

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 13	Total Age 407	
<input type="checkbox"/> Disease ↑ ▾	Patient: Patient Number ▾	Age ▾
<input type="checkbox"/> - (3)	PAT-0011	25
	PAT-0012	25
	PAT-0013	25
Subtotal		75
<input type="checkbox"/> Asthma (1)	PAT-0008	35
Subtotal		35
<input type="checkbox"/> Cold (2)	PAT-0003	32
	PAT-0005	30
Subtotal		62
<input type="checkbox"/> Diabetes (2)	PAT-0004	40
	PAT-0007	40
Subtotal		80
<input type="checkbox"/> fever (2)	PAT-0001	23
	PAT-0006	25
Subtotal		48



Report: Patients

Patients grouped by Disease

Total Records
13

Total Age
407

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

Outline

Filters 1

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

Update

Groups

GROUP ROWS

Add group...

Disease

GROUP COLUMNS

Add group...

Age

Columns

Add column...

Patient: Patient Number

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

<div> Previewing a limited number of records. Run the report to see everything. </div>		
	<div> Patients Patients block 1 </div>	<div> Appointments Appointments block 1 </div>
<div> Patient: Owner Name ↑ ▾ </div>	<div> Patient: Patient Number ▾ </div>	<div> Appointment: Appointment Name ▾ </div>
Mitali Mitali	PAT-0001	APT-0002
	PAT-0002	
	PAT-0003	
	PAT-0004	
	PAT-0005	
	PAT-0006	
	PAT-0007	
	PAT-0008	
	PAT-0009	
	PAT-0010	
	PAT-0011	
	PAT-0012	
	PAT-0013	
Subtotal	Count: 13	Count: 1
Total	Count: 13	Count: 1

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.

Patients with Appointments

[Preview Layout](#)[Edit Layout](#)[Clone](#)[Delete](#)[Close](#)

Below is the information for this custom report type. You can click the buttons on this to preview or update information for the custom report type

Details

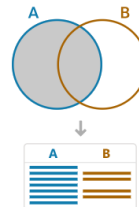
Display Label Patients with Appointments
API Name Patients_with_Appointments
Description Report of patients with appointments
Created By Mitali Mitali, 25/09/25, 11:52 am
Store in Cate... admin
Deployment ... Deployed
Modified By Mitali Mitali, 25/09/25, 11:52 am

Fields

Source Object	Included Fields
Patients	17
Appointments	18

Object Relationships

Patients (A)
with or without related records from Appointments (B)



REPORT ▾

New Patients with Appointments Report Patients with Appointments

↺

↻

Add Chart

Save & Run

Save ▾

Close

Run

Update Preview Automatically ☒

Field

Show Fields

Filters 1

Groups

GROUP ROWS

Add group...

Columns

Add column...

Patient Number X

Appointment Name X

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

	Patient Number	Appointment Name
1	PAT-0002	APT-0002
2	PAT-0011	-
3	PAT-0003	-
4	PAT-0012	-
5	PAT-0004	-
6	PAT-0005	-
7	PAT-0006	-
8	PAT-0007	-
9	PAT-0008	-
10	PAT-0009	-
11	PAT-0013	-
12	PAT-0001	-
13	PAT-0010	-

