**Compliance with GDPR and HIPAA**

1. **Data Retention and Patient Consent**:

* **Data retention policies** are fully compliant with both **GDPR** and **HIPAA**, specifying how long patient data is stored and ensuring that records are securely deleted after the retention period ends.
* The plan provides mechanisms for patients to **consent** to data collection and allows patients to exercise their **right to access** their data, as well as their **right to erasure** (under GDPR). All requests for access or deletion are handled promptly by the **Compliance Officer**.

1. **Audit Trails**:

* Comprehensive **audit trails** are in place to track all access and modifications to patient data. These logs are stored securely and are protected from tampering. Regular audits ensure compliance with data governance and security standards.

1. **Data Protection Policies**:

* **Data protection policies** are well-established, covering every aspect of data handling, storage, and sharing. These policies are reviewed regularly to ensure ongoing compliance with new GDPR and HIPAA updates.

1. **Compliance Requests**:

* **Mechanisms for handling compliance requests** are clearly outlined. The **Compliance Officer** is responsible for responding to requests from patients, regulators, or external auditors. All compliance reports are generated based on real-time data collected from audit logs and security systems.