ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH

TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN

**ĐỒ ÁN**

**MÔN AN TOÀN VÀ BẢO MẬT DỮ LIỆU TRONG HỆ THỐNG THÔNG TIN**

**Đề tài: Quản lý tài nguyên, người dùng, điều khiển truy cập và quản lý thông tin của một bệnh viện**

Giáo viên phụ trách: Phạm Thị Bạch Huệ.

Sinh viên thực hiện: 1512001 - Bùi Tú Anh.

1512065 - Nguyễn Thiên Duyên.

Tp. HCM, năm 2018

**MỤC LỤC**

|  |  |
| --- | --- |
| **MỤC** | **TRANG** |
| 1. BẢNG PHÂN CÔNG CÔNG VIỆC | 3 |
| 1. MÔ TẢ LẠI ĐỒ ÁN. | 4 |
| 1. PHÂN HỆ 1 | 6 |
| 1. PHÂN HỆ 2   2.1 Mô hình CSDL  2.2 Xác định chính sách bảo mật  2.3 Xác định loại người dùng trong hệ thống  2.4 Bảng quyền truy xuất  2.5 Phân tích | 8  8  9  11  12  19 |

1. **BẢNG PHÂN CÔNG CÔNG VIỆC**

|  |  |
| --- | --- |
| **Người thực hiện** | **Mục** |
| 1512001  Bùi Tú Anh | Mô tả đồ án phần 1,2,7 |
| Phân hệ 1 – Phân tích chức năng, metadata |
| Phân hệ 2 – Mô hình dữ liệu |
| Phát biểu chính sách bảo mật |
| Xác định loại người dùng trong hệ thống |
| Vẽ ma trận quyền truy xuất trên NHANVIEN, LOAINV, PHONG, CHAMCONG, BENHNHAN |
| Phân tích cơ chế xác thực người dùng |
| Phân tích cơ chế điều khiển truy cập, mã hóa |
| 1512065  Nguyễn Thiên Duyên | Mục II, phần 3,4,5,6,8 |
| Phân hệ 1 – Phân tích chức năng, metadata |
| Phân hệ 2 – Mô hình dữ liệu |
| Phát biểu chính sách bảo mật |
| Xác định loại người dùng trong hệ thống |
| Vẽ ma trận quyền truy xuất trên PHIEUKHAM, DICHVU, THUOC, PK\_DV, PK\_THUOC |
| Phân tích cơ chế điều khiển truy cập, mã hóa |
| Phân tích cơ chế Audit |

1. **MÔ TẢ LẠI ĐỒ ÁN.**

**1. Giai đoạn tiếp bệnh khi bệnh nhân đến bệnh viện**

* Bệnh nhân gặp bộ phận tiếp tân và điều phối bệnh để làm sổ và khai bệnh (tên, năm sinh, số điện thoại, triệu chứng bệnh).
* Nếu đã khám rồi thì chỉ cần cung cấp số điện thoại (để không phải khai lại) và triệu chứng bệnh để được điều phối tới bác sĩ đúng chuyên khoa.
* Sau khi hoàn tất giai đoạn tiếp bệnh, bệnh nhân đến phòng tài vụ đóng tiền khám bệnh và nhận hóa đơn, hóa đơn này phải có thông tin về bệnh nhân cùng triệu chứng bệnh.
* Bệnh nhân mang hóa đơn đến nhân viên tiếp tân chỉ định phòng khám và bác sĩ, từ nội dung hóa đơn mới điều phối đến bác sĩ phù hợp.

