DENTALXPAND LEARNING CENTER / PROVIDER AND DSO

Operate a DSO or Multi-Practice Workspace

A repository-grounded operator guide to one organization tenant, canonical locations, organization-wide totals, actual practice context, shared teams, practice-aware records, fair comparison, location lifecycle, and tenant isolation.

VERSION	1.0	AUDIENCE	DSO owners, organization administrators, and authorized managers
FORMAT	Website + PDF	SCOPE	DentalXpand DSO and multi-practice operations

Fictional screenshots and minimum necessary data
All screenshots use fictional training data. Never place passwords, MFA codes, recovery material, patient records, payer credentials, full identifiers, another tenant, another Xpand product, or Guardian Connect data in comparisons, screenshots, PDFs, support messages, exports, or AI prompts.

Contents

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

> Current release: no universal practice switch
> The Header and Sidebar do not provide a global practice selector. Context comes from membership scope, an explicit owning-workflow field, a canonical relationship, or the database default. Never infer or manipulate a practice context.

01 / OPERATING MODEL

Keep organization, practice, access, relationship, and record scope separate

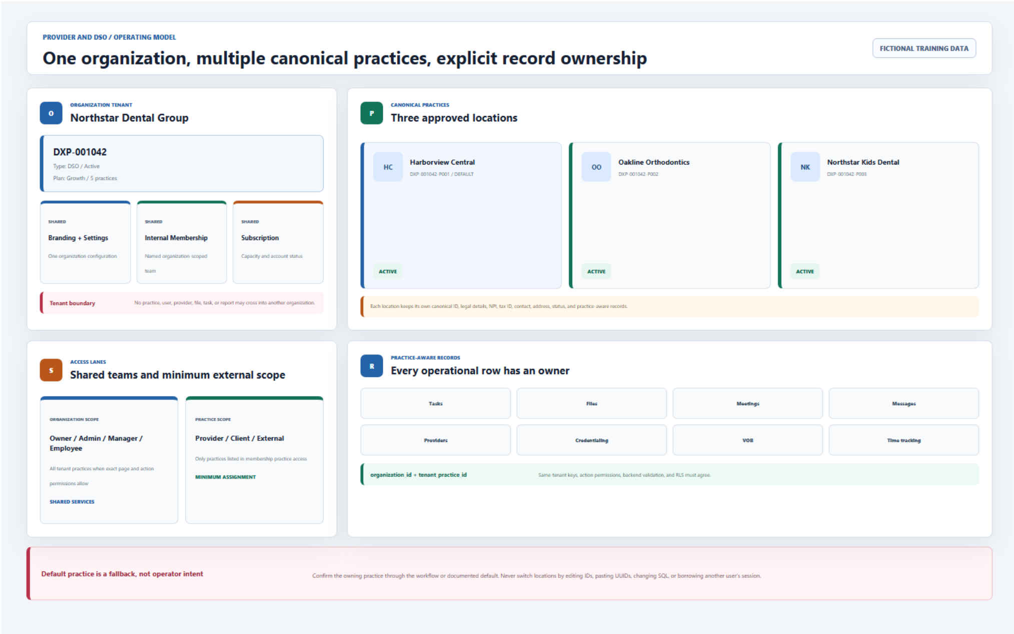

Figure 1. Fictional DSO operating model showing one organization, canonical practices, shared internal scope, minimum external assignments, practice-aware records, and tenant enforcement.

Layer	Purpose	Operator boundary
Organization	Tenant for DSO identity, subscription, shared branding, settings, and membership.	Nothing from another client, product, or Guardian Connect belongs here.
Practice	Canonical location with ID, code, legal details, NPI, tax ID, contact, status, and default marker.	Free text and provider metadata do not replace this record.
Organization scope	Internal roles can reach tenant practices when exact permissions allow.	It is broader than a selected location and is not automatic Admin.
Practice scope	External roles receive only approved membership-practice access rows.	Use the complete minimum assignment set.
Practice-aware record	Operational rows carry organization_id and tenant_practice_id.	Owning practice must be confirmed before and after Save.
Provider relationship	Links a provider to one or more canonical practices and an optional primary location.	It remains separate from external login assignments.

