# ****Phase 9: Reporting, Dashboards & Security Review****

**Prepared by:** Kakumani Naga Jahnavi

## ****Overview****

Phase 9 focuses on leveraging Salesforce’s reporting and dashboard capabilities to monitor hospital performance and patient data while ensuring security and compliance. This phase enables healthcare administrators and doctors to access actionable insights, track key metrics, and maintain patient data confidentiality.

## ****Reports****

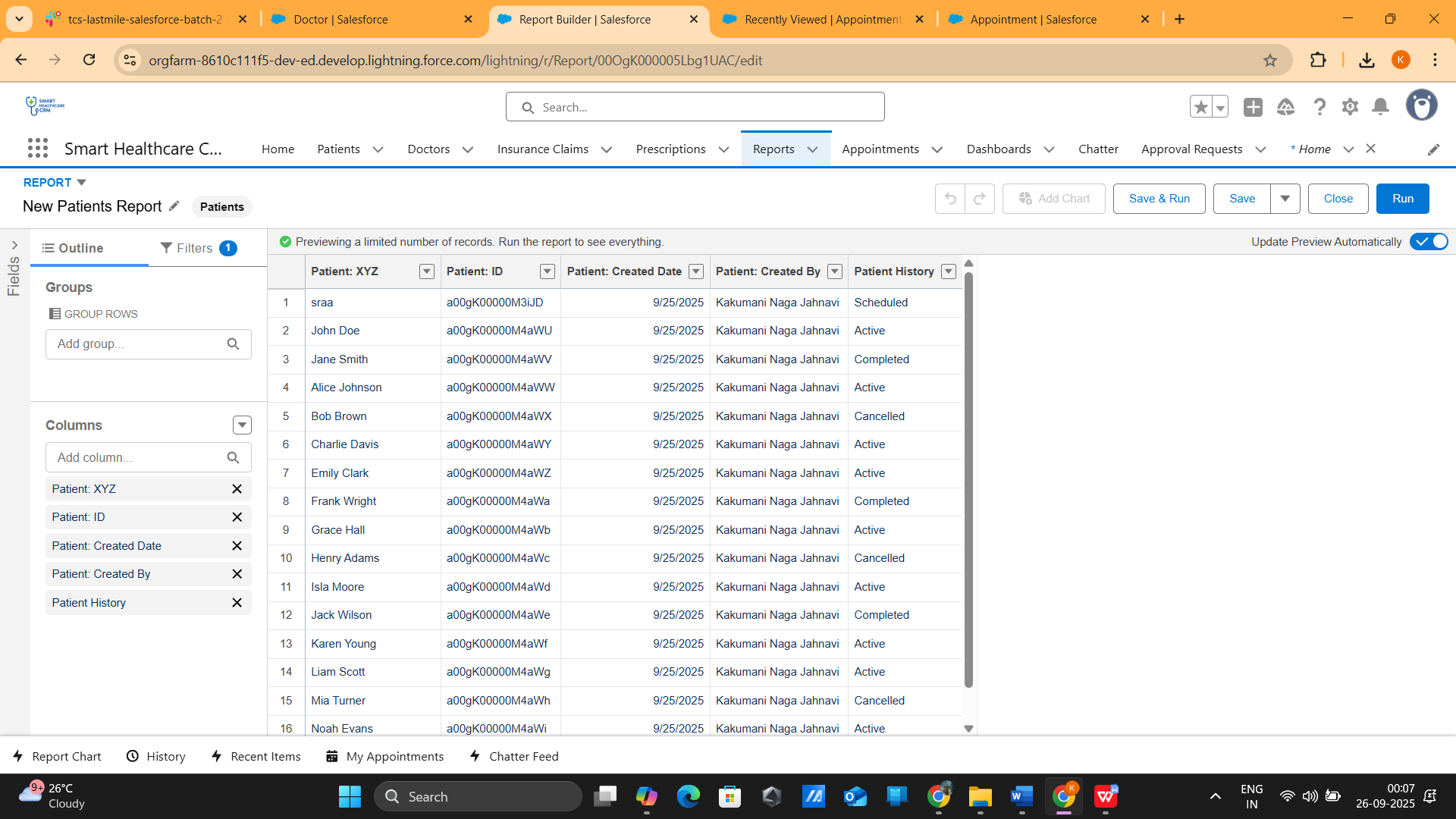
Reports are created to analyze critical data points such as appointments, doctors, and claims. The system includes:

