**TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN TPHCM**

**Khoa: Công nghệ thông tin**

**Bộ Môn: An toàn bảo mật trong hệ thống thông tin**

**ĐỒ ÁN MÔN HỌC**

* **Nhóm thực hiện**
* Nhóm 5
  + **Giảng viên hướng dẫn** 
    - Phạm Thị Bạch Huệ
    - Lương Vĩ Minh

**BẢNG THÔNG TIN CHI TIẾT CÁC THÀNH VIÊN**

Nhóm: 5

Số lượng: 5

|  |  |
| --- | --- |
| **MSSV** | **Họ và tên** |
| 1712415 | Nguyễn Thị Ngọc Hân |
| 1712 | Nguyễn Thành Sửu |
| 1712 | Nguyễn Trọng Thắng |
| 1712769 | Trịnh Đức Thanh |
| 1712899 | Dương Khánh Vi |

**BẢNG PHÂN CÔNG CÔNG VIỆC**

|  |  |  |
| --- | --- | --- |
| **Người thực hiện** | **Công việc thực hiện** | **Đánh giá** |
| 1712415 – Nguyễn Thị Ngọc Hân |  |  |
| 1712415 – Nguyễn Thành Sửu |  |  |
| 1712415 – Nguyễn Trọng Thắng |  |  |
| 1712769 – Trịnh Đức Thanh |  |  |
| 1712899 – Dương Khánh Vi |  |  |

**MỤC LỤC**

[A- YÊU CẦU 1](#_Toc49425234)

[B- KẾT QUẢ 3](#_Toc49425235)

[I. Phân hệ 1: Dành cho người quản trị cơ sở dữ liệu 3](#_Toc49425236)

[II. Phân hệ 2: Quản lí thông tin của một bệnh viện 4](#_Toc49425237)

[1. Lược đồ cơ sở dữ liệu 4](#_Toc49425238)

[2. Chính sách bảo mật 5](#_Toc49425239)

[3. Các chính sách đã cài đặt 7](#_Toc49425240)

[a. Cơ chế DAC 7](#_Toc49425241)

[b. Cơ chế RBAC 8](#_Toc49425242)

[c. Cơ chế VPD 8](#_Toc49425243)

[d. Cơ chế MAC (OLS) 8](#_Toc49425244)

[e. Mã hoá 8](#_Toc49425245)

[f. Audit 8](#_Toc49425246)

1. **YÊU CẦU**

**PHÂN HỆ 1: DÀNH CHO NGƯỜI QUẢN TRỊ CƠ SỞ DỮ LIỆU**

Sinh viên hãy xây dựng ứng dụng cho phép các người dùng có quyền quản trị thực hiện công việc sau:

* Xem danh sách người dùng trong hệ thống.
* Thông tin về quyền (privileges) của mỗi user/ role trên các đối tượng dữ liệu.
* Cho phép tạo mới, xóa, sửa (hiệu chỉnh) user hoặc role.
* Cho phép thực hiện việc cấp quyền: cấp quyền cho user, cấp quyền cho role, cấp role cho user. Quá trình cấp quyền có tùy chọn là có cho phép người quản trị được cấp quyền có thể cấp quyền đó cho user/ role khác hay không (có chỉ định WITH GRANT
* OPTION hay không). Quyền, select, update thì cho phép phân quyền tinh đến mức
* cột; quyền insert, delete thì không.
* Cho phép thu hồi quyền từ người dùng/ role.
* Cho phép kiểm tra quyền của các chủ thể vừa được cấp quyền.
* Cho phép chỉnh sửa quyền của user/ role.

Sinh viên hãy thực hiện chức năng ghi nhật ký hệ thống (chỉ yêu cầu thực hiện mức HQT CSDL Oracle):

* Admin có quyền enable/ disable việc ghi nhật ký toàn hệ thống.
* Admin được chỉ định ghi nhật ký của những hành động thực hiện bởi những user nào trên những đối tượng cụ thể. Các hành động đó là: đăng nhập, thay đổi thông tin user account, select, insert, update, delete, execute.; các đối tượng là table, view, stored procedure, function. Admin cũng được quyền chọn ghi nhật ký hành động được thực hiện thành công hay không thành công.
* Kiểm tra dữ liệu nhật ký hệ thống. Sinh viên nên đề ra một số kịch bản theo dõi hệ thống để phân tích dữ liệu nhật ký.

