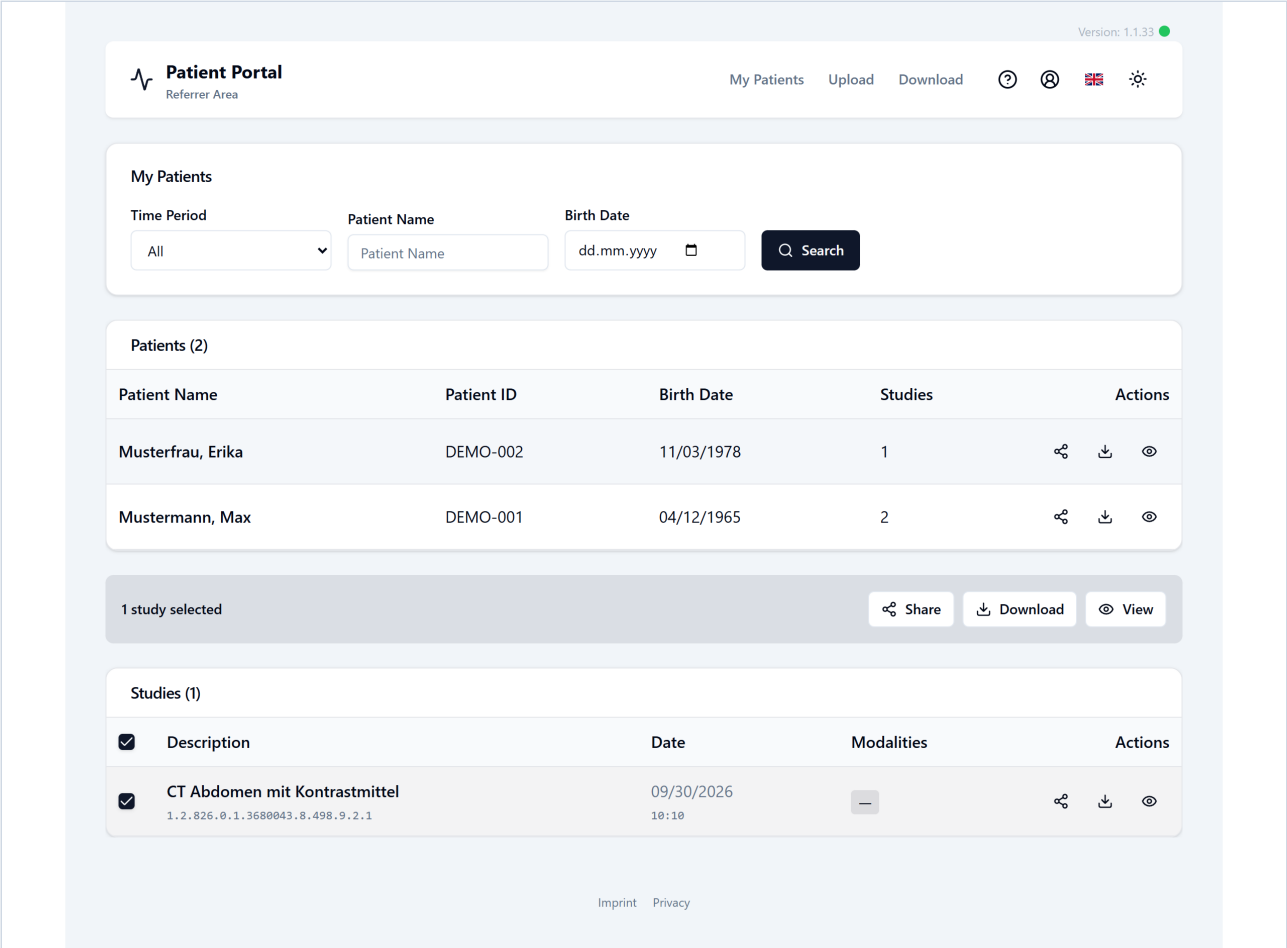

Figure 9. Patient selected, one study selected

Viewing, Downloading, Sharing

For patients (all studies) and for individual studies, three icons are available at the end of the row:

Icon	Action
Eye (**View**)	Opens the images in the image viewer in a new browser tab (scrolling with the mouse wheel, zoom, windowing, measuring).
Arrow (**Download**)	Downloads the study/studies as a ZIP archive in DICOM format.
Share (**Share**)	Creates an access link with QR code, see Sharing Examinations.