**Appointments by Type**: Tracks the number of consultations, follow-ups, and emergency visits.

**Doctors by Specialization**: Lists doctors according to their specialization for resource planning.

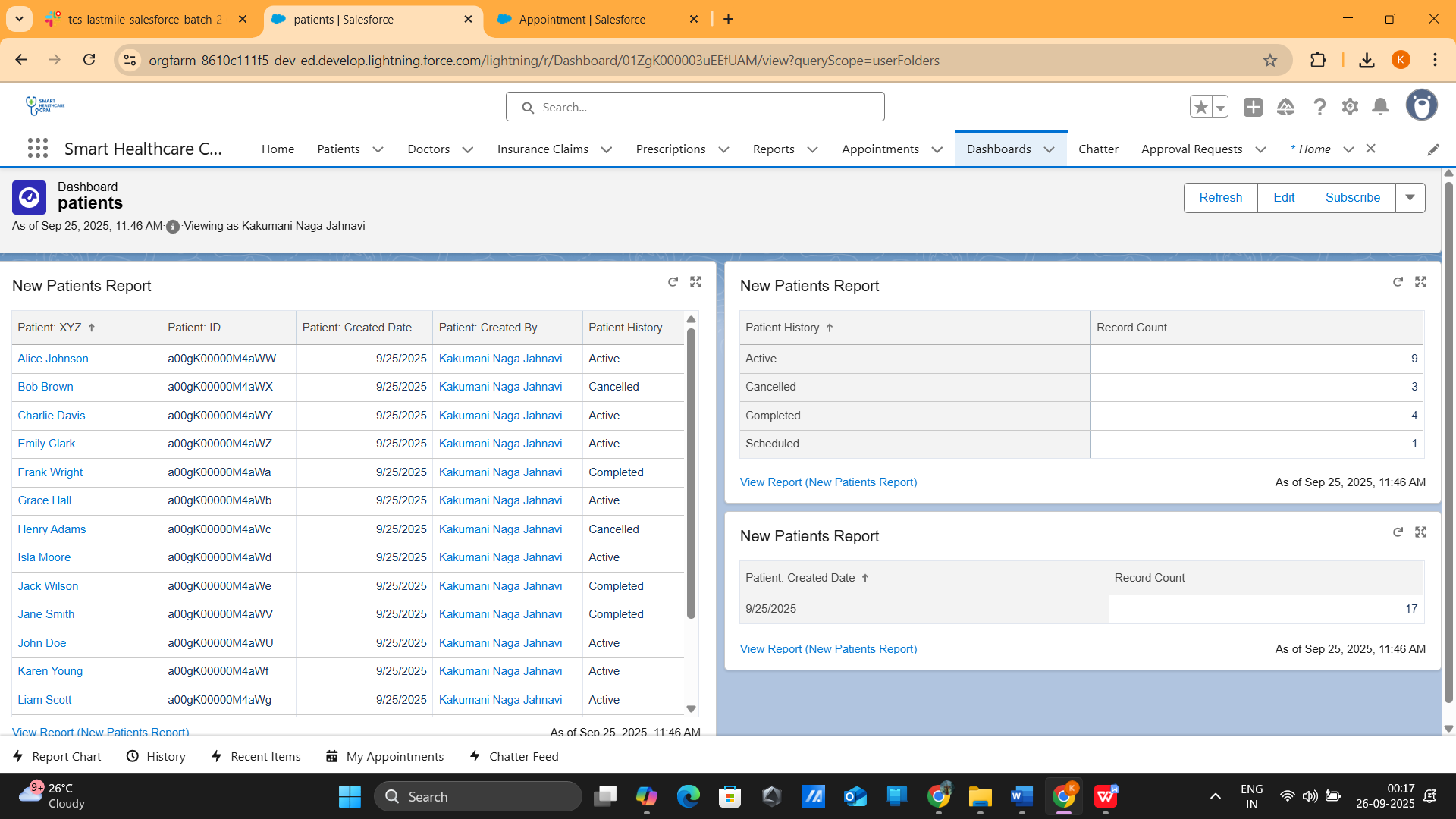
**Claims Processed**: Shows the number of insurance claims handled within a specific period.

Salesforce reports allow grouping, filtering, and summarization of data, providing detailed insights for decision-making and operational efficiency.