02 / READINESS

Define the approved operating map before production work

Confirm	Required evidence	Stop when
DSO organization	Exact active name, code, type, owner, subscription, and operating purpose.	The request combines unrelated entities or products.
Location roster	Approved legal directory with location name, NPI, tax ID, contact, address, and status.	A location is duplicated, informal, closed, or unmatched.
Default practice	Intentional catchment location for workflows without explicit practice context.	Default remains unexplained Unassigned or inactive.
Shared team	Named internal owners, managers, departments, exact pages, and actions.	A shared login or broad Admin workaround is proposed.
Record owner	Canonical practice for each provider, task, file, case, VOB, message, meeting, or report row.	Owning practice cannot be stated before Save.
Comparison rules	Same scope, period, timezone, statuses, source, denominator, refresh time, and currency.	An organization total is being called a practice result.

> Provisioned DSO workspaces can begin with Unassigned
> The platform creates one default practice so practice-aware tables have a valid key. Before production, an authorized administrator must rename and complete it as a real location or govern it as a temporary transition bucket. Do not leave operational records in an unexplained placeholder.

Practices / Locations	User Management
Practices / Locations	**User Management**

03 / ORGANIZATION OVERVIEW

Read Dashboard totals as the authorized tenant view

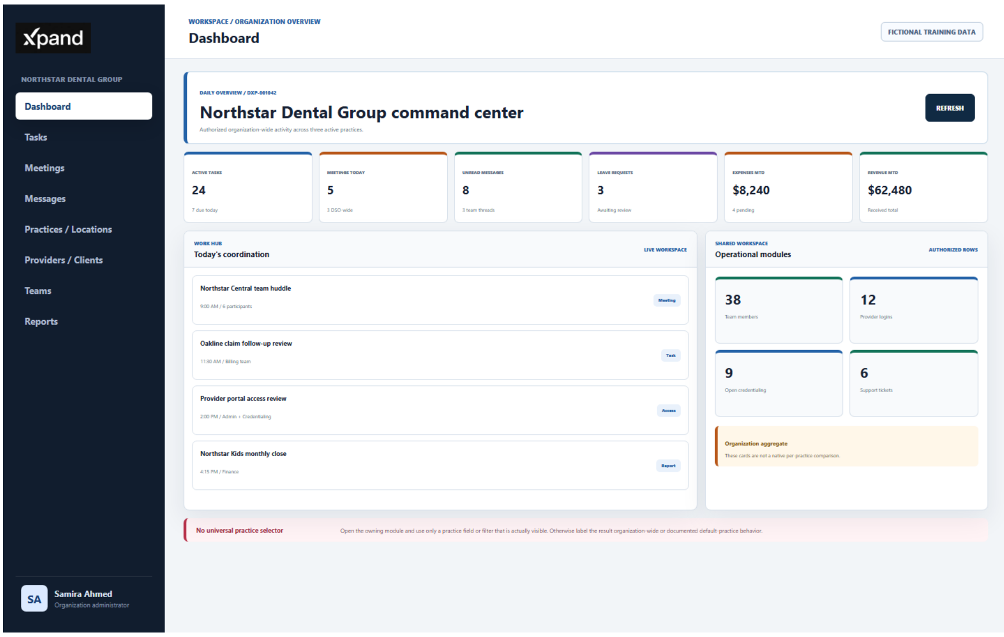

Figure 2. Fictional DSO Dashboard with organization-wide work, HR, finance, provider, credentialing, support, and recent-activity totals plus a no-global-switch warning.

