**BỘ MÔN HỆ THỐNG THÔNG TIN – KHOA CÔNG NGHỆ THÔNG TIN**

Logo

Description automatically generated**ĐẠI HỌC KHOA HỌC TỰ NHIÊN THÀNH PHỐ HỒ CHÍ MINH,**

Sinh viên thực hiện:

|  |  |
| --- | --- |
| 19120481 | Đàm Hồng Đức |
| 19120583 | Lê Thái Bình Minh |
| 19120416 | Nguyễn Anh Tuấn |
| 19120529 | Nguyễn Phước Huy |

GV phụ trách: Thầy Lương Vĩ Minh, cô Phạm Thị Bạch Huệ, cô Tiết Gia Hồng

  AN TOÀN & BẢO MẬT DỮ LIỆU TRONG HỆ THỐNG THÔNG TIN

HỌC KỲ II – NĂM HỌC 2021 - 2022

**Báo cáo đồ án môn học**

**ĐẠI HỌC QUỐC GIA TP HCM**

**BẢNG THÔNG TIN CHI TIẾT NHÓM**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Mã nhóm:** | ATBMCQ-05 | | | |
| **Số lượng:** | **4** | | | |
| **MSSV** | **Họ tên** | **Email** | **Điện thoại** | **Nhóm trưởng** |
| 19120481 | Đàm Hồng Đức | 19120481@student.hcmus.edu.vn | 0355211735 |  |
| 19120583 | Lê Thái Bình Minh | 19120583@student.hcmus.edu.vn | 0852576282 | x |
| 19120416 | Nguyễn Anh Tuấn | 19120416@student.hcmus.edu.vn | 0348379575 |  |
| 19120529 | Nguyễn Phước Huy | 19120529@student.hcmus.edu.vn | 0917966026 |  |

**YÊU CẦU ĐỒ ÁN**

|  |  |
| --- | --- |
| **Loại bài tập** | **Lý thuyết 🗹 Thực hành 🗹 Đồ án Bài tập** |
| **Ngày bắt đầu** | **30/03/2022** |
| **Ngày kết thúc** | **28/06/2022** |

**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 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.

**PHÂN HỆ 2:** Sở y tế tỉnh/ thành phố X cần gom dữ liệu về kho dữ liệu D (cấp sở), gồm

hồ sơ bệnh án (và một số dữ liệu liên quan) từ các cơ sở y tế trong tỉnh/ thành phố và

quản lý chuyên môn về việc khám chữa bệnh của các cơ sở y tế thông qua một hệ thống

thông tin quản lý S.

***HSBA (MÃHSBA, MÃBN, NGÀY, CHẨNĐOÁN, MÃBS, MÃKHOA, MÃCSYT,***

***KẾTLUẬN):*** mỗi hồ sơ bệnh án (HSBA) có một mã duy nhất (MÃHSBA), liên quan

đến một bệnh nhân (MÃBN), được lập vào một ngày (NGÀY), có chẩn đoán

(CHẨNĐOÁN) của bác sĩ điều trị (MÃBS), được tiếp nhận khám và điều trị tại khoa

(MÃKHOA), của cơ sở y tế (có mã là MÃCSYT), với kết luận của bác sĩ (KẾTLUẬN).

***HSBA\_DV (MÃHSBA, MÃDV, NGÀY, MÃKTV, KẾTQUẢ):*** ghi nhận lại các dịch

vụ (thông qua MÃDV) đã sử dụng theo chỉ định của bác sĩ điều trị (ví dụ các loại xét

nghiệm, chụp hình, ...), người thực hiện dịch vụ (MÃKTV) và kết quả (KẾTQUẢ).

***BỆNHNHÂN (MÃBN, MÃCSYT, TÊNBN, CMND, NGÀYSINH, SỐNHÀ,***

***TÊNĐƯỜNG, QUẬNHUYỆN, TỈNHTP, TIỀNSỬBỆNH, TIỀNSỬBỆNHGĐ,***

***DỊỨNGTHUỐC):*** mỗi bệnh nhân được cơ sở y tế có mã là MÃCSYT cấp mã duy nhất

(MÃBN), có tên (TÊNBN), ngày sinh (NGÀYSINH), địa chỉ (SỐNHÀ, TÊNĐƯỜNG,

QUẬNHUYỆN), và tiền sử bệnh của bệnh nhân (TIỀNSỬBỆNH) và gia đình

(TIỀNSỬBỆNHGĐ), cũng như tình trạng dị ứng thuốc (nếu có, DỊỨNGTHUỐC).