Select several studies using the checkboxes at the beginning of the rows; the actions then appear in the bar above the study list.



Retrieval from the archive: if a study is not yet available in the portal, it is first retrieved from the practice's PACS. The window "Retrieving Image Data" shows the progress; afterwards the chosen action starts automatically. Depending on the size of the study this can take from a few seconds to several minutes.

Which actions (download, share) are available to you is defined by the practice. If an icon is missing, the feature is not enabled for referrers.

To regularly transfer studies directly into your own PACS, use the desktop app RadioWeb Bridge.

Sharing Examinations

You can share examinations with your patients or with co-treating colleagues. For this, the portal creates a time-limited access link with a QR code.

Types of Shares

Patient share

Via the share icon in the **patient list**: the access covers all examinations of this patient.

Study share

Via the share icon in the **study list** or the action bar when several studies are selected: the access covers only the selected examinations.

Which types of shares you may create is defined by the practice.

Creating an Access Link

1. Click the share icon. If necessary, the images are first retrieved from the archive.
2. In the window **Generate Access Token** choose
   - the **Verification Type**: *None* (direct access), *Date of Birth* or *Password*,
   - the **Validity Period**.
3. Click **Generate Token**.
4. Pass on the access: **Print Page** (language of the printout via **Print in**), **Send as e-mail** (if set up) or copy the displayed link.



For patients, choose verification by *Date of Birth* – this protects the access without having to transmit an additional password. Always communicate a *Password* through a different channel than the link.

How recipients use the access is described in the Patient Portal's **User Guide**.

Uploading Prior Examinations

Upload lets you provide the radiology practice with images from other institutions – for example prior examinations for comparison. Which upload options are shown is defined by the practice.

