VIETNAM GENERAL CONFEDERATION OF LABOUR

**TON DUC THANG UNIVERSITY**

**FACULTY OF INFORMATION TECHNOLOGY**



**PHẠM NGỌC LINH - 521H0360**

**LÂM NGUYỄN ANH THY - 521H0377**

**NGUYỄN ĐÌNH VIỆT HOÀNG - 522H0120**

**ASSIGNMENT REPORT**

**INTRODUCTION TO INFORMATION SECURITY**

**HO CHI MINH CITY, YEAR 2024**

VIETNAM GENERAL CONFEDERATION OF LABOUR

**TON DUC THANG UNIVERSITY**

**FACULTY OF INFORMATION TECHNOLOGY**



**PHẠM NGỌC LINH - 521H0360**

**LÂM NGUYỄN ANH THY - 521H0377**

**NGUYỄN ĐÌNH VIỆT HOÀNG - 522H0120**

**ASSIGNMENT REPORT**

**INTRODUCTION TO INFORMATION SECURITY**

Instructor

**PhD. Huỳnh Ngọc Tú**

**HO CHI MINH CITY, YEAR 2024**

**ACKNOWLEDGEMENT**

We sincerely thank PhD. Huỳnh Ngọc Tú for teaching us the Introduction to Information Security course with great enthusiasm. We want to express our deep appreciation for the dedication and professional knowledge that you shared with us. Through your classes, we gained a better understanding of the fundamental aspects of the Introduction to Information Security, thanks to your detailed explanations and practical applications. You helped us grasp the knowledge and apply it effectively. Finally, we extend our heartfelt gratitude to PhD. Huỳnh Ngọc Tú for your commitment and invaluable support throughout our learning journey in this course. The skills and knowledge we acquired will continue to impact our future development. We sincerely thank you and wish your health, success, and happiness.

*Ho Chi Minh City, May 29, 2024*

*Authors:*

*Phạm Ngọc Linh*

*Lâm Nguyễn Ạnh Thy*

*Nguyễn Đình Việt Hoàng*

**DECLARATION OF AUTHORSHIP**

Our group assures that this is our own report and was guided by PhD. Huỳnh Ngọc Tú. The research content and results in this report are honest and have not been published in any form before. The figures in the tables used for analysis, comments, and evaluations were collected by the authors from various sources clearly stated in the reference section.

Additionally, the report includes some comments, evaluations, and data from other authors and organizations, all of which are cited and noted for their origin.

**If any fraud is detected, we fully take responsibility for the content of our assignment report for the second semester of the 2023-2024 academic year.** Ton Duc Thang University is not involved in any copyright or intellectual property violations that we may cause during the process (if any).

*Ho Chi Minh City, May 29, 2024*

*Authors:*

*Phạm Ngọc Linh*

*Lâm Nguyễn Ạnh Thy*

*Nguyễn Đình Việt Hoàng*

**INSTRUCTOR RUBRIC**

Supervisor’s Name: ……………………………………………………………..............

Comments: ……………………………………………………………………………...

Total Score Based on Rubric Evaluation: ………………………………………………

*Ho Chi Minh City, date … month … year …*

*Supervisor*

*(sign and write your full name**)*

Exercise 1:

Four privileges in OpenMRS Demo that seems most important to our:

1. View Patients: This privilege allows a user to view patient records. It is essential for healthcare providers who need to access patient information to deliver care, review medical histories, and make informed clinical decisions.
2. Edit Patients: This privilege permits a user to edit patient information. It's crucial for maintaining up-to-date and accurate patient records, including updating demographic details, medical history, and current treatments.
3. Manage Privileges: This privilege allows users to control and configure the specific actions that different roles within the system can perform.
4. View Observations: This privilege allows a user to view clinical observations and measurements recorded for patients. Observations are fundamental data points in patient care, including vital signs, lab results, and other clinical measurements that inform treatment decisions.