***CSYT (MÃCSYT, TÊNCSYT, ĐCCSYT, SĐTCSYT):*** ghi nhận thông tin về các cơ

sở y tế thuộc tỉnh/ thành phố gồm mã, tên, địa chỉ, số điện thoại.

***NHÂNVIÊN (MÃNV, HỌTÊN, PHÁI, NGÀYSINH, CMND, QUÊQUÁN, SỐĐT,***

***CSYT, VAITRÒ, CHUYÊNKHOA):*** Quan hệ NHÂNVIÊN chứa dữ liệu về các nhân viên trực thuộc cơ sở y tế hoặc thuộc sở y tế có vai trò trong hệ thống S. Mỗi nhân viên có mã (MÃNV) do đơn vị quản lý trực tiếp cấp, giả sử các mã này không trùng nhau trong phạm vi toàn tỉnh/ thành phố. Ngoài ra cũng cần ghi lại thông tin họ tên (HỌTÊN), phái (PHÁI), ngày sinh (NGÀYSINH), số chứng minh nhân dân (CMND), quê quán, số điện thoại, thuộc cơ sở y tế nào (CSYT). Thuộc tính VAITRÒ nhận một trong các giá trị sau: “Thanh tra”, “Cơ sở y tế”, “Y sĩ/ bác sĩ”, “Nghiên cứu”. Với các nhân viên có vai trò “Y sĩ/ bác sĩ” hoặc “Nghiên cứu” thì cần lưu thêm thông tin về chuyên khoa (CHUYÊNKHOA) mà người đó được cấp bằng cấp chuyên môn. Cơ sở dữ liệu được cài đặt trên Oracle. Hệ thống dùng chính sách đóng (người dùng u cần được cấp quyền p trên đối tượng dữ liệu o mới có thể thực hiện p trên o). DBA trong hệ thống S thực hiện việc cấp quyền cho nhân sự trong toàn hệ thống theo mô tả như sau:

***TC#1:*** Ngoài DBA, tất cả người dùng trong hệ thống S gồm những nhân viên trong

quan hệ NHÂNVIÊN và cả những bệnh nhân trong quan hệ BỆNHNHÂN. DBA tạo tài

khoản cho tất cả những người dùng này. DBA không tự định nghĩa bảng (table) dùng để

quản lý tài khoản người dùng mà sử dụng thông tin tài khoản do Hệ quản trị CSDL

Oracle quản lý. Bằng cách nào DBA có thể kết nối một tên tài khoản với 1 dòng dữ liệu

là người dùng tương ứng (trong quan hệ NHÂNVIÊN và BỆNHNHÂN) mà không phải

truy cập dữ liệu từ nhiều hơn 1 bảng, đồng thời phải ép thỏa các chính sách bảo mật liên

quan đến những người dùng này. DBA phụ trách thêm, cập nhật dữ liệu trong bảng

CSYT và thêm dữ liệu trong NHÂNVIÊN, gồm những nhân viên thuộc các cơ sở y tế

hoặc thuộc sở y tế có vai trò trong hệ thống S.

***TC#2:*** Có 5 nhân viên thuộc sở y tế với vai trò “Thanh tra”. Các nhân viên giữ vai trò

thanh tra có thể đọc dữ liệu trên tất cả các quan hệ được mô tả để kết xuất báo cáo định

kỳ, mà không có quyền thêm, xóa, sửa trên bất cứ quan hệ nào.

***TC#3:*** Mỗi cơ sở y tế được cấp duy nhất 01 tài khoản trên hệ thống S để thao tác trên

kho dữ liệu D. Có 50 nhân viên thuộc 50 cơ sở y tế trong tỉnh/ thành phố được cử để sử

dụng tài khoản được cấp. Các nhân viên thuộc cơ sở y tế có quyền thêm hoặc xóa dữ

liệu phát sinh từ chính cơ sở y tế mà nhân viên này trực thuộc, trong tháng hiện tại từ

ngày 5 đến 27 dương lịch hàng tháng, liên quan các nghiệp vụ:

a. Thêm, xóa dòng trên hồ sơ bệnh án (HSBA)

b. Thêm, xóa dòng dịch vụ (HSBA\_DV) liên quan 1 hồ sơ bệnh án.