Dashboard step	Current behavior	Operator rule
Confirm identity	Page loads for the signed-in user inside the active organization context.	Check named account and DSO before reading metrics.
Read admin totals	Administrator queries aggregate the rows returned by tenant and practice policies.	Label values organization-wide unless a module clearly filters one practice.
Separate roles	External users receive focused client views; employees receive personal work views.	Do not compare role-specific dashboards as equivalent totals.
Refresh	Live subscriptions and periodic refresh update current authorized rows.	Record refresh time and reconcile before decisions.
Investigate	Cards link to owning operational modules.	Use only practice fields and filters that the destination actually exposes.
Compare	Dashboard does not provide a universal native practice drilldown.	Build comparison from approved practice-aware evidence.

04 / CANONICAL ROSTER

Maintain one active record for every approved location

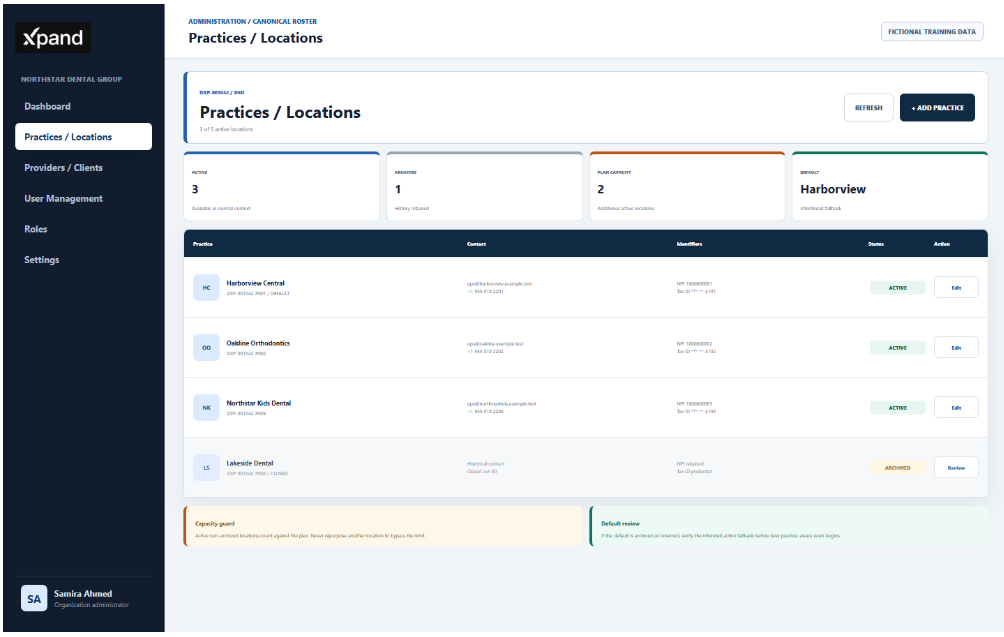

Figure 3. Fictional Practices / Locations page with active and archived locations, plan capacity, canonical codes, default practice, identifiers, and lifecycle notes.

Roster control	Current behavior	Required practice
DSO label	Navigation and page heading use Practices / Locations.	Use the canonical directory, not a provider nickname.
Code	New practice receives an organization-prefixed sequential code.	Use generated code for reconciliation; do not invent IDs.
Status	Archived records leave normal tenant context but preserve history.	Complete handoff before archive; do not recreate a duplicate.
Default	Organization-scoped database fallback prefers the active default, then another active practice.	Keep one intentional operational default.
Plan limit	Active non-archived practice count is checked against plan or override.	Resolve capacity through the approved subscription process.
Identifiers	Legal name, NPI, tax ID, contact, phone, and address belong to the canonical row.	Verify approved source and protect unnecessary disclosure.

05 / PRACTICE CONTEXT

Determine whether work is organization-wide, explicit, relationship-derived, or defaulted

