DENTALXPAND LEARNING CENTER / PROVIDER AND DSO

Use Provider Login and the Client Portal

A practical, security-first guide to external account readiness, practice-scoped provisioning, temporary-password and MFA onboarding, the provider dashboard, tasks, credentialing records, safe collaboration, access boundaries, and recovery.

VERSION	1.0	AUDIENCE	Providers, client users, and account administrators
FORMAT	Website + PDF	SCOPE	DentalXpand external portal access

Fictional screenshots and restricted data

All screenshots use fictional training data. Never place passwords, temporary keys, MFA codes, recovery material, patient records, full identifiers, another tenant, or Guardian Connect data in screenshots, messages, tickets, PDFs, downloads, or AI prompts.

Contents

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

Use the portal as a controlled window
An external account is not a smaller administrator account. Identity, password and MFA, active organization membership, assigned practices, page and action permissions, backend checks, row policies, and tenant keys must all agree before data is available.

01 / PORTAL MODEL

Separate provider identity, login account, assignment, and permission

Record or control	Purpose	Boundary
Provider/client directory	Identifies the external person or business contact.	A directory row is not a login or an access grant.
Application user	Named authenticated identity with one unique email.	Never share one account between multiple people.
Organization membership	Connects the user to one active tenant, role, status, scope, and onboarding state.	External roles use practice scope.
Practice assignment	Lists approved same-organization practices for the external membership.	A free-text Practice Name does not create this row.
Page/action permissions	Controls which destinations and operations are available.	An assigned practice does not grant every feature.
Provider-practice relationship	Links the provider record to canonical practice rows.	It is separate from membership practice access.

Portal role	Typical baseline	Still conditional
Provider	Dashboard, assigned tasks, chat, credentialing, notifications, profile, settings, and approved AI access.	AR and other pages require explicit page permissions and valid scoped data.
Client / external	Minimum pages selected for the approved workflow.	No internal administration, timers, or unrelated practice records.
Administrator	Creates and maintains the account through approved administration routes.	Must not impersonate the provider or request their password or MFA code.

Previous guide	Providers	User Management
Previous guide	**Providers**	**User Management**

02 / ACCOUNT READINESS

Verify every dependency before Create Login

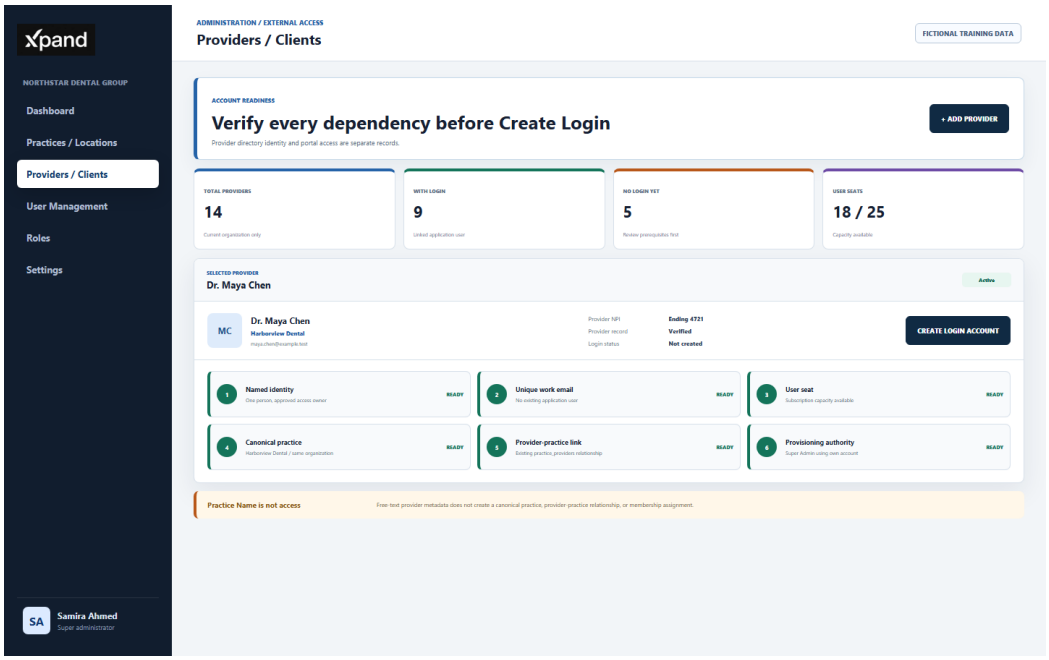

Figure 1. Fictional provider readiness view with identity, email, seat, canonical practice, provider-practice link, and provisioning authority checks.

