Sinh viên thực hiện:

18127022 - Phạm Ngọc Thuỳ Trang

18127215 - Quách Phú Thành

18127257 - Trần Huy Vũ

GV phụ trách: Cô Phạm Thị Bạch Huệ - Thầy Lương Vĩ Minh – Cô Tiết Gia Hồng

bài tập Môn học  - AN TOÀN VÀ BẢO MẬT DỮ LIỆU TRONG HTTT

HỌC KỲ II – NĂM HỌC 2021-2022

**môn AN TOÀN VÀ BẢO MẬT DỮ LIỆU TRONG HTTT**

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

**ĐẠI HỌC KHOA HỌC TỰ NHIÊN THÀNH PHỐ HỒ CHÍ MINH, ĐẠI HỌC QUỐC GIA TP HCM**

# BẢNG THÔNG TIN CHI TIẾT CÁ NHÂN

|  |  |  |  |
| --- | --- | --- | --- |
| MSSV | Họ tên | Email | Điện thoại |
| 18127022 | Phạm Ngọc Thùy Trang | [18127022@student.hcmus.edu.vn](mailto:18127022@student.hcmus.edu.vn) |  |
| 18127215 | Quách Phú Thành | [18127215@student.hcmus.edu.vn](mailto:18127215@student.hcmus.edu.vn) |  |
| 18127257 | Trần Huy Vũ | [18127257@student.hcmus.edu.vn](mailto:18127257@student.hcmus.edu.vn) |  |

# BẢNG PHÂN CÔNG CÔNG VIỆC

1. **Phân hệ 1**

|  |  |  |  |
| --- | --- | --- | --- |
| Tên công việc | Người thực hiện | Mức độ hoàn thành | Vấn đề gặp phải |
| Thiết kế và cài đặt cơ sở dữ liệu ở mức hệ thống | Phạm Ngọc Thùy Trang | 100% | Không có |
| Tạo user và role tương ứng với mô tả của hệ thống | Trần Huy Vũ | 100% | Không có |
| Cấp quyền cho các user và role tương ứng | Quách Phú Thành  Trần Huy Vũ | 100% | Không có |
| Viết các hàm kiểm tra các đối tượng dữ liệu và đăng nhập admin | Quách Phú Thành  Phạm Ngọc Thùy Trang | 100% | Không có |
| Fix bug và ghép code | Quách Phú Thành  Phạm Ngọc Thùy Trang | 100% | Không có |
| Kết nối Oracle DB với Winform và thiết kế giao diện cho ứng dụng | Phạm Ngọc Thùy Trang | 100% | Không có |
| Viết hàm xem danh sách người dùng hệ thống | Quách Phú Thành | 100% | Không có |
| Viết hàm xem thông tin các quyền của người dùng trên hệ thống | Trần Huy Vũ | 100% | Không có |
| Viết các hàm quản lý (bao gồm quản lý role, quản lý người dùng, cấp role cho người dùng) | Quách Phú Thành  Phạm Ngọc Thùy Trang | 100% | Không có |
| Viết các hàm thu hồi quyền | Quách Phú Thành  Trần Huy Vũ | 100% | Không có |
| Viết các hàm hiển thị thông tin các quyền tinh đến mức cột và bảng | Phạm Ngọc Thùy Trang | 100% | Không có |
| Viết các hàm cấp quyền insert và delete (theo role và user) | Quách Phú Thành  Phạm Ngọc Thùy Trang  Trần Huy VũVũ | 100% | Không có |
| Viết các hàm cấp quyền select và update (theo role và user) | Quách Phú Thành  Trần Huy Vũ  Phạm Ngọc Thùy Trang | 100% | Không có |
| Quay và chỉnh sửa video demo | Phạm Ngọc Thùy Trang | 100% | Không có |