**2. Quy trình khám bệnh:**

* Bệnh nhân đến phòng bác sĩ được điều phối.
* Bác sĩ nhìn thấy dữ liệu về bệnh nhân được điều phối.
* Mỗi bác sĩ chỉ được nhìn thấy dòng dữ của bệnh nhân được tiếp tân điều phối cho bác sĩ đó (không được xem thông tin của bệnh nhân do các bác sĩ khác điều trị).
* Sau khi khám bệnh:
  + Bác sĩ ghi kết luận (ghi vào phiếu khám chẩn đoán bệnh từ bác sĩ) và chỉ định bệnh nhân phải dùng thuốc gì (bác sĩ kê thuốc cho phiếu khám tương ứng).
  + Hoặc phải tiếp tục làm những thủ tục xét nghiệm hoặc chuẩn đoán hình ảnh nào (tất cả các dịch vụ bác sĩ yêu cầu thực hiện cho bệnh nhân đó đều được lưu lại theo phiếu khám tương ứng), sau khi hoàn tất tất cả các dịch vụ thì bác sĩ mới kết luận và kê thuốc (tương ứng như trên).

**3.  Bệnh nhân làm xét nghiệm - chụp hình chuẩn đoán:**

* Bác sĩ khám khám xong và gửi yêu cầu đến bộ phận tiếp tân và điều phối.
* Bộ phận tiếp tân và điều phối chịu trách nhiệm điều phối bệnh nhân vào đúng phòng.
* Kĩ thuật viên và các bác sĩ chịu trách nhiệm xét nghiệm hoặc chụp hình sẽ xem được thông tin về Họ tên, ngày tháng năm sinh, tên xét nghiệm, chuẩn đoán.

**4.  Bán thuốc cho bệnh nhân & thanh toán:**

* Bác sĩ sẽ kê toa thuốc và nhân viên phòng tài vụ và phòng thuốc có thể xem được thông tin về toa thuốc.
* Phòng thuốc nhận được các đơn thuốc và lấy thuốc đem đến phòng tài vụ.
* Nhân viên tài vụ sẽ tính tiền dựa vào các chỉ định xét nghiệm, chuẩn đoán và tất cả đơn thuốc của bệnh nhân đó
* Bệnh nhân đến phòng phòng tài vụ đóng tiền và nhận thuốc trực tiếp tại đó.

**5. Vấn đề tiền lương của bác sĩ và nhân viên**

* Nhân viên kế toán chịu trách nhiệm về việc tính lương dựa vào lương cơ bản, phụ cấp, số ngày công.

**6. Vấn đề về lịch làm việc**

* Lịch làm việc được bác sĩ trưởng khoa và ban quản lý của bệnh viện phụ trách (nhóm quản lý tài nguyên và quản lý chuyên môn).
* Bộ phận tiếp tân và điều phối sẽ xem được Lịch này để điều phối bệnh nhân.
* Từ lịch này có thể tính được số ngày công, dựa vào đó mà bộ phận kế toán tính lương cho bác sĩ và nhân viên.

1. **Vấn đề về thông báo**

* Mọi nhân viên đều có thể ghi lên bảng thông báo, tùy loại nhân viên mà có thể đọc được những thông báo nào.

1. **Vấn đề lưu nhật ký người dùng**

* DBA được xem nhật kí người dùng khi sử dụng để dễ dàng kiểm soát, quản lý và ngăn chặn hành động vi phạm  kịp thời.

