DENTALXPAND LEARNING CENTER / WORK HUB

Manage Documents, Files, Folders, and Previews

A detailed guide to the authorized Documents library, file types, search and view controls, administrator upload, file records, signed previews, download and deletion boundaries, folder metadata, tenant-aware paths, storage policy, troubleshooting, and verification.

VERSION	1.0	AUDIENCE	Authorized users and administrators
FORMAT	Website + PDF	UPDATED	July 2026

Every person, organization, practice, provider, patient, client, employee, file, filename, path, URL, document, date, size, count, status, and device state shown in this guide is fictional. Never use live protected data, credentials, tokens, signed URLs, private exports, unredacted third-party files, or another-tenant content in training material.

Contents

Select any section in supported PDF viewers. Use the Contents link in the upper-right corner of every content page to return here.

How to use this guide
Read identity, tenant scope, role boundaries, file purpose, source-of-truth, retention, and approved device guidance first. Then practice library navigation, search and type filters, authorized previews, privileged uploads and actions, signed-link discipline, storage controls, safe troubleshooting, and completion verification.

01 / PURPOSE

Use Documents as an authorized library, not an unrestricted file browser

Area	Current role	Boundary
File record	The current screen reads file records and orders the loaded set newest first.	A visible card is not a complete legal, audit, retention, organization-wide, or source-of-truth inventory.
Storage object	Uploads place a binary object in the files bucket and save a record with path, folder, uploader, size, and MIME type.	Both object and record must be allowed by current tenant, practice, database, and Storage policy.
Preview	View can open an available file URL in the in-app document viewer.	A preview is not a public copy, permanent identifier, download entitlement, approval, or current version guarantee.
File action	The reviewed page presents upload, download, and deletion controls to admin or super-admin roles.	Visible client controls never replace server-side authorization, Storage policy, retention, or source-workflow review.
Source workflow	Tasks, client instructions, agreements, credentialing, finance, and other permitted workflows can own the current decision.	Do not make a material decision only from a stored copy or file card.

A file card is a starting point

Before you rely on a file, confirm the current account, tenant, practice, role, source workflow, version, status, retention requirement, and legitimate purpose. A filename or type icon does not validate the content or grant permission.

Open Documents	Roles and access	Organization context
Open Documents	**Roles and access**	**Organization context**

02 / ACCESS

Confirm identity, expected tenant, and safe device context

Check	Confirm	Why it matters
Identity	Your own active DentalXpand account and current session.	A shared browser, copied signed link, local download, screenshot, cache, or another person's profile is not permission.
Organization and practice	Expected DentalXpand organization, practice, and operating context.	Files must not bridge Guardian Connect and DentalXpand or unrelated organizations, practices, patients, providers, clients, or employees.
Role and action	Whether you may view, upload, download, or delete the specific record.	The UI role condition is only one layer; current page, record, database, and Storage policy must all permit action.
Source and retention	The owner workflow, current file, retention need, and whether a newer approved version exists.	A library action can affect or misunderstand documents connected to tasks, client instructions, agreements, cases, or reports.
Local copy	Approved private device and controlled local storage when an authorized download is needed.	A local copy can escape the application through shared folders, browser history, sync, forwarding, backup, or an unapproved device.

Unexpected data is a security incident

If another tenant, Guardian Connect, patient, provider, client, practice, employee, or unrelated file appears, stop. Do not open, download, forward, copy, screenshot, or test more access. End the session according to policy and report minimum non-sensitive context.