Dashboards

Goal

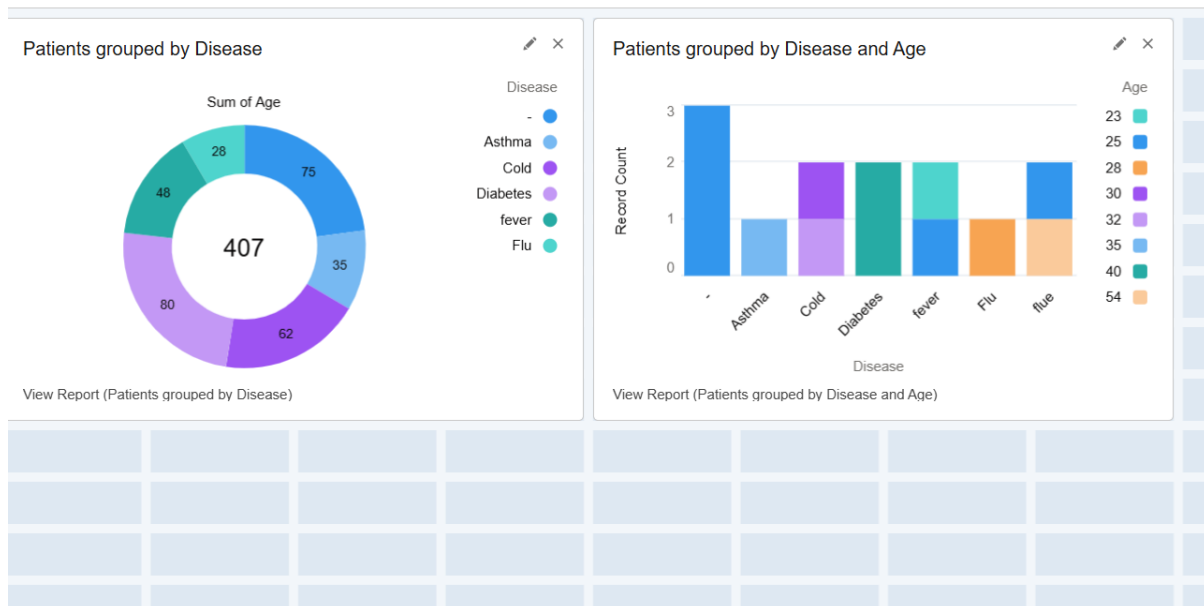
To visually represent reports in an interactive format for quick decision-making.