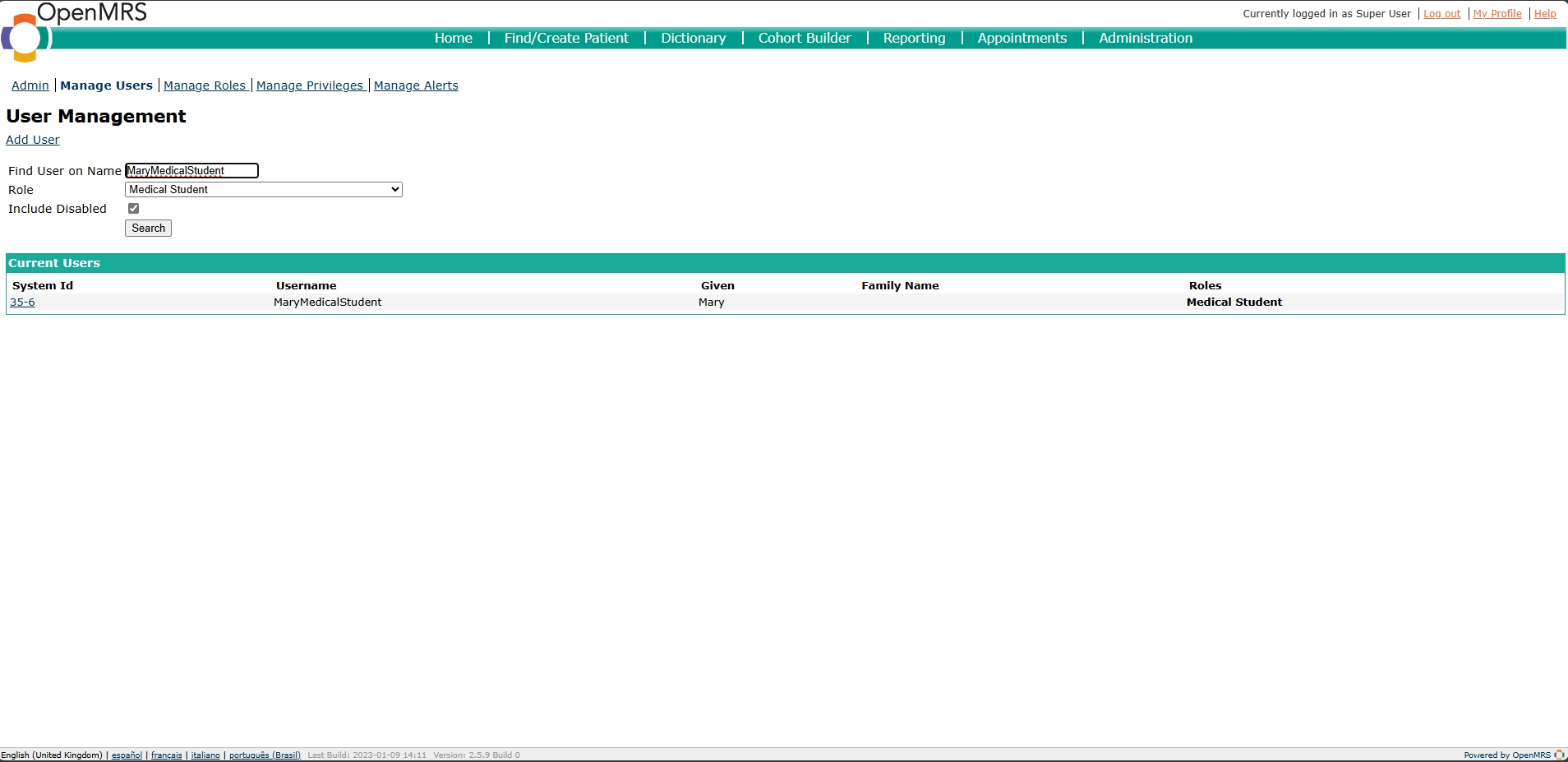
Exercise 2:

