# BÁO CÁO QUẢN TRỊ RỦI RO AN TOÀN THÔNG TIN HỆ THỐNG Y TẾ

**Kính gửi:** Ban Giám đốc **Ngày báo cáo:** 10/02/2026 **Đơn vị thực hiện:** HQG - Tư vấn An toàn thông tin & Quản trị rủi ro

# 1. TÓM TẮT ĐIỀU HÀNH

Dựa trên kết quả rà soát định kỳ, hệ thống CNTT y tế hiện tại đang tồn tại **50 lỗ hổng bảo mật**, trong đó có **8 lỗ hổng ở mức độ Nghiêm trọng và Cao** ảnh hưởng trực tiếp đến các hệ thống cốt lõi như EMR (Bệnh án điện tử), HIS (Quản lý bệnh viện) và PACS (Lưu trữ hình ảnh).

**Nhận định tổng thể:**

- **Mức độ rủi ro: CAO**. Hệ thống đang đối mặt với nguy cơ bị tấn công tê liệt hoặc lộ lọt dữ liệu quy mô lớn do các lỗ hổng thực thi mã từ xa và chiếm quyền điều khiển.
- **Tính tuân thủ:** Hiện tại hệ thống chưa đáp ứng đầy đủ các tiêu chuẩn về bảo mật dữ liệu cá nhân theo Nghị định 13/2023/NĐ-CP và các thông tư hướng dẫn của Bộ Y tế về an toàn thông tin cấp độ 3.
- **Ưu tiên:** Ban Lãnh đạo cần chỉ đạo khắc phục ngay nhóm lỗ hổng liên quan đến hạ tầng máy chủ và phân quyền truy cập để tránh rủi ro đình trệ hoạt động khám chữa bệnh.

# 2. NHÓM RỦI RO THEO BẢN CHẤT QUẢN LÝ

## 2.1. Nguy cơ gián đoạn hoạt động khám chữa bệnh (Business Continuity)

- **Tài sản ảnh hưởng:** Toàn bộ hệ thống HIS, LIS, PACS và các máy chủ ứng dụng Web.
- **Thực trạng:** Tồn tại các lỗ hổng gây từ chối dịch vụ (DDoS) và lỗi tràn bộ nhớ (Buffer Overflow).
- **Hậu quả quản trị:** Nếu bị khai thác, các dịch vụ trực tuyến sẽ bị đình trệ. Bệnh viện buộc phải chuyển sang quy trình thủ công (giấy tờ), gây ùn tắc tại khu vực tiếp đón, chậm trễ trong trả kết quả xét nghiệm và can thiệp điều trị, ảnh hưởng trực tiếp đến sự an toàn của người bệnh.

## 2.2. Nguy cơ lộ lọt thông tin bệnh án và dữ liệu cá nhân

- **Tài sản ảnh hưởng:** Máy chủ lưu trữ dữ liệu tập trung, hệ thống quản trị nội bộ.
- **Thực trạng:** Lỗ hổng cho phép đối tượng bên ngoài chiếm quyền kiểm soát tối cao (root/administrator) mà không cần mật khẩu hoặc thông qua chiếm quyền điều khiển đặc quyền.
- **Hậu quả pháp lý:** Vi phạm nghiêm trọng nghĩa vụ bảo vệ bí mật đời tư bệnh nhân. Ban Giám đốc có thể phải đối mặt với các đợt thanh tra đột xuất, án phạt hành chính nặng từ cơ quan chức năng và tổn hại uy tín thương hiệu không thể phục hồi.

## 2.3. Nguy cơ mất kiểm soát hạ tầng mạng nội bộ

- **Tài sản ảnh hưởng:** Thiết bị mạng Core, hệ điều hành máy chủ Linux/Windows.
- **Thực trạng:** Các lỗi như "Path Traversal" và "Privilege Escalation" cho phép kẻ tấn công di chuyển tự do trong mạng bệnh viện.
- **Hậu quả quản trị:** Hệ thống CNTT bị biến thành công cụ cho tội phạm mạng (phát tán mã độc tống tiền - Ransomware). Ban Lãnh đạo sẽ mất hoàn toàn khả năng điều hành thông qua các nền tảng số.