***TC#4:*** Có 500 nhân viên giữ vai trò “Y sĩ/ bác sĩ” trực tiếp khám chữa bệnh cho bệnh

nhân ở các cơ sở y tế thuộc tỉnh/ thành phố. Y sĩ/ Bác sĩ có quyền xem hồ sơ bệnh án

(HSBA) mà họ đã chữa trị và kết quả về các dịch vụ đã sử dụng (HSBA\_DV) và thông

tin bệnh nhân (BỆNHNHÂN) khi nhập thông tin mã bệnh nhân hoặc số CMND.

***TC#5:*** Có 50 nhân viên ở vai trò “Nghiên cứu” ở mỗi cơ sở y tế, chỉ có thể xem các hồ

sơ bệnh án (bảng HSBA và HSBA\_DV) được điều trị tại cùng cơ sơ y tế (với nhân viên

nghiên cứu đó), tại khoa giống chuyên khoa ghi trên bằng cấp của nhân viên nghiên cứu

đó.

***TC#6:*** Hệ thống hiện tại có khoảng 10000 bệnh nhân. Trên hệ thống S, trừ những người

giữ vai trò thanh tra (và DBA), mỗi nhân viên hoặc bệnh nhân đăng nhập chỉ có thể xem

thông tin của chính mình, (trên bảng NHÂN VIÊN nếu là nhân viên, trên bảng BỆNH

NHÂN nếu là bệnh nhân), và có thể chỉnh sửa các trường (trừ trường mã) liên quan đến

chính người đó.

***TC#7:*** Dựa vào chuyên môn, kỹ thuật của đơn vị mà Sở y tế tỉnh/ thành phố X chia các

cơ sở y tế trực thuộc thành 3 tuyến:

+ “Điều trị ngoại trú”: các cơ sở khám chữa bệnh ban đầu, điều trị ngoại trú.

+ “Điều trị nội trú”: các bệnh viện với các kỹ thuật chuyên khoa cơ bản và nâng cao.

+ “Điều trị chuyên sâu”: các bệnh viện đa khoa và chuyên khoa thực hiện được các kỹ

thuật chuyên sâu.

Ngoài ra, tùy vào vị trí địa lý của cơ sở y tế mà Sở y tế tỉnh/ thành phố X chia ra làm 3

vùng: trung tâm, cận trung tâm, ngoại thành. Có sự phân chia vai trò người dùng theo

03 cấp bậc: Giám đốc sở, Giám đốc cơ sở y tế và Y/ Bác sĩ. Sở cần gửi những dòng

trong quan hệ THÔNGBÁO, gồm các trường NỘIDUNG, NGÀYGIỜ và ĐỊAĐIỂM về

những cuộc họp khẩn đến các vai trò liên quan ở các cơ sở y tế. Dùng OLS (Oracle

Label Security). Hãy thiết lập hệ thống nhãn và thiết lập 5 loại người dùng khác nhau.

Cho minh họa cách phát tán dữ liệu.

Yêu cầu:

1. Hãy dùng các cơ chế bảo mật đã học của Oracle để hiện thực các chính sách bảo

mật đặt ra ở các TC#i, 1 <= i <= 6

Ở tiêu chí TC#7, 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 cho các kịch bản đã nêu, và các kịch bản khác (nếu có thể).

2. Sinh viên hãy đề xuất bối cảnh vận 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 dữ liệu

cần bảo vệ dữ liệu bằng phương pháp mã hóa, phương pháp quản lý khóa.

3. Sinh viên hãy thực hiện chức năng ghi nhật ký hệ thống (audit, chỉ yêu cầu thực

hiện mức HQT CSDL Oracle):

- Kích hoạt việc ghi nhật ký toàn hệ thống.

- Thực hiện ghi nhật ký hệ thống dùng standard audit: theo dõi hành vi của những

user nào trên những đối tượng cụ thể, trên các đối tượng khác nhau (table, view,

stored procedure, function), hay chỉ định theo dõi các hành vi hiện thành công

hay không thành công.

