Phase 9: Reporting, Dashboards & Security Review

AI-Enabled Hospital & Pharmacy Management System

Goal: The goal of Phase 9 is to strengthen both data visibility and data security within the CareTrack application. By creating different types of reports and dashboards, meaningful insights into patient care, appointments, and pharmacy management can be visualized. At the same time, configuring sharing settings, field-level security, session controls, IP restrictions, and audit trail ensures that sensitive healthcare data remains protected. This phase balances analytics for decision-making with robust security measures, making the application reliable and compliant.

Tasks in Phase 9:

- Reports (Tabular, Summary, Matrix, Joined)
- Report Types
- Dashboards
- Dynamic Dashboards
- Sharing Settings
- Field Level Security
- Session Settings
- Login IP Ranges
- Audit Trail

Reports (Tabular, Summary, Matrix, Joined)

Goal

To generate meaningful insights from Salesforce data using different report formats like Tabular, Summary, Matrix, and Joined for Patients, Doctors, Appointments, and Pharmacy data.

Steps

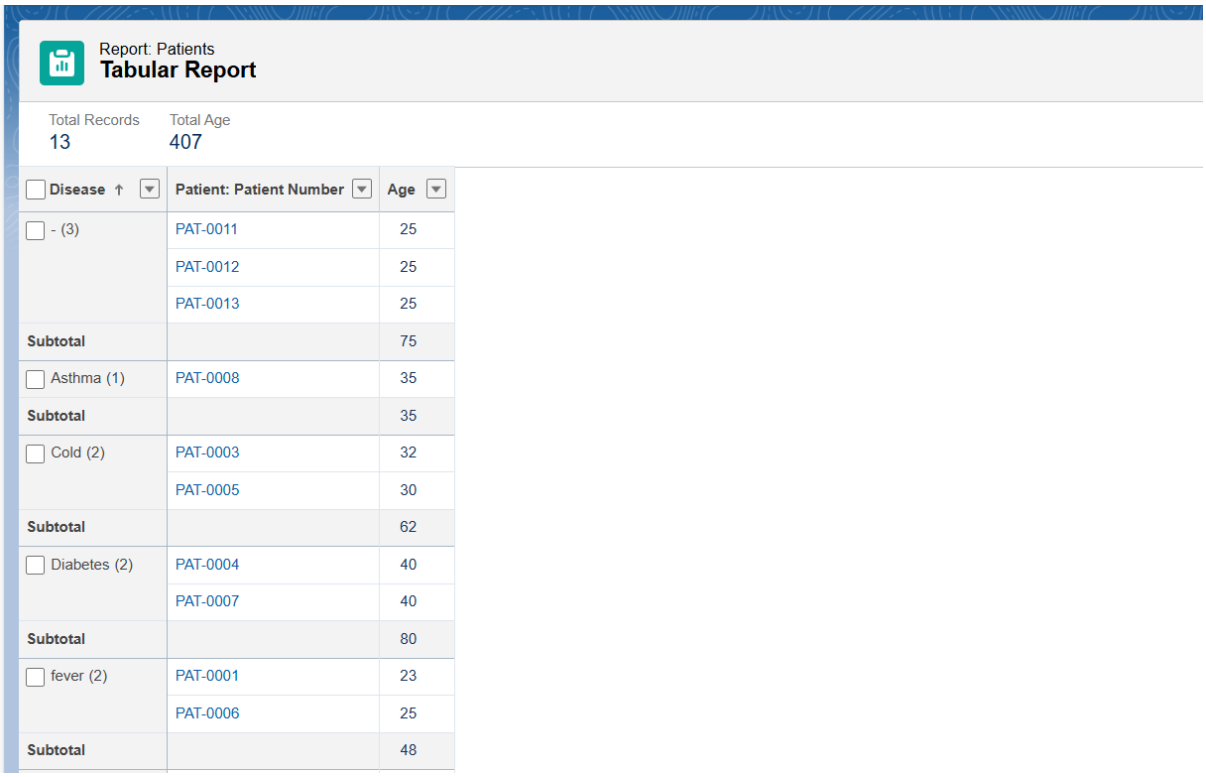
1. Navigated to Reports tab in Salesforce.
2. Clicked New Report → selected Patient object.
3. Created different reports:
    - Tabular Report: Displayed a simple list of Patient records.
    - Summary Report: Grouped patients by Disease to show case distribution.
    - Matrix Report: Grouped Patients by Disease (rows) and Age (columns).

- Joined Report: Combined Patients and Appointments into one report for correlation.

4. Saved and ran each report to verify output.

Conclusion

Reports provide flexible analysis of patient, doctor, and appointment data. Each type serves a purpose: Tabular for lists, Summary for grouping, Matrix for cross-analysis, and Joined for combined objects.