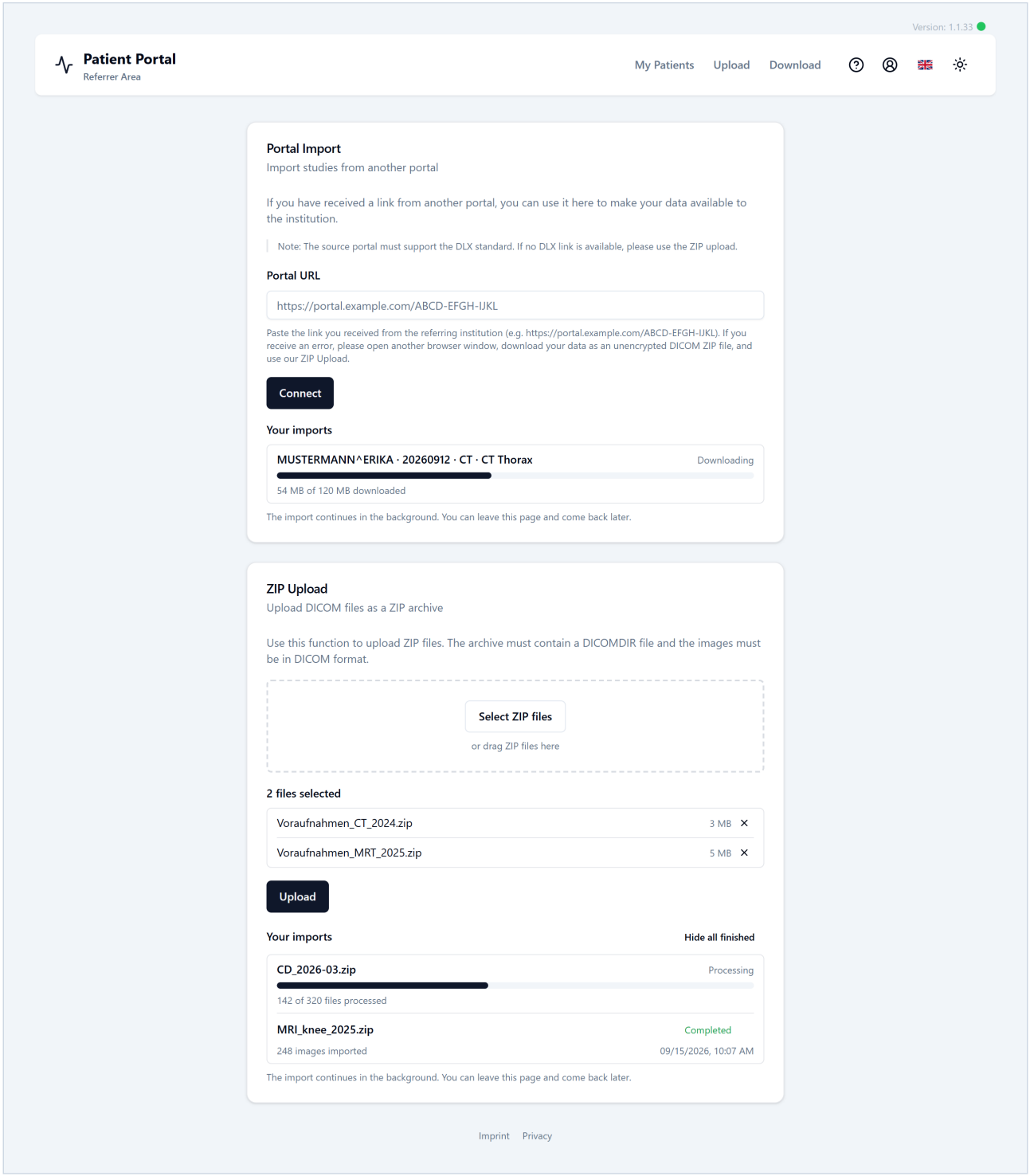

Figure 10. The upload page with running and completed imports

Portal Import (DLX)

If you have received a share link from another portal, the patient portal can fetch the studies directly

from there. This requires the other portal to support the **DLX** (DICOM Link Exchange) standard.

1. Paste the link into the **Portal URL** field and click **Connect**.
2. If asked, answer the other portal's security questions (for example the date of birth) and click **Verify**.
3. Select the studies and click **Import studies**.

The portal then downloads the selected studies from the other portal itself; you can follow the progress under **Your imports** (see Tracking progress).

If no DLX portal is found at the address, a notice appears: open the link yourself, download the data there as an (unencrypted) DICOM ZIP file and use the ZIP upload.

ZIP Upload

1. Click **Select ZIP files** and choose one or more archives – or drag the ZIP files into the dashed area.
2. Check the list of selected files; click **×** to remove a file again.
3. Click **Upload**.

Several files are uploaded one after another; each file then appears as its own entry under **Your imports**. Files that are not ZIP files are ignored. If uploading a file fails, the remaining files are still uploaded; the failed file stays selected so you can try again.

The ZIP archive must contain images in DICOM format – as provided by most patient CDs and portals when downloading. The images may also be located in subfolders or in further ZIP files inside the archive. A single file may be at most 512 MB unless your practice has set a different limit. Split larger amounts of data into several ZIP files.

Tracking progress

While uploading, a bar shows how much has already been transferred (for several files: "file 2 of 5 …"). The portal then processes the data in the background. Under **Your imports** you can see the current state of each import:

- **Waiting** – the import will start shortly.
- **Downloading** – Portal Import only: the study is being fetched from the other portal.
- **Processing** – the images are being stored; the bar shows how many files have already been processed.
- **Completed** or **Failed** – with the number of imported images or the reason for the failure.

You do not have to wait until an import has finished: you can leave the page and come back later. Imports from the last 24 hours remain visible (the time window and number of entries are configurable).

You can hide finished entries yourself: hover over an entry and click the **×** (always visible on tablets and smartphones), or click **Hide all finished**. Imports that are still running always remain visible.



You can conveniently read data from a CD or USB stick and upload it with the RadioWeb Bridge.

RadioWeb Bridge

The **RadioWeb Bridge** (labelled "DLX Download" under **Download** in the portal) is a desktop app for Windows and Linux. It transfers studies into your own infrastructure automatically:

- **DLX import** – download studies via a DLX share link,
- **CD / USB** – read DICOM data from storage media or folders,
- **DICOM sending** – send studies via DICOM (C-STORE) to your local PACS,

each optionally with upload into the Patient Portal, local storage, or both.

