DENTALXPAND LEARNING CENTER / WORK HUB

Maintain My Profile and Personal Details

A detailed guide to personal settings, linked employee identity, editable name and phone, approved avatar upload, protected employment fields, role-aware summaries, task and HR records, password self-service, management controls, tenant scope, and safe troubleshooting.

VERSION	1.0	AUDIENCE	All authorized users and profile managers
FORMAT	Website + PDF	SCOPE	DentalXpand My Profile

Fictional screenshots and privacy boundary
Every screenshot uses fictional training data. Profile, salary, attendance, billing, agreement, notice, contact, avatar, and authentication information is sensitive. Use only your own account and approved management workflows.

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
Start with identity, organization, practice, linked employee, and protected-field boundaries. Then complete permitted edits, avatar verification, role summaries, personal records, password re-login, management controls, tenant checks, and troubleshooting.

01 / PURPOSE AND ACCESS

Treat My Profile as a personal summary and self-service surface

Record	Reviewed role	Boundary
Personal settings	Stored profile settings can supply first name, last name, combined name, and phone.	Settings must remain keyed to the authenticated app user. Never save another user's ID to resolve an error.
Linked employee	The page matches by signed-in user ID or email and reads employment identity, avatar, verification, badges, and related summaries.	Deployed row policy must limit which employee rows are returned. Client-side matching is not tenant isolation.
Related modules	Tasks, attendance, billing, agreements, recruitment, notices, leave, loans, and shifts are loaded through their services.	My Profile is a summary. Use the owning workflow for source changes, approvals, and corrections.
Authentication	Security calls an authenticated backend to change the current user's own password.	Passwords, tokens, sessions, codes, and service credentials must never be sent to support or placed in profile fields.
Management target	Approved management roles can open another employee profile through a target ID workflow.	Never edit a URL or ID to discover people. A management UI check does not replace database policy.

Stop at unexpected data

If another person, organization, practice, Guardian Connect workspace, or unrelated record appears, stop. Do not open more tabs, compare values, download files, copy data, screenshot, or test IDs. Report minimum non-sensitive context.

Open My Profile	Roles and access	Organization context
Open My Profile	**Roles and access**	**Organization context**

