Defining_OpenMRS_Security_&_Privacy_Requirements

Let's identify some requirements! Do a quick scan of a relevant regulation or standard. For example, search online for "HIPAA Security Rule safeguards" or "OpenMRS security features". Find **at least three specific security or privacy requirements** that likely apply. Write them down in your own words. This exercise will give you a feel for turning high-level rules into concrete system requirements.

Answer:

1. Authentication: Must require strong, unique user credentials for all users. Enforce password quality, expiration, and force change of default admin passwords.
2. Authorization and Access Control: Implement role-based access control (RBAC) so users can only access data and functions necessary for their job. Make sure to regularly review and update the user permissions.
3. Fail-Safe Defaults: The default system settings should deny access unless explicitly granted, minimizing exposure even if misconfigurations do occur.
4. Data Export and Sharing Controls: Control and log all data exports. Encrypt exported data and restrict who can perform exports.
5. Incident Response: Ensure there's a well thought out plan in place. Have documented procedures for responding to security incidents, including breach notification and mitigation steps.
6. Automatic Session Timeout: Configure OpenMRS to automatically log users out after a period of inactivity, which

will help reduce the risk of unauthorized access from unattended sessions.

7. Employee Training and Policies: Provide regular training on privacy, security, and data handling policies. Ensure staff understand their responsibilities and the importance of protecting patient information.

Reflection Prompt:

Which requirement do you anticipate being most challenging for the OpenMRS project to meet, and why? Think about technical challenges or perhaps human/process challenges. For example, is implementing encryption difficult, or is getting users to adopt MFA a hurdle? Reflect on where the hardest compliance gaps might be so you can plan for them early.

Answer:

I anticipate that Employee Training and Policies will be difficult to implement because human beings generally like to find the easiest way to do things. Thus, staff may try to use shortcuts and in doing so they may not properly handle privacy, security, and data. So it is essential to regularly implement Employee Training and Policies multiple times to remind staff of what their responsibilities are, and how important it is to protect patient information.