Check	Ready when	Do not substitute
Named identity	One approved person owns the account.	Shared mailbox or team credential.
Unique work email	No existing application user owns it.	A second identity for the same email.
User seat	Subscription capacity is available.	Disabling an unrelated user without approval.
Canonical practice	Active practice belongs to the same organization.	Provider free-text Practice Name.
Provider-practice link	Existing same-tenant relationship is present for the helper path.	Matching text or a guessed ID.
Authority	Super Admin or approved tenant manager uses their own account.	Direct database mutation or account sharing.

03 / PROVISION THE ACCOUNT

Create one named, practice-scoped external membership

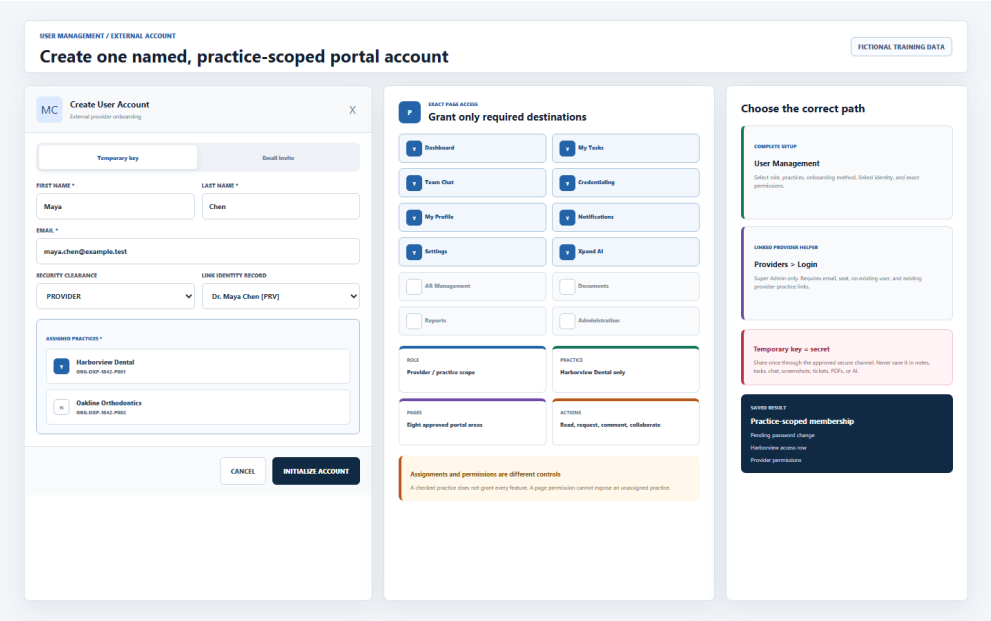

Figure 2. Fictional User Management provisioning form with Provider role, linked identity, selected practice, exact pages, and restricted temporary key.

Path	Use it when	Required outcome
User Management	Complete setup is needed: role, practice checkboxes, onboarding method, identity link, and permissions.	One external membership with minimum same-organization scope.
Providers > Create Login	Super Admin is linking a provider that already has email and provider-practice relationships.	The helper submits those existing practice IDs; it cannot invent a practice link.
Temporary key	Approved secure one-time handoff is available.	Share once through the approved channel and require immediate replacement.
Email invite	The approved invitation path is configured and monitored.	Recipient verifies the official application URL before continuing.

Temporary credentials are secrets

Never store a temporary key in provider notes, tasks, chat, screenshots, email threads, tickets, PDFs, browser recordings, or AI.