**PHÂN HỆ 2: QUẢN LÝ THÔNG TIN CỦA MỘT BỆNH VIỆN**

Một bệnh viện quy mô vừa có những vai trò sau: bộ phận quản lý, bộ phận tiếp tân và điều phối bệnh, bác sĩ điều trị, phòng tài vụ, phòng bán thuốc và bộ phận kế toán. Bệnh nhân đến bệnh viện sẽ gặp bộ phận tiếp tân và điều phối bệnh để khai bệnh ban đầu gồm tên, năm sinh, địa chỉ liên lạc, số điện thoại, triệu chứng bệnh. Nếu bệnh nhân trước đó đã khám bệnh thì đọc mã khám bệnh thì thông tin bệnh nhân đã có và không cần phải nhập lại. Sau khi hoàn tất giai đoạn tiếp bệnh, nhân viên tiếp tân chỉ định phòng khám và bác sĩ khám. Tại phòng tài vụ, nhân viên phòng tài vụ nhìn thấy thông tin khám bệnh của bệnh nhân mới sẽ thu tiền khám của bệnh nhân và hướng dẫn bệnh nhân đến gặp bác sĩ. Sau khi xem bệnh, bác sĩ chỉ định và ghi nhận vào CSDL liên quan đến bệnh nhân đó là phải dùng thuốc gì, hoặc phải tiếp tục làm những thủ tục xét nghiệm hoặc chẩn đoán hình ảnh nào. Nhân viên phòng tài vụ căn cứ vào đó thu tiền trước khi bệnh nhân được xét nghiệm hoặc chụp hình theo yêu cầu của bác sĩ. Bộ phận tiếp tân và điều phối bệnh dựa vào dữ liệu của hệ thống ghi lại yêu cầu của bác sĩ sẽ ghi lại trên CSDL thông tin điều phối bệnh vào các phòng liên quan và hướng dẫn bệnh nhân vào phòng nào gặp bác sĩ nào. Sau khi hoàn tất các yêu cầu, bệnh nhân mang kết quả về cho bác sĩ khám bệnh ban đầu đọc kết quả và đề nghị dùng thuốc theo toa bác sĩ kê. Nhân viên phòng thuốc căn cứ vào đó bán thuốc cho bệnh nhân. Chính sách bảo mật trong ứng dụng trên được mô tả như sau:

* Thành viên của bộ phận quản lý được chia ra làm 3 nhóm: nhóm quản lý tài nguyên và nhân sự (phòng ban, bác sĩ, nhân viên, chấm công), nhóm quản lý tài vụ (đơn giá các loại dịch vụ khám bệnh, đơn giá thuốc), và nhóm quản lý chuyên môn. Nhóm quản lý tài nguyên nhân sự chỉ được thêm, xóa, sửa các thông tin trong cách danh mục như: phòng ban, bác sĩ, nhân viên trong từng phòng ban, bác sĩ nào trực phòng nào vào thời gian nào, ...và được xem tất cả các thông tin khác kể cả thông tin nhân viên kế toán tạo ra nhưng không được quyền sửa. Nhóm quản lý tài vụ chỉ được nhập mới chỉnh sửa các thông tin liên quan, những thông tin khác được quyền xem tất cả nhưng không được phép sửa. Nhóm quản lý chuyên môn được xem tất cả thông tin trong đó có thông tin điều trị bệnh của các bác sĩ để theo dõi về chuyên môn của bệnh viện và có chiến lược trong tương lai mà không được chỉnh sửa bất cứ thông tin nào.
* Bộ phận tiếp tân và điều phối bệnh được quyền thêm, xóa, sửa, tìm kiếm thông tin bệnh nhân, được điều phối bệnh nhưng không thể xem các thông tin liên quan đến số tiền cho từng thủ tục khám, xét nghiệm hoặc chụp hình hoặc thông tin thuốc điều trị bệnh cho bệnh nhân.
* Nhân viên phòng tài vụ chỉ nhìn thấy các thủ tục mà bác sĩ yêu cầu bệnh nhân phải làm khi điều trị bệnh, thông tin mà bộ phận điều phối bệnh đã điều phối và tính tiền. Nhân viên phòng tài vụ chỉ được cập nhật số tiền phải trả cho từng chi tiết khám trị bệnh của bệnh nhân mà không được chỉnh sửa bất cứ thông tin gì.
* Bác sĩ: chỉ có thể thêm hoặc sửa thông tin liên quan đến việc điều trị bệnh và các loại thuốc phải dùng, liều dùng cho bệnh nhân mà bác sĩ chịu trách nhiệm điều trị. Bác sĩ không được xem hoặc chỉnh sửa thông tin khác của những bệnh nhân do bác sĩ khác điều trị hoặc những thông tin khác trong hệ thống.
* Nhân viên bộ phận bán thuốc: chỉ có thể nhìn thấy toa thuốc mà bác sĩ kê cho từng bệnh nhân để tính tiền thuốc cho bệnh nhân mà không thể xem được bệnh nhân bệnh gì hay bất cứ thông tin gì khác.
* Nhân viên kế toán: tính lương cho các bác sĩ và các nhân viên khác dựa vào lương cơ bản, phụ cấp, số ngày công. Nhân viên kế toán không nhìn thấy bất cứ thông tin gì trong hệ thống liên quan đến quá trình điều trị bệnh cho bệnh nhân của những bộ phận liên quan.