Report: Patients
Tabular Report

Total Records	Total Age
13	407

Disease ↑	Patient: Patient Number	Age
- (3)	PAT-0011	25
	PAT-0012	25
	PAT-0013	25
Subtotal		75
Asthma (1)	PAT-0008	35
Subtotal		35
Cold (2)	PAT-0003	32
	PAT-0005	30
Subtotal		62
Diabetes (2)	PAT-0004	40
	PAT-0007	40
Subtotal		80
fever (2)	PAT-0001	23
	PAT-0006	25
Subtotal		48

Report: Patients

Patients grouped by Disease

Total Records	Total Age
13	407

Disease	Patient: Patient Number	Age
- (3)	PAT-0011	25
	PAT-0012	25
	PAT-0013	25
Subtotal		75
Asthma (1)	PAT-0008	35
Subtotal		35
Cold (2)	PAT-0003	32
	PAT-0005	30
Subtotal		62
Diabetes (2)	PAT-0004	40
	PAT-0007	40
Subtotal		80
fever (2)	PAT-0001	23
	PAT-0006	25
Subtotal		48

Outline | Filters 1

Groups

GROUP ROWS

Add group...

Disease

GROUP COLUMNS

Add group...

Age

Columns

Add column...

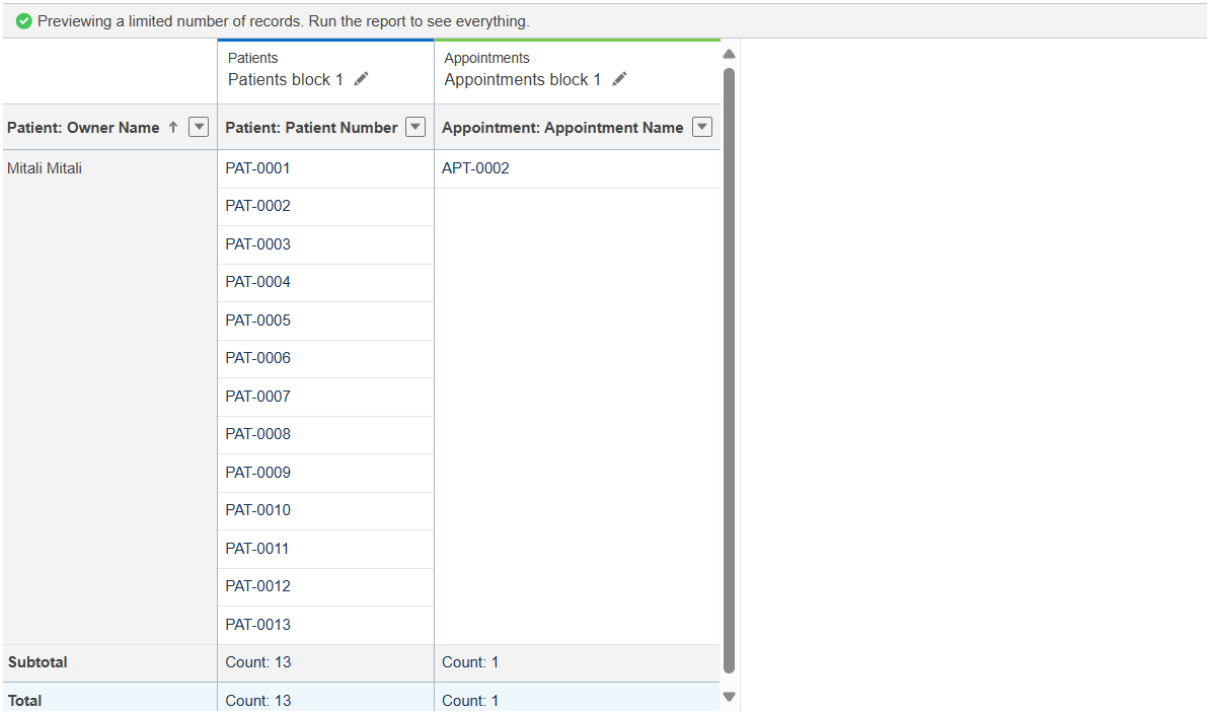
Patient: Patient Number

Previewing a limited number of records. Run the report to see everything.

Disease	Age	23	25	28	30	32	35	40	54	Total
-	Record Count	0	3	0	0	0	0	0	0	3
Asthma	Record Count	0	0	0	0	0	1	0	0	1
Cold	Record Count	0	0	0	1	1	0	0	0	2
Diabetes	Record Count	0	0	0	0	0	0	2	0	2
fever	Record Count	1	1	0	0	0	0	0	0	2
Flu	Record Count	0	0	1	0	0	0	0	0	1
flue	Record Count	0	1	0	0	0	0	0	1	2
Total	Record Count	1	5	1	1	1	1	2	1	13

Details (13 Rows) Click an intersection in the table above to filter details.