04 / FIRST SIGN-IN

Complete authentication, password replacement, and MFA in order

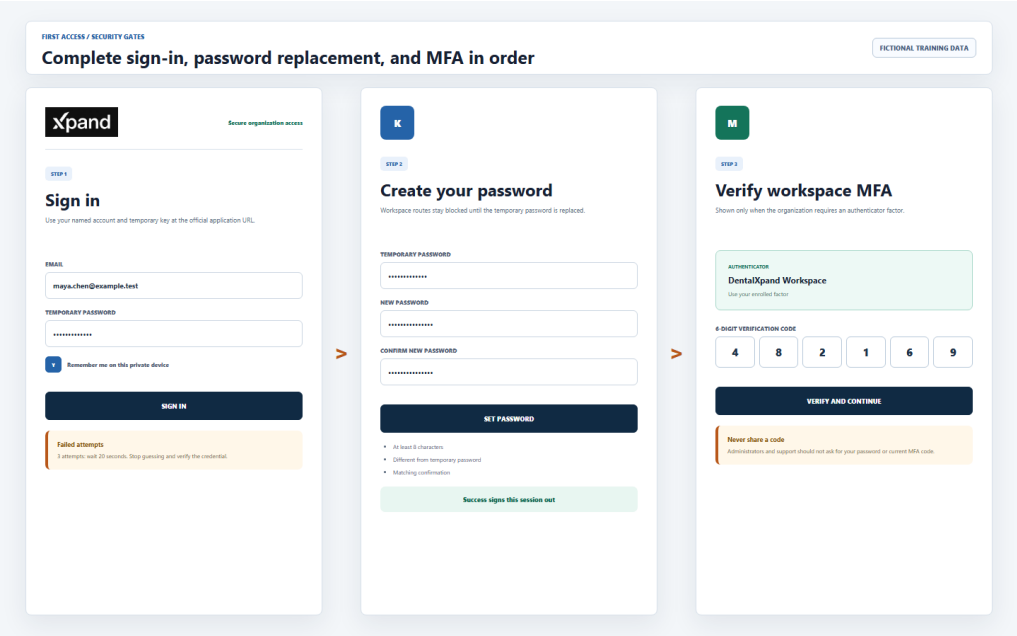

Figure 3. Fictional first-access sequence: sign in with the temporary credential, create a new password, sign out, then satisfy MFA when required.

Step	Current behavior	Safe action
Sign in	Use the named email and temporary credential at the official application URL.	Verify the URL and type the credential privately.
Failed attempts	After three failures, wait 20 seconds; repeated failures can cause a longer browser-local block.	Stop guessing, verify email, and use the approved reset path.
Replace password	New password must be at least eight characters, match confirmation, and differ from the temporary password.	Use a unique password manager-generated value.
Sign out	Successful replacement ends the temporary-password session.	Sign in again with the new password.
MFA	A six-digit authenticator gate appears when the organization requires it.	Use your enrolled factor; support must never ask for the current code.

05 / DASHBOARD

Use the focused provider command center

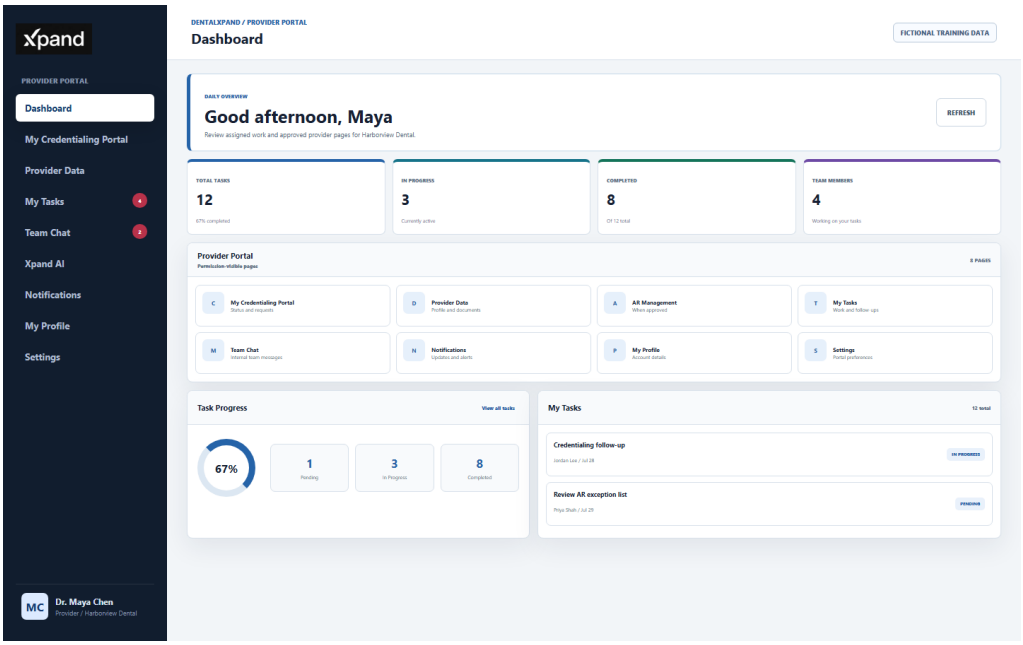

Figure 4. Fictional provider dashboard with permission-visible links, scoped task totals, progress, and assigned team context.