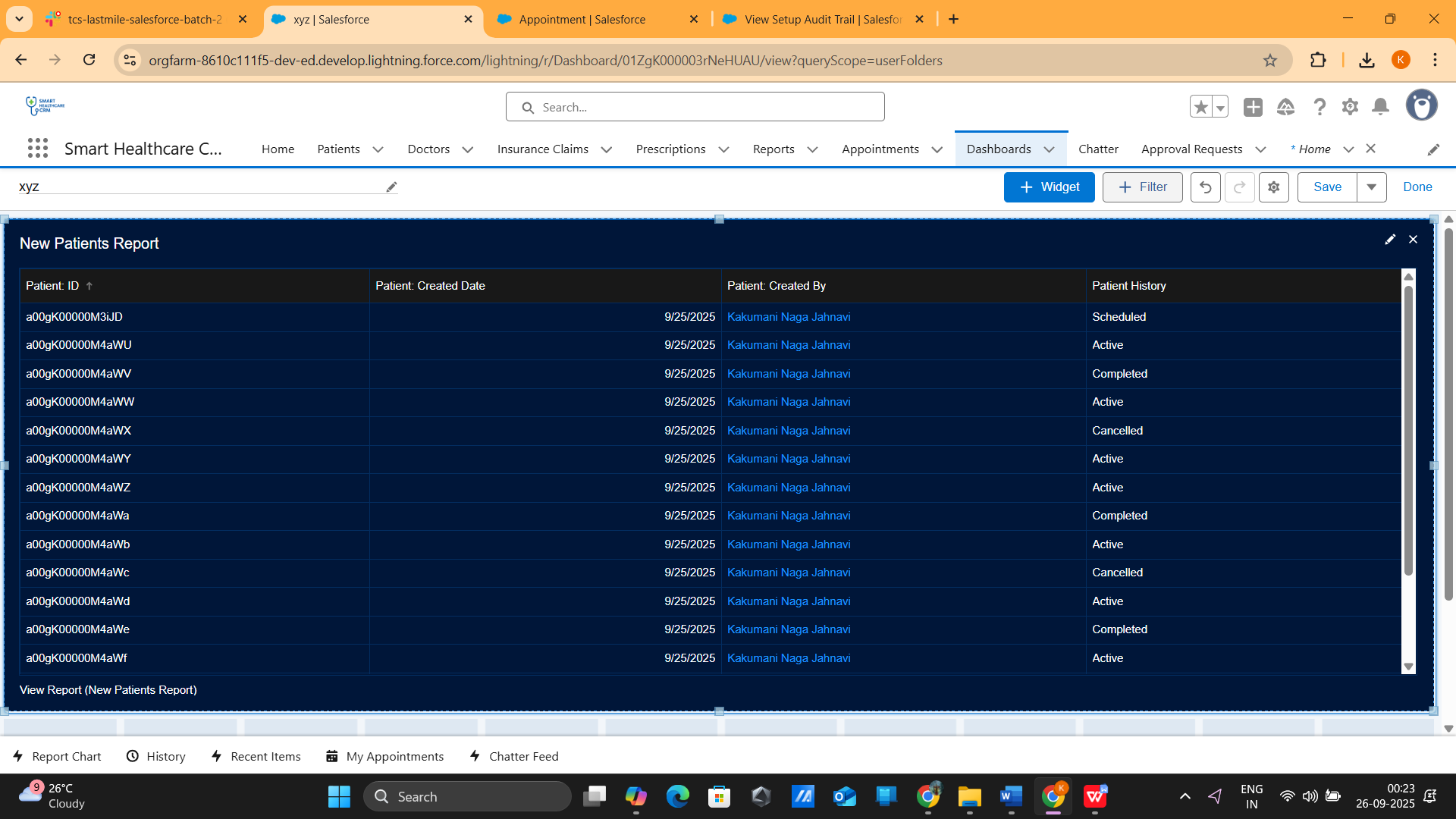
## ****Dashboards****

Dashboards visually present data from multiple reports in a consolidated format. The **Hospital Performance Tracker** dashboard aggregates key metrics, including appointment trends, doctor availability, and claim processing status. Components like bar charts, line graphs, and gauges provide a clear visual overview, enabling quick performance evaluation.



## ****Dynamic Dashboards****

Dynamic Dashboards allow users to view data tailored to their role. For example, each doctor sees only their patients and appointments. By setting the dashboard to run **as the logged-in user**, sensitive information is protected while ensuring personalized data visibility for healthcare staff.



## ****Security****

**Patient Data Encryption**: Sensitive fields such as patient names and medical history are encrypted using Salesforce Platform Encryption to ensure confidentiality.

**Audit Trail**: All configuration changes in Salesforce are tracked via the Setup Audit Trail. This provides a history of modifications, supporting compliance and monitoring.

**Additional Security Practices**:

Role-based access using **Profiles and Permission Sets**

Two-Factor Authentication (2FA) for portal users

Object-level sharing restrictions to protect sensitive patient information