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

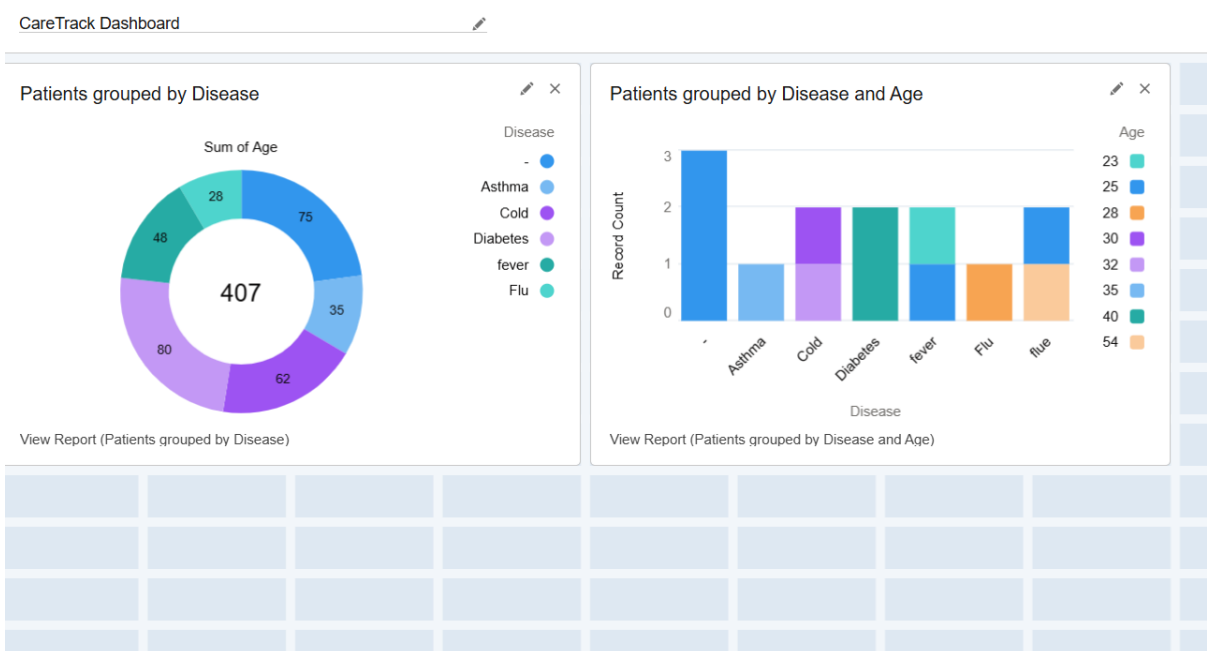
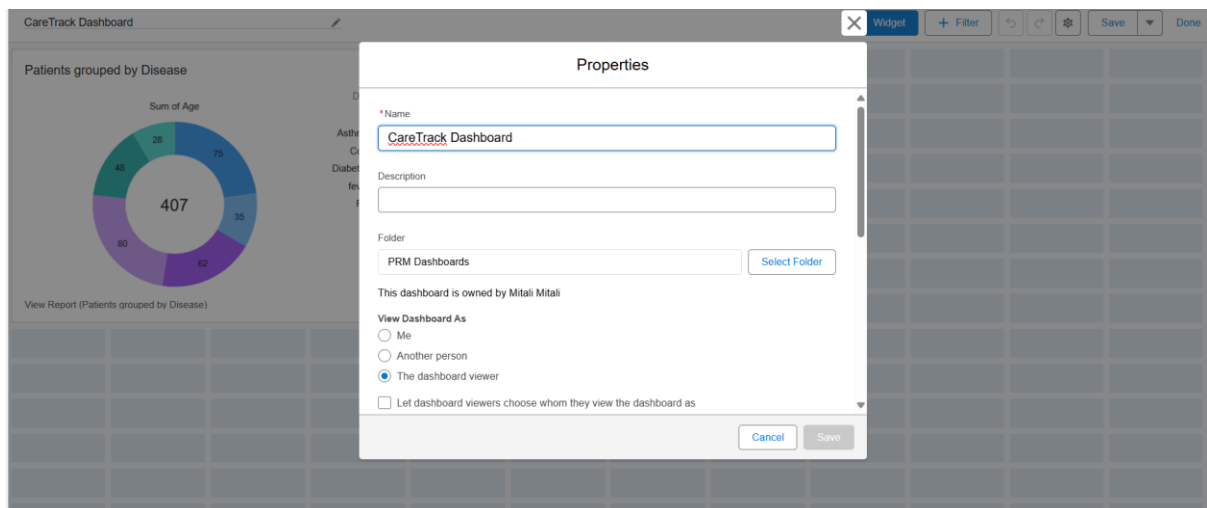
To allow different users (Doctors, Admin, Patients) to view dashboards according to their own data access.

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.

SETUP

Sharing Settings

Web Cart Document	Private	Private	✓
Work Order	Private	Private	✓
Work Plan	Private	Private	✓
Work Plan Template	Private	Private	✓
Work Step Template	Private	Private	✓
Work Type	Private	Private	✓
Work Type Group	Public Read/Write	Private	✓
Album	Public Read/Write	Private	✓
AppLog	Public Read/Write	Private	✓
Appointment	Public Read/Write	Private	✓
Artist	Public Read/Write	Private	✓
Billing	Private	Private	✓
Doctor	Public Read Only	Private	✓
Medicine Order	Private	Private	✓
Order Line Item	Controlled by Parent	Controlled by Parent	
Patient	Private	Private	✓
Pharmacy Inventory	Public Read Only	Private	✓
Song	Public Read/Write	Private	✓
Supplier (External Simulation)	Public Read/Write	Private	✓

Patient Sharing Rules

New Recalculate

Patient Sharing Rules Help ?

A sharing rule operation is currently in progress. The initiating user will receive an email when each operation finishes.

Action	Criteria	Shared With	Access Level
Edit Del	(Patient: Disease EQUALS fever) AND (Patient: Gender EQUALS Female)	Role: Doctor	Read Only
Edit Del	Owner in Role: Doctor	Role: Hospital Admin	Read/Write

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.

Session Settings

Set the session security and session expiration timeout for your organization.

