

ĐẠI HỌC KHOA HỌC TỰ NHIÊN ĐẠI HỌC QUỐC GIA TP.HCM
KHOA CÔNG NGHỆ THÔNG TIN



ĐỒ ÁN MÔN HỌC

MÔN: AN TOÀN BẢO MẬT DỮ LIỆU TRONG HTTT

Giảng viên hướng dẫn: Phạm Thị Bạch Huệ
Tiết Gia Hồng
Lương Vĩ Minh

Sinh viên thực hiện:

Nhóm 1		
MSSV	Họ tên sinh viên	Email
19120155	Huỳnh Ngọc Văn	19120155@student.hcmus.edu.vn
19120349	Lê Hùng Sơn	19120349@student.hcmus.edu.vn
19120418	Phan Công Tuấn	19120418@student.hcmus.edu.vn
19120461	Nguyễn Mạch Quan Bình	19120461@student.hcmus.edu.vn

NĂM HỌC 2021-2022

PHÂN CÔNG NHÓM 1

Công việc	SV thực hiện	Hoàn thành
Mô tả đề án, mô tả quy trình xây dựng hệ thống	Tuấn	100%
Script tạo bảng, vẽ sơ đồ ER	Văn	100%
Generate test data	Bình	100%
Phân hệ 1 - Phân tích chức năng 1, 2	Văn	100%
Phân hệ 1 - Phân tích chức năng 3, 6	Sơn	100%
Phân hệ 1 - Phân tích chức năng 4	Tuấn	100%
Phân hệ 1 - Phân tích chức năng 5, 7	Bình	100%
Thiết kế giao diện cho ứng dụng WPF	Cả nhóm	100%
Viết báo cáo	Cả nhóm	100%
Quay video demo phân hệ 1	Cả nhóm	100%
Triển khai phân hệ 1 lên ứng dụng	Cả nhóm	100%
Thanh tra + Tất cả bệnh nhân + tất cả nhân viên	Sơn	100%
Cài đặt các chính sách liên quan đến NV quản lý CSYT	Tuấn	100%
Cài đặt các chính sách liên quan đến bác sĩ	Bình	100%
Cài đặt các chính sách liên quan đến nghiên cứu	Văn	100%
Thực hiện chính sách mã hoá	Tuấn	100%
Audit	Sơn	100%
Thực hiện chính sách sử dụng OLS	Bình + Văn	100%

MỤC LỤC

I. MỤC TIÊU ĐỒ ÁN:	3
II. QUY TRÌNH XÂY DỰNG HỆ THỐNG	3
III. NỘI DUNG BÁO CÁO:.....	3
Phân hệ 1: Hệ thống dành cho quản trị viên.....	3
1. Các role/privileges được cấp cho phân hệ 1.....	3
2. Các metadata được sử dụng	4
3. Cách thực thi các chức năng của phân hệ 1	4
Phân hệ 2: Thực hiện các chính sách bảo mật cho người dùng.....	6
1. Mô hình dữ liệu quan hệ:.....	6
2. User/Role trong hệ thống.....	7
3. Phát biểu nội dung các chính sách bảo mật.....	7
4. Phân tích cách thực thi các chính sách bảo mật	8
5. Audit	12
6. Mã hoá	21
Tài liệu tham khảo:	24

I. MỤC TIÊU ĐỒ ÁN:

Xây dựng ứng dụng quản lý dữ liệu khám chữa bệnh và dữ liệu liên quan của một tỉnh/thành phố gồm 2 phân hệ:

- **Phân hệ 1:** Dành cho người quản trị người dùng và điều khiển truy cập. Tạo các user, role, cấp quyền và thu quyền, xem quyền được cấp của một đối tượng cụ thể, chỉnh sửa quyền của các nhóm đối tượng, ...
- **Phân hệ 2:** Cấp quyền truy cập cho từng đối tượng, thiết lập cơ chế, chính sách bảo mật.

II. QUY TRÌNH XÂY DỰNG HỆ THỐNG

- Xây dựng database:
 1. Tạo user admin cho hệ thống S (đặt tên là QLTT)
 2. Cấp quyền cho user QLTT
 3. Kết nối vào schema QLTT
 4. Tạo bảng và các ràng buộc toàn vẹn trên schema QLTT
 5. Tạo các trigger và procedure cần thiết
 6. Tạo các role
 7. Gán quyền cho các role
 8. Insert dữ liệu mẫu
 9. Tạo user từ dữ liệu vừa thêm
 10. Gán quyền và role cho user
- Xây dựng ứng dụng:
 1. Xây dựng giao diện
 2. Kết nối ứng dụng với database
 3. Xây dựng các chức năng

III. NỘI DUNG BÁO CÁO:

Phân hệ 1: Hệ thống dành cho quản trị viên

1. Các role/privileges được cấp cho phân hệ 1

Role/Privileges	Quyền
-----------------	-------

DBA	Là người chịu trách nhiệm quản trị và vận hành các hoạt động liên quan đến cơ sở dữ liệu như lên kế hoạch, cài đặt, cấu hình, tối ưu, backup, security, nhằm đảm bảo hệ thống luôn sẵn sàng cho người dùng truy cập.
CREATE SESSION	Cho phép user kết nối vào database
ALTER SESSION	Sử dụng câu lệnh ALTER SESSION để viết hoặc sửa đổi bất kỳ điều kiện hoặc tham số nào ảnh hưởng đến kết nối của bạn với cơ sở dữ liệu. Câu lệnh vẫn có hiệu lực cho đến khi bạn ngắt kết nối khỏi cơ sở dữ liệu.
CREATE VIEW	Tạo mới một View trong Database, hoặc thay thế nội dung của view có sẵn.
RESOURCE	Là nguồn dữ liệu mà DBA được toàn quyền sử dụng và có thể cấp cho các Role khác cùng sử dụng nhưng phạm vi hẹp hơn
UNLIMITED TABLESPACE	Cho phép mở rộng database không giới hạn

2. Các metadata được sử dụng

System Object	Chức năng
DBA_USERS	Danh sách người dùng trong hệ thống
DBA_ROLES	Danh sách role trong hệ thống
USER_TAB_PRIVS	Danh sách các quyền được gán cho user
ROLE_TAB_PRIVS	Danh sách các quyền được gán cho role
DBA_ROLE_PRIVS	Danh sách các role được gán cho đối tượng(user/role)
SESSION_ROLES	Danh sách các role của user hiện đang đăng nhập

