1. **Identifying Key Risks**:

* The risk management plan identifies critical risks such as **unauthorized access**, **data breaches**, **data loss**, and **system failures**. These risks are relevant to SecureHealth’s sensitive healthcare data, including patient medical records and personal information.

1. **Mitigation Strategies**:

* The plan implements **industry best practices** to mitigate these risks, such as:
* **Encryption**: All sensitive patient data, including medical records and insurance information, is encrypted both at rest and in transit, ensuring that even if data is intercepted, it cannot be read without proper decryption keys.
* **Access Control**: **Role-Based Access Control (RBAC)** ensures that only authorized personnel (e.g., doctors, nurses, and admins) have access to sensitive patient data, and access is restricted based on job roles.
* **Data Backups**: Regular **backups** of critical data are performed, and these backups are stored securely in separate locations to ensure data recovery in the event of a system failure or breach.
* **Incident Response Plan**: The plan includes a detailed **incident response strategy** that outlines steps for addressing data breaches, unauthorized access attempts, and system failures. This ensures rapid response to minimize damage and protect data integrity.