Identifying Stakeholders

Task:

List at least three stakeholder roles for your OpenMRS system. Think about who designs it, who builds or configures it, who uses it day-to-day, who maintains it, and who signs off on it. For each stakeholder role you list, add a note on what that person/group cares about most. *(For example: "Clinic Nurse – cares about easy data entry and quick patient lookup.")* This quick list will be your go-to reference to remember **who** you need to keep in mind for security and compliance decisions.

Mini Project - Stakeholder List:

1. Data Manager/Analyst - cares about clean, consistent data, export/ETL (Extract Transform, Load), and accurate indicators for decision-making.
2. System Administrator/DevOps - cares about uptime, backups, security, user provisioning, and performance monitoring.
3. Program Manager/Administrator - cares about reporting and dashboards, data quality, meeting program KPIs (Key Performance Indicators) and compliance.
4. Health Informatics Lead (Implementer) - cares about configuring forms/workflows, data standards (HL7/FHIR Health Level Seven/Fast Healthcare Interoperability Resources) and interoperability.

5. Funders (donors, NGOs, foundations) - care about impact, cost-effectiveness, sustainability, transparent reporting, and alignment with program goals.

Reflection:
Take a moment to review your stakeholder list. Ask yourself: **Have we involved all these people in our security planning?** Is there a group you interact with the least (maybe busy doctors or upper management)? How could you better include their perspective? Often, the people who use the system daily have insights about its vulnerabilities or crucial data. Likewise, stakeholders like funders or regulators can surprise you with requirements (e.g. a privacy officer might require extra consent forms). Reflect on one stakeholder you might engage more. How can understanding their needs make OpenMRS more secure and effective?

Answer:

I would say that the least engaged would most probably be busy clinicians and upper management. Both shape risk but are hard to convene because of their busy schedules. To include their perspective better, some possible solutions could be to:

1. Shadow a clinic session to spot insecure workarounds (sticky notes, shared passwords, unlocked workstations).
2. Run a tabletop incident exercise twice a year with SysAdmin/DevOps, Program Manager, and leadership, and invite a clinician champion.
3. Incentivise champions: nominate a clinician and a data manager as “security champions” with small stipends or recognition.

One stakeholder that I would like to engage more would be the Funders. These are the financial backers and lifeline of OpenMRS. Without them,

the company would not be able to operate properly. It is crucial to understand their needs, and engaging Funders can directly strengthen OpenMRS security and effectiveness by aligning security investments with measurable impact and sustainable operations. If you understand their (Funders) priorities - demonstrable outcomes, value for money, risk reduction, and long-term viability, you can: tie security controls to program KPIs (e.g., uptime, data integrity, incident MTTR), budget for ongoing security (patching, monitoring, audits) rather than one-off features, and secure funding for essentials like SIEM, backups, and training.