03 / LIBRARY

Read file totals, types, and actions without treating them as business proof

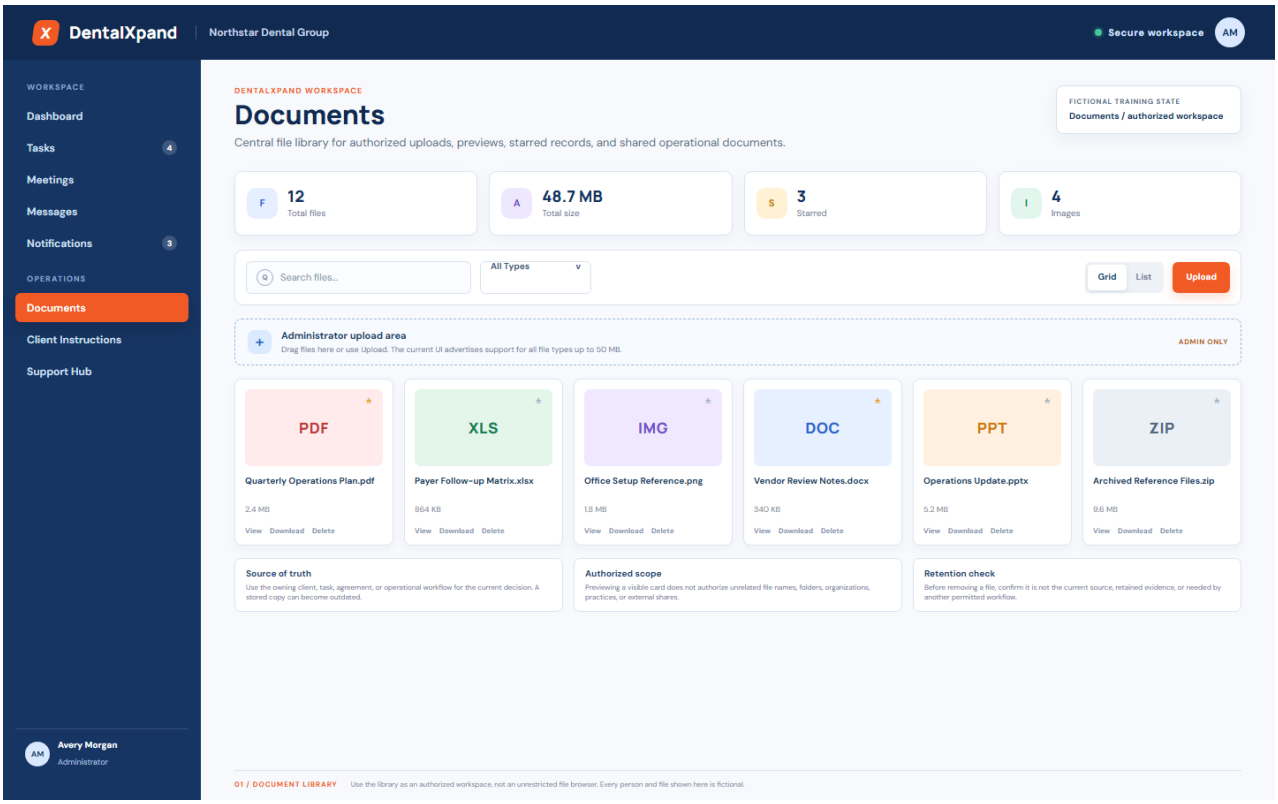

Figure 1. Fictional Documents library with loaded file summaries, type and search controls, administrator upload area, grid cards, and source, scope, and retention reminders.

1. Open Documents from the permitted sidebar or authorized route; respect a denied route instead of using a copied link or another person's session.
2. Read total files, size, starred count, and images as current display indicators, not full retention, audit, or organization-wide inventory evidence.
3. Use file type icons only as extension-derived display categories. They do not validate content, confidentiality, malware status, accuracy, or approval.
4. Open View only for a file you have a legitimate purpose to review, then verify its title, source, current version, and scope.
5. Treat upload, download, and delete as separate privileged actions with different operational effects.

> Example-looking entries need verification
> The current page uses a local mock-data fallback when an API fetch fails. If the library shows sample-looking records or an unexpected empty state after an error, refresh once and verify expected scope before treating it as live data.

