DENTALXPAND LEARNING CENTER / PROVIDER AND DSO

Manage Practices, Locations, and Assignments

A detailed guide to canonical practice and location records, subscription capacity, verified field entry, default-practice behavior, archive and reactivation, external-user assignments, provider relationships, layered tenant controls, and safe troubleshooting.

VERSION	1.0	AUDIENCE	Organization administrators
FORMAT	Website + PDF	SCOPE	DentalXpand practices, locations, and assignments

Fictional screenshots and sensitive practice data
Every screenshot uses fictional training data. Never place real passwords, credentials, patient records, claim details, full identifiers, another client, another tenant, or Guardian Connect data into a practice field, message, screenshot, ticket, or AI prompt.

Contents

Select a 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
Confirm account, organization, administrative authority, plan capacity, and approved source first. Then create or maintain the canonical practice, review lifecycle dependencies, assign the minimum external-user scope, and verify provider relationships without changing IDs or weakening tenant controls.

01 / MODEL AND ADMINISTRATION

Know which record, relationship, and permission layer you are changing

Record or layer	Purpose	Boundary
Organization	Tenant that owns its practices, users, providers, subscription, settings, and operational data.	Every practice and relationship must carry the same organization identity.
Practice / location	Canonical row with generated code, names, contact, group NPI, Tax ID, address, status, and default flag.	Use one approved row per operating location; it is not provider free-text metadata.
Provider directory	External provider or client identity and descriptive Practice Name.	Practice Name does not create a canonical practice or grant access.
Provider-practice	Same-organization provider relationship; one link can be primary.	Separate from the provider user's membership assignments.
Membership	User role, status, access scope, onboarding state, and permissions inside one organization.	Internal scope and external practice scope have different consequences.
Membership practice access	Approved practice IDs for a practice-scoped external account.	Does not grant unrelated page or action permissions.

Administration layer	Current behavior	Required interpretation
Navigation and route	Practices is admin-only and /practices uses the admin route.	Do not use a direct URL or API to bypass the hidden item.
Read gate	Requires active organization and membership, completed password change, MFA when required, and accessible rows.	Signed in is not the same as tenant access.
Create/update	Tenant manager authority plus backend validation and row policy.	A visible button is not final authorization.
Labels	Billing Company: Clients / Practices; DSO: Practices / Locations; single practice: Practice.	All labels use the same canonical data model.

Open Practices	Roles and access	Tenant context
Open Practices	**Roles and access**	**Tenant context**