Area	What it means	Operator rule
Portal links	Only pages allowed by the membership permissions are shown.	A missing page can be an intentional denial.
Task totals	Counts returned tasks linked to the provider, client-provider identity, or assigned employee context.	Do not infer access to hidden work.
Team members	People derived from the visible assigned task set.	It is not the entire organization directory.
Credentialing and Provider Data	Approved case status, identity fields, and supporting records.	Confirm provider and practice before opening or saving.
Profile, notifications, settings	Personal authenticated destinations remain available for the account.	Personal access does not widen practice scope.

Open dashboard	Open tasks	Credentialing
Open dashboard	**Open tasks**	**Credentialing**

06 / TASKS AND REQUESTS

Review assigned work and ask inside the relevant record

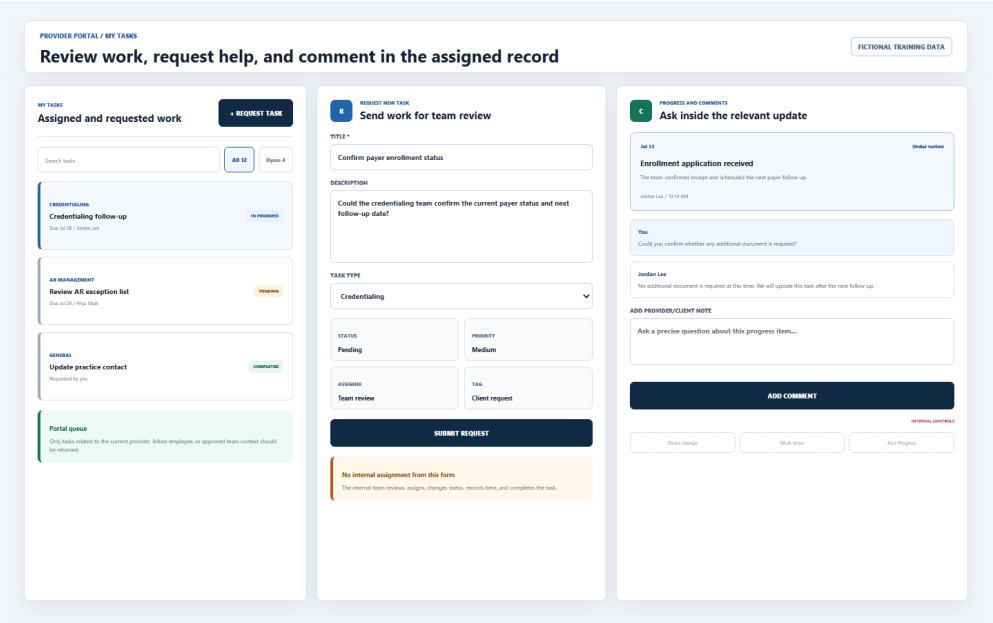

Figure 5. Fictional provider task list, Request Task form, progress history, comments, and internal-only controls.

Action	Provider/client behavior	Boundary
Read a task	Only assigned provider, client-provider, linked employee, or approved team context should return it.	No matching assignment means no task.
Request Task	Submits title, description, type, Pending status, Medium priority, unassigned owner, and client_request tag.	The internal team reviews and assigns it.
Comment	Adds a precise question or clarification to the relevant progress item.	Keep the message minimum necessary and case-specific.
Status, timers, progress	Provider/client controls are hidden or restricted in the portal.	Do not ask for an internal role to bypass the workflow.

Keep work in context

Use the task or credentialing case that already owns the work. Avoid duplicate requests, copied records, and credentials in comments.