The app's user interface is currently in German; the German labels are given in the text below.

Downloading

1. Click **Download** in the portal navigation.
2. Choose the matching package in the **DLX Download** area:
   - **Windows:** *Setup (.exe)* or *MSI Package (.msi)* for software distribution,
   - **Linux:** *Debian/Ubuntu (.deb)* or *AppImage (portable)*.
3. A notice appears that the file is downloaded from the download server `download.radioweb.de`, together with file name, size and SHA-256 checksum. Confirm with **Download anyway**.

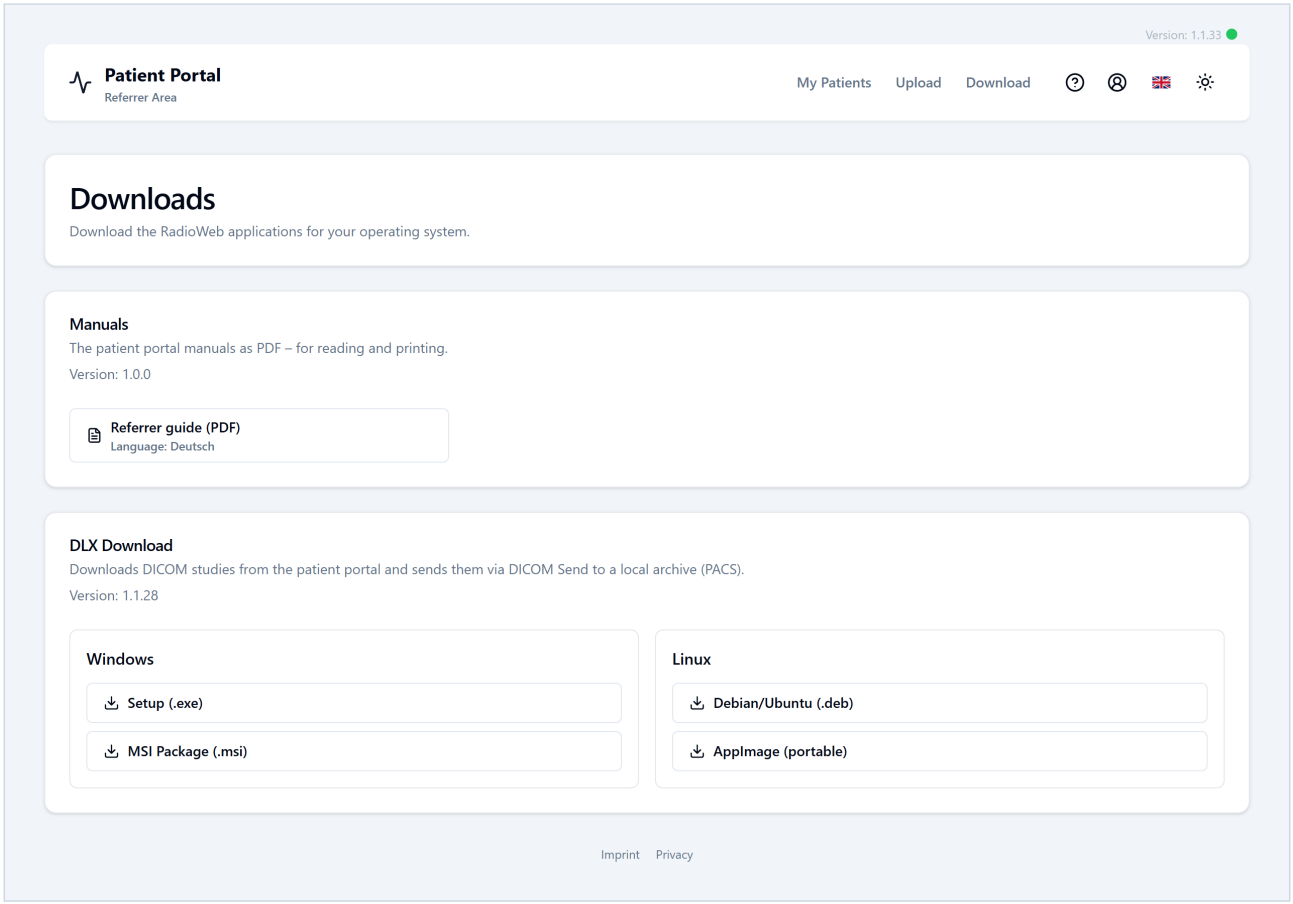

Figure 11. Download page with manual and RadioWeb Bridge

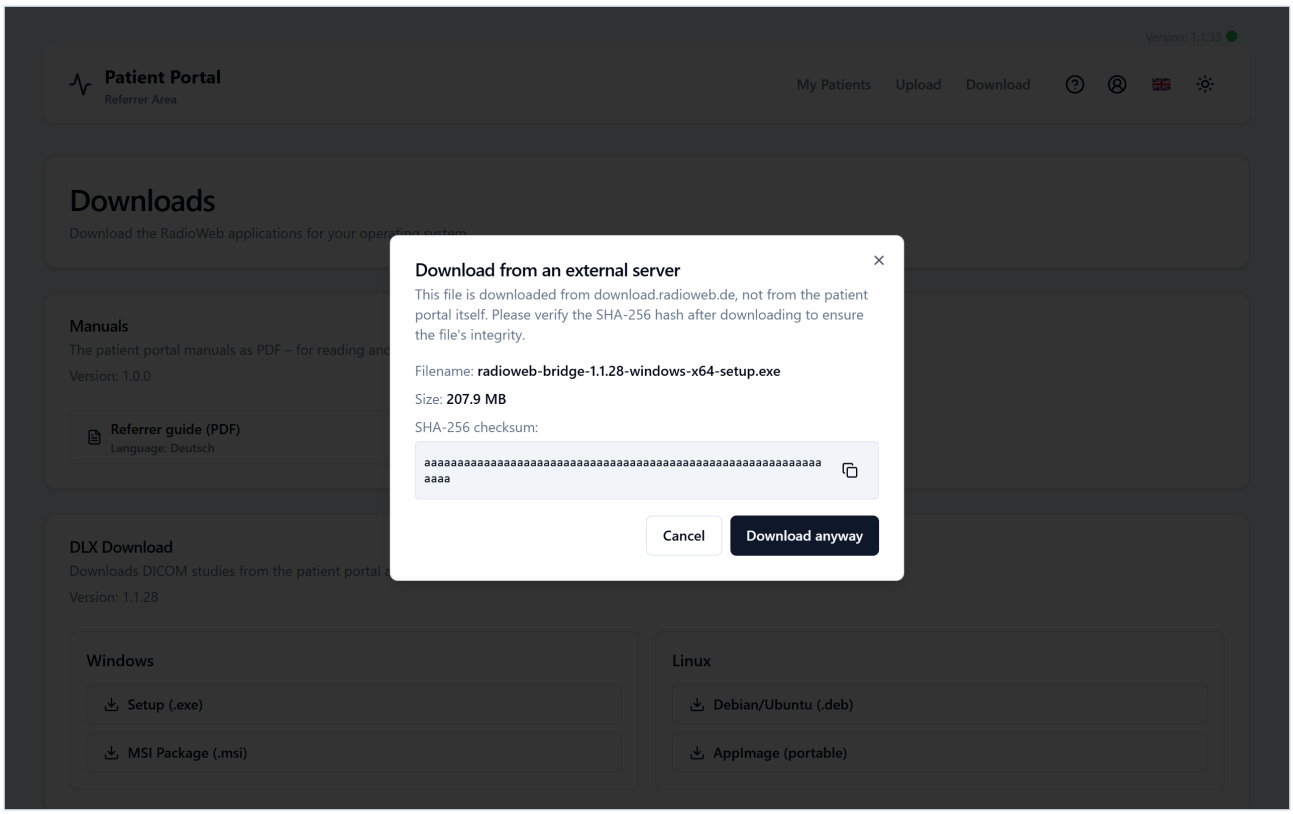

Figure 12. Notice before downloading with SHA-256 checksum



After downloading, verify the checksum to make sure the file is unchanged:

- Windows (PowerShell): `Get-FileHash .\radioweb-bridge-<version>-windows-x64-setup.exe -Algorithm SHA256`
- Linux: `sha256sum radioweb-bridge-<version>-linux-amd64.deb`

The value shown must match the one in the dialog (copy it to the clipboard using the copy icon).