02 / DIRECTORY AND PLAN LIMIT

Read the current organization and capacity before creating a location

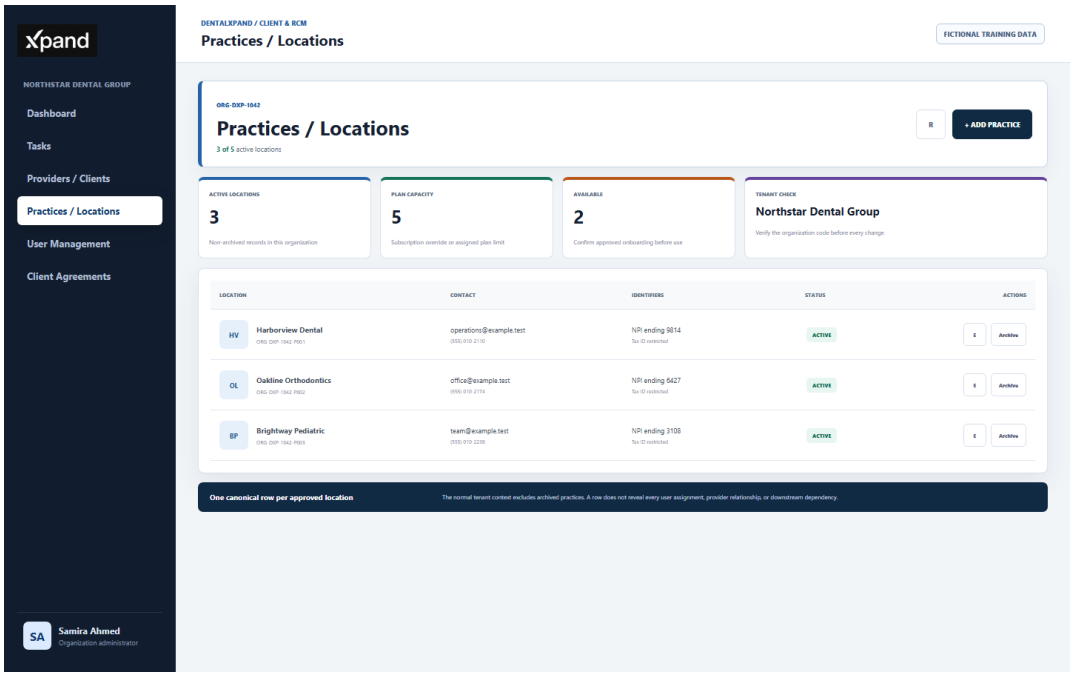

Figure 1. Fictional Practices / Locations directory with organization code, active count, plan limit, rows, statuses, and actions.

Element	Current behavior	Operator check
Organization code	Shown above the page heading.	Stop if it is not the expected tenant.
Active count	Counts non-archived practices returned in tenant context.	Archived rows are absent from the normal list and count.
Plan limit	Uses subscription max_practices override, otherwise the plan limit; null is unlimited.	Confirm capacity before onboarding another client or location.
Rows	Show name, generated code, contact, identifiers, status, edit, and lifecycle action.	A row does not show every assignment or downstream dependency.
Refresh	Reloads practices and tenant context.	Use once after a known change; it does not widen access.
Add	Creates an active same-organization record only when limit and policies allow it.	Resolve a limit conflict through plan or lifecycle governance.

03 / CREATE AND EDIT

Build one source-verified canonical practice record

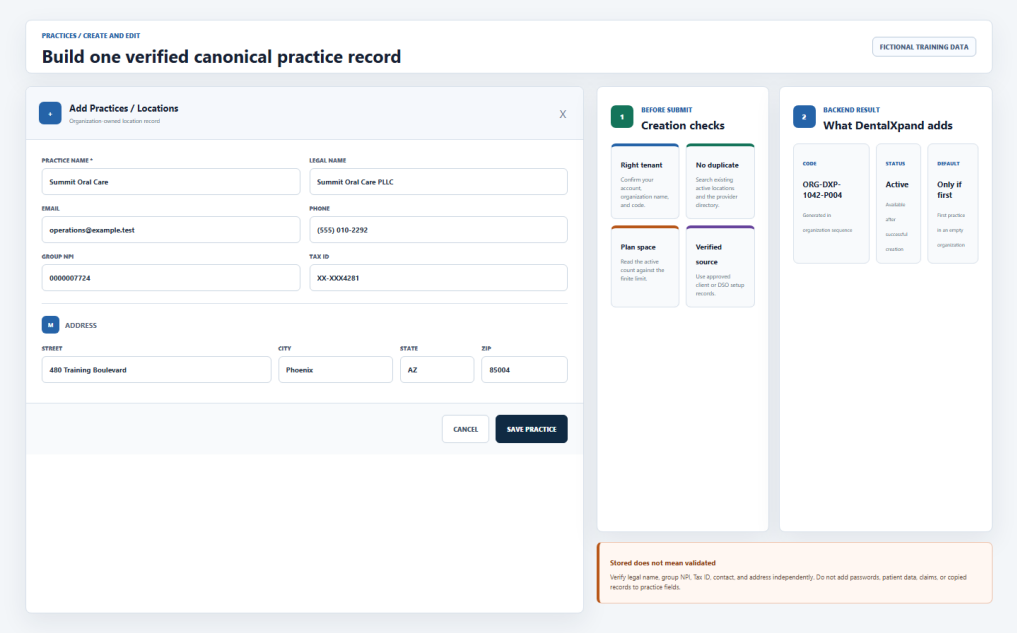

Figure 2. Fictional add-practice form with required name, optional details, generated code, active status, and first-practice default behavior.

Step	Reviewed behavior	Required discipline
Verify tenant/source	Confirm organization code and approved client or DSO setup information.	Search current practices and provider directory first to avoid duplicates.
Check capacity	Compare non-archived count to override or plan max_practices.	Do not create a placeholder or change data to avoid the limit.
Enter name	Practice name is required after trimming.	Use the recognizable operating name from the approved source.
Add details	Legal name, email, phone, group NPI, Tax ID, and structured address are optional.	Stored text is not complete validation; verify every sensitive value independently.
Submit	Backend generates organization code suffix, status active, and first-record default flag.	Submit once and wait for the refreshed row.
Edit	Name and optional fields can be updated; generated code and default flag are not form controls.	Compare every field before saving and never alter IDs through direct data access.

