

Healthcare

USA

A US healthcare organization matched workflow access to each department's roles

A multi-facility healthcare organization set role-based permissions on its configured forms and approval workflows, so each user sees and acts on only what their job requires.



AT A GLANCE

INDUSTRY
Healthcare

REGION
New York, with facilities across the US

SIZE
Multiple departments and operational teams

PREVIOUSLY
Broad access to configured workflows

FEATURES USED

Platform

01 The client

The client is a large healthcare organization headquartered in New York, with facilities across the United States and many departments and operational teams.

Different departments use their own configured forms and workflows in Asset Infinity. As those workflows grew in number, so did the people using them, each with a different job to do.

02 The challenge

Not every user needed the same information or the same actions. Broad access could expose operational information to people who did not need it, or let users act outside their responsibilities.

- Configured forms and workflows were growing across departments.
- Users could see information that was not part of their job.
- Some users could perform workflow actions outside their responsibilities.
- Permissions did not line up with departmental and functional roles.
- Responsibilities changed over time, and access needed to follow.

03 What they set up in Asset Infinity

The organization combined its configured workflows with defined roles in Asset Infinity, so access to information and actions follows each user's responsibilities.

Platform

Roles for each user group

Roles were defined for each department and function, and each user was given the role that matches their job.

Platform

Permissions on workflow actions

Each role decides who can view, submit, approve or close a step, so actions stay with the people responsible for them.

Platform

Configured forms and approval steps

Departmental processes run on custom fields, forms and approval stages, configured without code and covered by the same role permissions.

Platform

An audit trail of every action

Every submission, approval and change is recorded with who made it and when, so responsibility for each step is clear.

04 How it works day to day

Here is how roles shape a departmental workflow from start to finish.

- DEPARTMENT USER** **Signs in and sees their work**
When the user signs in, they see only the forms, records and actions their role allows.
- DEPARTMENT USER** **Submits a form**
The user fills in the department's configured form. Fields and actions outside their role are not available to them.
- SYSTEM** **Routes it to the right approver**
The submission moves to the approval stage, where only users with the approver role can act. A reminder follows if it waits.
- DEPARTMENT MANAGER** **Approves or returns**
The manager reviews and approves or returns the submission. The decision is recorded with their name and the time.
- OPERATIONS TEAM** **Completes the next step**
The team responsible for the next stage acts on it, without seeing information that belongs to other departments.
- ADMINISTRATOR** **Updates roles as jobs change**
When someone changes responsibilities, the administrator changes their role, and their access changes with it.
- COMPLIANCE LEAD** **Reviews the audit trail**
The audit trail shows who viewed, changed or approved each record, for internal review.

05 Before and after

	BEFORE	WITH ASSET INFINITY
Access to information	Broad, regardless of job	Limited by role
Workflow actions	Users could act outside their responsibilities	Actions allowed only to the responsible role
Permissions	Not aligned with departments	Mapped to departmental and functional roles
Consistency	Varied between processes	One permission structure across configured workflows
Changing responsibilities	Access did not follow	Roles reviewed and updated
Accountability	Hard to tell who did what	Recorded in the audit trail

06 How it rolled out

1

Groups and responsibilities reviewed. The team reviewed user groups, responsibilities, workflow access and security requirements.

2

Roles mapped and permissions tested. Roles were defined, applied to workflow actions and information, and tested across every role and stage.

3

Users trained, roles kept current. Users were trained on their role's access. Roles and permissions are reviewed as responsibilities change.

07 The results

- Less unnecessary access to operational information and workflow actions
- System permissions aligned with departmental and functional roles
- Stronger control over who can view or perform each workflow action
- The same permission structure applied across configured processes
- Clearer accountability for users working in customized workflows

08 Why it worked

Built into the workflows

Permissions sit on the same configured forms and approval steps departments already use, so there was nothing new to adopt.

Tested before go-live

Every role was checked at every workflow stage, so users met the right access on day one.

Kept current

Roles are reviewed as responsibilities change, so access does not drift from the job over time.

09 Looking ahead

The organization kept the configured workflows its departments rely on while making sure each user sees and does only what their role requires.

Because access is set by role, a new hire or a change of responsibility is a matter of assigning the right role, and the audit trail shows who did what afterward.

See it on your own assets

A 30-minute demo, set up for a hospital or health system.

The client's name is withheld for confidentiality. Results are as reported by the client.

[Book a demo](#)

[Start a 14-day free trial](#)