1. **Phân hệ 2**

|  |  |  |  |
| --- | --- | --- | --- |
| Tên công việc | Người thực hiện | Mức độ hoàn thành | Vấn đề gặp phải |
| Lên kế hoạch và vẽ ER | * Trần Huy Vũ * Phạm Ngọc Thùy Trang * Quách Phú Thành | 100% | Không có |
| Thiết kế lược đồ quan hệ | * Trần Huy Vũ * Phạm Ngọc Thùy Trang * Quách Phú Thành | 100% | Không có |
| Cài đặt CSDL ở mức thiết kế | * Phạm Ngọc Thùy Trang * Quách Phú Thành | 100% | Không có |
| Cài đặt các chính sách RBAC + DAC | * Quách Phú Thành | 100% | Không có |
| Tạo user, role và insert dữ liệu | * Trần Huy Vũ | 100% | Không có |
| Cài đặt các chính sách VPD | * Quách Phú Thành | 100% | Không có |
| Cài đặt các chính sách mã hóa | * Quách Phú Thành | 100% | Không có |
| Cài đặt cơ chế mật khẩu + cơ chế hạn chế SQL Injection khi đăng nhập | * Phạm Ngọc Thùy Trang | 100% | Không có |
| Cài đặt các chính sách audit | * Trần Huy Vũ | 100% | Không có |
| Thiết kế + Liên kết giao diện | * Phạm Ngọc Thùy Trang | 80% | Không cài đặt giao diện cho OLS và audit |
| Fix bug + viết các hàm bổ sung | * Phạm Ngọc Thùy Trang | 100% | Không có |
| Chỉnh sửa báo cáo | * Trần Huy Vũ * Phạm Ngọc Thùy Trang * Quách Phú Thành | 100% | Không có |

Nội dung

[BẢNG THÔNG TIN CHI TIẾT CÁ NHÂN 1](#_Toc72868377)

[BẢNG PHÂN CÔNG CÔNG VIỆC 2](#_Toc72868378)

[YÊU CẦU BÀI TẬP 5](#_Toc72868379)

[BẢN TÓM TẮT CÁC KẾT QUẢ ĐẠT ĐƯỢC 6](#_Toc72868380)

[A. Phân hệ 1: 6](#_Toc72868381)

[B. Phân hệ 2: 7](#_Toc72868382)

[I. Mô tả dữ liệu bằng ER 7](#_Toc72868383)

[II. Ràng buộc toàn vẹn 8](#_Toc72868384)

[III. Lược đồ quan hệ 11](#_Toc72868385)

[IV. Xác định các loại người dùng trong hệ thống 13](#_Toc72868386)

[V. Phân tích quyền truy xuất của các loại người dùng (có thể vẽ ma trận quyền truy xuất trên các bảng) 14](#_Toc72868387)

[VI. Phân tích cách dùng các cơ chế bảo mật 15](#_Toc72868388)

# YÊU CẦU BÀI TẬP

|  |  |
| --- | --- |
| Loại bài tập | 🗹 Lý thuyết 🗹 Thực hành Đồ án 🗹 Bài tập |
| Ngày bắt đầu | 25/01/2021 |
| Ngày kết thúc | 24/05/2021 |