02 / PROFILE OVERVIEW

Confirm identity, permitted fields, and protected employment values

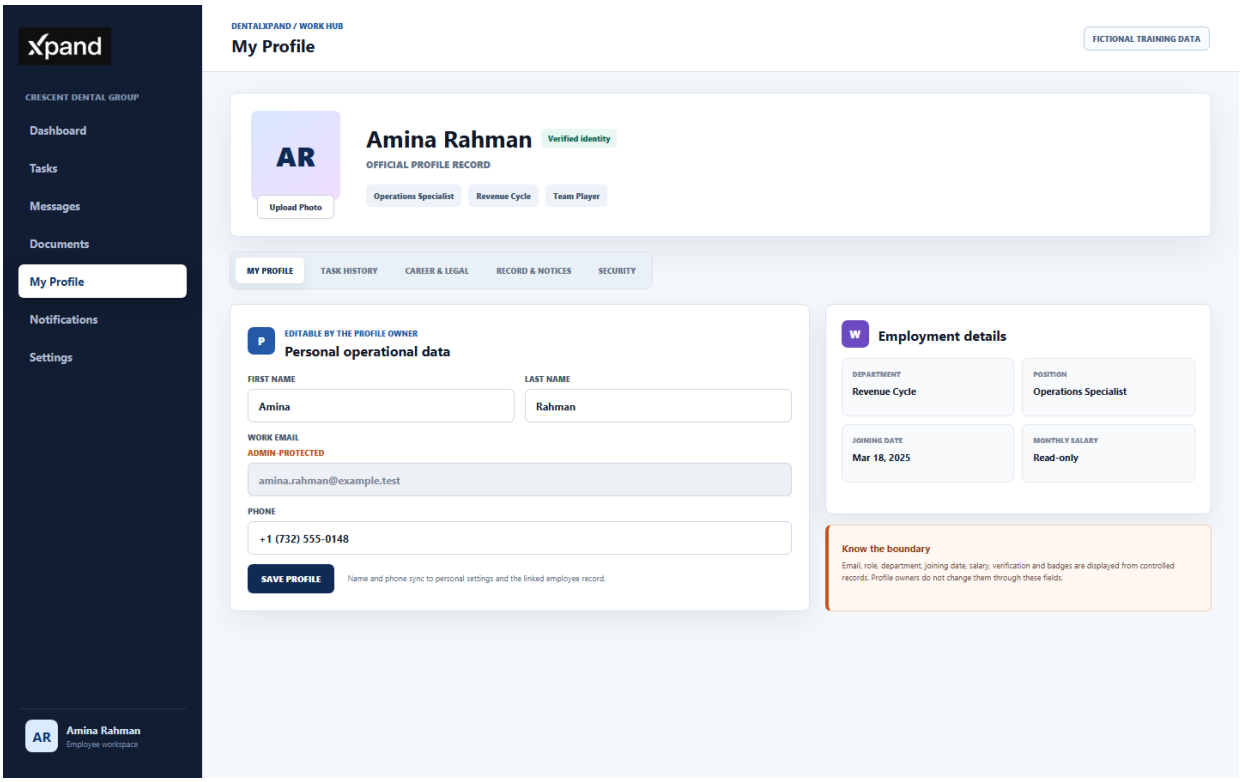

Figure 1. Fictional My Profile screen with identity summary, editable first and last name and phone, locked work email, employment details, and protected-field boundary.

1. Confirm the signed-in account, active organization and practice, displayed identity, work email, role, department, and linked employee context before relying on any values.
2. Use My Profile to edit first name, last name, and phone. The current form renders work email as disabled and does not submit an email change.
3. Treat verification and achievement badges as management-controlled statuses. They do not grant broader page, clinical, credentialing, or tenant access.
4. Treat department, position, joining date, salary, attendance, leave, loan, billing, agreement, recruitment, shift, and notice values as protected or source-owned summaries.
5. Use Task History, Career and Legal, Record and Notices, and Security for their documented purpose. Do not use tabs to explore another person's data.

> Disabled does not mean editable somewhere else
> When a protected field is wrong, request correction through the authorized user, HR, finance, or management workflow. Never change IDs, mappings, role values, or database rows manually from a profile incident.