Session Timeout

Timeout Value

15 minutes

☐ Disable session timeout warning popup
☒ Force logout on session timeout

Session Settings

☐ Lock sessions to the IP address from which they originated
☒ Lock sessions to the domain in which they were first used
☐ Terminate all of a user's sessions when an admin resets that user's password
☒ Force relogin after Login-As-User
☐ Require HttpOnly attribute
☐ Use POST requests for cross-domain sessions
☐ Enforce login IP ranges on every request
☐ When embedding a Lightning application in a third-party site, use a session token instead of a session cookie.

Extended use of IE11 with Lightning Experience

EXTENDED USE OF IE11 WITH LIGHTNING EXPERIENCE HAS NOW ENDED

AS OF DECEMBER 31, THE EXTENDED PERIOD HAS ENDED, AND USE OF INTERNET EXPLORER 11 (IE 11) WITH LIGHTNING EXPERIENCE IS NO LONGER SUPPORTED. ISSUES WITH PERFORMANCE OR FUNCTIONALITY THAT AFFECT ONLY IE 11 WILL NOT BE FIXED. PLEASE SWITCH TO A SUPPORTED BROWSER.

Session Settings ~ Salesforce - Developer Edition

Help for this Page

Caching

☒ Enable caching and autocomplete on login page

☒ Enable secure and persistent browser caching to improve performance

☒ Enable user switching

☒ Remember me until logout

☒ Enable Content Delivery Network (CDN) for Lightning Component framework

Identity Verification

1

Manage these settings on the [Identity Verification Setup](#) page.

Lightning Login

☒ Allow Lightning Login

☐ Allow only for users with the Lightning Login User permission

Clickjack Protection

☒ Enable clickjack protection for Setup pages [i](#)

☒ Enable clickjack protection for non-Setup Salesforce pages [i](#)

☐ Enable clickjack protection for customer Visualforce pages with standard headers [i](#)

☐ Enable clickjack protection for customer Visualforce pages with headers disabled [i](#)

Trusted Domains for Inline Frames

Visualforce Pages: Allow iframes of Visualforce pages with clickjack protection on external domains. To enable this feature, add external domains where you allow framing. Then, turn on one of the "Enable clickjack protection for customer Visualforce pages" preferences under Clickjack Protection.

Enabling this feature is optional and doesn't change existing clickjack protection

Trusted Domains

Add Domain

No records to display

Cross-Site Request Forgery (CSRF) Protection

☒ Enable CSRF protection on GET requests on non-setup pages [i](#)

☒ Enable CSRF protection on POST requests on non-setup pages [i](#)

Content Security Policy protection

☐ Override Restriction on Accessing Email Templates in Salesforce Classic Using Internet Explorer [i](#)

☒ Enable Stricter Content Security Policy [i](#)

Lightning Locker API Version

Use security enhancements in API version

64.0 [i](#)

Lightning Web Security

☒ Use Lightning Web Security for Lightning web components and Aura components [i](#)

Content Sniffing protection

☒ Enable Content Sniffing protection [i](#)

Referrer URL Protection

☒ Include Referrer-Policy HTTP header [i](#)

HTTP Referrer Policy:

origin-when-cross-origin [i](#)

Session Security Levels

Standard

Delegated Authentication

Activation

Lightning Login

Passwordless Login

Add

Remove

High Assurance

Multi-Factor Authentication

Username Password

Logout Page Settings

Logout URL [i](#)

☐ Store the redirect logout URL in your local browser [i](#)

New User Welcome Email Settings

Link expires in

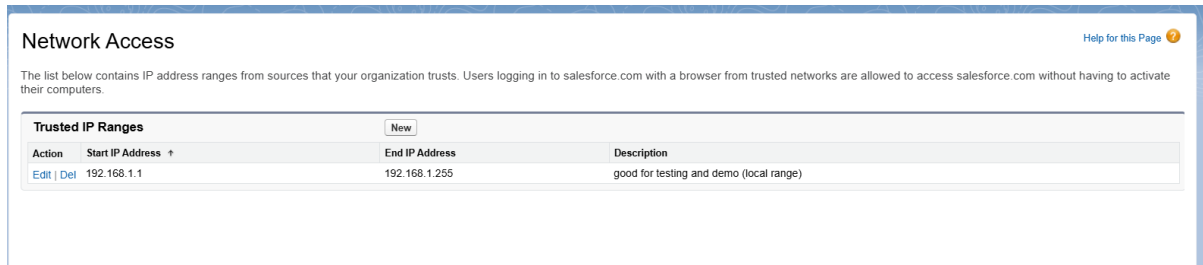
7 days [i](#)

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.