***Yêu cầu bài tập:***

**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.**

# BẢN TÓM TẮT CÁC KẾT QUẢ ĐẠT ĐƯỢC

## Phân hệ 1:

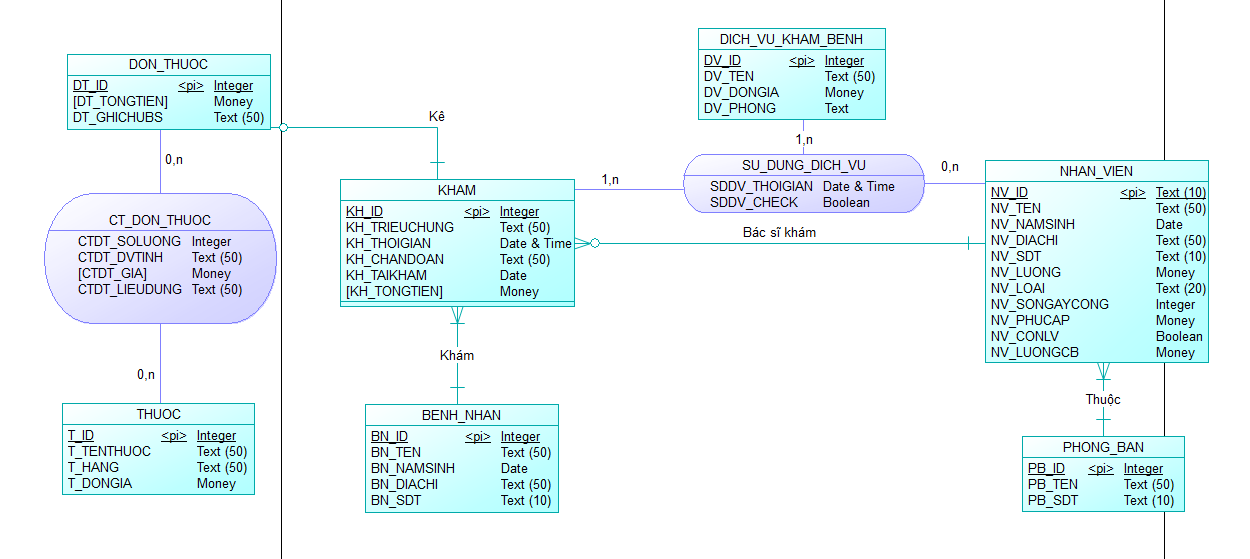
**1.      Phân tích từng chức năng của phân hệ 1, dữ liệu cần sử dụng (nếu có) và giao diện đi kèm**

* ***Xem danh sách người sử dụng trong hệ thống***
  + DBA có quyền xem danh sách tất cả các người dùng trong hệ thống.
  + Dữ liệu cần sử dụng là thông tin từ object system all\_users.
  + Giao diện:
* ***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.
  + Dữ liệu cần sử dụng là thông tin từ object system user\_tab\_privs
  + Giao diện:
* ***Cho phép tạo mới, xóa, sửa (hiệu chỉnh) user hoặc role***
  + DBA có quyền tạo mới, xóa, sửa (hiệu chỉnh) user hoặc role.
  + Giao diện:
* **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.
  + Giao diện:
* **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.
  + Giao diện:
* ***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).
  + Giao diện:
* ***Cho phép kiểm tra quyền của chủ thể vừa được cấp quyền***
  + DBA có quyền kiểm tra các users và quyền của họ.
  + Dữ liệu 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.
  + Giao diện:
* ***Cho phép chỉnh sửa quyền của user/role:***
  + DBA có quyền chỉnh sửa quyền của user/role bằng cách sử dụng câu lệnh grant, revoke.
  + Giao diện:

## Phân hệ 2:

### Mô tả dữ liệu bằng ER

ER vẽ bằng phần mềm Power Designer



### Ràng buộc toàn vẹn

1. **Mô tả RBTV:** Phí của các dịch vụ khám phải luôn lớn hơn 0, không được là số lẻ và luôn là một số chia hết cho 100. Chẳng hạn (phí của dịch vụ khám ngoài giờ là 21000 thay vì 21005)

**Bối cảnh: DICH\_VU\_KHAM\_BENH**

**Bảng tầm ảnh hưởng:**

|  |  |  |  |
| --- | --- | --- | --- |
|  | Thêm | Xóa | Sửa |
| DICH\_VU\_KHAM\_BENH | **+** | **-** | **+(DV\_DONGIA)** |

1. **Mô tả RBTV:** Lương của nhân viên và bác sĩ phải luôn lớn hơn hoặc bằng 0, không được là số lẻ và luôn là một số chia hết cho 100. Riêng phụ cấp và số ngày công có thể bằng 0

**Bối cảnh: NHAN\_VIEN**

**Bảng tầm ảnh hưởng:**

|  |  |  |  |
| --- | --- | --- | --- |
|  | Thêm | Xóa | Sửa |
| NHANVIEN | **+** | **-** | **+(LUONG, PHUCAP, SONGAYCONG)** |

1. **Mô tả RBTV:** Thời gian bệnh nhân tái khám phải lớn hơn thời gian bệnh nhân đi khám hiện tại

**Bối cảnh: KHAM**

**Bảng tầm ảnh hưởng:**

|  |  |  |  |
| --- | --- | --- | --- |
|  | Thêm | Xóa | Sửa |
| KHAM | **+** | **-** | **+(KH\_THOIGIAN, KH\_TAIKHAM)** |