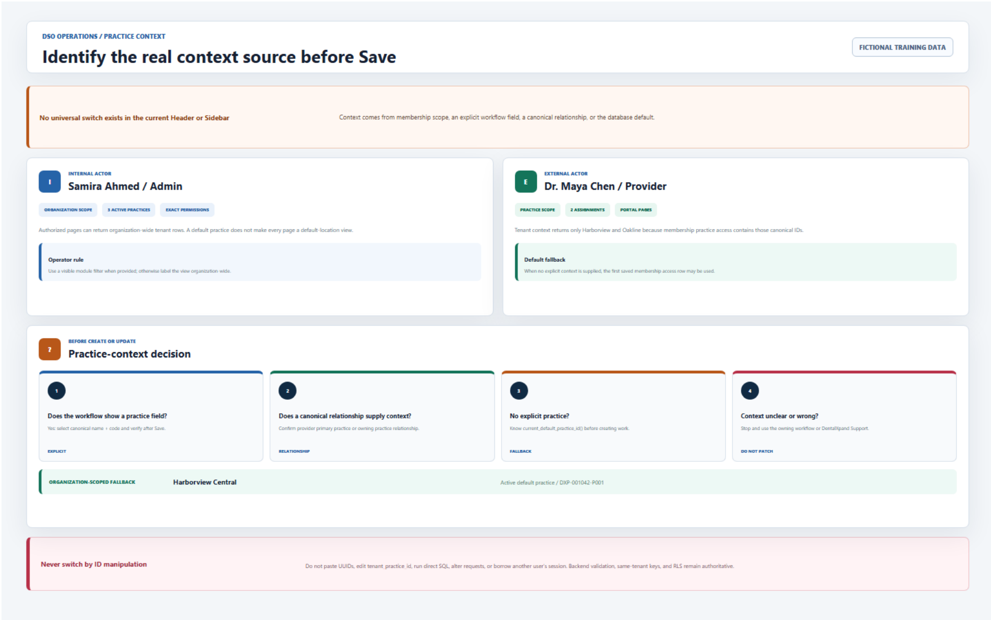

Figure 4. Fictional practice-context decision showing internal organization scope, external assigned-practice scope, explicit workflow selection, relationship context, default fallback, and stop conditions.

Situation	Context source	Required action
Internal user	Organization membership can reach tenant practices when exact permissions allow.	Assume organization-wide unless a module shows a practice field or filter.
External user	Tenant context returns only membership practice assignments.	Verify the complete saved set and refresh the user session.
Explicit selector	Workflow sends the selected canonical practice.	Confirm name, code, and saved result.
Canonical relationship	Provider primary practice, task, or case relationship supplies context.	Verify the relationship before creating downstream work.
No selector	Practice-aware table can use current_default_practice_id().	Know the active default and re-open the created record.
Context unclear	No supported evidence identifies the owning practice.	Stop and use the owning workflow or Support.

Default is not intent
Never switch or repair practice scope by editing tenant_practice_id, pasting UUIDs, changing SQL or requests, or borrowing another user's session.