1. **PHÂN HỆ 1**

**1.      Phân tích từng chức năng của phân hệ 1, metadata cần sử dụng và cách thức thực hiện.**

* Xem danh sách người sử dụng trong hệ thống
  + DBA có quyền xem danh sách tất cả các người dùng trong hệ thống.
  + Metadata cần sử dụng là thông tin từ object system all\_users.
  + Cách thức thực hiện: truy vấn đến object system all\_users, bảng này gồm 3 thuộc tính là USERNAME (tên user), USER\_ID (id của user) và CREATED (thời gian tạo user tương ứng). Truy vấn đến bảng này để biết được danh sách các người dùng.
* Thông tin về quyền (privileges) của mỗi user/role trên các đối tượng dữ liệu.
  + DBA có quyền xem thông tin về quyền (privileges) của mỗi user/role trên các đối tượng dữ liệu.
  + Metadata cần sử dụng là thông tin từ object system user\_tab\_privs.
  + Cách thức thực hiện: truy vấn đến object system user\_tab\_privs, bảng này gồm các thuộc tính là GRANTEE (người được cấp quyền), OWNER (chủ sở hữu của object), TABLE\_NAME (tên các object, không chỉ riêng các bảng dữ liệu), GRANTOR (người cấp quyền) và PRIVILEGE (quyền trên object TABLE\_NAME). Nghĩa là để xem quyền của USERA trên các đối tượng thì đầu tiên câp quyền SELECT trên user\_tab\_privs cho admin, sau đó admin sẽ truy vấn SELECT \* FROM user\_tab\_privs WHERE GRANTEE = ‘USERA’ thì sẽ xuất ra các thông tin về user là đối tượng nào (TABLE\_NAME), được sở hữu bởi ai (OWNER), được cấp quyền (PRIVILEGDE), được cấp quyền bởi ai (GRANTOR) cho USERA (USER).
* Cho phép tạo mới, xóa, sửa (hiệu chỉnh) user hoặc role
  + DBA có quyền tạo mới, xóa, sửa (hiệu chỉnh) user hoặc role.
  + Cách thức thực hiện: sử dụng câu lệnh create user, drop user, alter user, create role, drop role.
* Cho phép thu hồi quyền từ user/role.
  + DBA có quyền thu hồi quyền từ user hoặc role.
  + Cách thức thực hiện: sử dụng câu lệnh revoke.
* Cho phép thực hiện cấp quyền: cấp quyền cho user, cấp quyền cho role, cấp role cho user (có WITH GRANT OPTION hay không):
  + DBA có quyền thực hiện cấp quyền cho user/role, cấp role cho user, có tùy chọn WITH GRANT OPTION.
  + Cách thức thực hiện: sử dụng câu lệnh grant, cùng với tùy chọn có hoặc không có WITH GRANT OPTION.
* Cho phép cấp các quyền select/update cho user/role (tính đến mức cột), quyền insert, update.
  + DBA có quyền cấp các quyền select/update/insert/update cho user/role (đến mức cột đối với select/update).
  + Cách thức thực hiện: sử dụng câu lệnh grant, tạo view (đối với quyền select - đến mức côt).
* Cho phép thu hồi quyền từ user/role
  + DBA có quyền thu hồi quyền từ người dùng hoặc role.
  + Cách thức thực hiện: sử dụng câu lệnh revoke.
* Cho phép kiểm tra quyền của chủ thể vừa được cấp quyền
  + DBA có quyền kiểm tra các users và quyền của họ.
  + Metadata cần sử dụng là thông tin thì system object dba\_tab\_privs.
  + Cách thức thực hiện: truy vấn đến system object là dba\_tab\_privs.
* Cho phép chỉnh sửa quyền của user/role:
  + DBA có quyền chỉnh sửa quyền của user/role.
  + Cách thức thực hiện: sử dụng câu lệnh grant, revoke.

**2.   Giao diện đã cài đặt**

(Chụp một số giao diện chính)

1. **PHÂN HỆ 2**
2. **Mô hình dữ liệu**

**NHANVIEN** (MANV, TENNV, CHUCVU, LUONG, PHUCAP, LOAINV, MAPHONG)

**LOAINV** (MALOAI, TENLOAI)

Nhân viên và bác sĩ lưu chung trong NHANVIEN, căn cứ vào loại nhân viên để biết công việc cụ thể

**PHONG** (MAPHONG, TENPHONG)

**CHAMCONG** (MANV, NGAY, TUGIO, DENGIO)

Bảng chấm công ghi nhận thời gian làm việc của mỗi nhân viên, TUGIO, DENGIO: từ giờ, đến giờ cho biết thời điểm bắt đầu và thời điểm kết thúc của ngày làm việc, một ngày nhân viên có thể làm nhiều giờ khác nhau.