3. Cách thực thi các chức năng của phân hệ 1

- Xem danh sách người dùng trong hệ thống:

```
SELECT * FROM DBA_USERS WHERE ACCOUNT_STATUS = 'OPEN';
```

Ngoài ra có thể sử dụng câu lệnh dưới đây để loại bỏ các system user và default user:

```
SELECT *  
FROM dba_users
```

```
WHERE created > (SELECT created FROM sys.v_$database);
```

- Xem danh sách quyền trong hệ thống:

```
SELECT * FROM DBA_ROLES;
```

- Xem thông tin quyền của mỗi user trên các đối tượng dữ liệu:

```
SELECT * FROM user_tab_privs WHERE grantee = user;
```

- Xem thông tin quyền của mỗi role trên các đối tượng dữ liệu:

```
SELECT * FROM role_tab_privs WHERE role = rolename;
```

- Tạo user mới:

```
CREATE USER username IDENTIFIED BY password;
```

- Xoá user:

```
DROP USER username;
```

- Chỉnh sửa user:

Đổi mật khẩu:

```
ALTER USER username IDENTIFIED BY new_password;
```

Lock User:

```
ALTER USER username ACCOUNT LOCK;
```

Unlock User:

```
ALTER USER username ACCOUNT UNLOCK;
```

- Tạo role mới:

```
CREATE ROLE role_name;
```

- Xoá role:

```
DROP ROLE role_name;
```

- Chỉnh sửa role: (thay đổi mật khẩu hoặc không sử dụng mật khẩu)

```
ALTER ROLE role_name {NOT IDENTIFIED/IDENTIFIED BY password}
```

- Cấp quyền cho user:

```
GRANT privilege TO username;
```

- Cấp quyền cho role:

```
GRANT privilege TO rolename;
```

- Cấp role cho user:
`GRANT role TO user;`
- Thu hồi quyền từ user
`REVOKE privilege FROM username;`
- Thu hồi quyền từ role
`REVOKE privilege FROM rolename;`

Phân hệ 2: Thực hiện các chính sách bảo mật cho người dùng

1. Mô hình dữ liệu quan hệ:

BENHNHAN(MABN, MACSYT, TENBN, CMND, NGAYSINH, SONHA, SONHA, TENDUONG, QUAN
HUYEN, TINHTP, TIENSUBENH, TIENSUBENHGD, DIUNGTHUOC)

CSYT(MACSYT, TENCST, DCCSYT, SDTCSYT)

HSBA(MAHSBA, MABN, NGAY, CHANDOAN, MABS, MAKHOA, MACSYT, KETLUAN)

NHANVIEN(MANV, HOTEN, PHAI, NGAYSINH, CMND, QUEQUAN, SDT, CSYT, VAITRO, CHUYEN
KHOA)

DICHVU(MADV, TENDV, GIADV)

HSBA_DV(MAHSBA, MADV, MAKTV, NGAY, KETQUA)

THONGBAO(MATB, NOIDUNG, THOIGIAN, DIADIEM, OLS_THONGBAO)

2. User/Role trong hệ thống

DBA tạo tài khoản cho những nhân viên trong quan hệ NHÂNVIÊN và cả những bệnh nhân trong quan hệ BỆHNHAN bằng cách sử dụng thông tin tài khoản do Hệ quản trị CSDL Oracle quản lý và liên kết tài khoản đó với người dùng tương ứng trong bảng BENHNHAN và bảng NHANVIEN đồng thời phải ép thỏa các chính sách bảo mật liên quan đến những người dùng này.

Giải pháp:

User: Tạo user bằng CMND từ bảng NHANVIEN và bảng BENHNHAN.

- Username có dạng ký tự U + CMND. VD user có CMND là 123456789 thì có username là U123456789.
- Password là ngày sinh của người đó viết dưới dạng ddMMyyyy. VD user có ngày sinh là 01/12/2001 thì password mặc định là 01122001.

Role: Ngoại trừ DBA, các nhóm người dùng trong hệ thống được chia thành 5 role, tất cả đều được cấp quyền CREATE SESSION

- BAC_SI: Những nhân viên có vai trò bác sĩ
- THANH_TRA: Những nhân viên có vai trò thanh tra
- QL_CSYT: Những nhân viên có vai trò quản lý cơ sở y tế
- NGHIEN_CUU: Những nhân viên có vai trò nghiên cứu
- BENH_NHAN: Bệnh nhân trong bảng BENHNHAN

3. Phát biểu nội dung các chính sách bảo mật

- **Chính sách 1:** Tất cả loại người dùng (trừ DBA) đều có thể xem thông tin bảng CSYT nhưng không thể thay đổi chúng
- **Chính sách 2:** Tất cả loại người dùng (trừ DBA) đều có thể xem thông tin bảng DICHVU nhưng không thể thay đổi chúng

- **Chính sách 3:** Các nhân viên thuộc sở y tế với 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.
- **Chính sách 4:** Mỗi cơ sở y tế được cấp duy nhất 01 tài khoản trên hệ thống S để thao tác trên kho dữ liệu D. Các nhân viên thuộc cơ sở y tế có quyền thêm hoặc xóa hồ sơ bệnh án và các dịch vụ (HSBA_DV) liên quan đến 1 hồ sơ bệnh án 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.
- **Chính sách 5:** 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 (BENHNHAN) khi nhập thông tin mã bệnh nhân hoặc số CMND.
- **Chính sách 6:** Nhân viên giữ 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 sở y tế (với nhân viên nghiên cứu đó), tại khoa giống chuyên khoa ghi trên bảng cấp của nhân viên nghiên cứu đó.
- **Chính sách 7:** Mỗi bệnh nhân đăng nhập chỉ có thể xem và sửa thông tin (trừ mã bệnh nhân) của chính mình.
- **Chính sách 8:** Mỗi nhân viên (trừ nhân viên giữ vai trò “Thanh tra”) đăng nhập chỉ có thể xem và sửa thông tin (trừ mã nhân viên) của chính mình.
- **Chính sách 9:** Người dùng có thể xem thông báo (trên bảng THONGBAO) dựa vào cấp bậc (*Giám đốc sở, Giám đốc cơ sở y tế và Y/ Bác sĩ*), vị trí cơ sở y tế (*trung tâm, cận trung tâm, ngoại thành*) và chuyên môn kỹ thuật cơ sở y tế (*Điều trị ngoại trú, điều trị nội trú và điều trị chuyên sâu*) của người đó.
- **Chính sách 10:** Chỉ có bác sĩ và bệnh nhân có thể xem thông tin dị ứng thuốc của bệnh nhân. Những người khác chỉ có thể xem thông tin bị mã hoá.