06 / SHARED TEAMS

Centralize internal work without widening external access

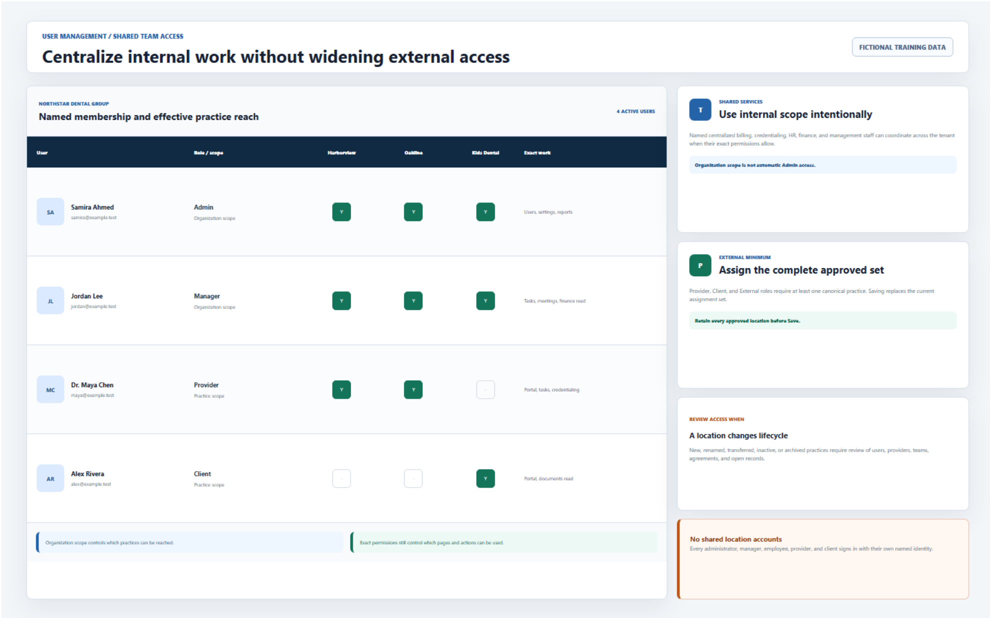

Figure 5. Fictional membership matrix showing named organization-scoped internal users, minimum practice-scoped external users, exact work permissions, and lifecycle review triggers.

Access decision	Purpose	Required control
Named account	Attributes every action to one person.	Never share a regional, billing, front-desk, provider, or location login.
Internal organization scope	Supports centralized billing, credentialing, HR, finance, and management.	Grant only required pages and actions; organization scope is not Admin.
External practice scope	Limits provider or client users to approved locations.	Save the complete minimum set and verify expected denial.
Team membership	Organizes departments and collaboration.	It does not replace record ownership or practice access.
Role preset	Provides an optional permission baseline.	Review every resulting page and action before Save.
Lifecycle review	New, renamed, transferred, inactive, or archived locations change operating needs.	Recheck users, providers, teams, agreements, and open records.

07 / RECORD ROUTING

Confirm the owning practice at every handoff

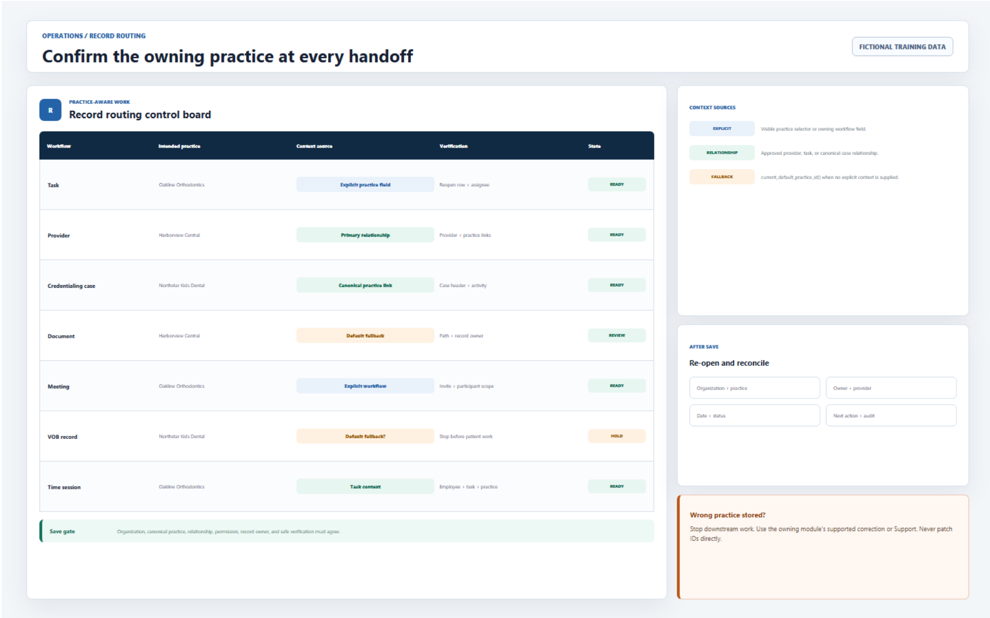

Figure 6. Fictional record-routing board for tasks, providers, credentialing, documents, meetings, VOB, and time sessions using explicit, relationship-derived, and default context.