04 / SEARCH AND VIEW

Narrow visible records without turning search into data discovery

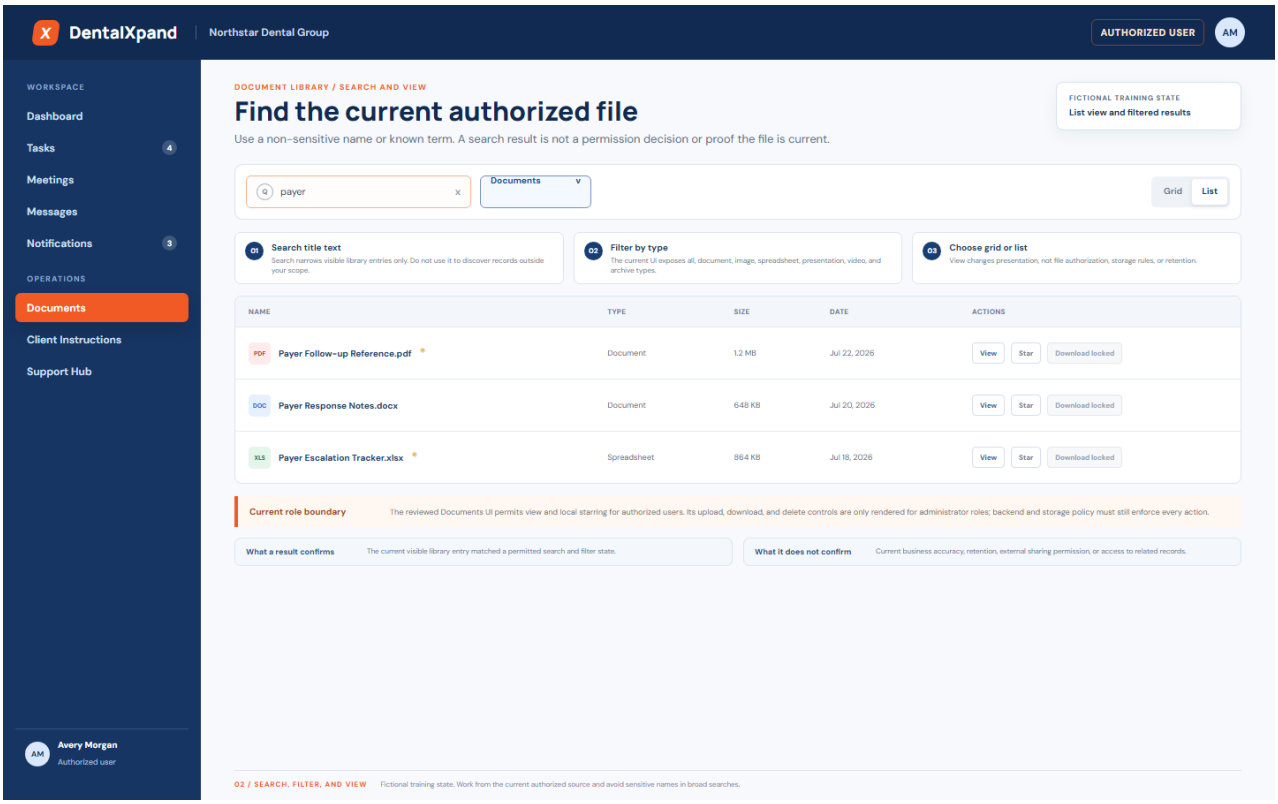

Figure 2. Fictional Documents list view with a text search, Documents type filter, grid and list control, current visible results, View and Star actions, and the administrator-only download boundary.

Control	Use it for	Do not assume
Text search	Finding currently visible filename text with a known non-sensitive term.	A result authorizes related records, proves a file is current, or a missing result means data should be exposed or is permanently absent.
Type filter	Choosing all, document, image, spreadsheet, presentation, video, or archive in the current selector.	A type icon or extension is malware validation, content classification, confidentiality label, retention class, or approval.
Grid and list	Grid supports visual scanning; list compares name, type, size, date, and exposed actions.	Changing view changes authorization, tenant scope, Storage policy, file content, ownership, or source truth.
Star	Marking a currently visible file as a useful personal visual cue.	The star is shared, audited, durable, an approval, completion, retention designation, or ownership record. The reviewed page changes local state only.
Visible actions	Opening an authorized preview and understanding which actions are exposed to the current role.	Client visibility alone proves server authorization. Backend, database, and Storage policy still decide the durable result.

