cloudy
Cloud & AI Solutions

CHECKLIST

Questions:

1. Is your patient data stored securely in a protected system or left in easily accessible locations?
2. Are your systems regularly tested for vulnerabilities before attackers do?
3. Do you have clear access controls for sensitive patient information?
4. Are data backups performed regularly and securely stored?
5. Is there a protocol in place for responding to potential data breaches?
6. Are staff trained on best practices for patient data protection?
7. Do you monitor who accesses sensitive data and how frequently?
8. Are all software and systems up to date with the latest security patches?
9. Have you conducted a recent risk assessment of your hospital's IT infrastructure?
10. Do you have an external audit or review process to ensure ongoing compliance?

powered by aws