# 3. CÁC RỦI RO NGHIÊM TRỌNG CẦN ƯU TIÊN

Dưới đây là các tình huống thực tế mà Ban Giám đốc sẽ phải đối mặt nếu không xử lý kịp thời:

1. **Tình huống Tấn công Tống tiền (Ransomware):** Với lỗ hổng CVE-2021-4034 và CVE-2021-44790, kẻ tấn công có thể mã hóa toàn bộ cơ sở dữ liệu bệnh án điện tử (EMR). Bệnh viện sẽ bị yêu cầu trả tiền chuộc, trong khi mọi hoạt động điều trị bị đóng băng.
2. **Trách nhiệm Người đứng đầu:** Theo luật An ninh mạng, khi xảy ra sự cố lộ lọt dữ liệu do thiếu các biện pháp bảo mật cơ bản (như không cập nhật bản vá lỗ hổng đã được cảnh báo), Ban Giám đốc chịu trách nhiệm trực tiếp về mặt quản lý và pháp lý trước Nhà nước.
3. **Hệ lụy tới An toàn người bệnh:** Việc gián đoạn hệ thống PACS/LIS khiến bác sĩ không có thông tin hình ảnh/xét nghiệm chính xác để ra quyết định phẫu thuật hoặc kê đơn, dẫn đến nguy cơ sai sót y khoa.

# 4. KIẾN NGHỊ BIỆN PHÁP KIỂM SOÁT

Để tối ưu hóa nguồn lực, chúng tôi đề xuất chiến lược **"Cập nhật tập trung - Bảo vệ đa lớp"**:

| Nhóm Giải pháp | Nội dung thực hiện | Giá trị quản lý |
|---|---|---|
| **Khắc phục Tập trung** | Thực hiện cập nhật bản vá (Patching) cho hệ điều hành máy chủ và các dịch vụ Web (Apache/Linux). Xử lý 1 lần sẽ khắc phục được 80% các lỗi nghiêm trọng. | **Giảm 90% rủi ro** bị xâm nhập từ xa; tiết kiệm nhân lực vận hành. |
| **Kiểm soát Truy cập** | Áp dụng nguyên tắc "Quyền hạn tối thiểu", rà soát và thu hồi các tài khoản có đặc quyền cao không cần thiết trên HIS/EMR. | **Tăng tính tuân thủ** Nghị định 13; ngăn chặn rủi ro từ nội bộ. |
| **Lớp phòng thủ tạm thời** | Cấu hình tường lửa ứng dụng (WAF) để chặn các mẫu tấn công vào lỗ hổng chưa kịp vá ngay. | **Duy trì vận hành** ổn định trong khi chờ kế hoạch nâng cấp phần mềm dài hạn. |

**Phân tích tài chính:** Chi phí thực hiện các biện pháp cập nhật và cấu hình này chủ yếu sử dụng nguồn lực nhân sự nội bộ và các công cụ sẵn có. So với chi phí khắc phục sự cố (ước tính hàng tỷ đồng nếu bị Ransomware), đây là khoản đầu tư phòng ngừa có lợi ích kinh tế cao nhất.

# 5. ĐỀ XUẤT THỨ TỰ ƯU TIÊN (SLA)

| Thứ tự | Nhóm lỗ hổng | Thời hạn xử lý (SLA) | Mục tiêu |
|---|---|---|---|
| **Ưu tiên 1** | Lỗ hổng Nghiêm trọng (DDoS, Chiếm quyền Root) | **Trong vòng 48 giờ** | Ngăn chặn sự cố dừng hệ thống tức thì. |
| **Ưu tiên 2** | Lỗ hổng Cao (Thực thi mã, Leo thang đặc quyền) | **Trong vòng 05 ngày** | Bảo vệ toàn vẹn dữ liệu bệnh nhân. |
| **Ưu tiên 3** | Các lỗi Trung bình & Thấp | Theo kế hoạch bảo trì tháng | Tối ưu hóa hiệu suất và bảo mật dài hạn. |

# 6. KẾT LUẬN DÀNH CHO BAN LÃNH ĐẠO

An toàn thông tin không còn là vấn đề kỹ thuật thuần túy mà là **nền tảng của chất lượng dịch vụ y tế**. Một hệ thống y tế hiện đại không thể phục vụ người bệnh tốt nếu dữ liệu của họ không được bảo vệ và dịch vụ luôn thường trực nguy cơ bị gián đoạn.

**Kiến nghị Ban Giám đốc:**

1. Phê duyệt kế hoạch cập nhật khẩn cấp trong 48h tới.
2. Giao bộ phận CNTT báo cáo tiến độ khắc phục hàng ngày cho đến khi các lỗi Nghiêm trọng được xóa bỏ.
3. Xem xét ngân sách cho việc kiểm tra đánh giá an ninh chuyên sâu định kỳ hàng năm.

Ban Giám đốc cần đóng vai trò quyết định trong việc thiết lập văn hóa an toàn thông tin để đảm bảo sự phát triển bền vững của Bệnh viện.

*Báo cáo được trích xuất từ hệ thống quản lý rủi ro HQG.*