Minimum necessary

Keep passwords, portal credentials, patient data, claims, copied records, other tenants, and Guardian Connect content out of practice fields and support material.

04 / DEFAULT AND LIFECYCLE

Protect effective practice context before archive or reactivation

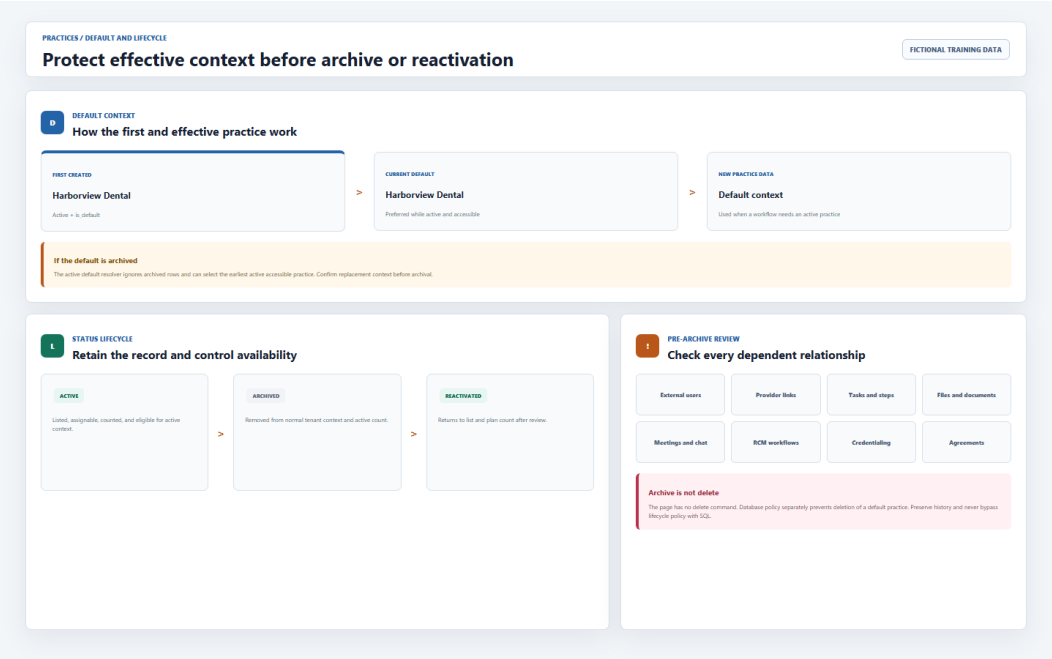

Figure 3. Fictional first-practice default flow, active/archive/reactivation lifecycle, dependency review, and delete protection.

State or action	Current effect	Required review
First practice	Created active and marked is_default when no non-archived practice exists.	Verify carefully because practice-scoped data can use default context.
Active	Listed, assignable, counted, and eligible for effective default selection.	Confirm current operational approval.
Archive	Status archived; normal tenant list and active count exclude it.	Review users, providers, tasks, files, meetings, RCM, credentialing, agreements, and retention.
Archived default	Default resolver ignores archived rows and can choose the earliest active accessible practice.	Confirm replacement context before archival.
Reactivate	Returns to active list and plan count.	Re-check capacity, details, assignments, permissions, and readiness.
Delete	No page command; database policy separately prevents deleting a default practice.	Use archive for normal lifecycle. Never bypass policy through SQL.