05 / ADMIN UPLOAD

Upload approved files only after confirming role, purpose, and tenant scope

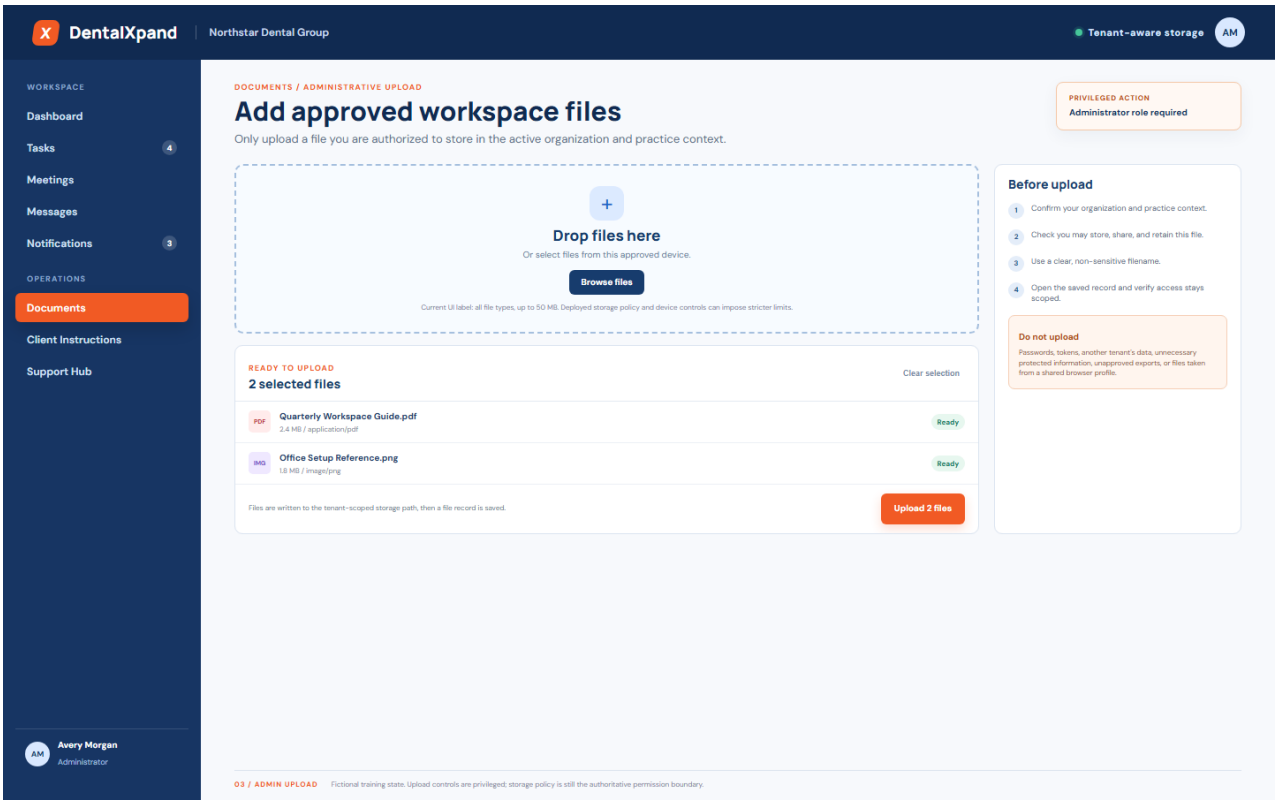

Figure 3. Fictional administrator upload screen with drag-and-drop area, file queue, tenant storage context, pre-upload checks, and unsafe-upload warning.

Step	Reviewed current behavior	Required discipline
Confirm authority	The page checks whether the current role is admin or super_admin before upload, drop, download, or delete behavior.	Use your own authorized account in the expected organization and practice. Client role logic is not a substitute for policy.
Select files	The current UI provides a multiple-file picker and drag-and-drop area. Its visible label says all file types up to 50 MB.	Treat this as UI guidance. Bucket limits, MIME handling, device rules, network, policy, and deployment configuration can still reject a file.
Build path	The API adds documents/timestamp_filename to a tenant-aware storage path when organization and practice context are present.	Do not forge or reuse another organization or practice path. Cross-organization and cross-practice path attempts are rejected by the client helper when tenancy context exists.
Store record	The API uploads to the files bucket, then inserts a record with storage reference, folder, uploader, size, and MIME type.	Verify the saved record using an authorized view. Do not share raw references, signed URLs, logs, or unapproved local copies.