Routing step	Operator action	Stop condition
Name owner	Put canonical practice name and code in the approved request.	Only provider, team, folder, or nickname is known.
Inspect workflow	Use a visible practice selector or documented relationship when available.	The control or relationship is ambiguous.
Understand fallback	Know current active default when the workflow supplies no practice.	Default is unexplained, archived, or unintended.
Save normally	Allow backend checks, same-tenant keys, permissions, and RLS to enforce the write.	A workaround is needed to force the ID.
Re-open	Verify organization, practice, owner, provider, date, status, and next action.	Saved result does not match approved owner.
Correct safely	Stop downstream work and use the owning module or approved Support path.	Someone proposes direct ID or SQL repair.

08 / PRACTICE COMPARISON

Compare like for like and keep aggregates separate

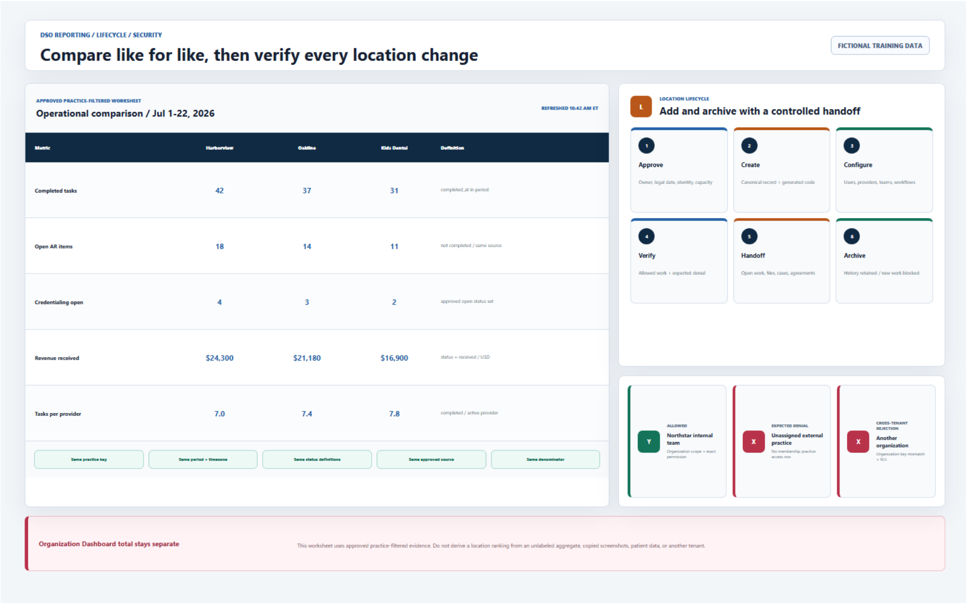

Figure 7. Fictional practice-filtered comparison, location lifecycle, and isolation verification. Organization Dashboard totals remain separate.

Control	Required method	Do not do
Scope	Use exact canonical practice ID or a clearly labeled practice filter.	Compare filtered practice to unlabeled organization total.
Time	Use the same timezone, period, and refresh time.	Mix live daily and closed monthly values.
Status	Use one documented pending, open, complete, denied, paid, or received definition.	Assume identical labels across modules.
Source	Use one approved module, report, or export for all practices.	Merge screenshots and copied estimates without lineage.
Denominator	Document claims, visits, tasks, providers, employees, or working days.	Rank raw totals when volume differs.
Privacy	Use minimum necessary totals and authorized recipients.	Include patient details, credentials, or another tenant.

Reports is not a universal practice comparison engine

Use only filters and fields visible in the current module. If practice filtering is absent, label the result organization-wide and obtain an approved practice-aware export or report.

09 / RELATIONSHIPS AND LIFECYCLE

Align provider access, then add or archive with a controlled handoff

Relationship	Purpose	Verification
Provider record	Stores operational and professional identity.	Same organization, named user, active status, approved metadata.
Primary practice	Canonical main location and provider tenant-practice alignment.	Primary marker matches approved operating home.
practice_providers	Links one provider to multiple canonical practices.	Every relationship is active, approved, and same-tenant.
Membership practices	Controls which locations external login receives.	Login need may be narrower than directory relationship.
Agreements	Connects approved commercial and compliance records to intended client context.	Correct organization, client, practice, signatory, dates, status, and file owner.
Operational record	Owns actual task, file, message, meeting, case, VOB, or credentialing work.	Saved tenant practice matches approved owner.