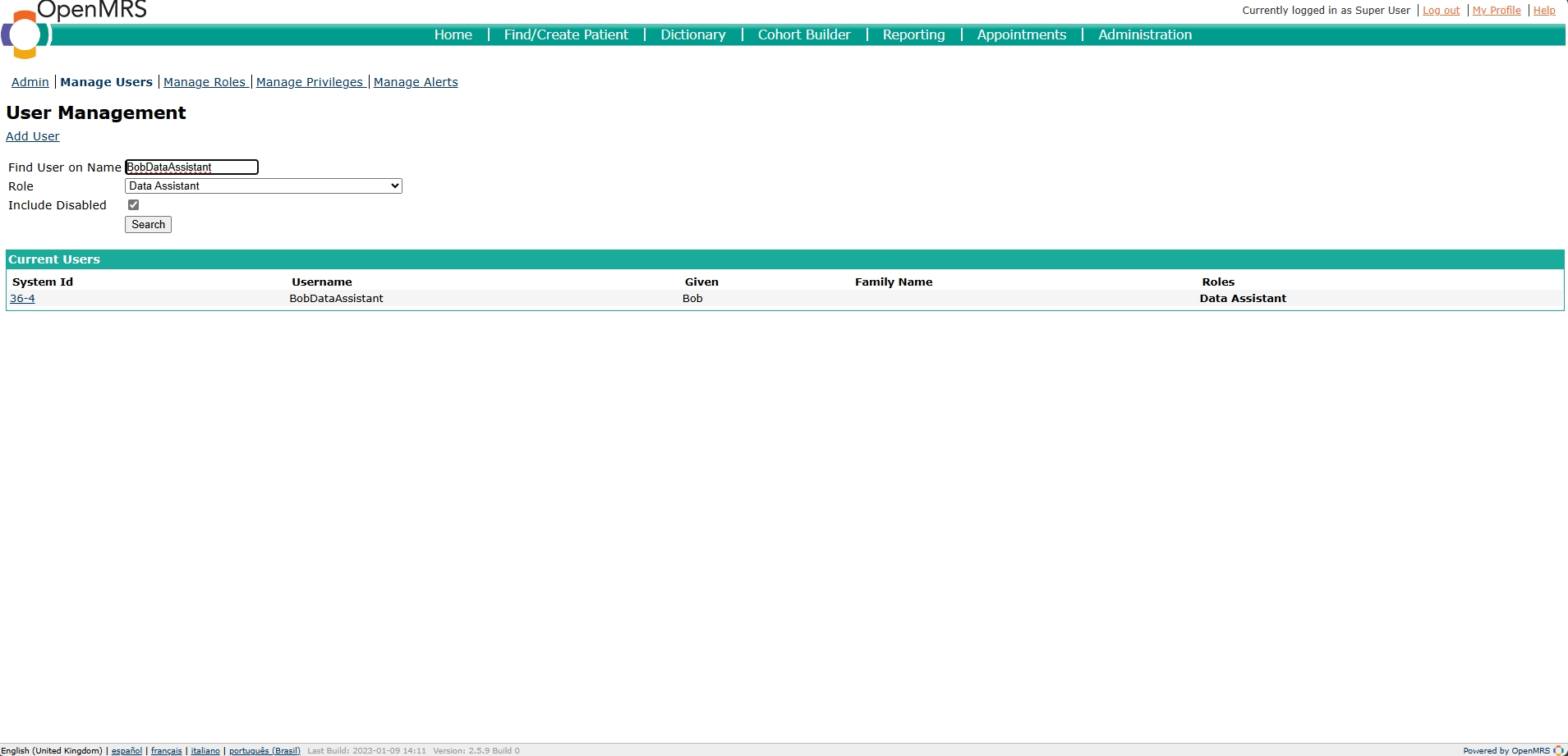
Four main roles that have maximum set of privileges:

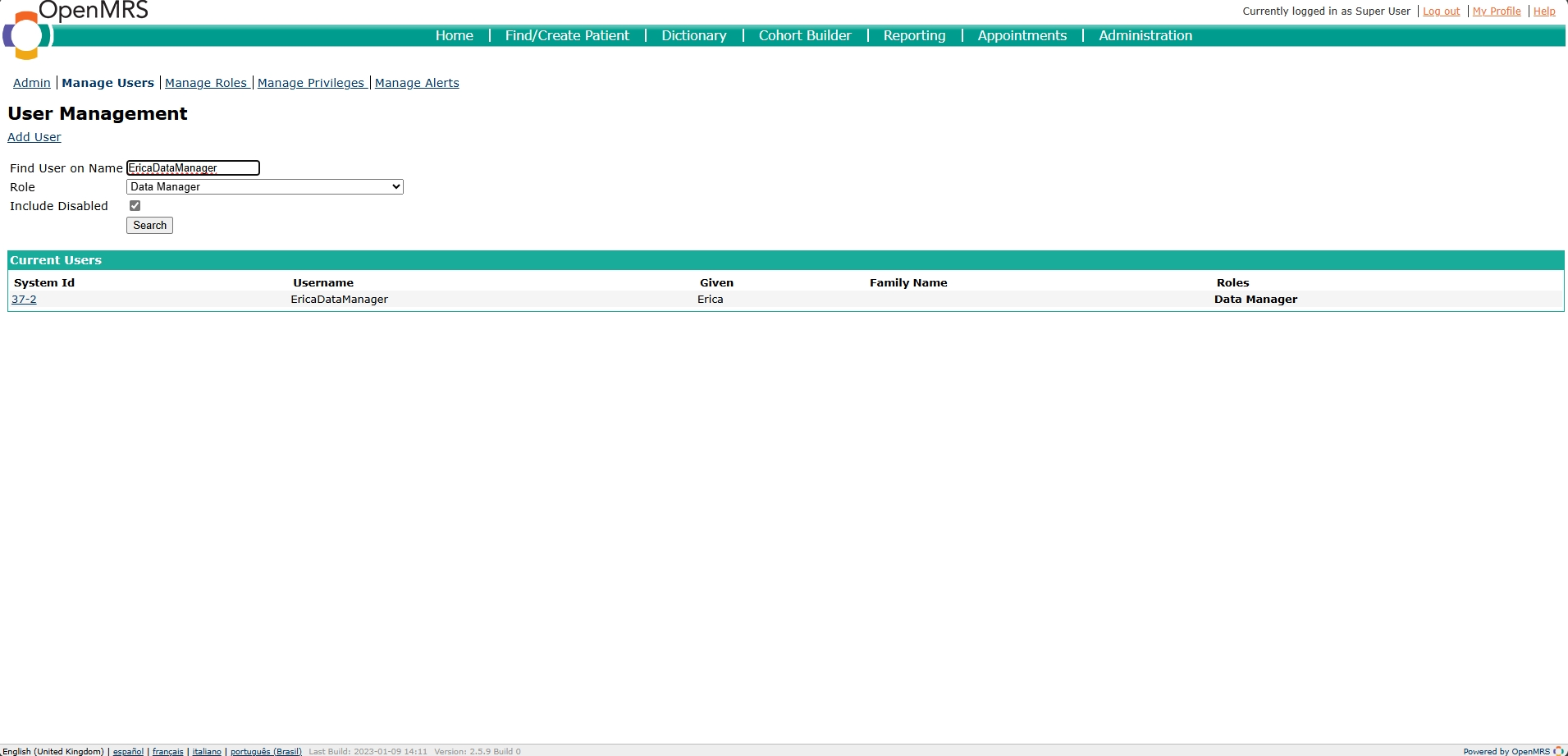
1. Organizational: Doctor because of inheriting privileges from other roles: Application: Enters ADT Events, Application: Records Allergies, Application: Requests Appointments, Application: Sees Appointment Schedule, Application: Uses Patient Summary, Application: Writes Clinical Notes and has numerous privileges for itself.
2. Organizational: Nurse because of inheriting privileges from other roles: Application: Enters ADT Events, Application: Enters Vitals, Application: Records Allergies, Application: Requests Appointments, Application: Sees Appointment Schedule, Application: Uses Patient Summary, Application: Uses Capture Vitals App and has numerous privileges for itself.
3. Organizational: System Administrator because of inheriting privileges from other roles: Application: Administers System, Application: Configures Appointment Scheduling, Application: Configures Forms, Application: Configures Metadata, Application: Manages Atlas, Application: Manages Provider Schedules and has numerous privileges for itself.
4. Organizational: Hospital Administrator because of inheriting privileges from other roles: Application: Configures Appointment Scheduling, Application: Manages Provider Schedules, Application: Requests Appointments, Application: Schedules And Overbooks Appointments and has numerous privileges for itself.