**BENHNHAN** (MABN, TENBN, DIACHI, DIENTHOAI, PHAI, NGAYSINH, CMND)

**PHIEUKHAM** (MAPK, MABN, MABS, NGAYKHAM, TRIEUCHUNG, CHANDOAN, MOTATHEM)

**DICHVU** (MADV, TENDV, GIADV)

**PK\_DV** (MAPK, MADV,MANV)

Cho biết lần khám bệnh có mã là MAPK, bác sĩ chỉ định bệnh nhân phải xét nghiệm hoặc dùng một kỹ thuật chẩn đoán hình ảnh nào.

**THUOC** (MATHUOC, TENTHUOC, QUYCACH, DONVITINH, GIATHUOC)

**PK\_THUOC** (MAPK, MATHUOC, SOLUONG, HUONGDAN)

Bác sĩ kê toa thuốc cho một phiếu khám

**THONGBAO** (NOIDUNG)

Bảng thông báo đến tất cả nhân viên trong bệnh viện, tùy loại thông báo mà người dùng nào có thể đọc.

1. **Phát biểu các chính sách bảo mật**

**Cấp quyền đọc trên toàn bảng**

CS1: Nhóm quản lý chuyên môn tất cả thông tin trong đó có thông tin điều trị bệnh nhưng không được chỉnh sửa (RBAC).

CS2: tất cả mọi nhân viên đều có thể đọc bảng LOAINV và PHONG.

**Không cấp quyền trên toàn bảng**

- Nhóm quản lý tài nguyên:  BENHNHAN, PHIEUKHAM, DICHVU, THUOC, PK\_DV, PK\_THUOC

- Nhóm quản lý tài vụ: không có

- Nhóm quản lý chuyên môn: CHAMCONG, BENHNHAN

- Bộ phận tiếp tân và điều phối: DICHVU, THUOC

- Nhân viên phòng tài vụ: NHANVIEN, LOAINV, PHONG, CHAMCONG, BENHNHAN, PHIEUKHAM, PK\_DV, PK\_THUOC

- Bác sĩ: NHANVIEN, LOAINV, PHONG, CHAMCONG, BENHNHAN

- Kỹ thuật viên: NHANVIEN, LOAINV, PHONG, CHAMCONG, BENHNHAN, THUOC, PK\_THUOC

- Nhân viên bộ phận bán thuốc: NHANVIEN, LOAINV, PHONG, CHAMCONG,BENHNHAN, DICHVU, PK\_DV

- Nhân viên kế toán: BENHNHAN, PHIEUKHAM, DICHVU, THUOC, PK\_DV, PK\_THUOC

**Các chính sách trên bảng NHANVIEN**

CS3: Nhân viên kế toán chỉ được chỉnh sửa LUONG, PHUCAP trong bảng NHANVIEN (VPD trên cột).

CS4: Bộ phận tiếp tân và điều phối không xem được LUONG, PHUCAP (tạo view).

CS5: Nhóm quản lý tài nguyên nhận chỉ định thêm, xóa, sửa, các thông tin trong danh mục như: phòng ban, bác sĩ, nhân viên trong tưng phòng ban, bác sĩ nào trực phòng nào trong thời gian nào,... (RBAC). (và CHAMCONG).

CS6: Nhân viên nào chỉ xem được LUONG,PHUCAP của nhân viên đó (VPD trên cột) nhưng nhân viên thuộc bộ phận quản lý được xem lương của nhân viên khác.

**Các chính sách trên bảng LOAINV và PHONG**

CS7: Nhóm quản lý tài nguyên nhận chỉ định thêm, xóa, sửa, các thông tin trong danh mục như: phòng ban, bác sĩ, nhân viên trong tưng phòng ban, bác sĩ nào trực phòng nào trong thời gian nào,... (RBAC).