Installing

Windows

Run the setup file and follow the installation wizard. The MSI package is suitable for automatic distribution by your IT.

Linux (Debian/Ubuntu)

```
sudo apt install ./radioweb-bridge-<version>-linux-amd64.deb
```

Linux (AppImage)

`chmod +x radioweb-bridge-<version>-linux-amd64.AppImage`, then start the file – no installation required.

Configuring

Open the tab **Einstellungen** (settings) in the app.

Portal

Field	Meaning
Backend-URL	Address of the Patient Portal, e.g. `https://portal.praxis.de`
API-Token (Bearer)	Access key for uploading into the portal. You receive it from the practice.

Use **Testen** (test) to check the connection to the portal. Without a portal connection, DLX download, local storage and DICOM sending are still possible.

DICOM

Field	Meaning
Lokaler AET	AE title the app uses for DICOM connections (e.g. `BRIDGE`). It must be registered as an allowed sender in your PACS.
Standard-DICOM-Knoten	Target for DICOM sending: **AE Title**, **Host / IP** and **Port** of your PACS.

Use **Echo testen** (test echo) to check the DICOM connection to the PACS (message "C-ECHO erfolgreich").

General

Field	Meaning
Downloadverzeichnis	Folder for locally stored studies (optional)
Temporäres Verzeichnis	Temporary storage during processing (optional)
History-Verzeichnis	Successfully processed files are moved here and deleted after the configured number of days (optional)
Fehler-Verzeichnis	Failed files are moved here (optional)
Nach Import – Modus	What happens to imported studies (see below)

Table 1. Modes "Nach Import" (after import)

Mode	Effect
Ins Portal laden	Studies are uploaded into the Patient Portal.
Lokal speichern	Studies are only stored in the download folder – no portal required.
Portal + lokal speichern	Upload into the portal plus a local copy.
Portal + DICOM-Versand	Upload into the portal; the portal forwards the studies to the DICOM node.
Nur DICOM-Versand	Studies are sent directly to your PACS via C-STORE – no portal required.

Save each section with **Speichern** (save).

Using

DLX import

1. Tab **DLX-Import**: paste the DLX link (e.g. `https://server.example.de/dlx/v1/token/ABCDE`) and click **Verbinden** (connect).
2. Answer the security questions if required.
3. Select the studies and click **Studien importieren** (import studies). The studies are processed according to the configured mode.

CD / USB

1. Tab **CD / USB**: choose the drive or folder and click **Verzeichnis scannen** (scan folder).
2. The DICOM files found are listed; select the ones you want and start processing.

DICOM sending

The tab **DICOM-Versand** shows the log of all transmissions: target, time and number of sent and failed objects with error messages.



Screenshots of the desktop app will follow in a later version of this guide.

Frequently Asked Questions

1. *Why can I not find a patient?*

   The PACS view only shows examinations in which you are registered as the referring physician at the practice. Also check the **Time Period** – the default is *Last Month*. If an examination is still missing, please contact the practice.

2. *The search shows outdated results.*

   Search results may be cached. Click **Refresh** (if shown) to query the archive again.

3. *Opening a study takes a long time.*

   If the study is not yet available in the portal, it is first retrieved from the practice's archive ("Retrieving Image Data"). Large CT or MRI studies need some time for this.

4. *The status light in the top right is red.*

   The coloured dot next to the version number shows the connection to the practice's archive. When it is red, retrieval is currently not possible – please try again later.

5. *The icons for downloading or sharing are missing.*

   These features are defined by the practice for referrers.

6. *Where can I find this guide?*

   In the portal under **Download** (**Manuals** area) and via the help icon (question mark in the top right) under **Manuals**.

Privacy

- You only see examinations of your own patients; every access is logged.
- Only pass access codes and share links to authorised persons and choose an appropriate validity period.
- Downloaded studies contain personal health data – store them only on protected systems.
- Sign out after use, especially at shared workstations.