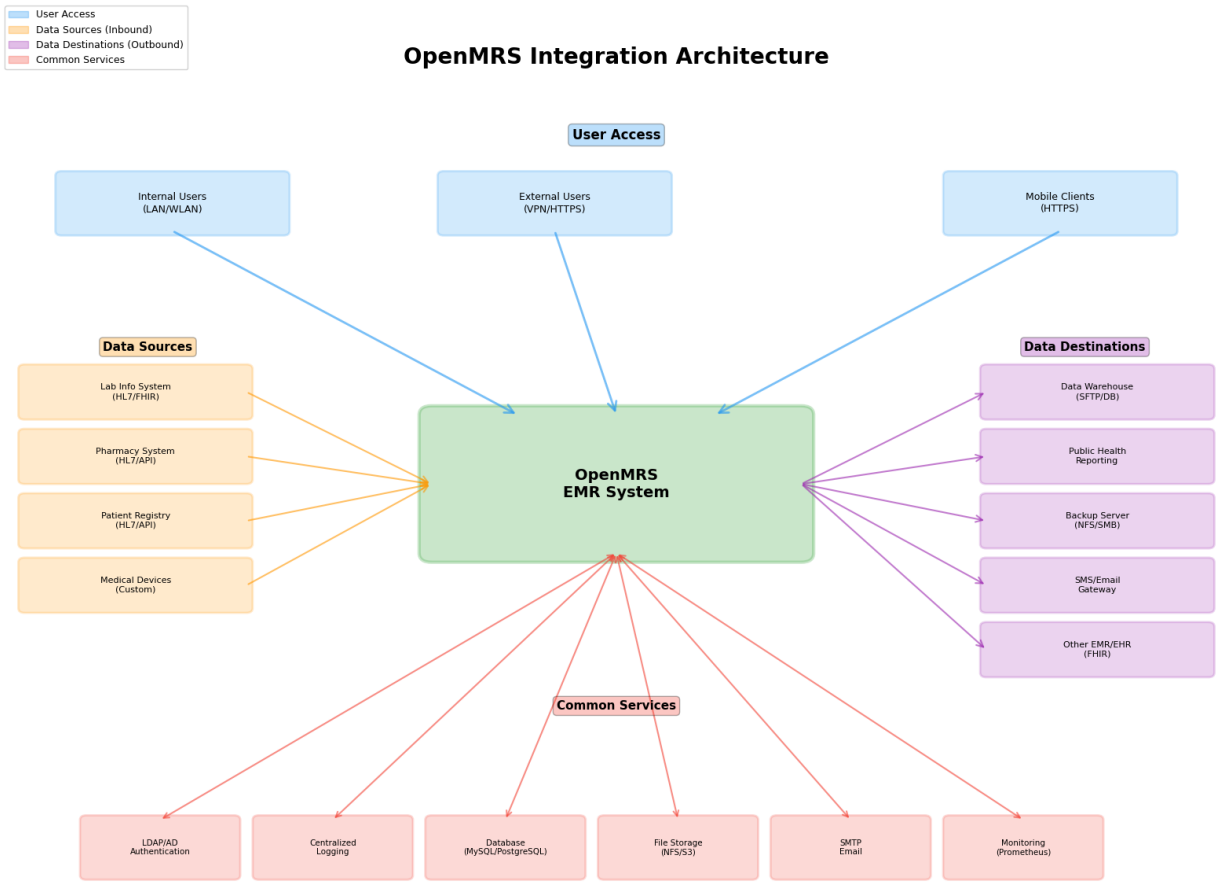
Fitting_OpenMRS_into_the_Bigger_IT_Picture

Task:

Outline how OpenMRS connects with other systems/services in your environment. Questions to guide you: *How do users access OpenMRS (through what network)? Where does OpenMRS get data from or send data to (other systems or services)? What common services (identity management, logging, etc.) does it use?*

Write down a few key integration points. For instance: “OpenMRS uses corporate LDAP for user login”, “OpenMRS sends nightly data backup to central backup server”, or “OpenMRS pulls lab results from LabSystem via API”. This will help you visualize the system in context, which is great for both security and design purposes.

Answer:



Reflection Prompt:

Why do you think it's important to align a new system like OpenMRS with the existing enterprise architecture? Consider the pitfalls if someone stood up a new application in isolation (separate accounts, credentials, no monitoring). Have you seen or experienced siloed systems that became headaches later? Reflect on how integration (or lack thereof) can impact security and efficiency. Which integration for OpenMRS do you think will provide the most value (or which one would you prioritize)?

Answer:

In my opinion, it’s extremely important to align a new system like OpenMRS with the existing enterprise architecture. If a system like OpenMRS is deployed in isolation, it is more or less invisible to central IT governance until something goes wrong, and when that happens, it’s usually a pretty bad situation.

Things that can occur when a system is isolated:

Security Blind Spots:

- **No centralized monitoring** = breaches go undetected for long periods of time, like months.
- **Separate credentials** = password reuse, weak passwords, no MFA enforcement, which is begging for an unauthorized security breach.
- **Isolated logging** = no correlation with other security events, thus making attack patterns invisible.
- **Patch management gaps** = the system falls off the radar for vulnerability scanning and updates, making it a cakewalk for hackers to access.

Operational Nightmares:

- **User frustration** = "Why do I need yet another username/password for this system?"
- **Access management chaos** = When employees leave, their OpenMRS account remains active because it's not in the central deprovisioning workflow.
- **Data silos** = Clinicians manually re-entering lab results because systems don't talk to each other, because of a lack of synchronization. Pure inefficiency.
- **Compliance failures** = Auditors discover the system wasn't included in SOC 2/HIPAA assessments. This is just poor GRC management.

The Efficiency Perspective:

With Integration**,** there is real-time data availability and automated workflows in which everything is synchronized. There is also enterprise-wide analytics and reporting, thereby ensuring that information does not get lost in the weeds and any deviation from the norm is immediately noticed.

Prioritization for OpenMRS Integrations:

Here's my prioritization based on risk reduction and value delivery:

LDAP/Active Directory Authentication

- **Security foundation** - Enables MFA, password policies, automated deprovisioning
- **Quick win** - Relatively straightforward and can be quickly implemented.
- **Immediate user value** - Single sign-on reduces friction.
- **Compliance requirement** - Most frameworks (HIPAA, SOC 2) require centralized identity management.

I would opine that this provides the most value, because if this is skipped, every day without it you would be accumulating orphaned accounts and weak credentials.