03 / PERSONAL DETAILS AND AVATAR

Save permitted contact details and an approved image

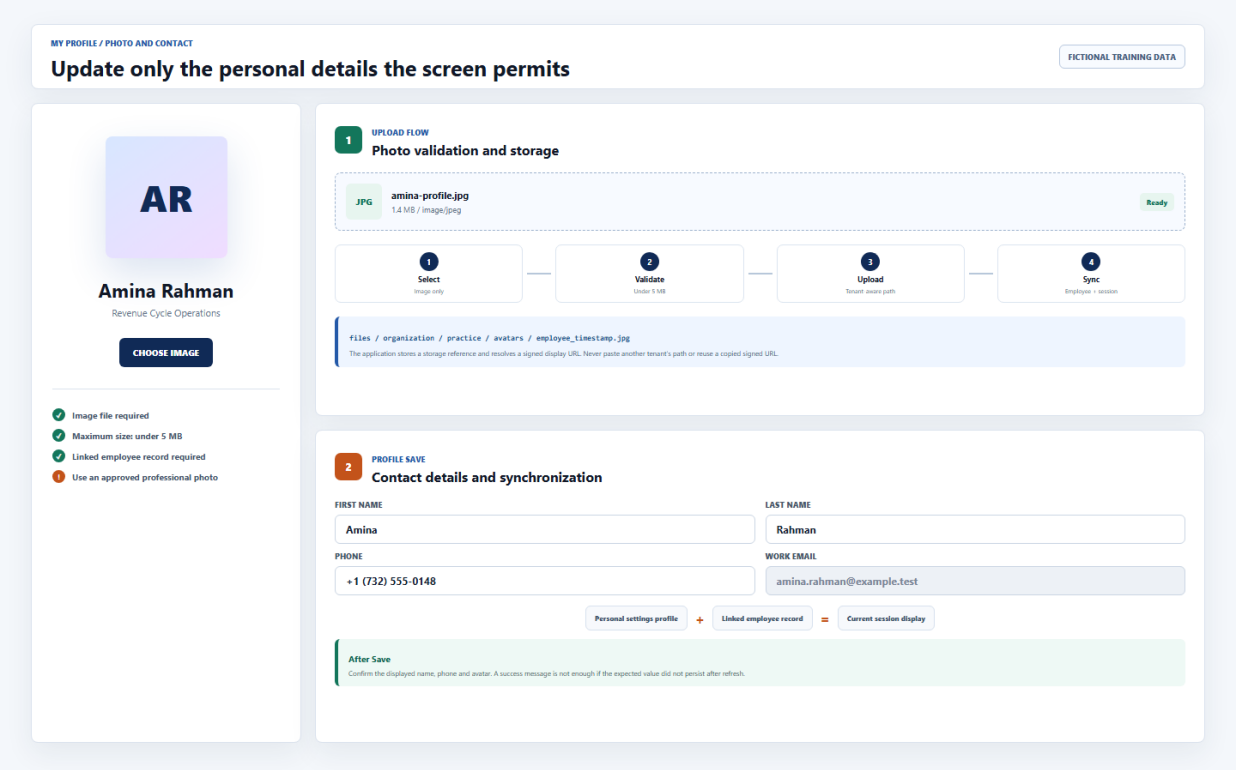

Figure 2. Fictional photo and contact workflow showing image-only validation, current 5 MB limit, linked employee requirement, tenant-aware avatar path, and settings plus employee synchronization.

Action	Current behavior	Required discipline
Save name and phone	Settings JSON is upserted first; the linked employee is updated next; the local session display is updated after both calls.	Refresh once and confirm persistence. A success message alone does not prove every source saved when a later request failed.
Work email	Displayed as a disabled field and not included in the profile save request.	Use the approved account-management workflow for correction. Do not write a different user ID or email mapping.
Choose avatar	The browser requires an image MIME type and rejects files 5 MB or larger.	Use a professional image without patient, client, screen, badge, document, or unrelated protected content.
Upload avatar	A linked employee ID is required. The service writes a tenant-aware avatars path in the files bucket.	Never upload under another employee, use a public file host, construct another tenant path, or reuse a copied signed URL.
Display avatar	The employee stores a normalized storage reference and the session receives a resolved signed display URL.	Signed URLs are temporary access artifacts. Keep the durable storage reference inside the authorized application.