	Patient: Patient Number
1	PAT-0011
2	PAT-0013
3	PAT-0012
4	PAT-0008
5	PAT-0005
6	PAT-0003



Report Types

Goal

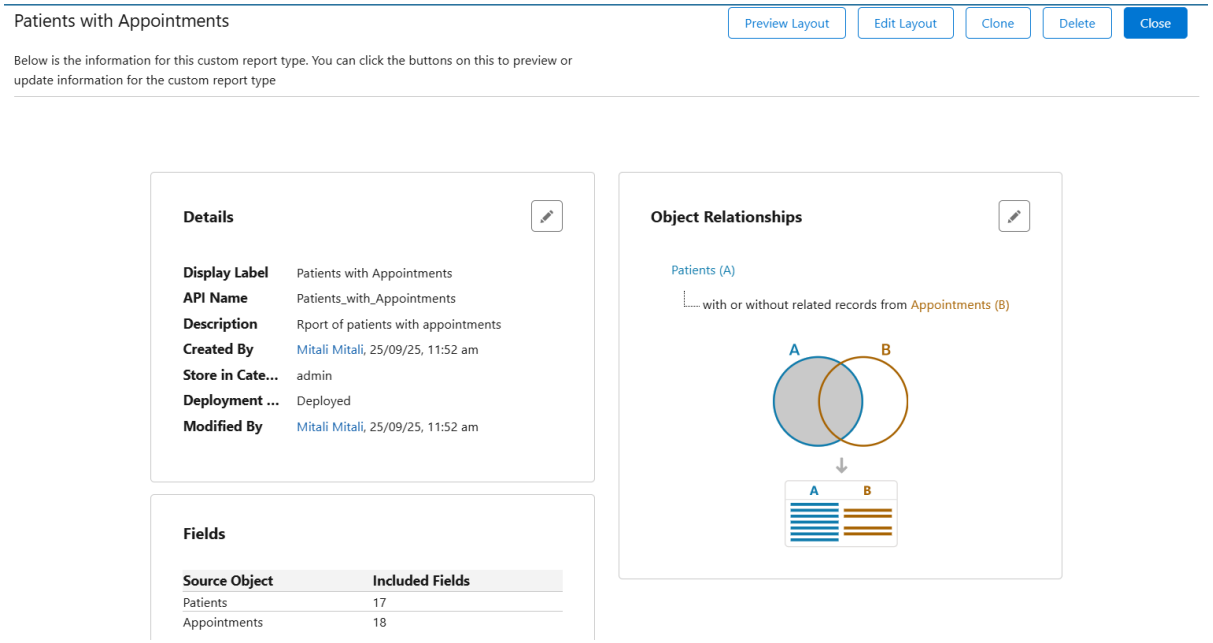
To define custom Report Types for generating specialized reports beyond the standard templates.

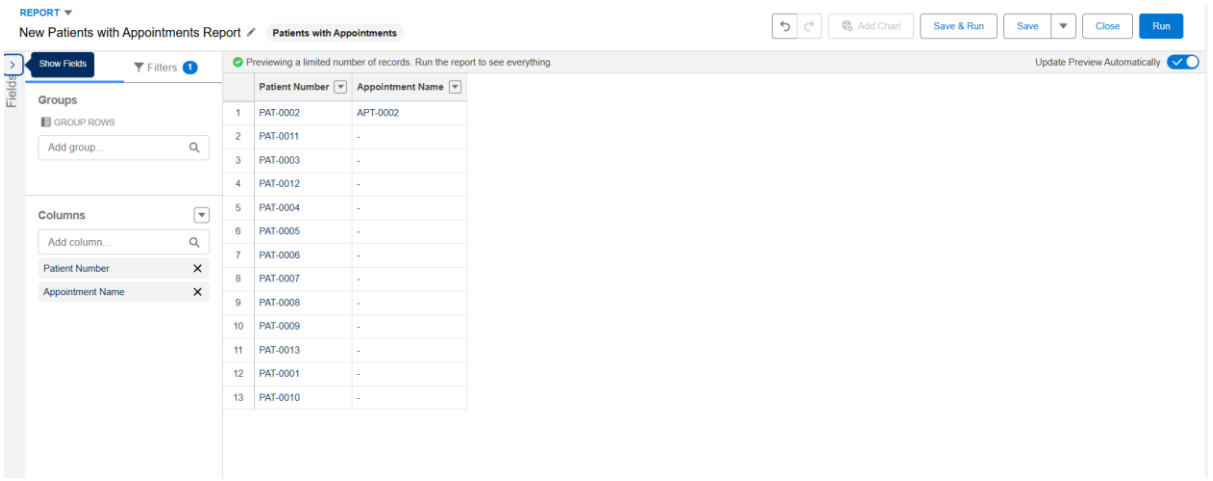
Steps

1. In Setup, searched for Report Types.
2. Created a new Report Type with Primary Object: Patients and related object Appointments.
3. Set it as Deployed for use in reports.
4. Verified by creating a new report with this custom report type.