Failure does not justify a bypass

Do not retry a failed upload through another person's account, public drive, personal storage, a shared browser profile, another tenant, or Guardian Connect. Preserve only a non-sensitive error description and use approved support.

06 / PREVIEW

Use a signed in-app preview as an authorized reading surface

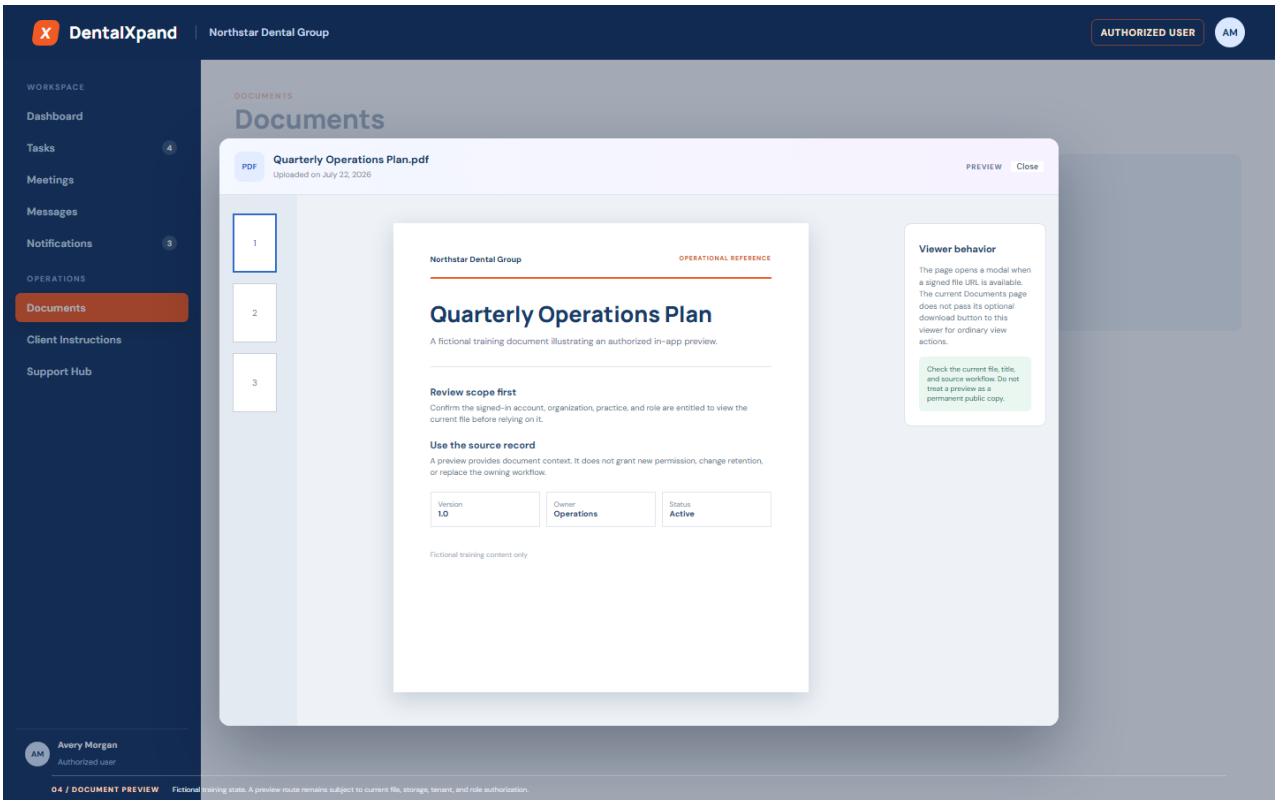

Figure 4. Fictional in-app document viewer showing file title, upload date, preview state, document pages, and source-verification guidance.

Area	Reviewed behavior	Boundary
View action	When a record has downloadUrl or url, the page passes the URL, title, and upload date into the document viewer.	No URL means the viewer cannot load the file. Do not obtain a URL through a copied link, another user, or external service.
Viewer	The viewer loads the supplied URL in an iframe and applies reduced-toolbar parameters for ordinary URLs. Google Drive-like links receive a preview route.	File format, browser support, URL policy, expiration, storage access, network, and source availability can affect rendering.
Download distinction	The reusable viewer can display an optional download button, but the current Documents page opens it without that option for ordinary View actions.	Preview is not a download entitlement and must not be used to create an uncontrolled local copy.
Signed URL	The file API creates signed Storage URLs for accessible listed objects; the helper default is 3,600 seconds.	A signed URL is sensitive, time-limited operational access, not a permanent public URL, tenant bypass, or sharing mechanism.