4. Phân tích cách thực thi các chính sách bảo mật

- **Chính sách 1:** Tất cả loại người dùng (trừ DBA) đều có thể xem thông tin bảng CSYT và bảng DICHVU nhưng không thể thay đổi chúng
Chủ thể: người dùng thuộc role THANH_TRA, BAC_SI, NGHIEN_CUU, QL_CSYT, BENH_NHAN
Quyền: SELECT
Đối tượng: bảng CSYT, bảng DICHVU
→ Sử dụng cơ chế RBAC
- **Chính sách 2:** Các nhân viên thuộc sở y tế với 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.
Chủ thể: người dùng thuộc role THANH_TRA
Quyền: SELECT
Đối tượng: bảng BENHNHAN, bảng NHANVIEN, bảng HSBA, bảng HSBA_DV
→ Sử dụng cơ chế RBAC
- **Chính sách 3:** Nhân viên quản lý cơ sở y tế có quyền thêm hoặc xóa hồ sơ bệnh án và các dịch vụ (HSBA_DV) liên quan đến 1 hồ sơ bệnh án 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.
Chủ thể: người dùng thuộc role QL_CSYT
Quyền: INSERT, DELETE
Đối tượng: bảng HSBA, bảng HSBA_DV
→ Sử dụng cơ chế RBAC, VPD
- **Chính sách 4:** Mỗi cơ sở y tế được cấp duy nhất 01 tài khoản trên hệ thống S để thao tác trên kho dữ liệu D. Các nhân viên thuộc cơ sở y tế có quyền thêm hoặc xóa hồ sơ bệnh án và các dịch vụ (HSBA_DV) liên quan đến 1 hồ sơ bệnh án 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.

Chủ thể: người dùng thuộc role QL_CSYT

Quyền: INSERT, DELETE

Đối tượng: bảng HSBA, bảng HSBA_DV

→ Sử dụng cơ chế RBAC, VPD

- **Chính sách 5:** 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 (BENHNHAN) khi nhập thông tin mã bệnh nhân hoặc số CMND.

Xem Hồ Sơ Bệnh Án

Chủ thể: người dùng thuộc role BAC_SI

Quyền: SELECT

Đối tượng: HSBA, HSBA_DV

→ Tạo view **V_CT_HSBA** xem thông tin những hồ sơ bệnh án họ đã chữa trị và kết quả dịch vụ họ đã sử dụng nhưng không có quyền chỉnh sửa

→ Sử dụng cơ chế RBAC, VPD

Xem Hồ Sơ Bệnh Nhân

Chủ thể: người dùng thuộc role BAC_SI

Quyền: SELECT

Đối tượng: BENHNHAN

→ Sử dụng cơ chế RBAC

- **Chính sách 6:** Nhân viên giữ 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 sở y tế (với nhân viên nghiên cứu đó), tại khoa giống chuyên khoa ghi trên bằng cấp của nhân viên nghiên cứu đó.

Xem Hồ Sơ Bệnh Án

Chủ thể: người dùng thuộc role NGHIEN_CUU

Quyền: SELECT

Đối tượng: HSBA, HSBA_DV

→ Sử dụng view **V_CT_HSBA** xem những hồ sơ bệnh án và kết quả của những dịch vụ có cùng cơ sở y tế và có khoa giống với khoa ghi trên bằng cấp của nhân viên nghiên cứu đó

→ Sử dụng cơ chế RBAC, VPD

- **Chính sách 7:** Mỗi bệnh nhân đăng nhập chỉ có thể xem và sửa thông tin (trừ mã bệnh nhân) của chính mình.

Chủ thể: người dùng thuộc role BENH_NHAN

Quyền: SELECT, UPDATE

Đối tượng: BENHNHAN

→ Sử dụng cơ chế RBAC, VPD

- **Chính sách 8:** Mỗi nhân viên (trừ nhân viên giữ vai trò “Thanh tra”) đăng nhập chỉ có thể xem và sửa thông tin (trừ mã nhân viên) của chính mình.

Chủ thể: người dùng thuộc role THANH TRA

Quyền: SELECT, UPDATE

Đối tượng: NHANVIEN

→ Sử dụng cơ chế RBAC, VPD

- **Chính sách 9:** Người dùng có thể xem thông báo (trên bảng THONGBAO) dựa vào cấp bậc (*Giám đốc sở, Giám đốc cơ sở y tế và Y/ Bác sĩ*), vị trí cơ sở y tế (*trung tâm, cận trung tâm, ngoại thành*) và chuyên môn kỹ thuật cơ sở y tế (*Điều trị ngoại trú, điều trị nội trú và điều trị chuyên sâu*) của người đó.

Chủ thể: người dùng thuộc role BAC_SI, QL_CSYT, THANH_TRA

NGHIEN_CUU

Quyền: SELECT

Đối tượng: THONGBAO

→ Sử dụng cơ chế OLS

- **Chính sách 10:** Chỉ có bác sĩ và bệnh nhân có thể xem thông tin dị ứng thuốc của bệnh nhân. Những người khác chỉ có thể xem thông tin bị mã hoá.

5. Audit

Khái niệm: Audit là hoạt động theo dõi và ghi lại nhật ký các hoạt động, thao tác của người dùng trên cơ sở dữ liệu

Ngữ cảnh: Check nhật ký các hoạt động liên quan đến **thêm/xóa/sửa/chọn** trên tất cả các bảng thuộc lược đồ cơ sở dữ liệu

Mục đích của việc auditing: Auditing cho phép ta bắt các user phải có trách nhiệm về hành động mà họ thực hiện, bằng cách theo dõi hành vi của họ.