**Các chính sách trên bảng CHAMCONG**

CS8: Bộ phận tiếp tân và điều phối bệnh cũng căn cứ vào dữ liệu bác sĩ chỉ định về việc xét nghiệm hoặc /và chẩn đoán hình ảnh để hướng dẫn bệnh nhân đúng phòng => nhân viên phòng tài vụ có thể đọc các thông tin trên bảng CHAMCONG để có thể hướng dẫn cho bệnh nhân (RBAC).

**Các chính sách trên bảng BENHNHAN**

CS9: Mỗi bác sĩ chỉ nhìn thấy dòng dữ liệu của bệnh nhân được tiếp tân điều phối cho bác sĩ đó (VPD trên dòng).

CS10: Bác sĩ không được xem các thông tin bệnh nhân mà bác sĩ đó không điều trị và các thông tin khác (tạo view).

CS11: Kỹ thuật viên tại phòng xét nghiệm và chuẩn đoán hình ảnh chỉ thấy những dòng dữ liệu về bệnh nhân đã được bác sĩ chi định cho họ (họ tên, ngày tháng năm sinh) (tạo view).

CS12: Nhân viên phòng tài vụ sẽ nhìn thấy thông tin của các bệnh nhân (RBAC).

CS13: Bộ phận tiếp tân và điều phối bệnh viện được quyền thêm, xóa , sửa, tìm kiếm thông tin bệnh nhân (RBAC).

CS14: Nhân viên bán thuốc không được xem thông tin bệnh nhân (RBAC).

**Các chính sách trên bảng PHIEUKHAM**

CS: Nhân viên tài vụ được xem thông tin mà bộ phận điều phối tiếp nhận nhưng không xem được thông tin chẩn đoán của bác sĩ (VPD cột)

CS: Bộ phận tiếp tân và điều phối không xem được thông tin chẩn đoán của bác sĩ (VPD cột)

CS: Chỉ có bác sĩ mới được quyền chỉnh sửa thông tin triệu chứng, chẩn đoán, mô tả thêm (DAC)

CS: Bộ phận tiếp tân và điều phối được quyền insert, chỉnh sửa các thông tin trong Phiếu khám, trừ những thông tin liên quan đến chẩn đoán của bác sĩ (RBAC)

CS: Bác sĩ chỉ xem và có quyền chỉnh sửa trên những phiếu khám của bệnh nhân mà mình điều trị (VPD dòng)

**Các chính sách trên bảng DICHVU**

CS: Bộ phận tiếp tân và điều phối, nhân viên tài vụ, bác sĩ và kỹ thuật viên được xem (RBAC)

CS: Nhân viên phòng tài vụ được cập nhật thông tin về giá tiền của dịch vụ (RBAC)

CS: Nhóm quản lý tài vụ được quyền thêm, xóa, sửa thông tin dịch vụ (RBAC)

CS: Bộ phận tiếp tân và điều phối không thể xem các thông tin liên quan đến số tiền (VPD cột)

**Các chính sách trên bảng PK\_DV**

CS: Bộ phận tiếp tân và điều phối, nhân viên tài vụ, bác sĩ và kỹ thuật viên được xem (RBAC)

CS: Bộ phận điều phối và tiếp tân được quyền chỉnh sửa Mã NV (RBAC)

CS: Bác sĩ chỉ định dịch vụ của bệnh nhân (RBAC)

CS: Bác sĩ chỉ có quyền trên những dòng do bệnh nhân mình điều trị (VPD dòng)

CS: Kỹ thuật viên chỉ nhìn thấy những dòng mình được phân công (VPD dòng)

**Các chính sách trên bảng THUOC**

CS: Nhóm quản lý tài vụ được quyền thêm, xóa, sửa thông tin thuốc (RBAC)

CS: Chỉ nhân viên phòng tài vụ, nhân viên bộ phận bán thuốc và bác sĩ mới có squyền xem (RBAC)