Documents guide	Tasks evidence	Client instructions
Documents guide	**Tasks evidence**	**Client instructions**

07 / FILE ACTIONS

Download and delete only with retention and source-workflow discipline

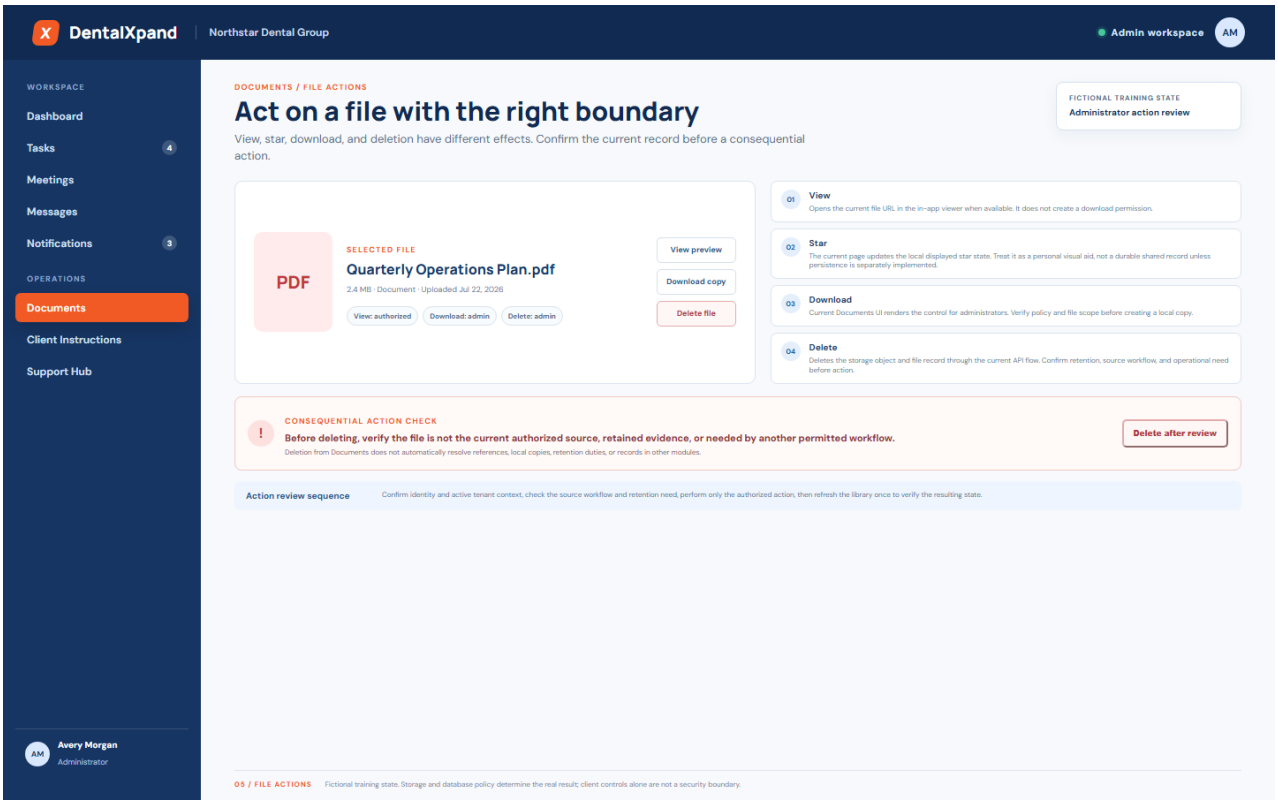

Figure 5. Fictional administrator file action screen distinguishing view, local star, download, deletion, and consequential-action review.