- Dữ liệu audit giúp phát hiện lỗi hổng trong chính sách bảo mật.
- Liên quan đến trách nhiệm giải trình của user. Cần phải đảm bảo rằng user chỉ được thực hiện những gì họ được phép. Ghi nhận sự lạm quyền hoặc dùng sai quyền.
- Auditing để ghi nhận lại những gì đã xảy ra và có hồi đáp thích hợp.
- Không thực hiện auditing ta sẽ không thể biết khía cạnh bảo mật của hệ thống có đảm bảo hay không hay có ai đã đọc hoặc cập nhật dữ liệu một cách bất hợp pháp hay không.
- Việc auditing hiệu quả khi: Có kế hoạch thực hiện auditing. Đọc lại và phân tích dữ liệu của quá trình auditing.
- Tuy nhiên:

- Auditing tất cả các hành động của tất cả các user trên tất cả dữ liệu sẽ không có ích mà còn làm chậm hệ thống, và dữ liệu có được từ quá trình audit khó sử dụng.
- Audit một cách có chọn lọc và đúng đắn, dựa trên dữ liệu, xử lý và người dùng có thật.

- Script thực hiện:

Đầu tiên ta kiểm tra xem đã bật Audit hay chưa

```
SQL*Plus: Release 18.0.0.0.0 - Production on Wed Jun 29 20:48:11 2022
Version 18.4.0.0.0

Copyright (c) 1982, 2018, Oracle. All rights reserved.

Enter user-name: / as sysdba

Connected to:
Oracle Database 18c Express Edition Release 18.0.0.0.0 - Production
Version 18.4.0.0.0

SQL> show parameter audit
```

NAME	TYPE	VALUE
audit_file_dest	string	C:\APP\HUNGSON\PRODUCT\18.0.0\ADMIN\XE\ADUMP
audit_sys_operations	boolean	TRUE
audit_trail	string	NONE
unified_audit_sga_queue_size	integer	1048576
unified_audit_systemlog	boolean	FALSE

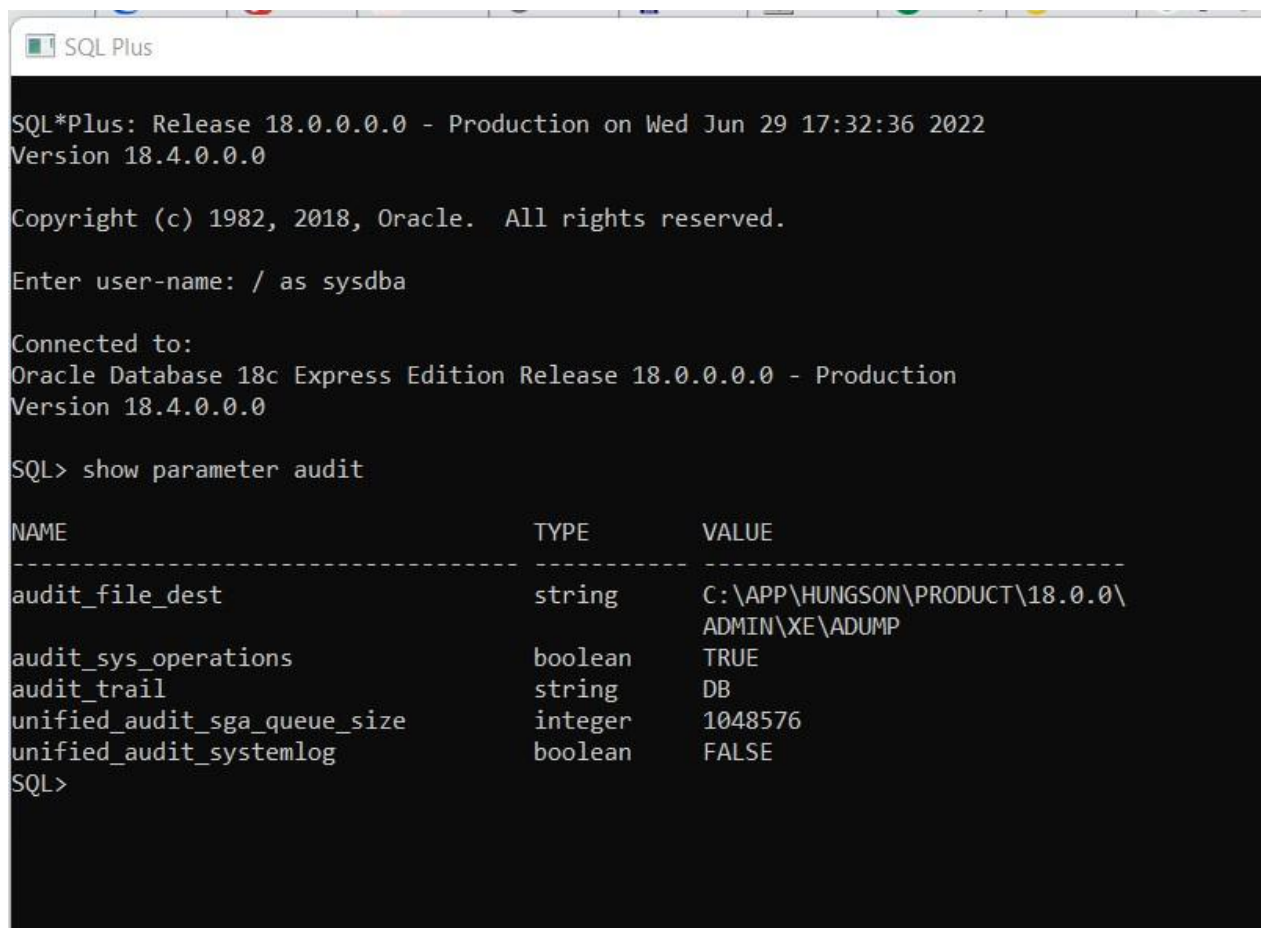
```
SQL>
```

Audit_trail là NONE tức là audit chưa được bật

Kích hoạt chức năng giám sát:

```
--Kích hoạt việc ghi nhật ký toàn hệ thống.
-- enable audit
alter system set audit_trail=DB scope=spfile;
```

Đã kích hoạt thành công



```
SQL*Plus: Release 18.0.0.0.0 - Production on Wed Jun 29 17:32:36 2022
Version 18.4.0.0.0

Copyright (c) 1982, 2018, Oracle. All rights reserved.

Enter user-name: / as sysdba

Connected to:
Oracle Database 18c Express Edition Release 18.0.0.0.0 - Production
Version 18.4.0.0.0

SQL> show parameter audit
```

