HIPAA & GDPR Compliance Guide for MedGPT

Overview of Compliance Standards

HIPAA (Health Insurance Portability and Accountability Act):
This U.S. regulation ensures protection of ePHI (electronic Protected Health Information). Organizations handling such data must implement safeguards to ensure its confidentiality, integrity, and availability. It also mandates breach notification.

GDPR (General Data Protection Regulation):
Applies to anyone handling data of EU citizens. It gives individuals the right to access, correct, and erase their data, and requires organizations to justify data processing, notify breaches within 72 hours, and potentially appoint a Data Protection Officer.

MedGPT-Specific Compliance Strategies

During model development, only open-source and properly licensed datasets were used. For testing with proprietary or actual patient data, strict rules were followed:
- Data was anonymized by reading DICOM files and stripping identifiable information.
- Files were converted to standard image formats.
- Testing data was stored in restricted S3 buckets with encryption.
- Access was controlled using IAM roles with limited permissions.

AWS Implementation

Data Storage:
- S3 buckets were encrypted using SSE-KMS.
- Bucket versioning and access logging were enabled.
- Public access was completely disabled.

IAM and Access:
- Roles were configured with the principle of least privilege.
- MFA was enforced.

Monitoring:
- CloudTrail and CloudWatch were used to log and monitor API activities.
- Alarms were set for suspicious activity.
- GuardDuty provided threat detection.

Azure Implementation

Storage:
- Azure Blob Storage used server-side encryption.
- Private Endpoints restricted access.

Identity:
- Azure Active Directory was used for authentication.
- Conditional access and RBAC were applied.

Monitoring:
- Azure Monitor and Security Center ensured continuous auditing.
- Alerts and policies were configured to maintain compliance.

Continuous Monitoring & Best Practices

Regular audits of access logs and periodic vulnerability scans were conducted.
Automation tools such as AWS Config Rules and Azure Policies were used.
Penetration testing was scheduled quarterly to identify potential security issues.

Testing Workflow (AWS Example)

1. Upload DICOM files.
2. Automatically de-identify and convert to JPEG using Lambda functions.
3. Store in encrypted S3 with restricted IAM access.
4. Enable CloudTrail and CloudWatch.
5. Set up alarms for unauthorized access or unusual activity.