05 / EXTERNAL USER ASSIGNMENTS

Assign only the practices required for approved work

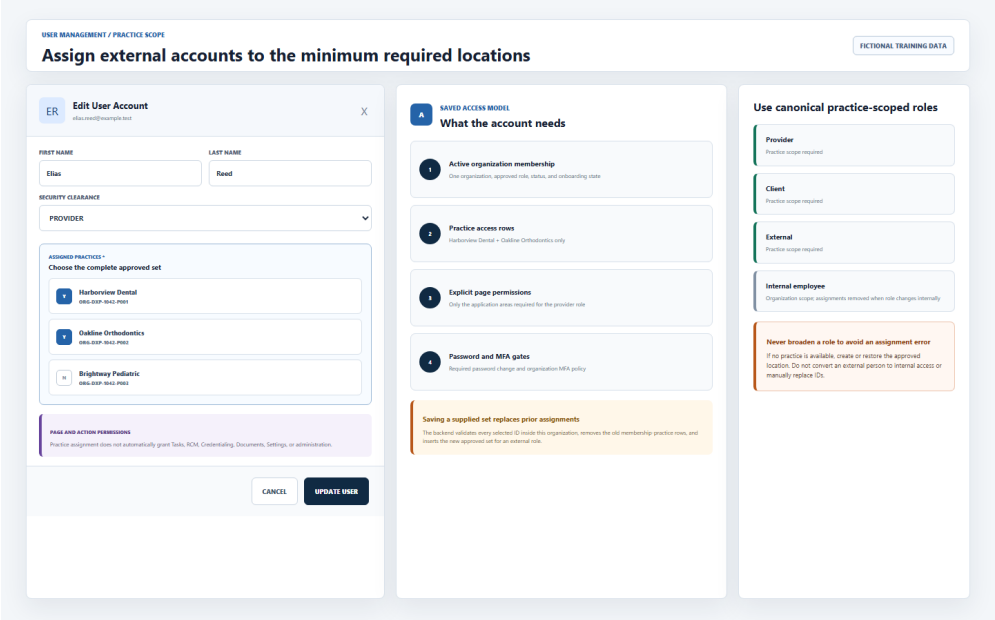

Figure 4. Fictional User Management form with Provider role, required practice checkboxes, permissions, and saved access layers.

Step or rule	Current implementation	Operator result
Create practice first	An empty practice list tells the administrator to create a practice before an external account.	Never create a placeholder solely to pass validation.
Canonical role	Provider, Client, and External are backend practice-scoped keys; form also recognizes legacy aliases.	Use the approved canonical role for new provisioning.
Required selection	Form rejects a client-oriented external account with zero practices.	Choose the minimum complete same-organization set.
ID validation	Backend loads selected practice IDs only from the active organization.	A stale, archived, or cross-tenant ID must fail.
Separate permissions	Assignments do not grant pages or actions.	Grant only required Tasks, RCM, Credentialing, Documents, or other permissions.
Update semantics	Supplied assignments remove prior membership-practice rows and insert the new set for an external role.	Review the full before-and-after set before saving.
Internal role change	Moving to an internal role changes scope to organization and removes practice assignment rows.	Never broaden a role merely to avoid an assignment error.

User Management	Roles guide	Open Practices
User Management	**Roles guide**	**Open Practices**

06 / PROVIDER RELATIONSHIPS

Keep provider links and provider-user assignments aligned

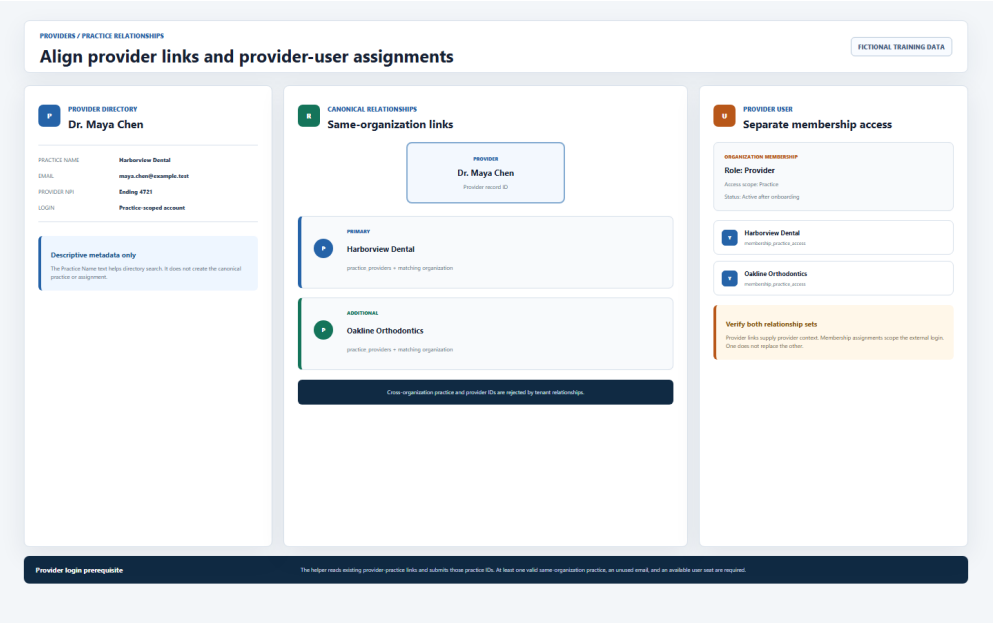

Figure 5. Fictional provider metadata, canonical practice links, primary relationship, membership, and separate practice-access rows.