NAME	TYPE	VALUE
audit_file_dest	string	C:\APP\HUNGSON\PRODUCT\18.0.0\ADMIN\XE\ADUMP
audit_sys_operations	boolean	TRUE
audit_trail	string	DB
unified_audit_sga_queue_size	integer	1048576
unified_audit_systemlog	boolean	FALSE

```
SQL>
```

Audit_trail là DB tức là đã kích hoạt giám sát trên toàn hệ thống

Giám sát mọi câu lệnh thêm/xóa/sửa/chọn trên các bảng:


```
--Giám sát việc thêm xóa sửa trên bảng bệnh nhân, hồ sơ bệnh án
audit select,insert,update, delete on QLTT.BENHNHAN by access;
audit select,insert,update, delete on QLTT.HSBA by access;
```

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

Sẽ giám sát tất cả hồ sơ bệnh án mà có mã dịch vụ là 4 , vì ở đây giá cao nhất, được nhiều người quan tâm

```
-- GIÁM SÁT TẤT CẢ HỒ SƠ BỆNH ÁN DỊCH VỤ MÀ CÓ MÃ DỊCH VỤ =4
-- FGA
--VÌ Ở ĐÂY DỊCH VỤ 4 LÀ KHÁM TỔNG QUÁT , GIÁ CAO , ĐƯỢC NHIỀU NGƯỜI QUAN TÂM NÊN TA GIÁM SÁT
BEGIN
  DBMS_FGA.add_policy(
    object_schema => 'QLTT',
    object_name   => 'HSBA_DV',
    policy_name   => 'FGA_HSBA_DV',
    AUDIT_CONDITION => 'MADV=4',
    statement_types => 'SELECT, INSERT,UPDATE,DELETE'
  );
END;
```

Sẽ giám sát những ai update cột giá trong bảng dịch vụ

```
-- MỖI KHI CÓ AI UPDATE CỘT GIÁ TRONG BẢNG DỊCH VỤ , HỆ THỐNG SẼ GHI NHẬN LẠI
BEGIN
  DBMS_FGA.add_policy(
    object_schema => 'QLTT',
    object_name   => 'DICHVU',
    policy_name   => 'FGA_DICHVU_UPDATEGIA',
    statement_types => 'UPDATE',
    audit_column => 'GIADV'
  );
END;
```

Kiểm tra dữ liệu đã ghi nhận:

```
----Kiểm tra kết quả Audit:Kiểm tra dữ liệu nhật ký hệ thống.
SELECT username,extended_timestamp,obj_name,action_name FROM dba_audit_trail;
```


→ Kết quả Audit:

```

----Kiểm tra kết quả Audit:Kiểm tra dữ liệu nhật ký hệ thống.
SELECT username,extended_timestamp,obj_name,action_name FROM dba_audit_trail;

```

USERNAME VARCHAR2(128)	EXTENDED_TIMESTAMP TIMESTAMP(6) WITH TIME ZONE	OBJ_NAME VARCHAR2(128)	ACTION_NAME VARCHAR2(28)
QLTT	6/21/2022 2:29:29 PM +07:00	BENHNHAN	SELECT
THANHTRA1	6/21/2022 2:35:25 PM +07:00	HSBA_DV	SELECT

6. Oracle Label Security (OLS)

Khái niệm:

Oracle Label Security (OLS) là một sản phẩm được thực hiện dựa trên nền tảng Virtual Private Database (VPD), cho phép các nhà quản trị điều khiển truy xuất dữ liệu ở mức hàng (row-level) một cách tiện lợi và dễ dàng hơn. Nó điều khiển truy xuất nội dung của các dòng dữ liệu bằng cách so sánh nhãn của hàng dữ liệu với nhãn và quyền của user.

Các nhà quản trị có thể dễ dàng tạo thêm các chính sách kiểm soát việc truy xuất các hàng dữ liệu cho các CSDL bằng giao diện đồ họa là Oracle Policy Manager hoặc các packages được xây dựng sẵn - có 6 package:

- SA_SYSDBA: tạo, thay đổi, xóa các chính sách
- SA_COMPONENTS: định nghĩa và quản lý các thành phần của nhãn
- SA_LABEL_ADMIN: thực hiện các thao tác quản trị chính sách, nhãn
- SA_POLICY_ADMIN: áp dụng chính sách cho bảng và schema
- SA_USER_ADMIN: quản lý việc cấp phát quyền truy xuất và quy định mức độ tin cậy cho các user liên quan
- SA_AUDIT_ADMIN: thiết lập các tùy chọn cho các tác vụ quản trị việc audit

Trong OLS, ta dùng các chính sách để quản lý truy xuất. Đối với mỗi chính sách, ta cần định ra một tập nhãn để phân lớp dữ liệu từ cao xuống thấp dựa theo mức độ nhạy cảm của dữ liệu. Sau đó ta áp dụng các chính sách lên các bảng hoặc schema mà mình mong muốn bảo vệ. Mỗi khi một người dùng muốn truy xuất một hàng dữ liệu nào đó, hệ thống sẽ so sánh nhãn của người dùng (user label) tại thời điểm đó với nhãn dữ liệu để quyết định có cho phép truy xuất hay không

Quy trình thực hiện OLS gồm 5 bước:

- Tạo chính sách OLS
- Định nghĩa các thành phần một nhãn thuộc chính sách trên có thể có
- Tạo các nhãn dữ liệu thật sự mà bạn muốn dùng
- Gán chính sách trên bảng cho các bảng hoặc schema muốn bảo vệ
- Gán các giới hạn quyền, các nhãn người dùng hoặc các quyền truy xuất đặc biệt cho những người dùng liên quan

Cách thực hiện:

B1. Tạo policy

```
--Tạo policy  
EXECUTE SA_SYSDBA.CREATE_POLICY('OLS_SO_YTE', 'OLS_THONGBAO', 'NO_CONTROL');  
--EXEC SA_SYSDBA.DROP_POLICY ('OLS_SO_YTE', TRUE);
```

Ngữ cảnh: Khi có thông báo từ cấp trên thì tùy vào mức độ quan trọng của thông báo qui định thông tin mà mỗi nhân viên được xem.