Action	Current behavior	Required discipline
View	Opens the current file URL in the in-app viewer when available.	Check title, source, tenant, role, and current version. Viewing does not approve, retain, or change the source record.
Star	Changes the current visible state in the Documents page.	Do not treat a star as a shared, durable, audited, approved, retained, or completed status.
Download	The Documents UI exposes download to admin or super-admin roles and triggers a browser anchor from the current URL.	Only download when policy permits. Keep copies in approved storage and do not forward the file or signed link.
Delete	The API retrieves the path, removes the Storage object when present, then deletes the database record.	Confirm retention, references, version, source workflow, and business need first. Deletion does not clean local copies or other module references automatically.
Confirm result	The reviewed page removes a card and reports success even in its delete-error fallback.	For material deletion, refresh the authorized library and check the owning workflow. Do not assume local disappearance proves durable deletion.

08 / STORAGE SCOPE

Keep file metadata, paths, signed delivery, and policy in the intended tenant

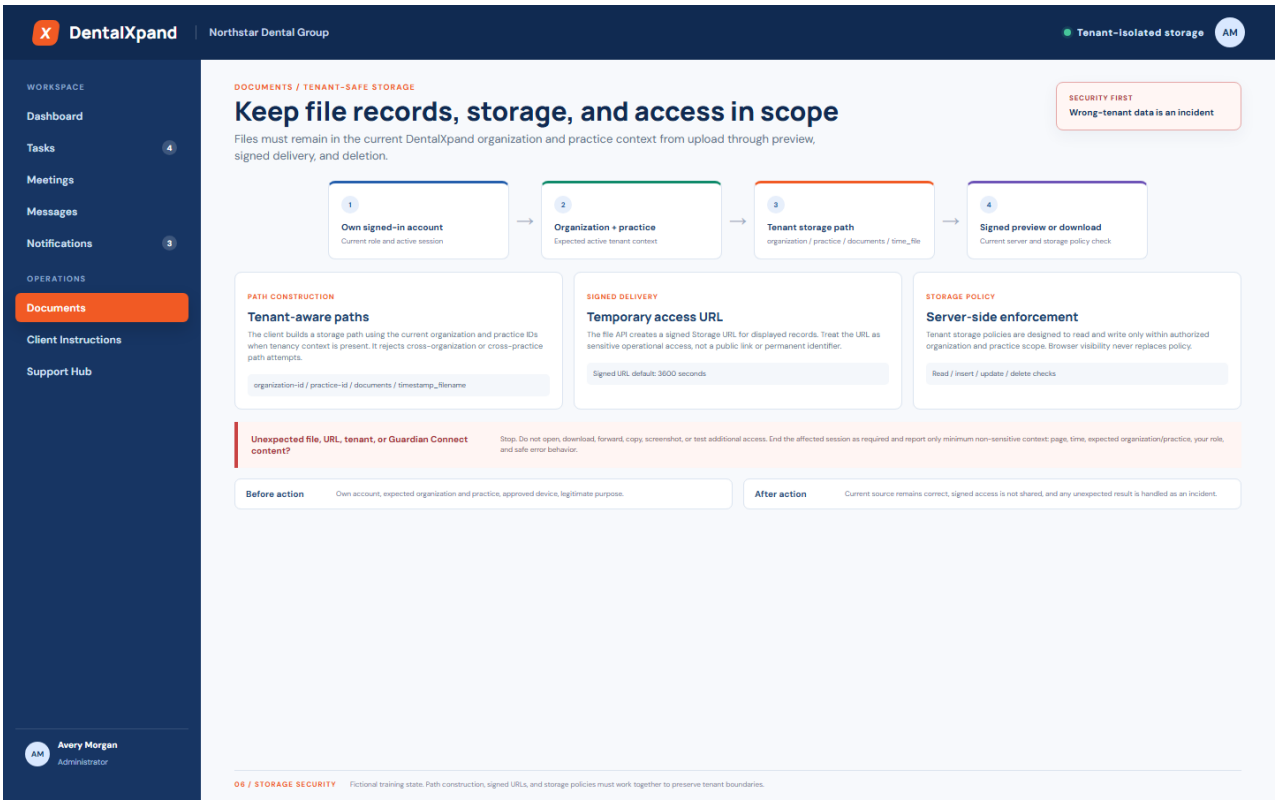

Figure 6. Fictional tenant-safe document storage path from signed-in account and expected organization/practice through storage path, signed delivery, policy enforcement, and incident response.