04 / ROLE-AWARE SUMMARIES

Read employee and provider profile cards as current summaries

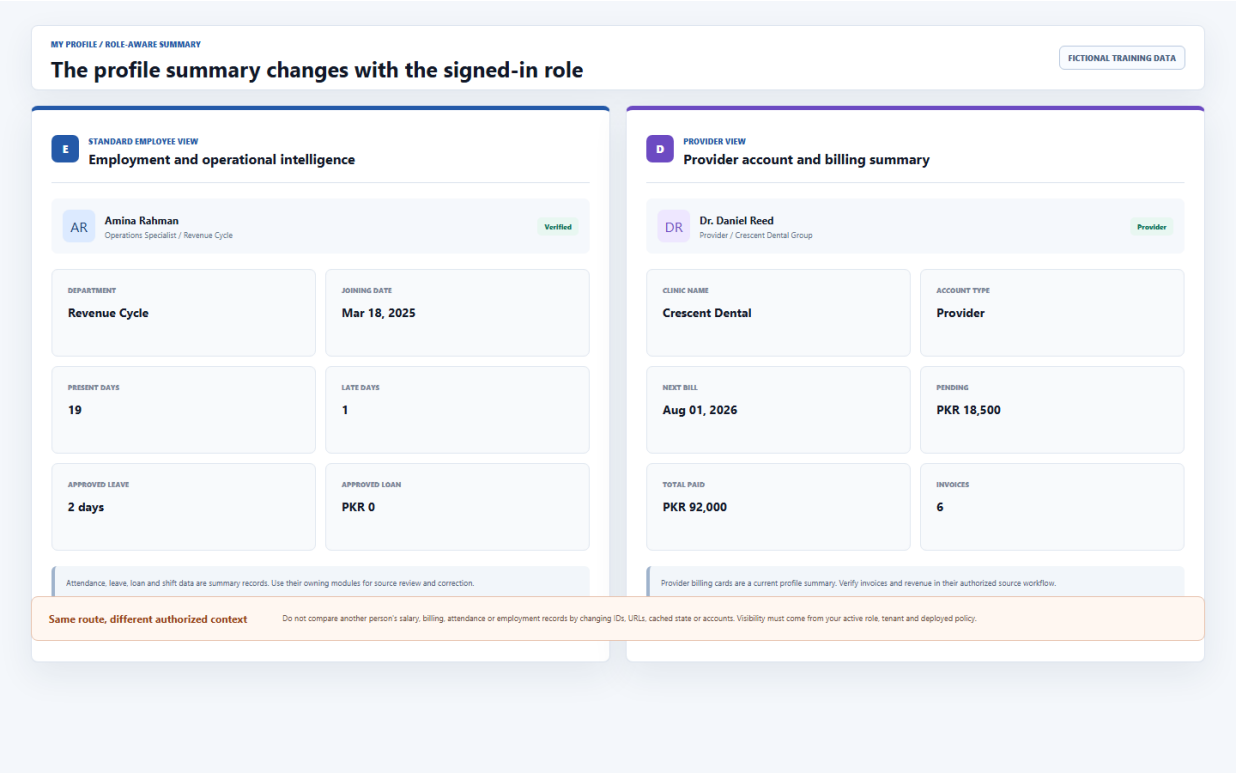

Figure 3. Fictional employee and provider profile views showing employment, attendance, leave and loan summaries beside clinic, billing, pending and invoice summaries.

View	Possible summary	Source rule
Employee	Department, position, joining date, salary, attendance, approved leave, loan totals, and shift context when data is returned.	Use HR, Attendance, Leaves, Loans, and Shifts for source review. Missing cards do not automatically mean zero.
Provider	Clinic or department, account type, next bill, pending amount, total received, and invoice count for the requested period.	Use Billing or Revenue for source review. A profile card is not a complete ledger or payment statement.
Partial profile	Independent related calls can fail without blocking every other card.	Report the unavailable summary and expected source. Do not infer complete absence from one empty or failed widget.
Sensitive data	Salary, attendance, leave, loan, billing, employment, agreement, recruitment, and notice data can appear together.	Use minimum necessary access. Do not forward screenshots, copy values into chat, or disclose records in public tickets.

Same route does not mean same data

The signed-in role, active tenant, linked employee, source records, and deployed policies determine the authorized view. Never compare people by changing IDs, accounts, cache, or browser state.

