

**SỞ Y TẾ ĐỒNG NAI  
BỆNH VIỆN MẮT  
HÀ NỘI – ĐỒNG NAI**

Số : 16 / QĐ-BVMHNEMR

V/v triển khai áp dụng hồ sơ bệnh án  
điện tử thay cho hồ sơ bệnh án giấy tại  
Bệnh viện Mắt Hà Nội – Đồng Nai

**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM  
Độc Lập – Tự Do – Hạnh Phúc**

Đồng Nai, ngày 01 tháng 12 năm 2025

**QUYẾT ĐỊNH**

**Về việc triển khai sử dụng và lưu trữ hồ sơ bệnh án điện tử  
thay cho hồ sơ bệnh án giấy, lưu trữ và truyền tải hình ảnh y tế  
thay cho in phim và lưu trữ thông tin xét nghiệm thay cho việc in giấy**

**GIÁM ĐỐC BỆNH VIỆN MẮT HÀ NỘI – ĐỒNG NAI**

Căn cứ Luật khám chữa bệnh số 15/2023/QH15 ngày 09/01/2023;

Căn cứ Luật giao dịch điện tử số 20/2023/QH15 ngày 22/06/2023;

Căn cứ Luật An toàn thông tin mạng số 86/2015/QH13 ngày 19/11/2015;

Căn cứ Luật Công nghệ thông tin số 67/2006/QH11, ngày 29/06/2006;

Luật An ninh mạng số 24/2018/QH14 ngày 12/06/2018 của Quốc hội;

Căn cứ Nghị định 96/NĐ-CP ngày 30/12/2023 của Chính phủ quy định Chi tiết một số điều của  
Luật khám bệnh, chữa bệnh;

Căn cứ Thông tư 32/2023/TT\_BYT ngày 31/12/2023 của Bộ Y Tế quy định chi tiết một số điều của  
Luật Khám bệnh, chữa bệnh;

Căn cứ Thông tin số 53/2014/TT-BYT ngày 29 tháng 12 năm 2014 của Bộ Y Tế về ban hành Quy  
định điều kiện hoạt động y tế trên môi trường mạng;

Căn cứ Thông tư số 48/2017/TT-BYT ngày 28 tháng 12 năm 2017 của Bộ Y Tế ban hành Quy định  
trích chuyển dữ liệu điện tử trong quản lý và thanh toán chi phí khám bệnh, chữa bệnh bảo hiểm y  
tế;

Căn cứ Thông tin số 53/2017/TT-BYT ngày 29 tháng 12 năm 2017 của Bộ Y Tế về ban hành Quy  
định về thời hạn bảo quản hồ sơ, tài liệu chuyên môn nghiệp vụ ngành Y tế;

Căn cứ Thông tin số 54/2017/TT-BYT ngày 29 tháng 12 năm 2017 của Bộ Y Tế về ban hành Bộ tiêu  
chí ứng dụng công nghệ thông tin tại các cơ sở khám bệnh, chữa bệnh;

Căn cứ Thông tin số 13/2025/TT-BYT ngày 06 tháng 06 năm 2025 của Bộ Y Tế về việc Hướng dẫn  
triển khai hồ sơ bệnh án điện tử;

Căn cứ Giấy phép hoạt động khám bệnh, chữa bệnh số 228/BYT-GPHĐ ngày 30 tháng 08 năm  
2019 của Bộ Y Tế;

Căn cứ Biên bản số 68/BBBVMEMR ngày 20/11/2025 của Hội đồng chuyên môn về việc thẩm định  
bệnh án điện tử tại Bệnh viện Mắt Hà Nội – Đồng Nai;

Xét đề nghị của Trưởng phòng KHTH

## QUYẾT ĐỊNH

**Điều 1.** Quyết định triển khai sử dụng và lưu trữ hồ sơ bệnh án điện tử thay cho hồ sơ bệnh án giấy, lưu trữ và truyền tải hình ảnh y tế thay cho in phim và lưu trữ thông tin xét nghiệm thay cho việc in giấy (gọi tắt là Hồ sơ bệnh án điện tử) của Bệnh viện Mắt Hà Nội – Đồng Nai từ ngày 07/12/2025

**Điều 2.** Hồ sơ bệnh án điện tử được lập, cập nhật, hiển thị, ký số, lưu trữ bằng phương tiện điện tử đáp ứng các Quy định theo thông tư số 13/2025/TT-BYT ngày 06 tháng 06 năm 2025 của Bộ Y Tế và có giá trị pháp lý như Hồ sơ bệnh án giấy quy định tại Điều 69 Luật khám bệnh, chữa bệnh