- Thực hiện Fine-grained Audit một số tình huống và cho kịch bản minh họa.

- Kiểm tra dữ liệu nhật ký hệ thống.

4. Nếu sinh viên cài đặt thêm các chính sách bảo mật có ứng dụng thực tế trong ngữ

cảnh ứng dụng trên thì sẽ được xem xét cộng điểm.

Mục Lục

[Phân hệ 1: 8](#_Toc107152968)

[1/ Giao diện đăng nhập: 8](#_Toc107152969)

[2/ Xem danh sách User và Role trong hệ thống: 9](#_Toc107152970)

[3/ Kiểm tra quyền của User/Role: 10](#_Toc107152971)

[4/ Tạo User mới: 11](#_Toc107152972)

[5/ Xoá User: 12](#_Toc107152973)

[6/ Hiệu chỉnh User: 13](#_Toc107152974)

[7/ Tạo Role mới: 14](#_Toc107152975)

[8/ Xoá Role: 15](#_Toc107152976)

[9/ Cấp quyền cho User/Role: 16](#_Toc107152977)

[10/ Cấp Role cho User: 17](#_Toc107152978)

[10/ Thu hồi Role khỏi User: 18](#_Toc107152979)

[Phân hệ 2 19](#_Toc107152980)

[I/ Mô hình cơ sở dữ liệu 19](#_Toc107152981)

[II/ Đặc tả dữ liệu 19](#_Toc107152982)

[III/ Ràng buộc toàn vẹn 19](#_Toc107152983)

[IV/ Xác định và phân quyền các loại người dùng 19](#_Toc107152984)

[V/ Các chính sách bảo mật 19](#_Toc107152985)

[1. Chính sách DAC 19](#_Toc107152986)

[2. Chính sách RBAC 19](#_Toc107152987)

[3. Chính sách VPD 20](#_Toc107152988)

[4. Chính sách OLS 20](#_Toc107152989)

[5. Chính sách Encrypt 20](#_Toc107152990)

[6. Chính sách Audit 20](#_Toc107152991)