**Yêu cầu:**

1. Sinh viên tự thiết kế mô hình dữ liệu và tạo dữ liệu thử cho ứng dụng trên. Hãy dùng các cơ chế bảo mật đã học của Oracle để hiện thực các cơ chế bảo mật đề ra.
2. Sinh viên hãy đề ra bối cảnh sử dụng cơ chế mã hóa trong ứng dụng trên, và dùng thư viện hỗ trợ mã dữ liệu của Oracle. Cho biết mục đích, đối tượng cần bảo vệ dữ liệu bằng phương pháp mã hóa, phương pháp quản lý khóa.
3. Sinh viên hãy đề ra bối cảnh sử dụng cơ chế OLS của Oracle. Nhãn gồm đầy đủ 3 thành phần: level, compartment và group. Hãy gán nhãn cho dữ liệu, người dùng và minh họa chính sách bảo mật đã cài đặt.
4. Nếu sinh viên cài đặt thêm các chính sách bảo mật có ứng dụng thực tế trong ứng dụng đã cho sẽ được xem xét cộng điểm.
5. **KẾT QUẢ**
6. **Phân hệ 1: Dành cho người quản trị cơ sở dữ liệu**

Bảng danh sách các yêu cầu đã thực hiện:

|  |  |  |
| --- | --- | --- |
| **STT** | **Yêu cầu** |  |
| 1 | Xem danh sách các đối tượng hiện có trên cơ sở dữ liệu (user, role, table, view,…). | ✓ |
| 2 | Thông tin về quyền (privileges) của mỗi user/ role trên các đối tượng dữ liệu. | ✓ |
| 3 | Cho phép tạo mới, xóa, sửa (hiệu chỉnh) user hoặc role. | ✓ |
| 4 | Cho phép thực hiện việc cấp quyền: cấp quyền cho user, cấp quyền cho role, cấp role cho user. | ✓ |
| 5 | Quá trình cấp quyền có tùy chọn là có cho phép người được cấp quyền có thể cấp quyền đó cho user/ role khác hay không (có chỉ định WITH GRANT OPTION hay không). | ✓ |
| 6 | Quyền, select, update thì cho phép phân quyền tinh đến mức cột; quyền insert, delete thì không. | ✓ |
| 7 | Cho phép thu hồi quyền từ user/ role. | ✓ |
| 8 | Cho phép kiểm tra quyền của các chủ thể vừa được cấp quyền. | ✓ |
| 9 | Cho phép chỉnh sửa quyền của user/ role. | ✓ |
| 10 | Admin có quyền enable/ disable việc ghi nhật ký toàn hệ thống. | ✓ |
| 11 | Admin được chỉ định ghi nhật ký của những hành động thực hiện bởi những user nào trên những đối tượng cụ thể.   * Các hành động đó là: đăng nhập, thay đổi thông tin user account, select, insert, update, delete, execute. * Các đối tượng là table, view, stored procedure, function. | ✓ |
| 12 | Admin được quyền chọn ghi nhật ký hành động được thực hiện thành công hay không thành công. | ✓ |
| 13 | Kiểm tra dữ liệu nhật ký hệ thống. | ✓ |
| 14 | Đề ra một số kịch bản theo dõi hệ thống để phân tích dữ liệu nhật ký. | ✓ |
| 15 | Giao diện cho người quản trị. | ✓ |

1. **Phân hệ 2: Quản lí thông tin của một bệnh viện**
2. **Lược đồ cơ sở dữ liệu**