SETUP

View Setup Audit Trail

The last 20 entries for your organization are listed below. You can [download](#) your organization's setup audit trail for the last six months (Excel .csv file).

View Setup Audit Trail

Date	User	Source Namespace Prefix	Action	Section	Delegate User ?
25/09/2025, 12:35:57 pm IST	mtalipanagol@gmail.com		Updated Ip AllowList from 192.168.1.1 to 192.168.1.255	Security Controls	
25/09/2025, 12:35:42 pm IST	mtalipanagol@gmail.com		Updated Ip AllowList from 192.168.1.1 to 192.168.1.255	Security Controls	
25/09/2025, 12:35:04 pm IST	mtalipanagol@gmail.com		Added Ip AllowList from 192.168.1.1 to 192.168.1.100	Security Controls	
25/09/2025, 12:21:05 pm IST	mtalipanagol@gmail.com		Organization setup action: retainloginhintson has changed.		
25/09/2025, 12:19:20 pm IST	mtalipanagol@gmail.com		Changed Session Timeout Value from 120 to 15 minutes	Session Settings	
25/09/2025, 12:19:20 pm IST	mtalipanagol@gmail.com		Session Security Level for Username Password was set to High Assurance	Session Settings	
25/09/2025, 12:19:20 pm IST	mtalipanagol@gmail.com		Session Security Level for Multi-Factor Authentication was set to High Assurance	Session Settings	
25/09/2025, 12:19:20 pm IST	mtalipanagol@gmail.com		Session Security Level for Passwordless Login was set to Standard	Session Settings	
25/09/2025, 12:19:20 pm IST	mtalipanagol@gmail.com		Session Security Level for Lightning Login was set to Standard	Session Settings	
25/09/2025, 12:19:20 pm IST	mtalipanagol@gmail.com		Session Security Level for Activation was set to Standard	Session Settings	
25/09/2025, 12:19:20 pm IST	mtalipanagol@gmail.com		Session Security Level for Delegated Authentication was set to Standard	Session Settings	
25/09/2025, 12:14:09 pm IST	mtalipanagol@gmail.com		Changed profile Patient Profile: field-level security for Patient. Disease was changed from Read/Write to Read Only	Manage Users	
25/09/2025, 12:10:50 pm IST	mtalipanagol@gmail.com		Completed Criteria Rule: Patient recalculation: shares patient with doctor	Sharing Rules	
25/09/2025, 12:10:47 pm IST	mtalipanagol@gmail.com		Initiated Criteria Rule: Patient recalculation: shares patient with doctor	Sharing Rules	
25/09/2025, 12:10:47 pm IST	mtalipanagol@gmail.com		Created Patient Criteria-Based Sharing Rule shares patient with doctor	Sharing Rules	
25/09/2025, 12:06:39 pm IST	mtalipanagol@gmail.com		Finished Organization-Wide Defaults update	Sharing Defaults	
25/09/2025, 12:06:29 pm IST	mtalipanagol@gmail.com		Changed default internal access for Appointment from Private to Public Read/Write	Sharing Defaults	
25/09/2025, 12:06:18 pm IST	mtalipanagol@gmail.com		Started default internal access update for Appointment from Private to Public Read/Write	Sharing Defaults	
25/09/2025, 12:06:17 pm IST	mtalipanagol@gmail.com		Started Organization-Wide Defaults update	Sharing Defaults	
25/09/2025, 5:27:33 am IST	m60178315@gmail.com		Set new password for user Doctor Doctor	Manage Users	

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.