CAPMINDS

Security Due Diligence Checklist for Vendor Evaluation

1. Company Information

□ Company name, registration, and physical address verified
□ Years of experience with OpenEMR
□ References from previous OpenEMR projects
□ Proof of insurance (e.g., cybersecurity insurance, general liability)

2. Compliance & Certifications

□ HIPAA compliance certification (if handling PHI).
□ GDPR compliance (if serving EU clients).
□ SOC 2 Type II certification (optional, but great).
□ ISO 27001 certification (optional, shows strong security culture).
□ Familiarity with U.S. healthcare regulations (HITECH Act, CMS rules).

3. Staff & Training

□ Background checks conducted for employees.
□ Security awareness training provided regularly.
□ Named security officer or CISO.
□ Access control policies enforced (least privilege principle).

4. Technical Security Practices

□ Experience with securing OpenEMR like security patching, hardening
□ Use of secure development practices such as code reviews, secure coding
□ Regular vulnerability scanning of hosted OpenEMR instances.
□ Penetration testing conducted (internally or via third party).
□ Data encryption (in transit & at rest) implemented.
□ Secure backup processes in place.
□ Audit logging and log monitoring.

5. Hosting & Infrastructure Security

□ Data centers used are HIPAA-compliant (for U.S. healthcare clients).
□ Clear description of hosting setup (cloud provider, VPS, on-premises).
□ Server hardening standards (firewalls, OS patching, SSH access control).
□ Business Continuity and Disaster Recovery (BC/DR) plans documented.

6. Application Management

□OpenEMR versioning strategy like upgrades, patches
□ Security patches applied within defined SLAs (e.g., 72 hours).
□ Custom code security (OWASP Top 10 compliance).
□ Database security measures such as access controls, encryption

7. Contracts & Legal

□ Business Associate Agreement ready to sign for HIPAA compliance
□ Clear Service Level Agreements for uptime, incident response
□ Non-Disclosure Agreements signed before access to sensitive information

8. Incident Management

□ Incident Response Plan (IRP) available
□ Defined breach notification procedures especially for HIPAA breaches
□ Regular tabletop exercises or breach drills conducted

9. Third-Party Risk Management

- □ List of third-party vendors they use (subcontractors, cloud providers).
- □ Risk assessments conducted on their vendors.
- □ Contracts in place with subcontractors for security obligations.

10. Support & Maintenance

- □ 24/7 emergency support availability (optional but ideal).
- □ Defined process for urgent security patch deployment.
- □ Documentation provided for customizations and deployments.