Kết quả thực hiện

# Phân hệ 1:

## 1/ Giao diện đăng nhập:

Graphical user interface, application

Description automatically generated

## 2/ Xem danh sách User trong hệ thống:

Table

Description automatically generated

## 3/ Kiểm tra quyền của User/Role:

* Theo mức bảng: Table

  Description automatically generated
* Theo mức cột: Table

  Description automatically generated

## 4/ Tạo User mới:

Graphical user interface

Description automatically generated

## 5/ Xoá User:

Graphical user interface

Description automatically generated

## 6/ Hiệu chỉnh User:

Graphical user interface

Description automatically generated

## 7/ Tạo Role mới:

Graphical user interface, text, website

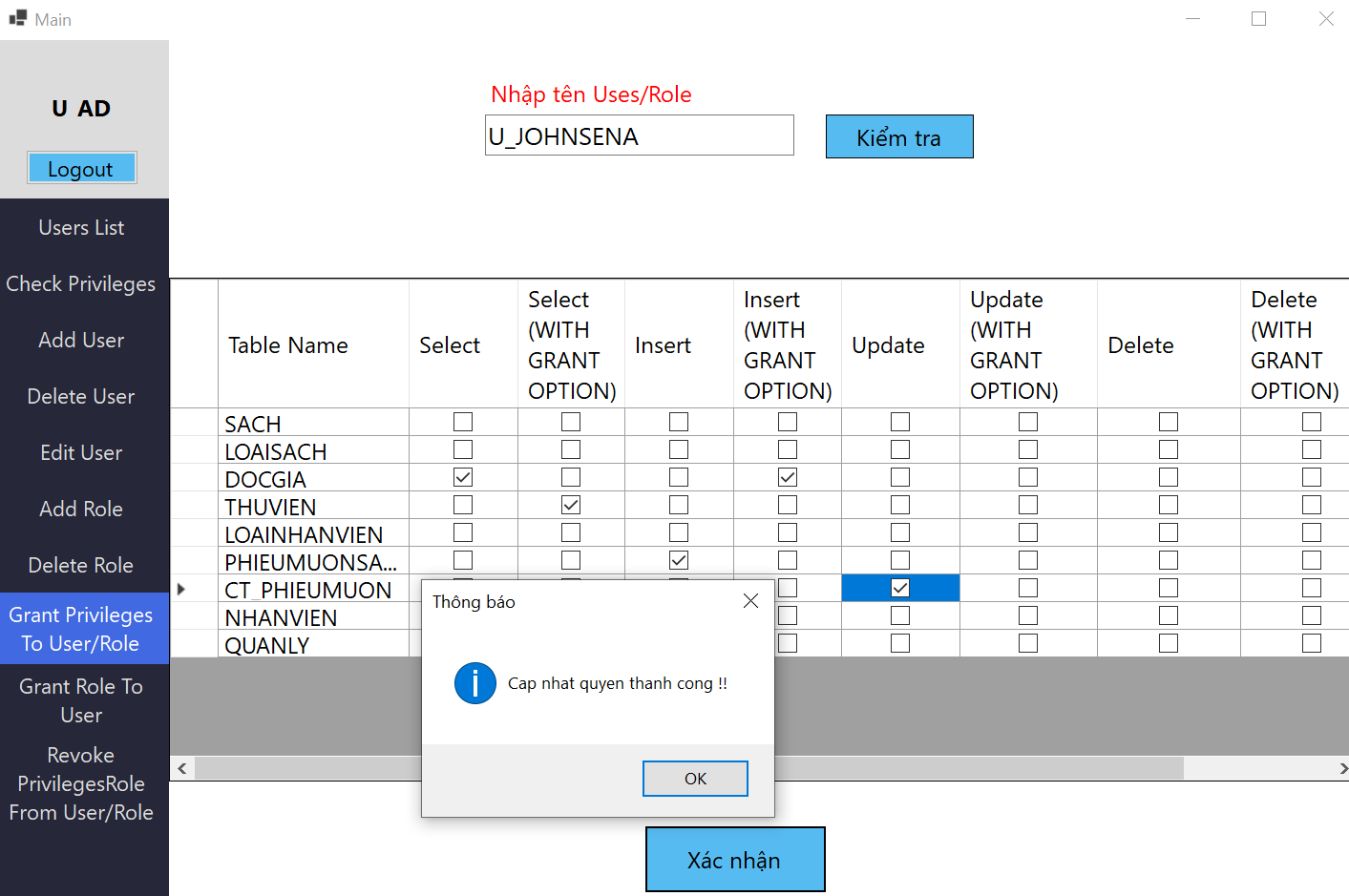
Description automatically generated

## 8/ Xoá Role:

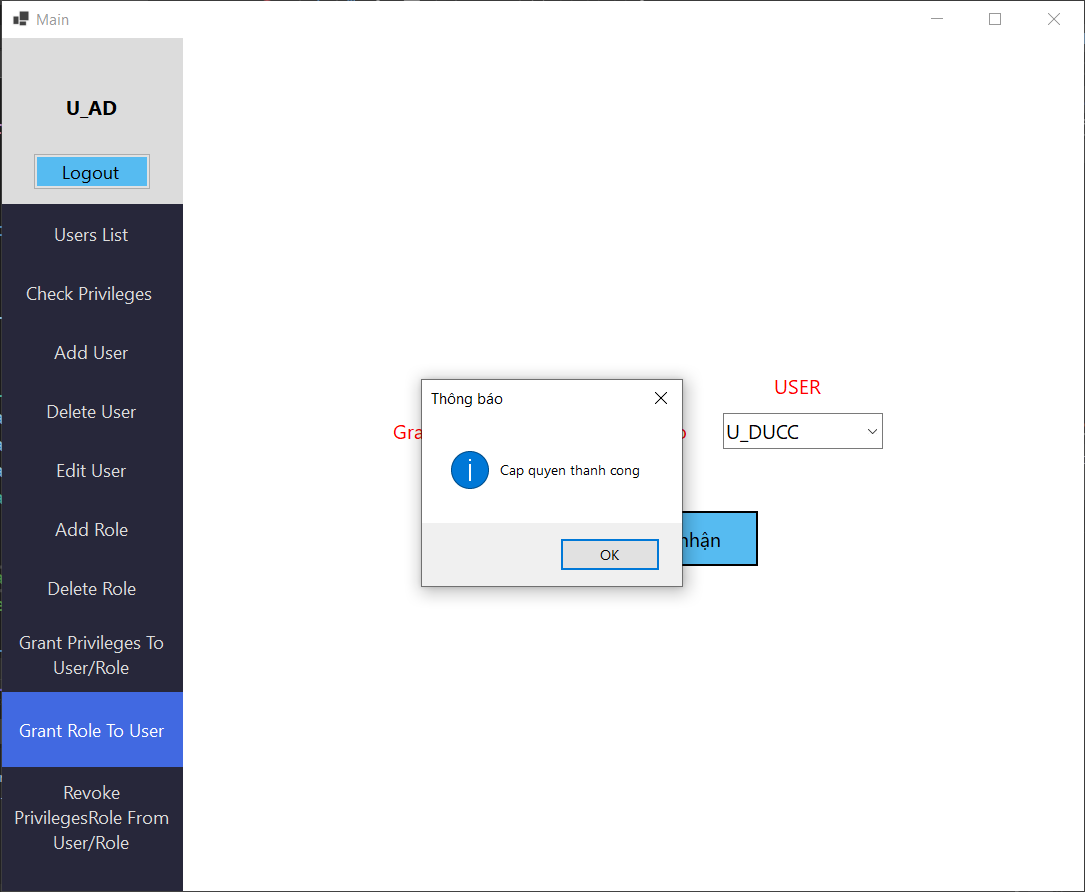
Graphical user interface

Description automatically generated

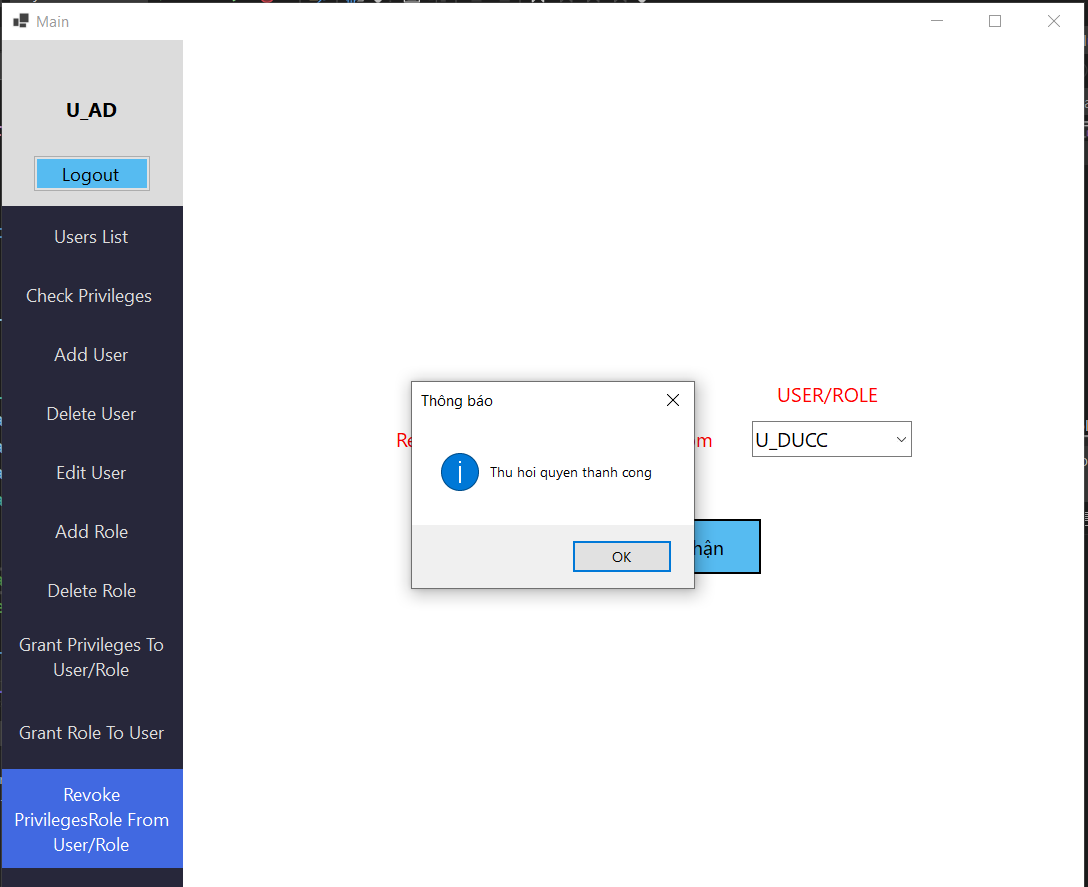
## 9/ Cấp quyền cho User/Role:



## 10/ Cấp Role cho User:



## 10/ Thu hồi Role khỏi User:



# Phân hệ 2

# I/ Mô hình cơ sở dữ liệu

Diagram

Description automatically generated

# II/ Đặc tả dữ liệu

Chú thích: Khoá chính, Khoá ngoại

|  |  |  |
| --- | --- | --- |
| CSYT | KIỂU DỮ LIỆU | Lưu trữ thông tin cơ sở y tế thuộc tỉnh/ thành phố |
| macsyt | NUMBER | Mã duy nhất của mỗi cơ sở y tế phân biệt với các cơ sở y tế khác trong cùng tỉnh/thành phố. |
| TENCSYT | NVARCHAR2(50) | Tên cơ sở y tế |
| DCCSYT | NVARCHAR2(255) | Địa chỉ của cơ sở y tế |
| SDTCSYT | VARCHAR(15) | Số điện thoại của cơ sở y tế |

|  |  |  |
| --- | --- | --- |
| benhnhan | KIỂU DỮ LIỆU | Lưu trữ thông tin mỗi bệnh nhân |
| mabn | NUMBER | Mã duy nhất của mỗi bệnh nhân dùng để phân biệt với các bệnh nhân khác trong cùng một cơ sở y tế |
| maCSYT | NUMBER | Mã cơ sở y tế |
| tenbn | NVARCHAR2(50) | Tên bệnh nhân |
| cmnd | NVARCHAR(255) | Chứng minh nhân dân của bệnh nhân |
| ngaysinh | DATE | Ngày sinh của bệnh nhân |
| sonha | NVARCHAR(50) | Số nhà của bệnh nhân |
| tenduong | NVARCHAR2(50) | Tên đường nhà của bệnh nhân |
| quanhuyen | NVARCHAR2(50) | Quận, huyện nơi ở của bệnh nhân |
| tinhtp | NVARCHAR2(50) | Tỉnh, thành phố nơi ở của bệnh nhân |
| tiensubenh | NVARCHAR2(255) | Tiền sử bệnh của bệnh nhân |
| tiensubenhgd | NVARCHAR2(255) | Tiền sử bệnh của gia đình bệnh nhân |
| diungthuoc | NVARCHAR2(255) | Dị ứng thuốc của bệnh nhân |
| username | VARCHAR(50) | Tên đăng nhập vào CSDL của bệnh nhân |

|  |  |  |
| --- | --- | --- |
| nhanvien | KIỂU DỮ LIỆU | Lưu trữ thông tin mỗi nhân viên |
| manv | NUMBER | Mã duy nhất của mỗi nhân viên dùng để phân biệt với các nhân viên khác trong cùng một tỉnh/thành phố. |
| hoten | NVARCHAR2(50) | Họ tên của nhân viên |
| phai | NVARCHAR2(3) | Giới tính của nhân viên |
| cmnd | NVARCHAR(255) | Chứng minh nhân dân của nhân viên |
| ngaysinh | DATE | Ngày sinh của nhân viên |
| quequan | NVARCHAR(50) | Quê quán của nhân viên |
| sdt | VARCHAR(15) | Số điện thoại của nhân viên |
| csyt | NUMBER | Cơ sở y tế mà nhân viên đang làm việc |
| vaitro | NUMBER | Vai trò của nhân viên. Chỉ nhận một trong các giá trị sau:  1 – Thanh tra  2 – Cơ sở y tế  3 – Y sĩ/ Bác sĩ  4 – Nghiên cứu |
| chuyenkhoa | NVARCHAR2(255) | Tên chuyên khoa mà nhân viên được cấp bằng chuyên môn |
| username | VARCHAR(50) | Tên đăng nhập vào CSDL của nhân viên |