1. **Mô tả RBTV:** Đơn giá thuốc phải là một số luôn lớn hơn 0, không được là số lẻ và luôn là một số chia hết cho 100

**Bối cảnh:**

**Bảng tầm ảnh hưởng: THUOC**

|  |  |  |  |
| --- | --- | --- | --- |
|  | Thêm | Xóa | Sửa |
| THUOC | **+** | **-** | **+(T\_DONGIA)** |

1. **Mô tả RBTV:** Giá của thuốc ở chi tiết đơn thuốc phải trùng với giá hiện tại của thuốc, và số lượng của thuốc ở chi tiết đơn thuốc phải nhỏ hơn hoặc bằng số lượng tồn của thuốc đó

**Bối cảnh: THUOC, CT\_DON\_THUOC**

**Bảng tầm ảnh hưởng:**

|  |  |  |  |
| --- | --- | --- | --- |
|  | Thêm | Xóa | Sửa |
| THUOC | **+** | **-** | **+(T\_DONGIA)** |
| CT\_DON\_THUOC | **+** | **-** | **+(CTDT\_GIA)** |

1. **Mô tả RBTV:** Tổng tiền của 1 đơn thuốc = (với n là số lượng thuốc của chi tiết đơn thuốc).

**Bối cảnh: DON\_THUOC, CT\_DON\_THUOC**

**Bảng tầm ảnh hưởng:**

|  |  |  |  |
| --- | --- | --- | --- |
|  | Thêm | Xóa | Sửa |
| DON\_THUOC | **+** | **-** | **+(DT\_TONGTIEN)** |
| CT\_DON\_THUOC | **+** | **-** | **+(CTDT\_GIA)** |

1. **Mô tả RBTV:** Đối với mỗi lần khám phải có ít nhất một hóa đơn (được tích hợp vào quan hệ KHAM) vì khám bệnh cũng là một loại dịch vụ cần tính tiền. Nếu ở trường hợp bình thường thì KH\_TONGTIEN = Tổng tiền của tất cả các loại dịch vụ sử dụng + tiền thuốc

|  |  |  |  |
| --- | --- | --- | --- |
|  | Thêm | Xóa | Sửa |
| DONTHUOC | **+** | **-** | **+(KH\_TONGTIEN)** |

### Lược đồ quan hệ

|  |  |  |  |
| --- | --- | --- | --- |
| Quan hệ | Thuộc tính (Khóa chính in đậm) | Khóa ngoại | Dạng chuẩn |
| PHONG\_BAN | **PB\_ID**, PB\_TEN, PB\_SDT | Không | BCK |
| NHAN\_VIEN | **NV\_ID**, NC\_TEN, NV\_NAMSINH, NV\_DIACHI, NV\_SDT, NV\_LUONG,  NV\_LUONGCB,  NV\_LOAI, NV\_SONGAYCONG, NV\_PHUCAP, NV\_PB,  NV\_CONLV | NV\_PB 🡪 PHONG\_BAN(PB\_ID) | BCK |
| BENH\_NHAN | **BN\_ID**, BN\_TEN, BN\_NAMSINH, BN\_DIACHI, BN\_SDT | Không | BCK |
| DICH\_VU\_KHAM\_BENH | **DV\_ID**, DV\_TEN, DV\_DONGIA,  DV\_PHONG | Không | BCK |
| THUOC | **T\_ID**, T\_TENTHUOC, T\_HANG, T\_SLTON, T\_DONGIA | Không | BCK |
| DON\_THUOC | **DT\_ID**, DT\_TONGTIEN, DT\_GHICHUBS, DT\_IDKHAM | DT\_IDKHAM 🡪 KHAM(KH\_ID) | BCK |
| CT\_DONTHUOC | **CTDT\_IDDON**, **CTDT\_IDTHUOC**, CTDT\_SOLUONG, CTDT\_DVTINH, CTDT\_GIA, CTDT\_LIEUDUNG | CTDT\_IDDON 🡪 DONTHUOC(DT\_ID)  CTDT\_IDTHUOC 🡪 THUOC(T\_ID) | BCK |
| KHAM | **KH\_ID**, KH\_TRIEUCHUNG, KH\_THOIGIAN, KH\_CHANDOAN, KH\_TAIKHAM,  KH\_IDBN,  KH\_TONGTIEN,  KH\_BSKHAM | KH\_IDBN 🡪 BENH\_NHAN(BN\_ID)  KH\_BSKHAM 🡪 NHAN\_VIEN(NV\_ID) | BCK |
| SU\_DUNG\_DICH\_VU | **SDDV\_IDDV**, **SDDV\_IDKHAM,**  **SDDV\_NGTHUCHIEN,**  **SDDV\_THOIGIAN**  SDDV\_CHECK | SDDV\_IDDV 🡪 DICH\_VU\_KHAM\_BENH(DV\_ID)  SDDV\_IDKHAM 🡪 KHAM(KH\_ID),  SDDV\_NGTHUCHIEN 🡪 NHANVIEN(NV\_ID) | BCK |