**Các chính sách trên bảng PK\_THUOC**

CS: Chỉ nhân viên phòng tài vụ, nhân viên bộ phận bán thuốc và bác sĩ mới có squyền xem (RBAC)

CS: Bác sĩ chỉ định thuốc của bệnh nhân. Bác sĩ chỉ có quyền trên những dòng do bệnh nhân mình điều trị (RBAC, VPD dòng)

**Các chính sách trên bảng THONGBAO**

CS: Tất cả nhân viên đều có quyền đọc, nhóm quản lý được quyền thêm xóa sửa. (RBAC)

CS: Tùy theo người dùng để có thể đọc được những thông báo có mức bảo mật khác nhau (OLS).

1. **Xác định các loại người dùng trong hệ thống**

* Nhóm quản lý tài nguyên.
* Nhóm quản lý tài vụ.
* Nhóm quản lý chuyên môn.
* Bộ phận tiếp tân và điều phối.
* Nhân viên phòng tài vụ.
* Bác sĩ.
* Kỹ thuật viên.
* Nhân viên bộ phận bán thuốc.
* Nhân viên kế toán.

1. **Vẽ ma trận quyền truy xuất**

Ma trận quyền truy xuất trên NHANVIEN

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | MANV | TENNV | CHUCVU | LUONG | PHUCAP | LOAINV | MA PHONG |
| Nhóm quản lý tài nguyên | 11 | 11 | 11 | 11 | 11 | 11 | 11 |
| Nhóm quản lý tài vụ | 10 | 10 | 10 | 10 | 10 | 10 | 10 |
| Nhóm quản lý chuyên môn | 10 | 10 | 10 | 10 | 10 | 10 | 10 |
| Bộ phận tiếp tân và điều phối | 10 | 10 | 10 | 00 | 00 | 10 | 10 |
| Nhân viên phòng tài vụ | 00 | 00 | 00 | 00 | 00 | 00 | 00 |
| Bác sĩ | 00 | 00 | 00 | 00 | 00 | 00 | 00 |
| Kỹ thuật viên | 00 | 00 | 00 | 00 | 00 | 00 | 00 |
| Nhân viên bộ phận bán thuốc | 00 | 00 | 00 | 00 | 00 | 00 | 00 |
| Nhân viên kế toán | 10 | 10 | 10 | 11 | 11 | 10 | 10 |

Ma trận quyền truy xuất trên LOAINV và PHONG

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | MALOAI | TENLOAI | MAPHONG | TENPHONG |
| Nhóm quản lý tài nguyên | 11 | 11 | 11 | 11 |
| Nhóm quản lý tài vụ | 10 | 10 | 10 | 10 |
| Nhóm quản lý chuyên môn | 10 | 10 | 10 | 10 |
| Bộ phận tiếp tân và điều phối | 10 | 10 | 10 | 10 |
| Nhân viên phòng tài vụ | 10 | 10 | 10 | 10 |
| Bác sĩ | 10 | 10 | 10 | 10 |
| Kỹ thuật viên | 10 | 10 | 10 | 10 |
| Nhân viên bộ phận bán thuốc | 10 | 10 | 10 | 10 |
| Nhân viên kế toán | 10 | 10 | 10 | 10 |

Ma trận quyền truy xuất trên CHAMCONG

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | MANV | NGAY | TUGIO | DENGIO |
| Nhóm quản lý tài nguyên | 11 | 11 | 11 | 11 |
| Nhóm quản lý tài vụ | 10 | 10 | 10 | 10 |
| Nhóm quản lý chuyên môn | 00 | 00 | 00 | 00 |
| Bộ phận tiếp tân và điều phối | 10 | 10 | 10 | 10 |
| Nhân viên phòng tài vụ | 00 | 00 | 00 | 00 |
| Bác sĩ | 00 | 00 | 00 | 00 |
| Kỹ thuật viên | 00 | 00 | 00 | 00 |
| Nhân viên bộ phận bán thuốc | 00 | 00 | 00 | 00 |
| Nhân viên kế toán | 10 | 10 | 10 | 10 |

