Vendor Due Diligence Questionnaire – OpenMRS Canadian Clinic

OpenMRS Canadian Clinic
Purpose: Assesses 3rd party vendors that handle or could access personal health information
Vendor Name: [To be filled]
Date: [To be filled]

Questions (10 Practical Questions)

1. What types of personal health information (PHI) will your company access, store, or process on our behalf?
2. How do you protect PHI in transit and at rest? (encryption standard)
3. Do you have a documented breach notification process that meets PHIPA timelines (e.g., notify us within 24-48 hours)?
4. Are you willing to sign a Business Associate Agreement or data processing agreement?
5. What security certifications or audits do you hold (e.g., SOC 2, ISO 27001)?
6. How do you manage access controls and user authentication for our data?
7. Have you had any security incidents or breaches involving PHI in the last 24 months? If yes, please describe.
8. Can you provide your most recent penetration test report or compliance audit summary?

Recommendation Use: Send this to any vendor (e.g., OpenMRS support provider, cloud hosting service, billing software vendor, or medical device supplier). Review responses and document them in your vendor risk folder.