### 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.
* Nhân viên bộ phận bán thuốc.
* Nhân viên kế toán.

### Phân tích quyền truy xuất của các loại người dùng (có thể vẽ ma trận quyền truy xuất trên các bảng)

Nhân viên bộ phận tiếp tân và điều phối bệnh được insert, update, delete, select trên quan hệ BENH\_NHAN. Được phép select trên quan hệ DICH\_VU\_KHAM\_BENH, sau đó insert vào quan hệ SU\_DUNG\_DICH\_VU, KHAM (chỉ tạo mới một dòng để có khóa chính) và select trên trường NV\_ID, NV\_TEN của quan hệ NHAN\_VIEN.

Nhân viên phòng tài vụ chỉ được phép select toàn bộ trường và update trên trường SDDV\_CHECK ở quan hệ SU\_DUNG\_DICH\_VU. Được phép Select, update trên trường KH\_TONGTIEN ở quan hệ KHAM.

Bác sĩ được SIUD trên quan hệ CT\_DON\_THUOC, DON\_THUOC. Được phép select toàn bộ trường, update (trừ trường KH\_BSKHAM, KH\_IDBN, KH\_TONGTIEN) quan hệ KHAM và select, delete, insert trên quan hệ SU\_DUNG\_DICH\_VU. Cuối cùng là được phép select trên quan hệ DICH\_VU\_KHAM\_BENH, THUOC. Tất cả các quyền kể trên đều trên những dòng thuộc về bệnh nhân được chính bác sĩ đó chịu trách nhiệm.

Nhân viên bộ phận bán thuốc được phép select trên tất cả trường, update (chỉ trường DT\_TONGTIEN) ở quan hệ DON\_THUOC. Được phép select tất cả trên quan hệ CT\_DON\_THUOC.

Nhân viên kế toán select trên các trường NV\_ID, NV\_TEN, NV\_NAMSINH, NV\_SONGAYCONG, NV\_PHUCAP, NV\_CONLV, NV\_LUONG và update trường NV\_LUONG, NV\_LUONGCB ở quan hệ NHAN\_VIEN.

Nhóm quản lý tài nguyên và nhân sự được phép SIUD trên quan hệ PHONG\_BAN. Được phép insert, select trên tất cả trường và chỉ được update trên trường NV\_SONGAYCONG, NV\_PHUCAP, NV\_LUONGCB, NV\_PB ở quan hệ NHAN\_VIEN. Được update trường DV\_PHONG ở quan hệ DICH\_VU\_KHAM\_BENH.