Relationship	Current implementation	Required interpretation
Practice Name	Descriptive provider directory text and search field.	No canonical practice or access relationship is created.
Provider practice context	Provider primary and tenant practice fields align to an eligible location context.	Confirm the intended primary practice through approved provisioning.
practice_providers	Links one provider to one or more same-organization practices; linked account provisioning can mark the first selected link primary.	Do not create cross-tenant links or rely on matching names.
Provider login helper	Reads existing provider-practice links and submits their practice IDs.	Requires at least one valid link, unused email, and available seat.
Membership access	Separate rows scope the provider user's external login.	Verify in User Management even when provider links exist.
Tenant constraints	Composite keys require provider, practice, membership, and organization identities to agree.	Invalid cross-organization relationships must be rejected.

Providers page	Providers guide	Portal lesson
Providers page	**Providers guide**	**Portal lesson**

07 / TENANT BOUNDARY

Require every authorization layer to agree

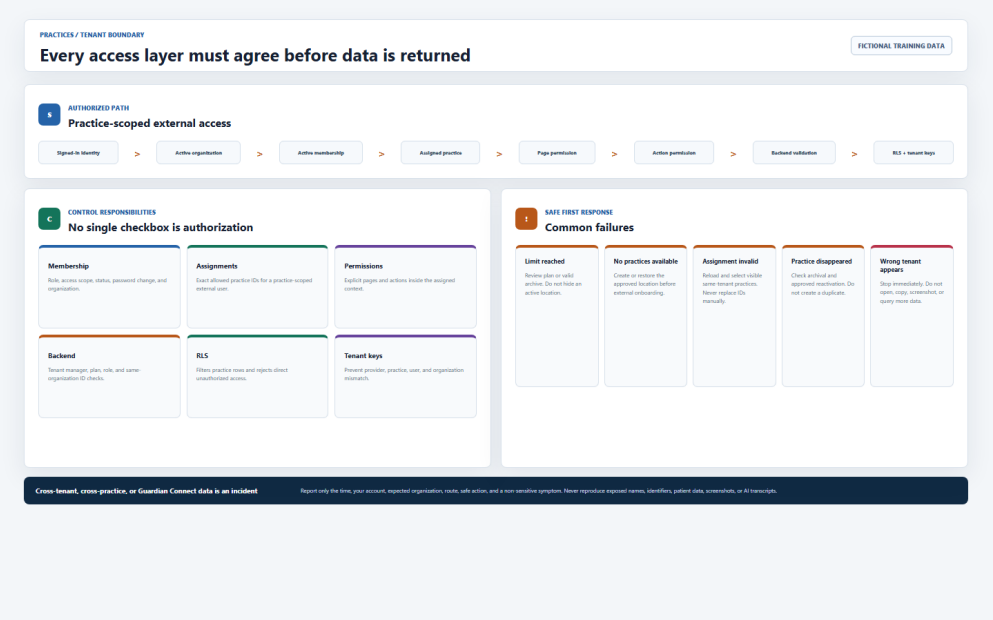

Figure 6. Fictional authentication, membership, assignment, permission, backend, row-policy, and tenant-key access path.

Control	Purpose	Required denial
Authentication	Identifies the person and satisfies password and MFA gates.	Reject anonymous, incomplete onboarding, or unmet MFA access.
Organization membership	Connects user to one active organization with role, status, and scope.	Reject missing, suspended, or wrong-tenant membership.
Practice assignment	Lists practices for a practice-scoped external member.	Hide and reject unassigned rows.
Page/action permission	Controls available modules and operations.	Assignment alone is insufficient.
Backend	Checks manager authority, organization, plan, role, and IDs.	Return a safe error without partial or cross-tenant links.
RLS	Filters reads and requires tenant management for writes.	Reject guessed IDs and direct unauthorized requests.
Tenant foreign keys	Require related practice, provider, user, and organization identities to match.	Reject invalid relationships rather than re-parenting data.