A screenshot of a cell phone

Description automatically generated

1. **Chính sách bảo mật**

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Chính sách** | **Phân loại** | **Cách thực hiện** |
| 1 | Bộ phận quản lý tài nguyên nhân sự chỉ được thêm, xóa, sửa các thông tin trong các danh mục: phòng ban, bác sĩ, nhân viên trong từng phòng ban, bác sĩ nào trực phòng nào vào thời gian nào. | RBAC | Gán quyền INSERT, DELETE, UPDATE trên các bảng PHONGKHAM, NHANVIEN cho role QLTNNS. |
| 2 | Bộ phận quản lý tài nguyên nhân sự được xem tất cả các thông tin khác kể cả các thông tin nhân viên kế toán tạo ra nhưng không được quyền sửa. | RBAC | Gán quyền SELECT trên bảng PHONGKHAM, NHANVIEN, NVCHAMCONG cho role QLTNNS. |
| 3 | Bộ phận quản lý tài nguyên nhân sự không được quyền sửa các thông tin của nhân viên kế toán. | VPD | Tạo hàm chính sách ngăn role QLTNNS sửa thông tin liên quan đến các user là nhân viên kế toán. |
| 4 | Nhóm quản lý tài vụ chỉ được chỉnh sửa những thông tin liên quan. | RBAC | Gán quyền UPDATE trên cột DONGIA của THUOC và GIATIEN của DICHVU cho role QLTV. |
| 5 | Nhóm quản lý tài vụ được quyền xem tất cả thông tin nhưng không được phép sửa. | RBAC | Gán quyền SELECT trên bảng THUOC, DICHVU cho role QLTV. |
| 6 | Nhóm quản lý chuyên môn được xem tất cả thông tin trong đó có thông tin điều trị bệnh của các bác sĩ để theo dõi về chuyên môn của bệnh viện, không được chỉnh sửa bất cứ thông tin nào. | RBAC | Gán quyền SELECT ANY TABLE cho role QLCM. |
| 7 | Bộ phận tiếp tân và điều phối bệnh được quyền thêm, xóa, sửa, tìm kiếm thông tin bệnh nhân. | RBAC | Gán quyền INSERT, DELETE, UPDATE, SELECT trên bảng HSBENHNHAN cho role TT\_DP. |
| 8 | Bộ phận tiếp tân và điều phối bệnh được quyền xem thông tin trên bảng DV\_BN, TOATHUOC nhưng không được xem trên thuộc tính tổng tiền; không được xem trên thuộc tính thuốc điều trị cho bệnh nhân. | RBAC hoặc Mã hoá | Gán quyền INSERT, DELETE, UPDATE, SELECT trên bảng HSBENHNHAN cho role TT\_DP. |
| 9 | Nhân viên phòng tài vụ chỉ nhìn thấy các thủ tục mà bác sĩ yêu cầu bệnh nhân phải làm khi điều trị bệnh, thông tin mà bộ phận điều phối bệnh đã điều phối, xem được luôn cột tính tiền | DAC | Gán quyền SELECT trên bảng PHIEUKHAMBENH, TOATHUOC, HSBENHNHAN cho user là nhân viên phòng tài vụ. |
| 10 | Nhân viên phòng tài vụ chỉ được cập nhật số tiền phải trả cho từng chi tiết khám trị bệnh của bệnh nhân mà không được chỉnh sửa bất cứ thông tin gì. | DAC | Gán quyền UPDATE trên cột PHIDV của bảng PHIEUKHAMBENH và cột THANHTIEN của TOATHUOC cho user là nhân viên phòng tài vụ. |
| 11 | Bác sĩ có thể thêm/sửa thông tin liên quan đến việc điều trị bệnh và các loại thuốc phải dùng, liều dùng cho bệnh nhân cho bệnh nhân mà mình chịu trách nhiệm. | VPD | Tạo hàm chính sách cho phép user là bác sĩ thêm, sửa thông tin liên quan đến các bệnh nhân mà mình điều trị. |
| 12 | Bác sĩ không được xem thông tin khác của những bệnh nhân do bác sĩ khác điều trị hoặc những thông tin khác trong hệ thống. | DAC hoặc VPD | DAC: Tạo view gồm thông tin các bệnh nhân mà học điều trị. Và gán quyền SELECT trên view đó cho user là bác sĩ.  VPD: Tạo hàm chính sách ngăn user là bác sĩ xem thông tin liên quan đến các bệnh nhân mà bác sĩ khác điều trị. |
| 13 | Bác sĩ chỉ được xem toa thuốc của bệnh nhân mình điều trị. | DAC | Tạo view BS\_Tthuoc gồm thông tin bảng TOATHUOC và CHITIETTOATHUOC, và gán quyền SELECT trên view BS\_TThuoc cho user là bác sĩ. |
| 14 | Bác sĩ không được chỉnh sửa thông tin khác của những bệnh nhân do bác sĩ khác điều trị. | VPD | Tạo hàm chính sách ngăn user là bác sĩ thêm, sửa thông tin liên quan đến các bệnh nhân mà bác sĩ khác điều trị. |
| 15 | Bộ phận bán thuốc chỉ có thể nhìn thấy toa thuốc mà bác sĩ kê cho từng bệnh nhân mà không xem được thông tin khác của bệnh nhân. | RBAC | Gán quyền SELECT trên bảng TOATHUOC, CHITIETTOATHUOC cho role BPBN. |
| 16 | Nhân viên kế toán xem được lương cơ bản, phụ cấp, số ngày công của nhân viên. | DAC | Tạo view NVKT\_Luong gồm các thông tin lương cơ bản phụ cấp, số ngày công của nhân viên, và gán quyền SELECT trên view NVKT\_Luong cho user là nhân viên kế toán. |
| 17 | Nhân viên kế toán tính lương cho các bác sĩ và các nhân viên khác dựa vào lương cơ bản, phụ cấp, số ngày công. | DAC | Gán quyền UPDATE trên cột LUONG của bảng NHANVIEN cho user là nhân viên kế toán. |
| 18 | Nhân viên kế toán không nhìn thấy bất cứ thông tin gì liên quan đến quá trình điều trị bệnh cho bệnh nhân của những bộ phận liên quan. | VPD | Tạo hàm chính sách ngăn user là nhân viên kế toán xem thông tin liên quan quá trình điều trị bệnh cho bệnh nhân của những bộ phận liên quan. |
| 19 | Mỗi nhân viên chỉ được xem lương của chính họ. | VPD | Tạo hàm chính sách cho phép tất cả nhân viên chỉ có thể xem được lương của chính họ. |