Conclusion

Custom report types allowed building reports combining Patients and Appointments, which are crucial for CareTrack’s healthcare insights.





Dashboards

Goal

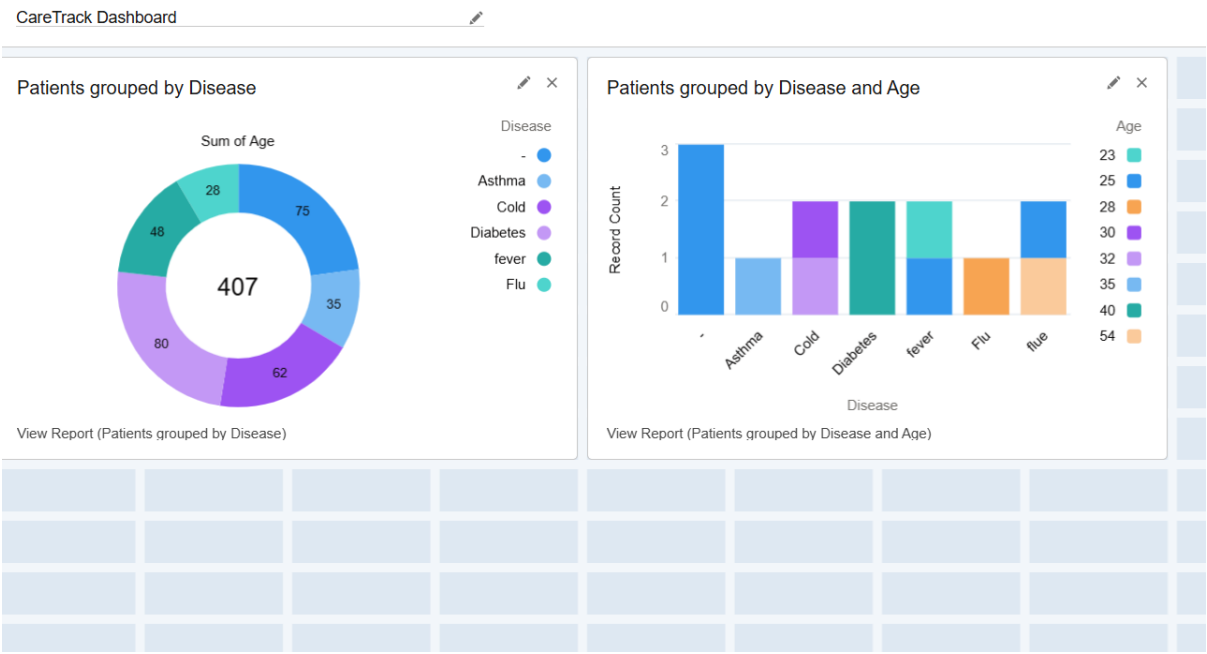
To visually represent reports in an interactive format for quick decision-making.

Steps

1. Navigated to Dashboards tab → New Dashboard.
2. Added components like bar charts, pie charts linked to Patient grouped by disease and age reports.
3. Saved and refreshed the Dashboard.

Conclusion

Dashboards provided a graphical summary of Patients by Disease, Patients by disease and age. It improved clarity and management oversight.



Dynamic Dashboards

Goal

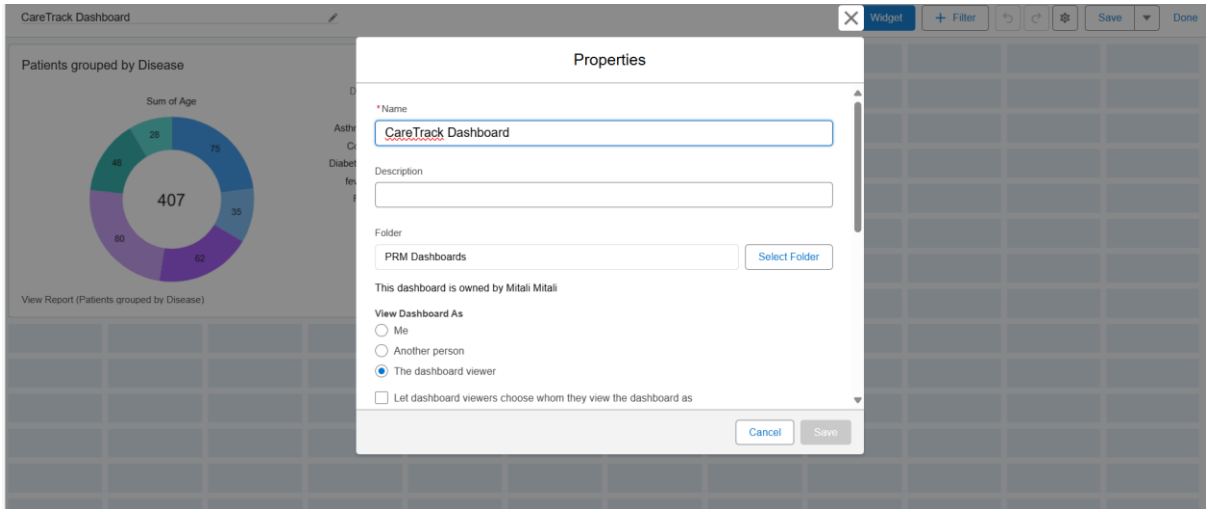
To allow different users (Doctors, Admin, Patients) to view dashboards according to their own data access.