B2. Định nghĩa thành phần của nhãn

Dựa vào phân chia vai trò người dùng chia theo 3 cấp bậc Giám đốc sở, Giám đốc Sở Y Tế, Y/Bác sĩ → Chia theo 3 level GDS, GDCSYT, Y_BACSI

```
--Tạo level theo 3 cấp bậc theo mức độ quan trọng từ thấp đến cao: Y/Bác sĩ, Giám đốc cơ sở y tế, Giám đốc sở  
EXEC SA_COMPONENTS.CREATE_LEVEL('OLS_SO_YTE', 300, 'GDS', 'GIAM DOC SO');  
EXEC SA_COMPONENTS.CREATE_LEVEL('OLS_SO_YTE', 200, 'GDCSYT', 'GIAM DOC CO SO Y TE');  
EXEC SA_COMPONENTS.CREATE_LEVEL('OLS_SO_YTE', 100, 'BS', 'Y_BAC SI');
```

Dựa vào chuyên môn, kỹ thuật mà sở y tế chia các cơ sở y tế theo các tuyến: Điều trị ngoại trú, điều trị nội trú, điều trị chuyên sâu → Chia theo 3 compartment DT_CT, DT_NGT, DT_NT

```
] --Chia theo trình độ chuyên môn, tạo 3 compartment gồm điều trị ngoại trú, điều trị nội trú, điều trị chuyên sâu
--Tạo Compartment
--EXEC SA_COMPONENTS.DROP_COMPARTMENT('OLS_SO_YTE',50);
EXEC SA_COMPONENTS.CREATE_COMPARTMENT('OLS_SO_YTE',50,'DT_CS','DIEU TRI CHUYEN SAU');
--EXEC SA_COMPONENTS.DROP_COMPARTMENT('OLS_SO_YTE',100);
EXEC SA_COMPONENTS.CREATE_COMPARTMENT('OLS_SO_YTE',100,'DT_NT','DIEU TRI NOI TRU');
--EXEC SA_COMPONENTS.DROP_COMPARTMENT('OLS_SO_YTE',150);
EXEC SA_COMPONENTS.CREATE_COMPARTMENT('OLS_SO_YTE',150,'DT_NGT','DIEU TRI NGOAI TRU');
```

Dựa vào vị trí địa lý, chia cơ sở y tế theo 3 vùng trung tâm, cận trung tâm, ngoại thành → Chia theo 3 group TT, CTT, NT

```
] --Chia theo vị trí địa lý, tạo 3 group gồm trung tâm, cận trung tâm, ngoại trú
--Định nghĩa Group
--EXEC SA_COMPONENTS.DROP_GROUP('OLS_SO_YTE',110);
EXEC SA_COMPONENTS.CREATE_GROUP('OLS_SO_YTE',110,'TT','TRUNG TAM');
--EXEC SA_COMPONENTS.DROP_GROUP('OLS_SO_YTE',90);
EXEC SA_COMPONENTS.CREATE_GROUP('OLS_SO_YTE',90,'CTT','CAN TRUNG TAM');
--EXEC SA_COMPONENTS.DROP_GROUP('OLS_SO_YTE',70);
EXEC SA_COMPONENTS.CREATE_GROUP('OLS_SO_YTE',70,'NT','NGOAI THANH');
```

B3. Thực hiện gán nhãn cho dữ liệu

```
--Cap GDS
--Nhãn dữ liệu ở level tối quan trọng--Giám đốc sở
EXECUTE SA_LABEL_ADMIN.CREATE_LABEL('OLS_SO_YTE',40000,'GDS');

--Cap GDCSYT, Cấp này gồm 1 người dùng
--Điều trị chuyên sâu (Quản lý cơ sở y tế chuyên sâu xem)
--Để xem những thông tin mật chỉ dành riêng cho các cơ sở điều trị chuyên sâu
EXECUTE SA_LABEL_ADMIN.CREATE_LABEL('OLS_SO_YTE',31030,'GDCSYT:DT_CS:TT');
EXECUTE SA_LABEL_ADMIN.CREATE_LABEL('OLS_SO_YTE',31020,'GDCSYT:DT_CS:CTT');
EXECUTE SA_LABEL_ADMIN.CREATE_LABEL('OLS_SO_YTE',31010,'GDCSYT:DT_CS:NT');
```

```
--Cấp BS, Cấp này gồm 3 người dùng
--Để xem thông báo chung dành cho các cơ sở y tế
--Điều trị chuyên sâu
EXECUTE SA_LABEL_ADMIN.CREATE_LABEL('OLS_SO_YTE',24030,'BS:DT_CS:TT');
EXECUTE SA_LABEL_ADMIN.CREATE_LABEL('OLS_SO_YTE',24020,'BS:DT_CS:CTT');
EXECUTE SA_LABEL_ADMIN.CREATE_LABEL('OLS_SO_YTE',24010,'BS:DT_CS:NT');
--Điều trị nội trú
EXECUTE SA_LABEL_ADMIN.CREATE_LABEL('OLS_SO_YTE',23030,'BS:DT_NT:TT');
EXECUTE SA_LABEL_ADMIN.CREATE_LABEL('OLS_SO_YTE',23020,'BS:DT_NT:CTT');
EXECUTE SA_LABEL_ADMIN.CREATE_LABEL('OLS_SO_YTE',23010,'BS:DT_NT:NT');
--Điều trị ngoại trú
EXECUTE SA_LABEL_ADMIN.CREATE_LABEL('OLS_SO_YTE',22030,'BS:DT_NGT:TT');
EXECUTE SA_LABEL_ADMIN.CREATE_LABEL('OLS_SO_YTE',22020,'BS:DT_NGT:CTT');
EXECUTE SA_LABEL_ADMIN.CREATE_LABEL('OLS_SO_YTE',22010,'BS:DT_NGT:NT');

--Nhan dung chung cho toan nhan vien o trung tam, can trung tam, ngoai thanh
EXECUTE SA_LABEL_ADMIN.CREATE_LABEL('OLS_SO_YTE',10030,'BS::TT');
EXECUTE SA_LABEL_ADMIN.CREATE_LABEL('OLS_SO_YTE',10020,'BS::CTT');
EXECUTE SA_LABEL_ADMIN.CREATE_LABEL('OLS_SO_YTE',10010,'BS::NT');
```

B4. Áp dụng policy thực thi OLS lên bảng Thông Báo

```
BEGIN
SA_POLICY_ADMIN.APPLY_TABLE_POLICY(
POLICY_NAME => 'OLS_SO_YTE',
SCHEMA_NAME => 'QLTT',
TABLE_NAME => 'THONGBAO',
TABLE_OPTIONS => NULL);
END;
```