07 / CREDENTIALING

Use status, provider data, and documents as one assigned case

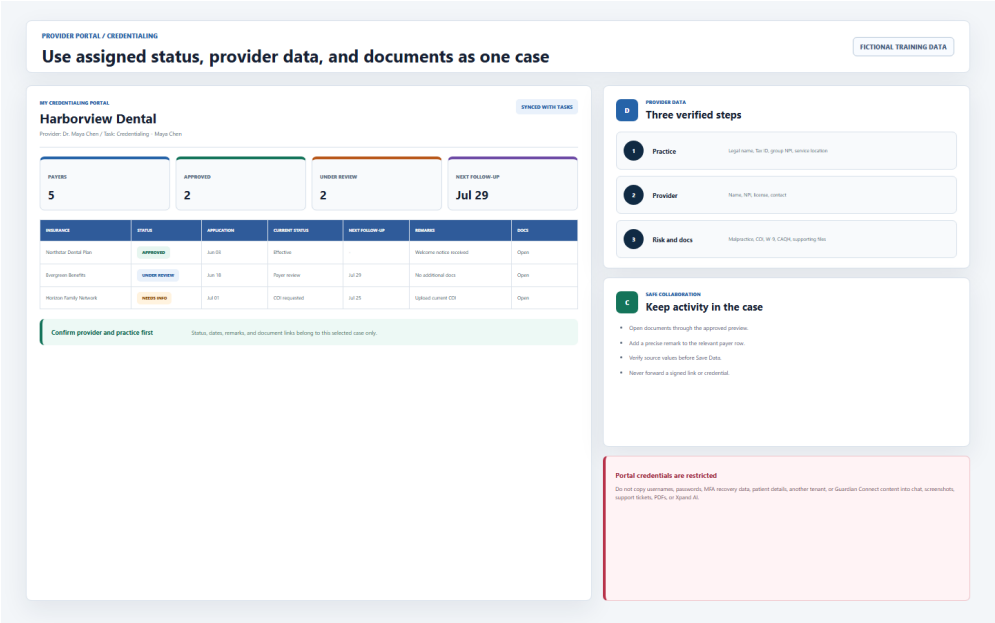

Figure 6. Fictional credentialing status board, provider data steps, case collaboration rules, and restricted credential warning.

Destination	Approved use	Verification
My Credentialing Portal	Review payer rows, application dates, current status, next follow-up, remarks, and documents.	Confirm the selected provider and practice first.
Provider Data	Maintain approved practice, provider, risk, and document fields through the guided steps.	Verify the source before Save Data.
Documents	Open files through approved preview and case links.	Never forward signed URLs or download more than required.
Remarks	Add a precise case-specific update to the relevant payer row.	Do not paste portal credentials, patient detail, or unrelated tenant content.
Client Login	Use only for the restricted approved workflow when permission and assignment allow it.	Never expose usernames, passwords, MFA, or recovery data in training or support.

Credentialing	Team Chat	All resources
Credentialing	**Team Chat**	**All resources**

08 / DAILY PORTAL WORKFLOW

Use a repeatable minimum-access routine

1. Open only the official DentalXpand application and sign in with your named account.
2. Complete required password replacement and MFA before normal work.
3. Confirm the organization and expected practice before opening records.
4. Use the dashboard only as a map to permission-visible destinations.
5. Open assigned tasks, read the full relevant context, and avoid duplicate requests.
6. Use Request Task when new work needs internal review and assignment.
7. Ask questions through the task progress or credentialing case that owns the work.
8. Verify provider, practice, source values, and document identity before saving.
9. Use chat and notifications for approved coordination, not for passwords or patient records.
10. Keep personal profile and settings changes limited to your own account.
11. Sign out on shared or unmanaged devices and report a lost factor immediately.
12. Stop at any unexpected tenant, practice, product, or Guardian Connect data boundary.

Portal destination	Use it for	Do not use it for
Team Chat	Short approved coordination around known work.	Credentials, patient detail, or cross-client records.
Notifications	Review alerts and navigate to the authorized source record.	Treating an alert preview as the final record.
My Profile	Your own contact and account details.	Changing another person's identity.
Settings	Your approved preferences and account settings.	Organization administration or scope changes.
Xpand AI	Approved tenant-scoped assistance for permitted content.	Another product, tenant, practice, patient, or credential data.