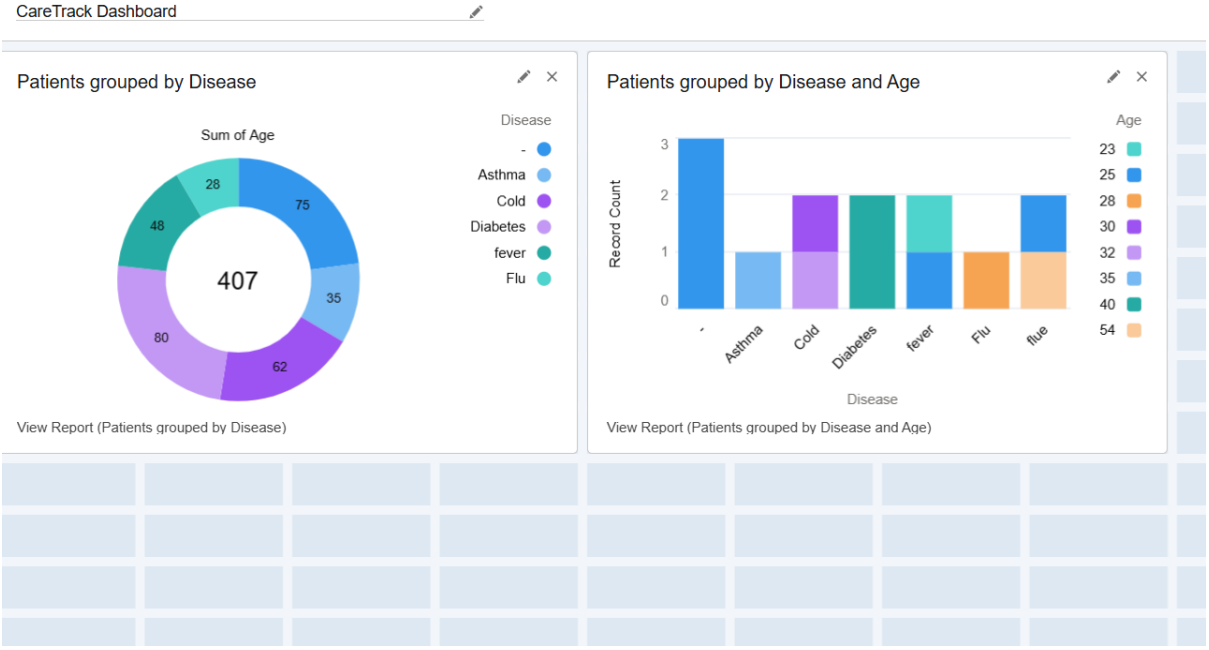
Steps

- Opened the created dashboard → Clicked Edit.
- In properties, changed View Dashboard As → Logged-in User.
- Saved the dashboard.

Conclusion

Dynamic Dashboards ensured each user only viewed their relevant records, enhancing personalization and security.





Sharing Settings

Goal

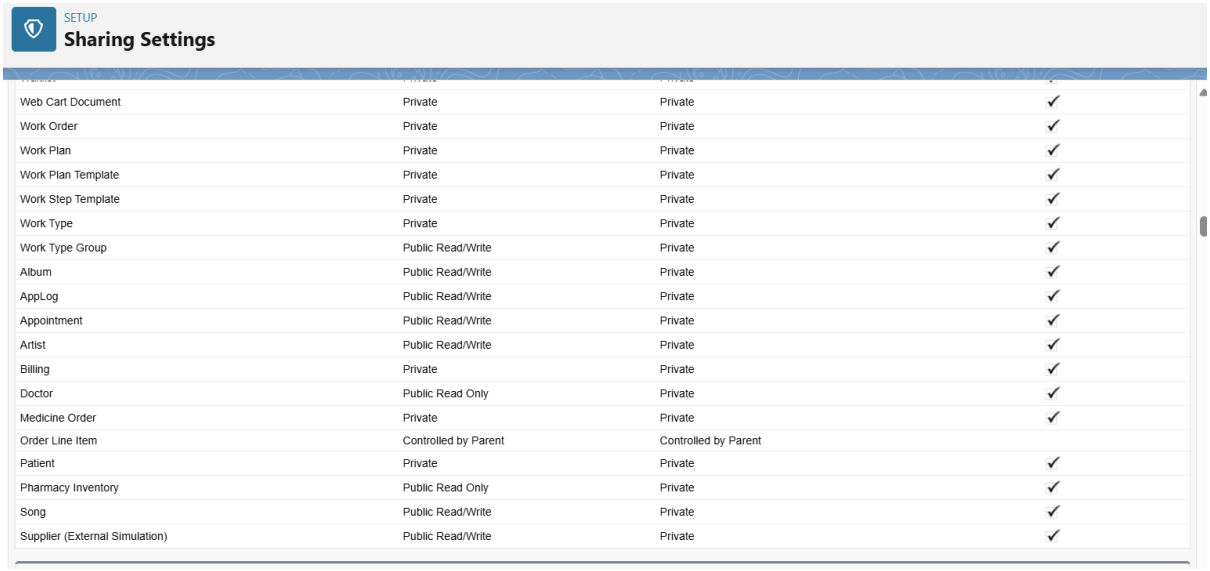
To control record-level access to maintain data security.