Ma trận quyền truy xuất trên BENHNHAN

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | MABN | TENBN | DIACHI | DIEN THOAI | PHAI | NGAY SINH | CMND |
| Nhóm quản lý tài nguyên | 00 | 00 | 00 | 00 | 00 | 00 | 00 |
| Nhóm quản lý tài vụ | 10 | 10 | 10 | 10 | 10 | 10 | 10 |
| Nhóm quản lý chuyên môn | 00 | 00 | 00 | 00 | 00 | 00 | 00 |
| Bộ phận tiếp tân và điều phối | 11 | 11 | 11 | 11 | 11 | 11 | 11 |
| Nhân viên phòng tài vụ | 00 | 00 | 00 | 00 | 00 | 00 | 00 |
| Bác sĩ | 10 | 10 | 10 | 10 | 10 | 10 | 10 |
| Kỹ thuật viên | 10 | 10 | 00 | 00 | 00 | 10 | 00 |
| Nhân viên bộ phận bán thuốc | 00 | 00 | 00 | 00 | 00 | 00 | 00 |
| Nhân viên kế toán | 00 | 00 | 00 | 00 | 00 | 00 | 00 |

Ma trận quyền truy xuất trên PHIEUKHAM

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | MAPK | MABN | MABS | NGAYKHAM | TRIEU CHUNG | CHAN DOAN | MOTA THEM |
| Nhóm quản lý tài nguyên | 00 | 00 | 00 | 00 | 00 | 00 | 00 |
| Nhóm quản lý tài vụ | 10 | 10 | 10 | 10 | 10 | 10 | 10 |
| Nhóm quản lý chuyên môn | 10 | 10 | 10 | 10 | 10 | 10 | 10 |
| Nhân viên bộ phần tiếp tân và điều phối | 11 | 11 | 11 | 11 | 00 | 00 | 00 |
| Nhân viên phòng tài vụ | 10 | 10 | 10 | 10 | 00 | 00 | 00 |
| Bác sĩ | 10 | 10 | 10 | 10 | 11 | 11 | 11 |
| Kĩ thuật viên | 10 | 10 | 10 | 10 | 00 | 00 | 00 |
| Nhân viên bán thuốc | 00 | 00 | 00 | 00 | 00 | 00 | 00 |
| Nhân viên kế toán | 00 | 00 | 00 | 00 | 00 | 00 | 00 |

Ma trận quyền truy xuất trên DICHVU và PK\_DV

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | MADV | TENDV | GIADV | MAPK | MADV | MANV |
| Nhóm quản lý tài nguyên | 00 | 00 | 00 | 00 | 00 | 00 |
| Nhóm quản lý tài vụ | 11 | 11 | 11 | 10 | 10 | 10 |
| Nhóm quản lý chuyên môn | 10 | 10 | 10 | 10 | 10 | 10 |
| Nhân viên bộ phần tiếp tân và điều phối | 10 | 10 | 00 | 10 | 10 | 11 |
| Nhân viên phòng tài vụ | 10 | 10 | 11 | 10 | 10 | 00 |
| Bác sĩ | 10 | 10 | 00 | 10 | 11 | 00 |
| Kĩ thuật viên | 10 | 10 | 00 | 10 | 10 | 10 |
| Nhân viên bán thuốc | 00 | 00 | 00 | 00 | 00 | 00 |
| Nhân viên kế toán | 00 | 00 | 00 | 00 | 00 | 00 |