09 / ACCESS BOUNDARY

Require every authorization layer to agree

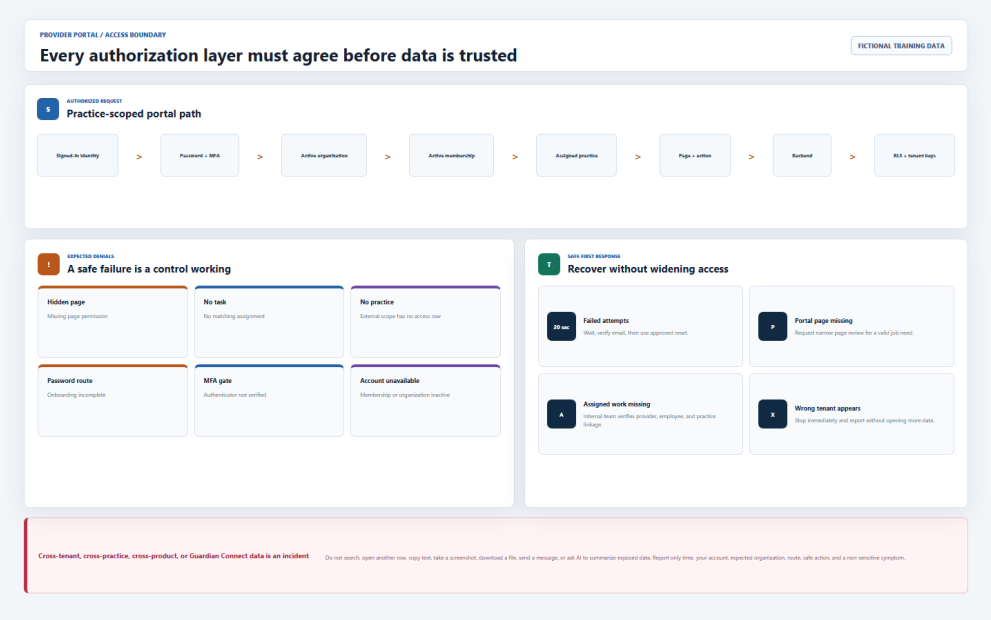

Figure 7. Fictional identity-to-RLS authorization chain, expected denials, safe recovery actions, and isolation-incident rule.

Layer	Required state	Expected denial
Identity	Authenticated named user.	Anonymous or invalid session is rejected.
Password and MFA	Onboarding complete and required factor satisfied.	Redirect to password or MFA gate.
Organization and membership	Both active and selected consistently.	Account unavailable or tenant context error.
Assigned practice	Practice ID exists in membership practice access.	No practice data is returned.
Page and action	Exact destination and operation are permitted.	Page hidden, redirected, or action denied.
Backend and RLS	Tenant checks and database policies accept the request.	Safe error with no cross-tenant result.

Isolation incident

If another tenant, practice, product, or Guardian Connect data appears, stop. Do not search, open more rows, copy, screenshot, download, message, or ask AI to summarize it. Report only minimum non-sensitive context.

10 / TROUBLESHOOT AND COMPLETE

Recover without widening access

What you see	Likely control	Correct first response
Wait 20 seconds	Three failed sign-in attempts triggered local rate limiting.	Wait, verify email, then use the approved reset path.
Password route	Temporary password still requires replacement.	Complete the current-password and new-password form.
MFA gate	Organization requires the enrolled authenticator.	Use your factor or approved MFA recovery process.
Page missing	Page permission is absent.	Request narrow access review for a valid job need.
Assigned work missing	Provider, employee, client-provider, task, or practice link does not match.	Internal admin verifies the specific relationships; do not broaden the role.
Provider login creation fails	Email, seat, existing user, practice relationship, or authority is invalid.	Recheck readiness and use User Management for complete setup.
Account unavailable	Membership or organization is inactive or tenant context failed.	Contact the administrator without sharing credentials.
Wrong tenant or product	Isolation, session, cache, query, or policy failure.	Stop immediately and report without reproducing exposed data.

Completion check

- I can separate directory identity, application user, membership, practice assignment, page permissions, and provider-practice relationships.
- I verify email, seat, canonical practice, provider-practice link, authority, and minimum permissions before provisioning.
- I protect temporary credentials, replace the password immediately, follow the failed-attempt wait, and complete MFA without sharing a code.
- I use only permission-visible pages and assigned practice data, and I keep task requests and comments inside the approved workflow.
- I verify provider, practice, payer row, source value, and document before saving, and keep credentials, patient data, other tenants, and Guardian Connect out of support and AI.
- I diagnose safe denials without widening access and stop immediately at any cross-tenant, cross-practice, or cross-product exposure.

Next lesson
Continue with Control provider and practice access for assignment boundaries, least privilege, access changes, verification, and offboarding. Also open the website guide or sign in.