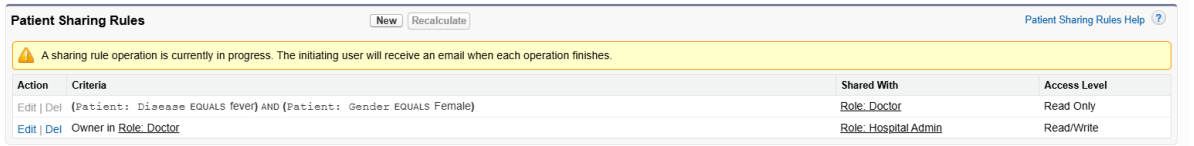
Steps

1. In Setup, searched for Sharing Settings.
2. Set Organization-Wide Defaults (OWD) for objects:
    - Patients: Private
    - Doctors: Public Read Only
    - Appointments: Controlled by Parent
3. Added Sharing Rules to allow access between related records.

Conclusion

Sharing settings enforced data security by restricting sensitive patient details while ensuring required visibility for doctors.





Field Level Security

Goal

To ensure only authorized users can view/edit sensitive fields like Patient Phone, Address, or Disease.

Steps

1. In Setup, searched for Field Accessibility.
2. Selected Patient object → Chose field Disease.
3. Made fields Read-only or Hidden for non-admin profiles.
4. Verified by logging in as a different user.

Conclusion

Field Level Security protected sensitive patient information by restricting access at the field level.

The below figure represents field level security for the object Patient and field Disease

Profiles	Master	Inpatient	Outpatient
Admin Profile	Editable	Editable	Editable
Patient Profile	Read-Only	Read-Only	Read-Only
Doctor Profile	Editable	Editable	Editable

Session Settings

Goal

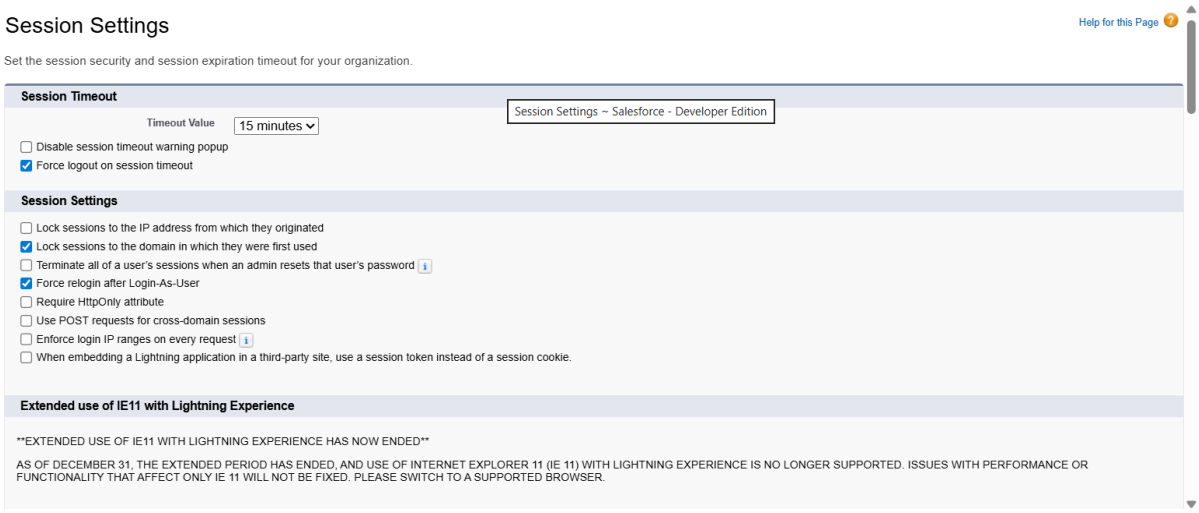
To improve login and session security in Salesforce.