B5. Cập nhật lại nhãn dữ liệu cho các dòng của bảng Thông Báo

```
UPDATE THONGBAO SET OLS_THONGBAO=CHAR_TO_LABEL('OLS_SO_YTE','GDS') WHERE MATB=1;
UPDATE THONGBAO SET OLS_THONGBAO=CHAR_TO_LABEL('OLS_SO_YTE','GDCSYT:DT_CS:TT') WHERE MATB=2; --
UPDATE THONGBAO SET OLS_THONGBAO=CHAR_TO_LABEL('OLS_SO_YTE','GDCSYT:DT_CS:CTT') WHERE MATB=3;
```

Bỏ chính sách thực thi OLS lên bảng Thông Báo và áp dụng policy thực thi OLS mới đầy đủ hơn

```
--policy moi
BEGIN SA_POLICY_ADMIN.APPLY_TABLE_POLICY(
POLICY_NAME => 'OLS_SO_YTE',
SCHEMA_NAME => 'QLTT',
TABLE_NAME => 'THONGBAO',
TABLE_OPTIONS => 'READ_CONTROL,WRITE_CONTROL,CHECK_CONTROL');
```

B6. Gán nhãn cho người dùng

Kịch bản:

Khu vực: Trung tâm, cận trung tâm, ngoại thành

- Thanh Tra xem được tất cả thông tin bao gồm thông tin mật khu vực mà mình phụ trách. Ví dụ: Thanh tra ở khu vực cận trung tâm có username là U232630930

```
--Thanh Tra xem được tất cả thông báo chung ,thông báo riêng dành cho các cơ sở điều trị chuyên sâu của khu vực
--Ví dụ:Thanh tra ở khu vực cận trung tâm
BEGIN
SA_USER_ADMIN.SET_USER_LABELS(
  policy_name => 'OLS_SO_YTE',
  user_name => 'U232630930',
  MAX_READ_LABEL => 'GDCSYT:DT_CS,DT_NT,DT_NGT:CTT',
  MAX_WRITE_LABEL => 'GDCSYT:DT_CS,DT_NT,DT_NGT:CTT');
END;
```

- Y,bác sĩ,nguyên cứu sinh xem được thông báo chung của các cơ sở y tế cùng cấp với cơ sở y tế mà họ đang phục vụ. Ví dụ: Bác sĩ của thuộc cơ sở y tế điều trị ngoại trú khu vực ngoại thành có username là U868387298

```
--Y/Bác sĩ/Nghiên cứu sinh xem được các thông báo chung của cơ sở y tế cùng cấp với cơ sở y tế họ đang thực hiện nhiệm vụ
--Ví dụ:Bác sĩ thuộc cơ sở y tế điều trị ngoại trú khu vực ngoại thành
BEGIN
SA_USER_ADMIN.SET_USER_LABELS(
  policy_name => 'OLS_SO_YTE',
  user_name => 'U868387298',
  MAX_READ_LABEL => 'BS:DT_NGT:NT',
  MAX_WRITE_LABEL => 'BS:DT_NGT:NT');
END;
```

- Quản lý cơ sở y tế điều trị chuyên sâu xem được tất cả thông báo chung các cơ sở y tế cùng khu vực và thông báo mật dành riêng cho các cơ sở y tế chuyên sâu của khu vực.Ví dụ: Quản lý cơ sở y tế của cơ sở y tế điều trị chuyên sâu khu vực trung tâm có username = U231353133

```
--Quản lý cơ sở y tế điều trị chuyên sâu xem được các thông báo chung của các cơ sở y tế ngoại trú, nội trú thuộc cùng khu vực và thông báo
--quan trọng chỉ dành riêng cho cơ sở y tế điều trị chuyên sâu của khu vực
--Ví dụ:Quản lý cơ sở y tế của cơ sở y tế điều trị chuyên sâu khu vực trung tâm
BEGIN
SA_USER_ADMIN.SET_USER_LABELS(
  policy_name => 'OLS_SO_YTE',
  user_name => 'U231353133',
  MAX_READ_LABEL => 'GDCSYT:DT_CS,DT_NT,DT_NGT:TT',
  MAX_WRITE_LABEL => 'GDCSYT:DT_CS,DT_NT,DT_NGT:TT');
END;
```

- Quản lý cơ sở y tế nội trú xem được các thông báo chung của các cơ sở y tế nội trú, ngoại trú cùng khu vực. Ví dụ: Quản lý cơ sở y tế điều trị nội trú khu vực trung tâm có user = U312457842

```
--Quản lý cơ sở y tế điều trị nội trú xem được các thông báo chung của các cơ sở y tế ngoại trú, nội trú thuộc cùng khu vực
--Ví dụ: Quản lý cơ sở y tế điều trị nội trú khu vực trung tâm
BEGIN
SA_USER_ADMIN.SET_USER_LABELS(
policy_name => 'OLS_SO_YTE',
user_name => 'U312457842',
MAX_READ_LABEL => 'BS:DT_NT,DT_NGT:TT',
MAX_WRITE_LABEL => 'BS:DT_NT,DT_NGT:TT');
END;
```

- Quản lý cơ sở y tế ngoại trú xem được thông báo chung của các cơ sở y tế ngoại trú cùng khu vực. Ví dụ: Quản lý cơ sở y tế ngoại trú có user = U251186655

```
--Quản lý cơ sở y tế ngoại trú xem được thông báo chung của các cơ sở y tế ngoại trú cùng khu vực
--Ví dụ: Quản lý cơ sở y tế ngoại trú khu vực ngoại thành sẽ xem được thông tin chung của các cơ sở y tế ngoại trú khác ở khu vực ngoại thành
BEGIN
SA_USER_ADMIN.SET_USER_LABELS(
policy_name => 'OLS_SO_YTE',
user_name => 'U251186655',
MAX_READ_LABEL => 'BS:DT_NGT:NT',
MAX_WRITE_LABEL => 'BS:DT_NGT:NT');
END;
```

6. Mã hoá

- **Khái niệm**: Mã hóa là quá trình biến đổi dữ liệu từ dạng văn bản bình thường sang dạng mã (không có nghĩa). Từ dạng mã muốn chuyển về cần phải giải mã

- **Ngữ cảnh**: Chỉ có các đối tượng được cấp quyền mới xem thông tin dị ứng thuốc của bệnh nhân