Exercise 3:

|  |  |  |
| --- | --- | --- |
| Given | Role | Privilege(s) |
| Mary | Medical Student | View Patients |
| Bob | Data Assistant | View Patients  Edit Patients |
| Erica | Data Manager | View Patients  Edit Patients  Add Patients |







|  |  |  |
| --- | --- | --- |
| Role | Inherit Privilege(s) from Role(s) | Additional Privilege(s) |
| Patient Data Manager |  | Add/ Edit/ View Patients |
| Lab Manager |  | Add/ Edit/ View Laboratory Orders |
| User Manager |  | Add/ Edit/ View Users |
| Dietary Manager |  | Add/ Edit/ View Diet Orders |
| Encounter Manager |  | Add/ Edit/ View Encounters |
| Ambulance Personnel |  | View Patients  Add Reports |
| Nurse | Patient Data Manager  Lab Manager  Ambulance Personnel | Add/ Edit/ View Observations  Edit/ View Reports |
| Doctor | Patient Data Manager  Lab Manager  Encounter Manager | Add/ Edit/ View Visits |
| Health Secretary | Encounter Manager  Dietary Manager |  |
| Physiotherapist | Encounter Manager | Add/ Edit/ View Physiotherapy Orders |
| Psychologist | Encounter Manager | Add/ Edit/ View Psychology Orders |
| Radiologist | Lab Manager | Add/ Edit/ View Radiology Orders |
| Dentist | Encounter Manager  Dietary Manager |  |
| System Administrator | User Manager | Add/ Edit User Passwords  Add/ Edit/ View Roles |
| Registration Clerk | User Manager  Patient Data Manager | Add/ Edit/ View Appointments |

**Exercise 4:** Our role hierarchy:

Exercise 5:































Exercise 6:

The challenges we encounter while working with access control model in OpenMRS:

1. Complex User Roles and Permissions: OpenMRS supports a wide range of user roles (e.g., clinician, nurse, pharmacist, administrator) with varying levels of access and permissions. Properly defining, managing, and enforcing these roles and permissions can be challenging, especially in complex healthcare environments.
2. Granular Access Control: The ability to grant fine-grained access control, such as restricting access to specific patient records or data fields, may be limited in the current OpenMRS model. This can be a concern for sensitive healthcare data.
3. Dynamic Access Control: Healthcare environments are often fast-paced and dynamic, with the need to quickly adjust user access based on changing circumstances (e.g., emergency situations, staff changes). The current access control model may not be flexible enough to accommodate such dynamic requirements.
4. Integration with External Systems: OpenMRS may need to integrate with other healthcare systems, and the access control model may need to be extended to support seamless and secure cross-system access.
5. Auditing and Logging: Robust auditing and logging capabilities are critical for healthcare systems to ensure compliance and investigate potential security incidents. The access control model should provide comprehensive logging and reporting features.

Our suggestions for improving the access control model of OpenMRS:

1. Implement Role-Based Access Control (RBAC): Consider a more structured RBAC model, where user roles are well-defined, and permissions are assigned to these roles. This can simplify the management of user access and permissions.
2. Introduce Attribute-Based Access Control (ABAC): Incorporate ABAC, which allows for more granular access control based on user attributes, resource attributes, and environmental conditions. This can enable more fine-grained access control policies.
3. Enhance Dynamic Access Control: Explore mechanisms to quickly adapt user access based on specific events or changing circumstances, such as emergency situations or staff changes.
4. Improve Integration with External Systems: Develop robust integration mechanisms to seamlessly share access control information and policies with other healthcare systems, ensuring consistent and secure access across the ecosystem.
5. Strengthen Auditing and Logging: Enhance the access control model to provide comprehensive auditing and logging capabilities, allowing for thorough monitoring, compliance reporting, and incident investigation.
6. Consider Centralized Access Management: Explore the possibility of a centralized access management system that can manage user identities, roles, and permissions across multiple OpenMRS instances or healthcare systems.
7. Engage the OpenMRS Community: Collaborate with the OpenMRS community to gather feedback, share best practices, and contribute to the ongoing development and improvement of the access control model.