Area	Reviewed implementation	Boundary
Folder metadata	The files API stores a folder value and can filter records by it; Documents uploads default to the documents folder label.	The current Documents UI has type filters but no folder tree, create, rename, move, or folder-navigation control. Do not describe unimplemented folder actions as available.
Tenant path	With organization and practice context, the client helper prefixes the relative path with those IDs and validates both identifiers.	A missing context keeps a legacy relative path for compatibility. Production needs the tenant migration and context setup applied and verified.
Signed delivery	The file API signs an available Storage object for temporary access.	Signed access must not be shared, copied into another product, treated as public, or used after it is no longer authorized.
Storage policy	The multi-tenant migration defines Storage read, insert, update, and delete checks by organization and practice, and marks buckets non-public when that policy block can run.	Verify actual policies in the deployed Supabase project. Source code cannot prove a production policy is installed or working.
Unexpected data	Wrong tenant, unrelated file, path, signed URL, preview, or Guardian Connect content indicates a potential isolation fault.	Stop exposure immediately and report safe context only. Do not inspect deeper, download, forward, screenshot, or test related access.

09 / TROUBLESHOOT

Resolve expected file states without bypassing access or exposing data

What you see	Possible reason	Correct first response
Documents is missing or direct route is denied	Page permission, role, current session, organization, practice, or route policy may deny access.	Respect the response, confirm expected account and context, then use the authorized administrator or support path.
Sample-looking records or an unexpected empty list	The page has a local mock-data fallback after a file query error, or current scope has no visible records.	Refresh once and verify expected tenant context. Treat displayed samples as unverified until current authorized backend state is confirmed.
Upload fails	Role, size, MIME handling, network, bucket, tenant path, practice context, policy, or record-save state can fail.	Keep the file in approved storage, record a non-sensitive error, and report through support. Do not use public, personal, another-tenant, or Guardian Connect storage.
Preview does not load	Signed URL, expiration, format, iframe policy, browser, network, storage access, or file URL may be unavailable.	Refresh the authorized page once and report safe symptoms. Do not paste a signed URL into an external testing service.
Download or delete is unavailable	Current role is not administrator, policy denies the action, file state changed, or object URL is unavailable.	Do not borrow another user account. Confirm retention and workflow need, then ask an authorized administrator or support.
Wrong tenant or Guardian Connect content appears	Potential tenant, cache, Storage, URL, API, session, policy, or configuration isolation issue.	Stop, avoid further exposure, end the affected session, and report only page, time, expected context, role, safe description, and steps tried.

Support safely

A support request should contain minimum necessary, non-sensitive context. Never paste the file itself, a signed URL, raw Storage path with live IDs, credential, token, screenshot with protected content, or another user's details into a ticket.

10 / COMPLETION

Verify safe Documents handling

- I can distinguish a file card, file record, Storage object, signed URL, preview, and local download as separate surfaces with different authorization and privacy risks.
- I confirm my own account, expected organization and practice, role, source workflow, file purpose, version, and retention need before acting.
- I can use search, the current type filter, grid, list, and local star state without treating them as authorization, source truth, retention, or audit controls.
- I know current Documents UI exposes upload, download, and delete only to admin or super-admin roles, and that server/database/Storage policy must still enforce the result.
- I understand that the 50 MB visible upload label is not the only enforcement point and deployment conditions can reject a file.
- I can distinguish API folder metadata from a folder browser and know this screen does not currently provide folder creation, moving, renaming, or tree navigation.
- I understand that previews use available signed URLs, are not permanent public links, and do not automatically create download access.
- I verify material deletion after refresh because local UI state can differ from durable Storage and database persistence.
- I know deployed tenant context, tenant-aware paths, signed delivery, and Storage policies must protect the intended organization and practice at every stage.
- I stop and report immediately if another tenant, Guardian Connect, patient, provider, client, practice, employee, or unrelated file appears.

Next lesson
Continue to Manage Client Instructions, Options, and Versions. That workflow adds client-facing structure and version history while keeping the same tenant, source-record, signed-file, and retention discipline.

Next guide	All resources	Documents website
Next guide	**All resources**	**Documents website**