Ma trận quyền truy xuất trên THUOC

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | MATHUOC | TENTHUOC | QUY CACH | DONVI TINH | GIATHUOC |
| Nhóm quản lý tài nguyên | 00 | 00 | 00 | 00 | 00 |
| Nhóm quản lý tài vụ | 11 | 11 | 11 | 11 | 11 |
| Nhóm quản lý chuyên môn | 00 | 00 | 00 | 00 | 00 |
| Nhân viên bộ phần tiếp tân và điều phối | 00 | 00 | 00 | 00 | 00 |
| Nhân viên phòng tài vụ | 10 | 10 | 10 | 10 | 11 |
| Bác sĩ | 10 | 10 | 10 | 10 | 00 |
| Kĩ thuật viên | 00 | 00 | 00 | 00 | 00 |
| Nhân viên bán thuốc | 10 | 10 | 10 | 10 | 00 |
| Nhân viên kế toán | 00 | 00 | 00 | 00 | 00 |

Ma trận quyền truy xuất trên PK\_THUOC

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | MAPK | MATHUOC | SOLUONG | HUONGDAN |
| Nhóm quản lý tài nguyên | 00 | 00 | 00 | 00 |
| Nhóm quản lý tài vụ | 10 | 10 | 10 | 10 |
| Nhóm quản lý chuyên môn | 00 | 00 | 00 | 00 |
| Nhân viên bộ phần tiếp tân và điều phối | 00 | 00 | 00 | 00 |
| Nhân viên phòng tài vụ | 10 | 10 | 10 | 10 |
| Bác sĩ | 11 | 11 | 11 | 11 |
| Kĩ thuật viên | 00 | 00 | 00 | 00 |
| Nhân viên bán thuốc | 10 | 10 | 10 | 10 |
| Nhân viên kế toán | 00 | 00 | 00 | 00 |

Ma trận quyền truy xuất trên THONGBAO

|  |  |
| --- | --- |
|  | NOIDUNG |
| Nhóm quản lý tài nguyên | 11 |
| Nhóm quản lý tài vụ | 11 |
| Nhóm quản lý chuyên môn | 11 |
| Nhân viên bộ phần tiếp tân và điều phối | 11 |
| Nhân viên phòng tài vụ | 11 |
| Bác sĩ | 11 |
| Kĩ thuật viên | 11 |
| Nhân viên bán thuốc | 11 |
| Nhân viên kế toán | 11 |

1. **Phân tích**

* Các chính sách bảo mật được phân loại như phần IV.2.
* Cơ chế xác thực người dùng: người dùng đăng nhập vào hệ thống, từ đó tùy loại người dùng mà họ có thể thực hiện các chức năng liên quan từ các quyền được cấp.
* Cơ chế điều khiển truy cập:
  + RBAC: cấp các quyền đọc, ghi cho từng loại người dùng trên các bảng sao cho phù hợp với chính sách bảo mật.
  + Không dùng DAC.
  + Tạo view: do một người dùng có thể không thể đọc hết tất cả các thông tin (các cột) trên 1 bảng dữ liệu, nên tạo view từ 1 bảng để tạo ra khung nhìn chỉ gồm các thông tin mà người dùng đó có thể đọc.
  + VPD: cấp quyền truy cập tới mức cột, hoặc chỉ cho phép truy cập đến những dòng dữ liệu mà người dùng được phép truy cập.
  + OLS:  chỉ thực hiện trên bảng THONGBAO, tùy loại người dùng mà họ có thể xem được những dòng thông báo nào trong bảng này.
* Cơ chế mã hóa:
  + Mã hóa CHANDOAN trong PHIEUKHAM (chỉ có bác sĩ và nhóm quản lý chuyên môn xem được)
  + Mã hóa LUONG, PHUCAP trong NHANVIEN (nhân viên chỉ xem được lương của chính mình, riêng nhóm quản lý và nhân viên kế toán có thể xem được lương của người khác)
  + Mã hóa thông tin CMND trong BENHNHAN
* Có sử dụng audit ở phân hệ 1,  DBA có thể xem nhật kí sử dụng và truy cập của những người dùng khác.