- **Cách thực hiện**

- Tạo package Encrypt_Decrypt gồm 2 function thực hiện mã hoá và giải mã dữ liệu truyền vào
- Tạo trigger tự động mã hoá khi thêm BENHNNHAN hoặc cập nhật DIUNGTHUOC
- Gán quyền thực thi package cho những đối tượng được phép xem thông tin dị ứng thuốc của bệnh nhân.


```

----- MÃ HOÁ -----
-- Mã hoá thông tin dị ứng thuốc của bệnh nhân, sử dụng key mã hoá là cmdnd
grant execute on dbms_crypto TO QLTT;
-- Tạo package hỗ trợ mã hoá - giải mã
CREATE OR REPLACE PACKAGE ENCRYPT_DECRYPT
AS
    FUNCTION ENCRYPT_BENHNHAN(p_in IN NVARCHAR2,p_key IN CHAR)
        RETURN RAW DETERMINISTIC;
    FUNCTION DECRYPT_BENHNHAN(p_in IN RAW,p_key IN CHAR)
        RETURN NVARCHAR2 DETERMINISTIC;
END ENCRYPT_DECRYPT;
/
-- Cài đặt các function trong package trên
CREATE OR REPLACE PACKAGE BODY ENCRYPT_DECRYPT
IS
    encryption_type PLS_INTEGER :=
        DBMS_CRYPTO.ENCRYPT_DES
        +DBMS_CRYPTO.CHAIN_CBC
        +DBMS_CRYPTO.PAD_PKCS5;

    FUNCTION ENCRYPT_BENHNHAN(p_in IN NVARCHAR2,p_key IN CHAR)
        RETURN RAW DETERMINISTIC
    IS
        encrypted_raw RAW(2000);
    BEGIN

```

```

    FUNCTION ENCRYPT_BENHNHAN(p_in IN NVARCHAR2,p_key IN CHAR)
        RETURN RAW DETERMINISTIC
    IS
        encrypted_raw RAW(2000);
    BEGIN
        encrypted_raw := dbms_crypto.encrypt(
            src => utl_raw.cast_to_raw(p_in),
            typ => encryption_type,
            key => utl_raw.cast_to_raw(p_key)
        );
        RETURN encrypted_raw;
    END ENCRYPT_BENHNHAN;

    FUNCTION DECRYPT_BENHNHAN(p_in IN RAW,p_key IN CHAR)
        RETURN NVARCHAR2 DETERMINISTIC
    IS
        decrypted_raw raw(2000);
    BEGIN
        decrypted_raw := dbms_crypto.decrypt(
            src => p_in,
            typ => encryption_type,
            key => utl_raw.cast_to_raw(p_key)
        );
        return utl_raw.CAST_TO_NVARCHAR2(decrypted_raw);
    END DECRYPT_BENHNHAN;
END ENCRYPT_DECRYPT;
/

```

Kết quả mã hoá:

81
82

```
SELECT MABN,DIUNGTHUOC FROM BENHNHAN b;
```

MABN NUMBER(38)	DIUNGTHUOC NVARCHAR2(100)
1	692ECBD033F759B7723F172440085433F38BB0B162DD8F1FCD83440F78BEC0C0
2	(null)
3	731F38A5C1866236850A45AFA27DD1BE0BA1929016843153
4	E11FCF1040763A9AE3AFCA01D2A09E15B67AAF5169BA2D4B168AD1EF943B68D6
5	(null)
6	CCCAC19214DF2F489F0AD6C01D901CCD82CE26D160DDA1D4
7	(null)
8	D6E0CEE05D278FC1F261F42077D308A4040A7E2FC9732053
9	9BCCE22CD62415B196D2608DE8F3D6A521419FE493FCAEA1C39BA8099A28A3C6

Cấp quyền mã hoá và giải mã thông tin bệnh nhân cho bác sĩ và bệnh nhân

```
-- Cấp quyền mã hoá, giải mã thông tin bệnh nhân cho bác sĩ, bệnh nhân
GRANT EXECUTE ON QLTT.ENCRYPT_DECRYPT TO BAC_SI;
GRANT EXECUTE ON QLTT.ENCRYPT_DECRYPT TO BENH_NHAN;
```

Xem thông tin dị ứng thuốc được giải mã

TENBN NVARCHAR2(30)	DIUNGTHUOC NVARCHAR2(100)	DIUNGTHUOC_GIAMA NVARCHAR2(2000)
Letha Bolt	692ECBD033F759B7723F172440085433F38BB0B162DD8F1FCD83440F78BEC0C0	Veniatracose
Vanita Kelleher	(null)	(null)
Marcos Abraham	731F38A5C1866236850A45AFA27DD1BE0BA1929016843153	Acotaphane
Miyoko McKinney	E11FCF1040763A9AE3AFCA01D2A09E15B67AAF5169BA2D4B168AD1EF943B68D6	Xylobutamvant
Adolph Francisco	(null)	(null)
Oma Lawler	CCCAC19214DF2F489F0AD6C01D901CCD82CE26D160DDA1D4	Medfatex
Felix Alba	(null)	(null)
Eusebia Noland	D6E0CEE05D278FC1F261F42077D308A4040A7E2FC9732053	Alfinaxol
Denisha McGinnis	9BCCE22CD62415B196D2608DE8F3D6A521419FE493FCAEA1C39BA8099A28A3C6	Etothromytex
Stanford Sullivan	4B782C7712A0A248F64EF21D70655500F651C218F5687915	Lefusinal
Nathan Salisbury	(null)	(null)
Burton Bunnell	3415110CC1FA972B10CDE0BCC3841F9118368EA144A940BC	Acafacept

Ta đang đăng nhập với user U868387298 là 1 bác sĩ và có thể coi được dị ứng thuốc được mã hoá

Tài liệu tham khảo:

- ❖ Các slide lý thuyết + thực hành môn ATBM trong HTTT của trường ĐH KHTN
- ❖ <https://docs.oracle.com/>
- ❖ <https://www.tranvanbinh.vn/search/label/H%E1%BB%8Dc%20Oracle%20Database%20t%E1%BB%AB%20A-Z>
- ❖ <https://openplanning.net/11309/oracle-standard-database-auditing>
- ❖ <https://developernote.com/2020/01/oracle-database-19c-auditing-with-multitenant-architecture/>