05 / TASK, CAREER, AND NOTICE RECORDS

Use profile tabs for reference and owning modules for changes

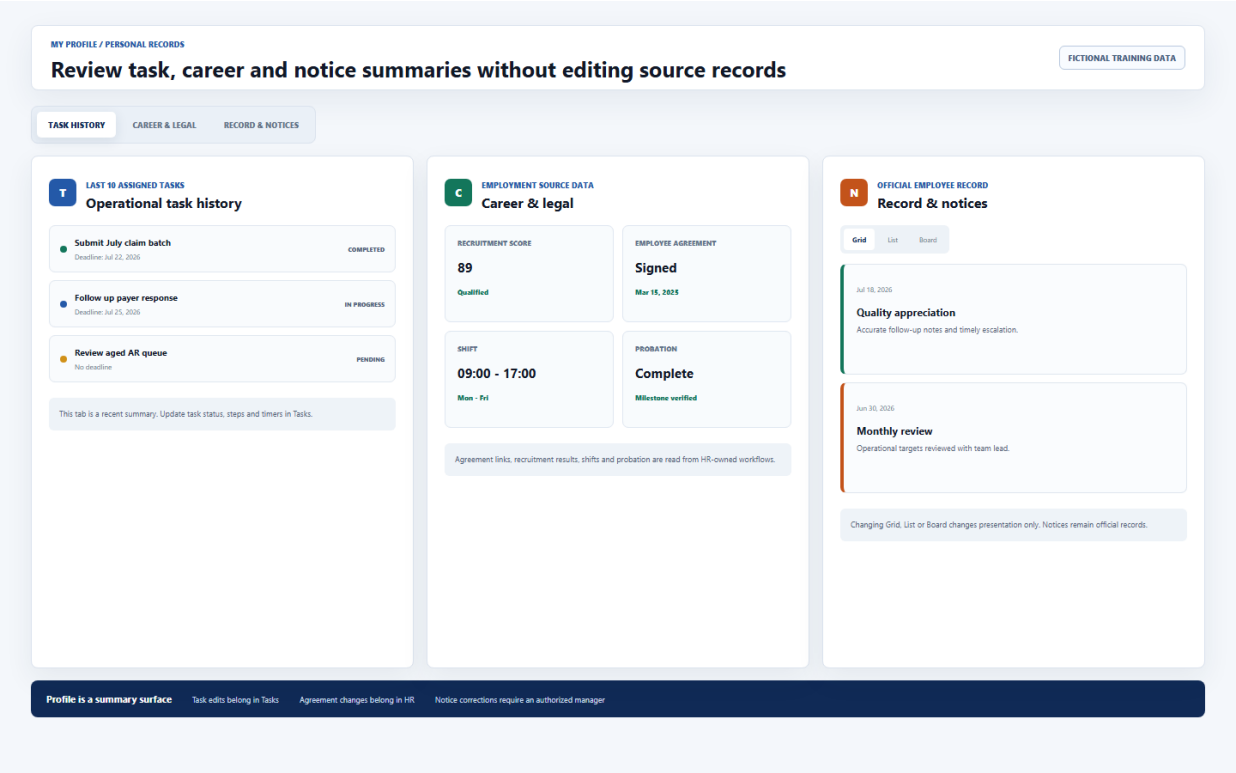

Figure 4. Fictional Task History, Career and Legal, and Record and Notices summaries with source ownership and display-mode boundaries.

Tab	Reviewed content	Correct workflow
Task History	Up to ten assigned tasks with title, due date, and status.	Use Tasks for assignments, steps, comments, timers, status changes, and complete task context.
Career and Legal	Agreements, recruitment result, assigned or default office shift, employment terms, and probation progress when available.	Use approved HR, agreement, recruitment, and shift workflows. Do not alter signed files outside their process.
Record and Notices	Employee notices rendered in Grid, List, or Board presentation.	Use the authorized notice workflow for corrections, disputes, acknowledgments, or retention. Changing view does not change the record.
Empty state	The page may report no tasks, evaluation, agreement, notice, or summary when no authorized result is returned.	Do not assume a record never existed. Confirm with the source owner when a business process requires it.

Task lesson	My Profile guide	All resources
Task lesson	**My Profile guide**	**All resources**