Location lifecycle

1. Approve owner, legal date, identity, subscription capacity, data owner, and reviewers.
2. Check duplicates and capacity, then create one canonical location through Practices / Locations.
3. Configure users, providers, teams, agreements, exact permissions, and practice-aware workflows separately.
4. Run a fictional readiness test for create, reopen, filter, export, allowed work, and expected denial.
5. Before archive, hand off tasks, cases, claims, VOB, credentialing, files, messages, time, agreements, provider links, and external access.
6. Archive rather than deleting history, then verify the intended active default before new work begins.

10 / TENANT ENFORCEMENT

Verify organization isolation, practice scope, exact actions, and safe denial

Control	Repository-backed behavior	Expected result
Tenant context	Returns active organization, membership, role permissions, subscription, branding, and non-archived accessible practices.	User starts inside one expected tenant.
Internal scope	can_access_organization authorizes tenant practices for active organization-scoped membership.	Authorized shared services can coordinate across DSO.
External scope	Practice access requires an active membership access row.	External user receives only assigned locations.
Default practice	Internal fallback prefers active default; practice-scoped fallback uses first saved access row.	Unspecified writes still receive a valid accessible practice key.
Record keys	Practice-aware tables use organization_id and tenant_practice_id with same-tenant constraints.	Unrelated practice ID cannot become a valid relationship.
Write checks	Practice access and exact table action permission must pass.	Visibility does not imply create, update, export, or delete.
RLS	Protected tables apply organization or practice predicates to authenticated reads and writes.	Typed routes and direct client requests do not widen scope.
Acceptance tests	Assigned-practice visibility and cross-organization rejection are asserted in repository tests.	Approved staging and deployment suites pass after policy changes.

Isolation incident
If another practice, provider, tenant, Xpand product, or Guardian Connect record appears, stop. Do not search, open more rows, copy, screenshot, download, export, send, change access, or ask AI to analyze it. Report account, expected organization, route, time, safe action, and a minimum non-sensitive symptom.

11 / TROUBLESHOOT AND COMPLETE

Fix the failed context without manipulating tenant keys

What you see	Likely cause	Correct first response
No practice switch	Current release has no universal selector.	Identify organization-wide, explicit, relationship, or default context.
Record saved to default	Workflow supplied no explicit practice.	Stop downstream work and use approved correction path.
External user sees one practice	Membership has one assignment.	Compare complete approved set; do not choose internal role.
Internal user sees all practices	Organization scope and permissions allow the page.	Use module filter or minimum permissions; do not call one selected.
Practice limit reached	Active non-archived count meets plan or override.	Review roster and subscription; do not repurpose another location.
Archived practice absent	Normal context intentionally excludes archived records.	Use approved history; reactivate only with authorization.
Totals do not reconcile	Scope, time, status, source, denominator, or refresh differs.	Rebuild like-for-like and separate organization aggregate.
Wrong tenant or product	Session, context, query, cache, deployment, integration, or policy failure.	Stop immediately and report without reproducing exposure.

Completion check

- I separate organization, canonical practice, internal scope, external assignments, provider relationships, and practice-aware records.
- I verify the roster, active default, plan capacity, shared-team model, record owner, and comparison rules before production work.
- I read Dashboard totals as authorized organization values, not a practice leaderboard, and determine context from membership, workflow, relationship, or documented default.
- I use named internal accounts and minimum external practice assignments plus exact page and action permissions.
- I confirm the owning practice before Save, re-open afterward, and never edit tenant practice IDs directly.
- I compare identical evidence and align provider links, login assignments, agreements, and operational ownership separately.
- I complete handoff before archive, verify the active default, and stop at cross-practice, cross-tenant, cross-product, or Guardian Connect exposure.

Next lesson: Continue with Create client BAA and service agreements. Also open the website guide, previous lesson, or all resources.