1. **Các chính sách đã cài đặt**
2. *Cơ chế DAC*

|  |  |  |
| --- | --- | --- |
| **Kịch bản** | Bác sĩ chỉ được xem toa thuốc của bệnh nhân mình điều trị. | Bác sĩ không được xem thông tin khác của những bệnh nhân do bác sĩ khác điều trị hoặc những thông tin khác trong hệ thống. |
| **Thực hiện** | Tạo view BS\_Tthuoc gồm thông tin bảng TOATHUOC và CHITIETTOATHUOC, và gán quyền SELECT trên view BS\_TThuoc cho user là bác sĩ. | Tạo view gồm thông tin các bệnh nhân mà học điều trị. Và gán quyền SELECT trên view đó cho user là bác sĩ. |

1. *Cơ chế RBAC*

|  |  |  |
| --- | --- | --- |
| **Kịch bản** | Nhóm quản lý chuyên môn được xem tất cả thông tin trong đó có thông tin điều trị bệnh của các bác sĩ để theo dõi về chuyên môn của bệnh viện, không được chỉnh sửa bất cứ thông tin nào. | Bộ phận tiếp tân và điều phối bệnh được quyền thêm, xóa, sửa, tìm kiếm thông tin bệnh nhân. |
| **Thực hiện** | Gán quyền SELECT ANY TABLE cho role QLCM. | Gán quyền INSERT, DELETE, UPDATE, SELECT trên bảng HSBENHNHAN cho role TT\_DP. |

1. *Cơ chế VPD*

|  |  |  |
| --- | --- | --- |
| **Kịch bản** | Bác sĩ có thể thêm/sửa thông tin liên quan đến việc điều trị bệnh và các loại thuốc phải dùng, liều dùng cho bệnh nhân cho bệnh nhân mà mình chịu trách nhiệm. | Mỗi nhân viên chỉ được xem lương của chính họ. |
| **Thực hiện** | Tạo hàm chính sách cho phép user là bác sĩ thêm, sửa thông tin liên quan đến các bệnh nhân mà mình điều trị. | Tạo hàm chính sách cho phép tất cả nhân viên chỉ có thể xem được lương của chính họ. |

1. *Cơ chế MAC (OLS)*

|  |  |
| --- | --- |
| **Kịch bản** | Khi cấp trên tạo thông báo và gửi cho các nhân viên thuộc hệ thống thì tất cả mọi người đều nhận được. |
| **Thực hiện** |  |

1. *Mã hoá*

|  |  |
| --- | --- |
| **Kịch bản** |  |
| **Thực hiện** |  |

1. *Audit*

|  |  |  |
| --- | --- | --- |
| **Kịch bản** |  |  |
| **Thực hiện** |  |  |