06 / PASSWORD SELF-SERVICE

Change your own password and complete a fresh sign-in

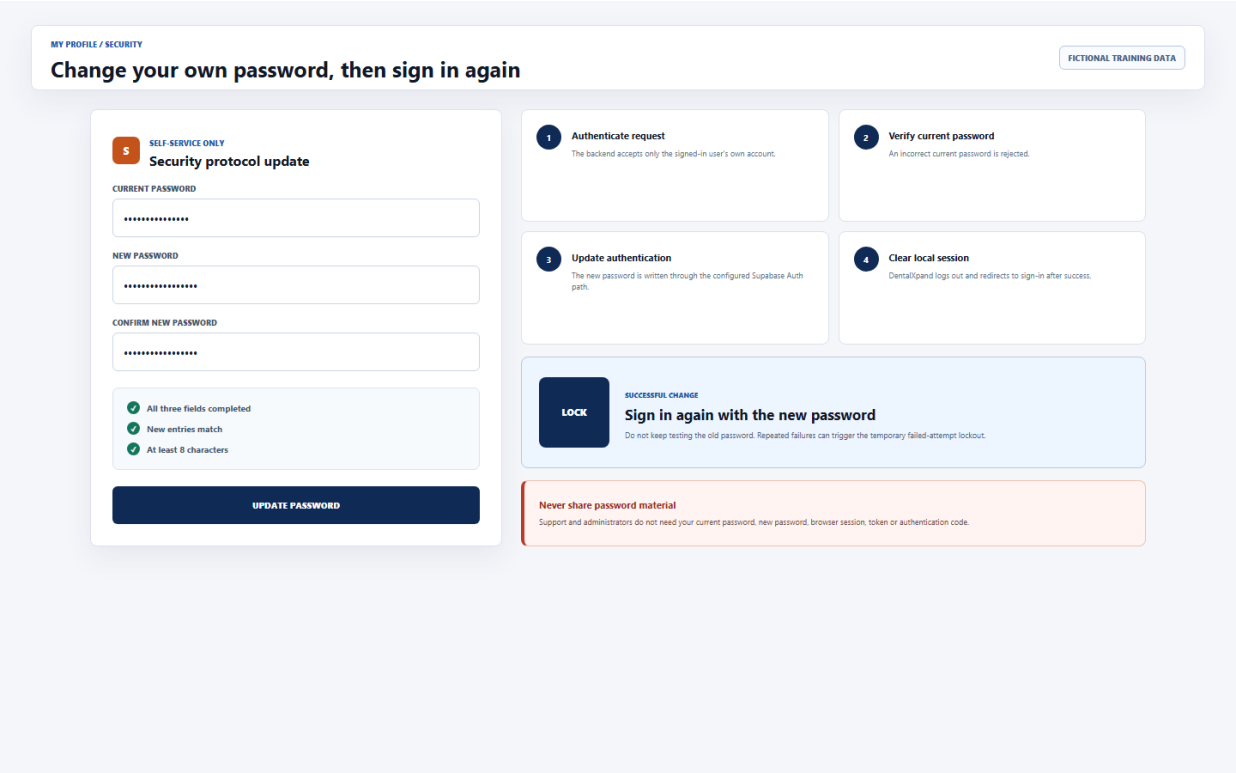

Figure 5. Fictional Security tab with current, new, and confirmation password fields, UI checks, backend self-service controls, forced logout, and re-login guidance.

Step	Reviewed behavior	Boundary
Complete fields	Current password and new password are required; the UI also requires matching confirmation.	Never paste a password from chat, email, notes, tickets, screenshots, or another person's account.
Meet minimum	The current UI and backend require at least eight characters.	Follow any stronger organization password policy. Do not reuse exposed or shared credentials.
Verify account	The backend resolves the app user, rejects a different user, rejects an inactive account, and verifies the current password.	Self-service cannot be used to change another person's account, even when an ID is supplied.
Update Auth	The configured Supabase Auth path updates the password; profile membership state is synchronized when applicable.	Service-role secrets stay server-only. Never expose them in browser variables or support messages.
Re-login	The client clears local authentication storage, logs out, and redirects to /auth after success.	Sign in again with the new password. Stop repeated attempts if temporary failed-attempt protection appears.

Support never needs your password

Do not send current or new passwords, one-time codes, tokens, browser sessions, secret keys, or screenshots of authentication fields. Use the approved recovery workflow.