|  |  |  |
| --- | --- | --- |
| KHOA | KIỂU DỮ LIỆU | Lưu trữ thông tin CÁC CHUYÊN KHOA |
| maKHOA | NUMBER | Mã duy nhất của mỗi chuyên khoa dùng để phân biệt với các nhân viên khác trong CSDL. |
| tenkhoa | NVARCHAR2(255) | Tên chuyên khoa |

|  |  |  |
| --- | --- | --- |
| hsba | KIỂU DỮ LIỆU | Lưu trữ thông tin CÁC hồ sơ bệnh án |
| mahsba | NUMBER | Mã duy nhất của mỗi hồ sơ bệnh án dùng để phân biệt với các hồ sơ bệnh án khác trong CSDL. |
| mabn | NUMBER | Mã bệnh nhân tiếp nhận điều trị |
| ngay | DATE | Ngày lập hồ sơ |
| chandoan | NVARCHAR2(255) | Chẩn đoán của bác sĩ |
| mabs | NUMBER | Mã bác sĩ điều trị |
| macsyt | NUMBER | Cơ sở y tế mà bệnh nhân điều trị |
| makhoa | NUMBER | Mã khoa mà bệnh nhân được tiếp đón và điều trị |
| ketluan | NVARCHAR2(255) | Kết luận của bác sĩ |

|  |  |  |
| --- | --- | --- |
| hsba\_DV | KIỂU DỮ LIỆU | Lưu trữ thông tin CÁC hồ sơ bệnh án dịch vụ đã sử dụng theo chỉ định của bác sĩ điều trị |
| mahsba | NUMBER | Mã hồ sơ bệnh án. |
| madv | NUMBER | Mã duy nhất của mỗi dịch vụ dùng để phân biệt với các dịch vụ khác trong CSDL. |
| ngay | DATE | Ngày lập hồ sơ |
| maktv | NUMBER | Mã người thực hiện dịch vụ |
| ketqua | NVARCHAR2(255) | Kết quả |

# III/ Ràng buộc toàn vẹn

* Các thuộc tính của bảng CSYT không nhận giá trị NULL.
* Các thuộc tính của bảng KHOA không nhận giá trị NULL.
* Các thuộc tính của bảng HSBA không nhận giá trị NULL.
* Các thuộc tính của bảng HSBA\_DV không nhận giá trị NULL.
* Thuộc tính VAITRO của bảng NHANVIEN chỉ nhận 1 trong 4 giá trị: 1, 2, 3, 4.

# IV/ Xác định và phân quyền các loại người dùng

Asdasdasd

# V/ Các chính sách bảo mật

## Chính sách DAC

* DAC (Direct Access Control) được sử dụng để phân quyền trên đối tượng dữ liệu cho từng người dùng khác nhau trong hệ thống thông qua các câu lệnh GRANT và REVOKE. Các quyền ở đây có thể Select, Insert, Update, Delete, Execute.
* DAC được cài đặt như sau:
  + TC2: Nhân viên có vai trò là “Thanh tra” thì sẽ được quyền truy đọc dữ liệu trên tất cả các bảng (HSBA\_DV, HSBA, NHANVIEN, BENHNHAN, KHOA, CSYT). nhưng không có quyền thêm, xoá, sửa.

## Chính sách RBAC

* RBAC (Role-based access control) là một cơ chế phân quyền cho một nhóm người dùng có quyền tương tự nhau thông qua các role và cấp các role cho người dùng.
* RBAC được cài đặt như sau:
  + TC5: Nhân viên ở vai trò “Nghiên cứu” ở mỗi cơ sở y tế, chỉ có thể xem các hồ sơ bệnh án (bảng HSBA và HSBA\_DV) được điều trị tại cùng cơ sơ y tế (với nhân viên nghiên cứu đó), tại khoa giống chuyên khoa ghi trên bằng cấp của nhân viên nghiên cứu đó.

Role Nhân viên được cấp quyền Select trên View xem hồ bệnh án.

* + asd

## Chính sách VPD

Asdasd

## Chính sách OLS

Asdasd

## Chính sách Encrypt

Asdasdasd

## Chính sách Audit