OpenMRS System/Authorization Boundary

Task:

Draw your OpenMRS System Boundary. You can do this on paper or a whiteboard (or mentally but try to visualize it clearly). Sketch out the main components you listed yesterday. Now draw a big circle or box around the ones you consider part of the OpenMRS system. Label anything outside the box that OpenMRS interacts with. For example, draw a box around “OpenMRS app server” and “OpenMRS DB.”

Outside the box, you might note “Clinic PCs (clients)” and “External billing service – via API.” If drawing isn’t your thing, simply make two lists: one labeled “In Boundary” and one labeled “Out of Boundary.” Put each asset or component into one of those lists. Don’t agonize too much. This is a quick sketch. The goal is to see if you have a clear idea of what’s included.

OpenMRS System/Authorization Boundary (In-Boundary)

OpenMRS Core Application: All code and services that make up the main OpenMRS platform, including its user interface, service layer, and data access layer.

OpenMRS Modules: Any installed modules that extend or modify the core functionality, as these operate within the same environment and access the same data.

Databases: All databases used by OpenMRS, including primary data stores and any auxiliary databases for logging, analytics, or module-specific data.

Backup Data: All backup copies of OpenMRS databases and files, regardless of format (full, incremental, differential), as these contain sensitive information and must be protected as rigorously as the live data.

Backup Storage Locations: Any physical or cloud-based storage locations where OpenMRS backups are kept, including external drives, network shares, cloud buckets, or tape archives.

Application Servers: All servers (physical, virtual, or cloud) running OpenMRS services, including web servers, API endpoints, and background processing nodes.

Network Infrastructure: Firewalls, routers, switches, and VPNs that provide connectivity and security for OpenMRS components.

Authentication and Access Control Systems: Systems and services that manage user authentication, authorization, and auditing for OpenMRS.

Logging and Monitoring Systems: Any systems that collect, store, or analyze logs and security events from OpenMRS and its infrastructure.

Disaster Recovery Systems: Infrastructure and processes used for restoring OpenMRS from backups, including recovery servers and storage.

Configuration Files and Secrets: All configuration files, environment variables, and secrets (such as database passwords, API keys, and encryption keys) used by OpenMRS and its modules.

Third-party Integrations: Any external systems or services directly integrated with OpenMRS (e.g., for data exchange, reporting, or authentication), if they have access to OpenMRS data or resources.

Out of-Boundary

These items are outside the system boundary because they are not under the direct control of OpenMRS administrators, do not store or process OpenMRS data, or are managed by external entities. Security,

compliance, and risk management for these components are handled separately and may require different controls or agreements.

External Microservices and Third-party Applications: Any microservices, external APIs, or third-party applications that communicate with OpenMRS but are not hosted, managed, or maintained within the OpenMRS environment.

External Data Sources: Data repositories, registries, or external databases that are not part of the OpenMRS deployment and do not store OpenMRS data.

External Backup Storage: Backup locations managed by third parties or outside organizational control, such as offsite cloud storage not governed by OpenMRS policies.

External Networks and Internet: The public internet, external leased lines, and any network segments not protected or managed by OpenMRS network controls.

User Devices Not Managed by OpenMRS: Personal devices, unmanaged laptops, or mobile devices that access OpenMRS via the web but are not subject to organizational security controls.

External Authentication Providers: Identity providers or authentication systems not integrated or managed within the OpenMRS system boundary.

External Configuration Management: Configuration files, secrets, or environment variables managed outside the OpenMRS infrastructure.

Unmanaged Frontend Deployments: Static frontend files or modules delivered outside the OpenMRS backend, such as those hosted on third-party CDNs or not included in the official deployment.

External Concept Dictionaries: Concept IDs or dictionaries managed in external systems (e.g., OCL, CIEL) that are referenced but not stored within OpenMRS.

External Monitoring and Logging Systems: Security monitoring, SIEM, or logging platforms not directly integrated or managed within the OpenMRS environment.

Neighbor Discovery Protocols and Unmanaged Network Services: Protocols and services running on external-facing interfaces, not managed or disabled per OpenMRS security policy.

Unrelated Organizational Systems: Any other IT systems, business applications, or infrastructure not involved in OpenMRS operations or data management.