07 / MANAGEMENT CONTROLS

Open target profiles, verification, and badges only for an approved purpose

Action	Reviewed page behavior	Required control
Target profile	Admin, super admin, manager, or CEO role checks can select a target employee from the id query value.	Open only through an authorized workflow link. Do not edit the query to discover employee records.
Verification	Eligible management users can toggle identity verification and may trigger an announcement.	Verify through the approved identity process. A checkmark is not clinical, credentialing, licensing, or broad-access proof.
Achievement badge	Predefined badges can be added or removed and may trigger an announcement.	Use documented criteria, approval, and correction processes. Avoid disclosing private performance information.
Sensitive tabs	A target profile can expose tasks, career, legal, notices, salary, attendance, leave, loan, shift, or billing summaries.	Use minimum necessary access and the owning workflow. Do not export or forward profile content.
Enforcement	The page has role-based UI checks and the employee service filters non-management updates.	Deployed row policy, authenticated backend, organization and practice mapping, and source permissions remain the final boundary.

Visible control is not proof of authorization

If a management control appears unexpectedly, do not use it to test access. Stop and report the current page, role, expected scope, and non-sensitive behavior.

08 / TENANT, SETTINGS, AND STORAGE

Verify each enforcement layer before trusting a profile write or read

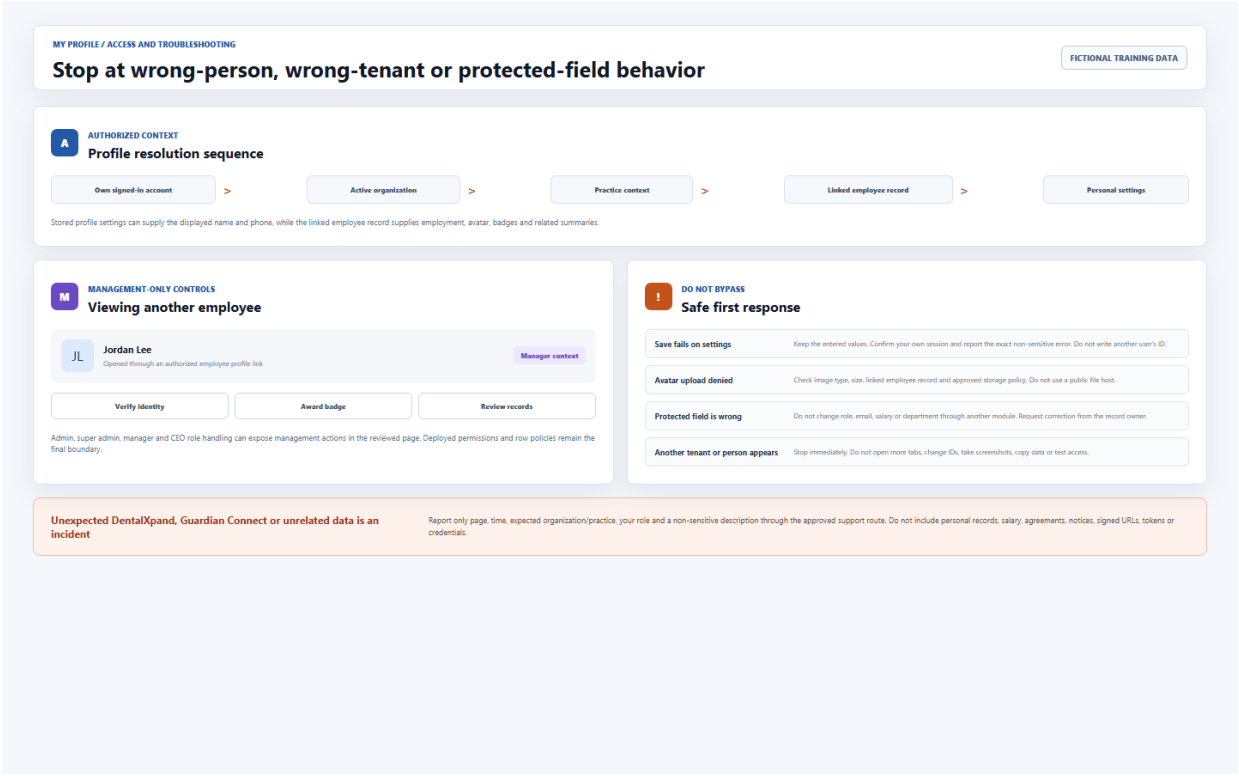

Figure 6. Fictional profile resolution, management, troubleshooting, and cross-product incident workflow.