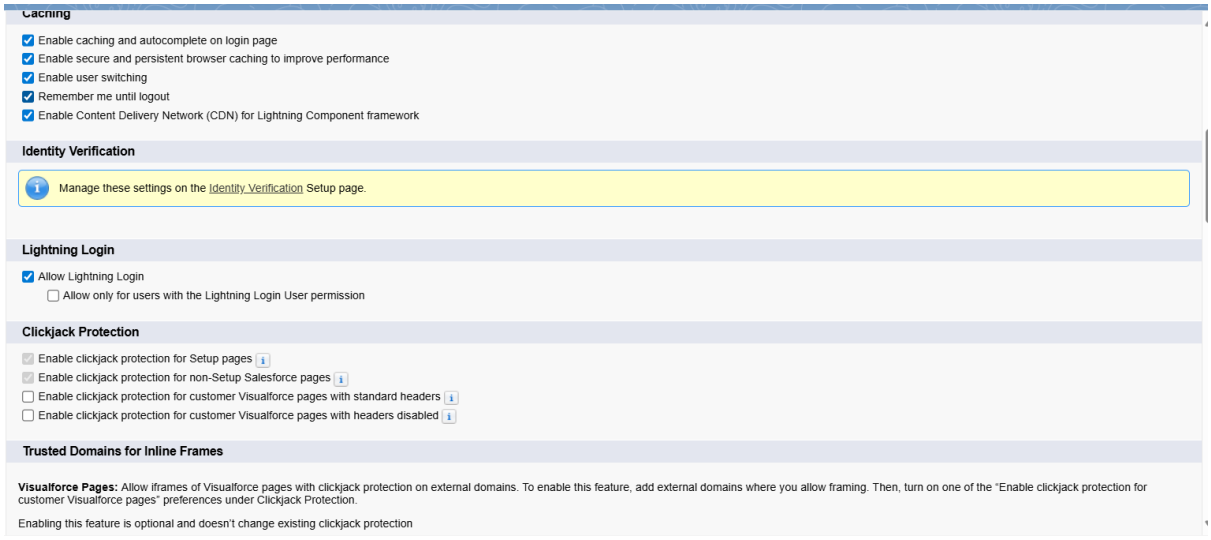
Steps

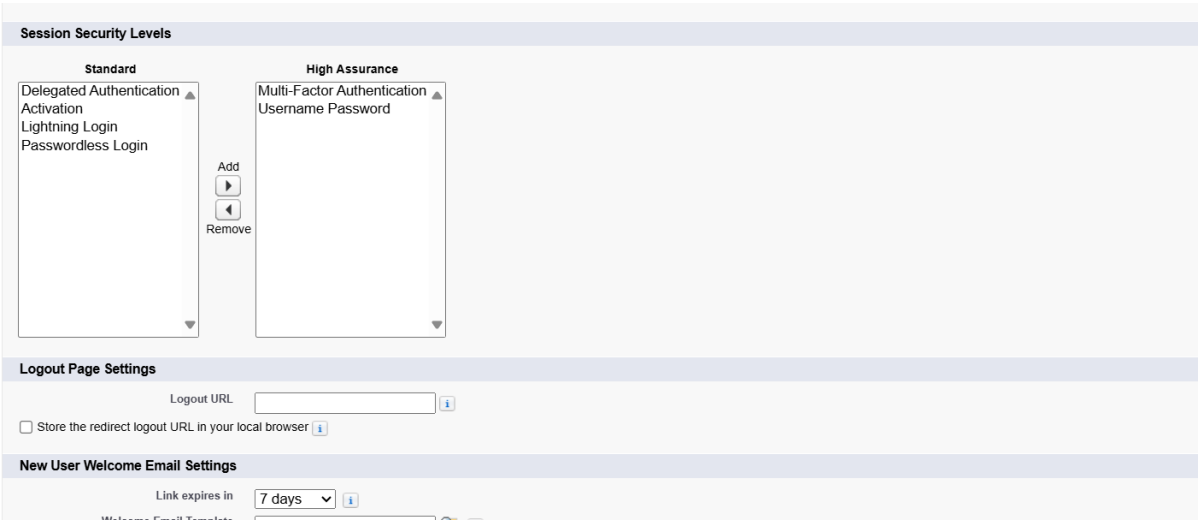
1. In Setup, searched for Session Settings.
2. Enabled features like:
    - Session Timeout: 30 minutes
    - Require Secure Connections (HTTPS)
    - Prevent Concurrent Sessions
3. Saved the changes.

Conclusion

Session Settings strengthened org security by enforcing session expiry and preventing unauthorized simultaneous logins.