Nhóm quản lí tài vụ được phép SIUD trên quan hệ THUOC, DICH\_VU\_KHAM\_BENH

### Phân tích cách dùng các cơ chế bảo mật

* **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. Chẳng hạn, mỗi loại nhân viên khác nhau sẽ được cấp tài khoản gồm tên đăng nhập và mật khẩu để có thể làm những công việc mà mình có liên quan. Những thông tin hay công việc không liên quan thì họ sẽ không được phép
* Cơ chế điều khiển truy cập:
  + **RBAC + DAC + Tạo view**: cấp các quyền đọc, ghi cho từng loại người dùng trên các bảng sao cho phù hợp với chính sách bảo mật. **Gồm 2 kịch bản**:
* Chỉ có nhân viên tiếp nhận mới được phép xem danh sách các bệnh nhân trong hệ thống cũng như thêm thông tin bệnh nhân mới vào hệ thống
* Chỉ có nhân viên kế toán mới được phép xem các thông tin của các nhân viên khác bao gồm mã nhân viên, tên, năm sinh, số ngày công, phụ cấp, lương, trạng thái còn làm việc hay không
* **Lý do áp dụng cơ chế mã hóa như trên:** Vì những trường bị giấu đi là những trường dữ liệu nhạy cảm (thông tin cá nhân, lương) bắt buộc phải bảo mật vì quyền riêng tư của người dùng.
  + **VPD**: Chỉ cho phép truy cập đến những dòng dữ liệu mà người dùng được phép truy cập. ***Gồm 2 kịch bản***:
* Bác sĩ chỉ có thể thêm thông tin khám do mình khám.
* Bác sĩ chỉ có thể xem thông tin khám và thông tin sử dụng dịch vụ do mình khám.
* **Lý do áp dụng cơ chế mã hóa như trên:** Đây là kịch bản giúp cho thông tin nhạy cảm về các bệnh hay triệu chứng của bệnh nhân được bảo mật và đồng thời cũng bảo đảm an toàn dữ liệu (không có người thứ hai tham gia vào quá trình thay đổi 1 dòng dữ liệu)
  + **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. Nhãn gồm đầy đủ 3 thành phần: level, compartment và group. Trong đó, level gồm 2 mức là admin (tức admin của phân hệ 1) và nhân viên (các nhân viên nói chung của phân hệ 2), compartment là các loại nhân viên, và group tương ứng với phòng ban mà nhân viên thuộc về. Ở đây cụ thể là phòng cấp cứu và phòng chữa bệnh của bác sĩ
* **Cơ chế mã hóa (gồm 3 kịch bản):**
* **Kịch bản 1:** Mã hóa những thông tin nhạy cảm mà chỉ có bác sĩ khám mới được biết trong quá trình khám cho bệnh nhân bao gồm: chẩn đoán và triệu chứng
* **Kịch bản 2:** Mã hóa những thông tin nhạy cảm của các nhân viên trong bệnh viện, khi cần thiết thì mới được giải mã để thực hiện các hành động chỉnh sửa như: phụ cấp và lương của nhân viên
* **Kịch bản 3:** Mã hóa các trường nhạy cảm của bệnh nhân như thông tin về địa chỉ và số điện thoại
* **Lý do áp dụng cơ chế mã hóa như trên:** Vì các cơ chế RBAC và VPD chỉ mới là các cơ chế điều khiển truy cập nên chưa thể tránh việc các user cấp cao như admin hay các hacker xem được các dữ liệu nhạy cảm từ bảng dữ liệu gốc nên ta cần mã hóa các trường cần thiết để làm tuyến phòng thử cuối cùng trước các nhân tố có thể truy cập vào dữ liệu gốc**.**
* Nhóm cũng cài đặt thêm hàm băm để băm mật khẩu của các nhân viên để tăng tính bảo mật dữ liệu của người dùng
* Nhóm cũng hạn chế các tấn công SQL Injection bằng cách bắt các giá trị mà người dùng nhập vào khi đăng nhập thông qua regex expression.
* Có sử dụng audit ở phân hệ 1, DBA có thể xem nhật kí sử dụng và truy cập của những người dùng khác. Gồm 2 kịch bản:
* **Kịch bản 1:** Hệ thống sẽ kiểm tra sự thay đổi trên bảng nhân viên (trường Lương), những hoạt động cập nhật diễn ra đối với trường Lương này sẽ được ghi nhận lại
* **Kịch bản 2:** Hệ thống sẽ kiểm tra sự thay đổi trên bảng Đơn thuốc (trường Tổng tiền), những hoạt động cập nhật diễn ra đối với trường Tổng tiền này sẽ được ghi nhận lại
* **Lý do áp dụng cơ chế mã hóa như trên:** Vì đây là những trường nhạy cảm (có liên quan đến vấn đề tiền bạc), nên để có thể thấy được những hành động bất thường, hệ thống cần ghi nhận những hành động liên quan tới các trường này.