Layer	Reviewed implementation	Production requirement
Employee rows	The list service selects employee rows, and My Profile matches the intended employee in the client.	Row-level security must restrict the result by current account, organization, practice, and role. Client filtering cannot secure a broad response.
Employee writes	Non-management users are checked against their own user ID and limited to an allowlist of personal fields.	Database policy must enforce equal or stricter ownership. Hidden or disabled inputs are not a write boundary.
Settings	The app resolves the current app-user ID and upserts settings by user_id.	Foreign key and RLS must map the Auth identity to the correct app user. Never insert a random or other user's UUID.
Avatar storage	A tenant-aware avatars path is written to the files bucket and resolved to a signed display URL.	Storage policy must keep writes and reads tenant-scoped. A signed URL is temporary and sensitive, not a public share.
Product isolation	My Profile combines personal, HR, operational, billing, and authentication data inside DentalXpand.	Guardian Connect data must not appear here, and DentalXpand data must not appear there. Crossing is an incident.

09 / TROUBLESHOOT

Resolve profile errors without bypassing identity or tenant controls

What you see	Possible reason	Correct first response
Empty profile or initials	Linked employee, avatar reference, signed URL, source record, or authorized query is unavailable.	Confirm your own account and tenant, refresh once, then request an authorized mapping review.
Settings RLS or foreign-key error	Auth identity may not map to the expected app user, or the approved settings migration and live policy may be incomplete.	Keep the exact non-sensitive error. Do not disable RLS or write another ID. Ask the deployment owner to verify mapping, constraint, migration, and policy.
Saved value returns	Settings or employee update failed, a source overrode display, or session state did not refresh.	Refresh once, note which value persisted, and report the safe symptom. Do not repeatedly overwrite both sources.
Avatar denied	File is not an image, is too large, employee link is absent, or Storage policy denied the path.	Use an approved image inside the limit. Do not rename files, use public storage, or upload under another employee.
Password rejected or locked	Current password is wrong, account is inactive or mismatched, or repeated failures triggered protection.	Stop retries, verify the account email, wait for the shown interval, then use the approved reset or recovery workflow.
Management control missing	Current role, target workflow, route, or deployed permission does not authorize it.	Respect the response. Do not change role data, URL, browser state, session, or database to make the control appear.
Wrong person, tenant, or product	Session, mapping, cache, row policy, Storage policy, or deployment isolation may be incorrect.	Stop immediately. Do not investigate with more access. Report minimum non-sensitive context through the incident route.

10 / COMPLETION

Verify safe My Profile maintenance

- I can distinguish personal settings, linked employee, authentication account, avatar storage, and related module summaries.
- I confirm my own signed-in identity, active organization, expected practice, linked employee, and route permission before using profile data.
- I update only first name, last name, phone, an approved avatar, and my own password through the documented controls.
- I know work email, role, department, designation, salary, joining date, verification, badges, agreements, recruitment, shifts, notices, attendance, leave, loans, and billing are protected or source-owned.
- I use an image file under 5 MB, require the correct employee link, and never reuse another tenant path or copied signed URL.
- I treat employee and provider cards as summaries and use their owning modules for source review and correction.
- I change only my own password, verify the current value, meet the minimum checks, and sign in again after success.
- I use management target profiles, verification, badges, and sensitive tabs only for an approved purpose and minimum necessary access.
- I never resolve RLS, foreign-key, avatar, password, or permission errors by disabling policy, changing IDs, borrowing an account, or using another product.
- I stop and report any wrong-person, cross-tenant, cross-practice, Guardian Connect, or unrelated data event without investigating further.

Continue safely
Use the Support Hub lesson next to learn approved requests, complaints, feedback, and quick-support routes.
Keep personal, employment, billing, legal, and authentication data inside their approved source workflows.

Website guide	Open My Profile	All resources
Website guide	**Open My Profile**	**All resources**