Isolation incident

If another tenant, practice, product, or Guardian Connect data appears, stop. Do not search, edit, copy, screenshot, message, or ask AI about more exposed data. Report only minimum non-sensitive context.

08 / SAFE OPERATING WORKFLOW

Use one controlled sequence for setup, assignment changes, and offboarding

1. Verify your account, organization code, administrative purpose, approved source, and requested location.
2. Search non-archived practices and provider records before creating a canonical location.
3. Check subscription capacity for creation or current dependencies before archive.
4. Create or update the canonical practice with verified minimum-necessary fields and one deliberate save.
5. Confirm the generated code, contact, identifiers, address, status, and active count on the refreshed row.
6. Maintain provider metadata and provider-practice relationships through the approved provisioning process.
7. Assign external users in User Management with a canonical role and the minimum practice set.
8. Grant page and action permissions separately from practice assignments.
9. Complete password-change and MFA onboarding before normal external access.
10. Verify the saved user checkboxes and confirm the external account sees only approved practices and modules.
11. Before archive, review external users, provider links, operational records, retention, and replacement default context.
12. Keep credentials, patient data, full identifiers, other tenants, and Guardian Connect content out of notes and support material.

Change discipline
A practice rename does not automatically rename provider metadata, and a provider relationship does not replace membership practice access. Verify each affected record separately.

Open Practices	User Management	All resources
Open Practices	**User Management**	**All resources**

09 / TROUBLESHOOT

Recover without changing IDs, roles, limits, or database policy

What you see	Possible reason	Correct first response
Practices redirects	Not approved admin, blocked membership, required password change, or MFA.	Confirm your own account and approved access; do not alter route or role data.
Unable to load	Session, backend, tenant context, migration, or connectivity issue.	Refresh once and preserve the safe error; do not query tables with elevated credentials.
Limit reached	Non-archived count equals subscription override or plan limit.	Review valid archive or plan change; do not hide an active location.
Name required	Required name is blank after trimming.	Use the verified operating name, never a placeholder.
No practices available	No non-archived practice is accessible in tenant context.	Create or restore the approved location before external onboarding.
Assign at least one	External account has no selected practice.	Select minimum approved same-organization scope; do not change to an internal role.
Assignment invalid	ID is stale, archived, missing, or outside the organization.	Reload and select current visible practices; never replace an ID manually.
Practice disappeared	Archive removes it from normal tenant context.	Use approved reactivation; do not recreate a duplicate.
Provider login fails	Missing provider-practice link, duplicate user/email, exhausted seat, or provisioning issue.	Check same-tenant links, assignments, seat, and the safe backend error.
Wrong tenant/product	Session, membership, query, cache, policy, deployment, or isolation failure.	Stop immediately and report without reproducing exposed data.

Do not reproduce exposure

Report only time, your account, expected organization, route, safe action, and a non-sensitive symptom.

Exclude exposed names, email, NPI, Tax ID, patient detail, screenshots, copied rows, and AI transcripts.

10 / COMPLETION

Verify tenant-safe practice and assignment management

- I can distinguish organization, canonical practice, provider metadata, provider-practice link, membership, and membership practice access.
- I use an approved administrator account and confirm organization code before practice work.
- I understand Billing Company, DSO, and Single Practice labels use the same canonical model.
- I read the non-archived count and subscription override or plan limit before creation.
- I search for duplicates, use a verified source, enter the required name, and confirm the generated row.
- I treat legal name, contact, address, group NPI, and Tax ID as sensitive source-verified data, not automatically validated values.
- I understand first-practice default behavior and review dependencies before archive or reactivation.
- I use canonical Provider, Client, or External roles and assign minimum same-organization practices.
- I grant page and action permissions separately from practice assignment.
- I understand a supplied assignment update replaces the external member's prior practice set.
- I keep provider Practice Name, provider-practice links, primary context, and membership assignments distinct.
- I verify both provider relationships and user assignments before provider login.
- I never bypass plan limits, role checks, assignment validation, RLS, or tenant foreign keys.
- I stop and report cross-tenant, cross-practice, cross-product, or Guardian Connect exposure without reproducing it.

Next lesson
Continue with Use provider login and the client portal for external authentication, required password change, practice-scoped navigation, approved records, and client collaboration.

Website guide	Open Practices	Next lesson
Website guide	**Open Practices**	**Next lesson**