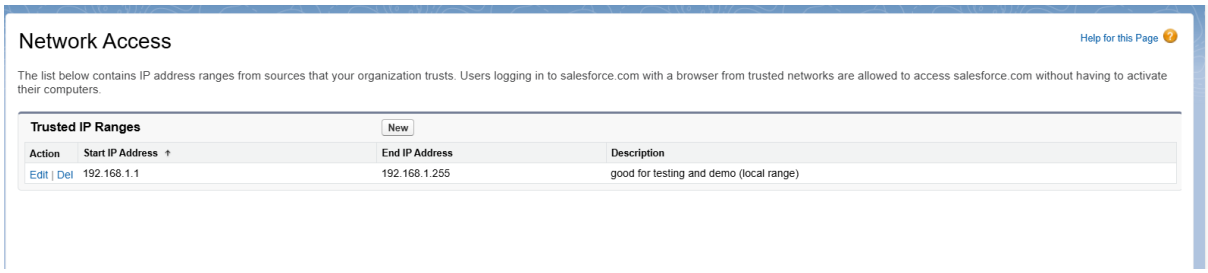


Login IP Ranges

Goal: Secure user sessions by enforcing timeout and HTTPS.

Steps: Configured session timeout, enabled secure connections, and forced logout on timeout.

Conclusion: Prevents unauthorized access and improves overall security of CareTrack



Audit Trail

Goal

The goal of Audit Trail is to monitor and track all administrative changes made in Salesforce Setup, such as creation or modification of objects, fields, rules, and security settings. This ensures accountability, transparency, and compliance by keeping a history of who changed what and when.

Steps Executed

1. Logged in to Salesforce and navigated to Setup.

2. In the Quick Find box, searched for View Setup Audit Trail.

3. Opened the Audit Trail page, which displayed the 20 most recent setup changes.

4. Verified details such as date, user, action, and object modified.

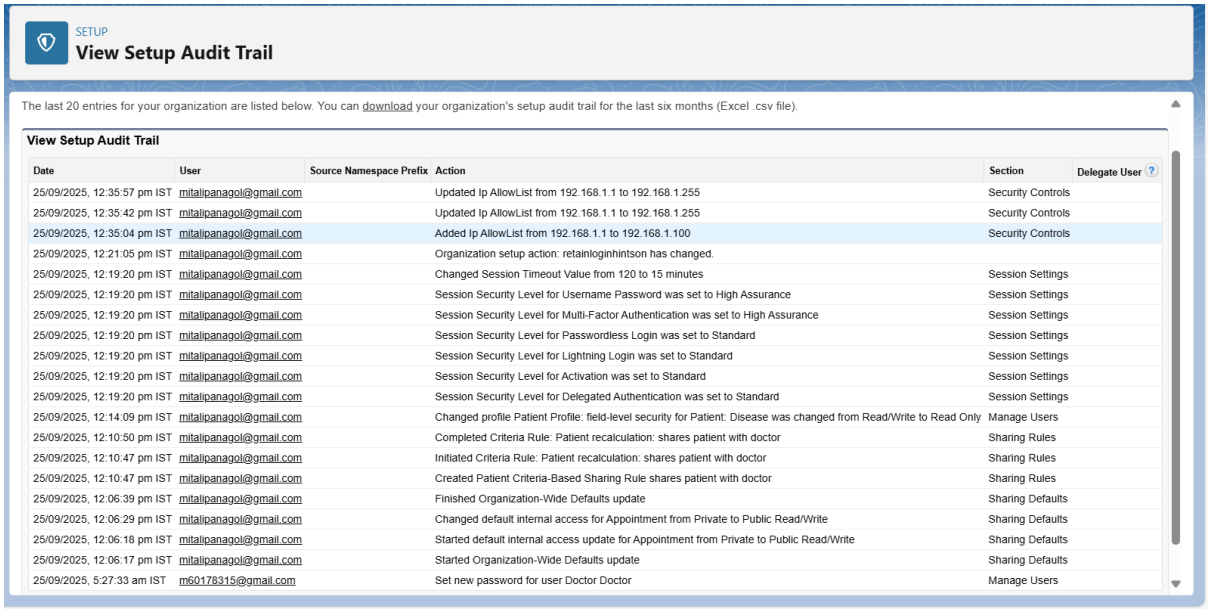
Observation

The audit log displayed changes such as creation of custom objects (e.g., Patient, Appointment) and configuration updates (e.g., fields, rules).

Each change clearly showed who performed the action and when.

Conclusion

Audit Trail provides a clear record of all setup changes in Salesforce. It helps administrators maintain system integrity, identify unauthorized modifications, and improve security by ensuring accountability. For the CareTrack project, it ensures that all critical modifications (like adding Patients, Appointments, and Security rules) are traceable for compliance and future audits.



Conclusion

Phase 9 established reporting, dashboards, and security measures for CareTrack. Reports and dashboards gave insights into Patients, Appointments, and Pharmacy. Dynamic dashboards personalized access for users. Security configurations like Sharing Settings, Field Level Security, Session Settings, IP Ranges, and Audit Trail ensured data confidentiality, integrity, and compliance.