**Điều 3.** Các loại và nội dung của Hồ sơ bệnh án điện tử (EMR):

- Hồ sơ bệnh án điện tử (EMR) bao gồm hồ sơ bệnh án nội trú, hồ sơ bệnh án ngoại trú và các loại hồ sơ khác theo quy định của Bộ Y Tế
- Nội dung của Hồ sơ bệnh án điện tử (EMR) gồm đầy đủ các trường thông tin theo mẫu của hồ sơ bệnh án sử dụng trong khám bệnh, chữa bệnh theo quy định của Bộ Y Tế hiện hành và cập nhật theo quy định mới (nếu có)

**Điều 4.** Sử dụng chữ ký số và chữ ký điện tử trong hồ sơ bệnh án điện tử

Thực hiện theo Luật giao dịch điện tử số 20/2023/QH15 ngày 22/06/2023 và Quyết định số 05/QĐ-ĐNEMR ngày 01/10/2025 của Bệnh viện Mắt Hà Nội – Đồng Nai về việc ban hành Quy chế quản lý, sử dụng chữ ký điện tử, chữ ký số tại bệnh viện

Nhân viên y tế sử dụng chữ ký điện tử hoặc chữ ký số hợp pháp trong hồ sơ bệnh án điện tử tại Bệnh viện Mắt Hà Nội – Đồng Nai theo sự phân công của Giám Đốc Bệnh viện

Trong các văn bản cần có chữ ký gốc khoa phòng scan để đưa vào hồ sơ bệnh án điện tử tương ứng và chuyển bản có chữ ký gốc về Phòng KHTH và lưu trữ theo quy định

**Điều 5.** Trưởng khoa, phụ trách các Khoa, Phòng và cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

Quyết định có hiệu lực từ ngày ký.

Nơi nhận:

- Như điều 5
- Cục KHCN &ĐT-Bộ Y Tế (để báo cáo)
- Sở Y Tế Đồng Nai (để báo cáo)
- BHXH Đồng Nai (để phối hợp)
- BGĐ
- Lưu: VT, KHTH





Số : 17 / OĐ-BVMHNEMR

V/v triển khai áp dụng hồ sơ bệnh án  
điện tử thay cho hồ sơ bệnh án giấy tại  
Bệnh viện Mắt Hà Nội – Đồng Nai

**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM**  
**Độc Lập – Tự Do – Hạnh Phúc**

Đồng Nai, ngày 01 tháng 12 năm 2025

**Kính gửi: Cục Khoa Học Công Nghệ và Đào Tạo – Bộ Y Tế**

Căn cứ *Thông tư số 54/2017/TT-BYT* ngày 29/12/2017 của Bộ Y Tế về việc ban hành Bộ tiêu chí ứng dụng công nghệ thông tin tại các cơ sở khám bệnh, chữa bệnh;

Căn cứ *Thông tư số 13/2025/TT-BYT* ngày 06 tháng 06 năm 2025 của Bộ Y Tế về việc Hướng dẫn triển khai hồ sơ bệnh án điện tử;

Căn cứ *Biên bản số 68/BBBVMEMR* ngày 20/11/2025 của Hội đồng chuyên môn về việc  
thẩm định bệnh án điện tử tại Bệnh viện Mắt Hà Nội – Đồng Nai;

Căn cứ *Quyết định số 16/QĐ-BVMHNEMR* ngày 01 tháng 12 năm 2025 của Bệnh viện Mắt Hà Nội – Đồng Nai về việc triển khai sử dụng và lưu trữ hồ sơ bệnh án điện tử thay cho hồ sơ bệnh án giấy, lưu trữ và truyền tải hình ảnh y tế thay cho in phim và lưu trữ thông tin xét nghiệm thay cho việc in giấy;

Bệnh viện Mắt Hà Nội – Đồng Nai đã đáp ứng các điều kiện được quy định tại Thông tư số 54/2017/TT-BYT ngày 29/12/2017 của Bộ Y Tế về việc ban hành bộ tiêu chí ứng dụng công nghệ thông tin tại các cơ sở khám bệnh, chữa bệnh và Thông tư số 46/2018/TT-BYT ngày 28/12/2018 của Bộ Y Tế quy định Hồ sơ bệnh án điện tử;

Bệnh viện Mắt Hà Nội – Đồng Nai quyết định triển khai sử dụng và lưu trữ hồ sơ bệnh án điện tử thay thế bệnh án giấy, lưu trữ và truyền tải hình ảnh y tế thay cho in phim và lưu trữ thông tin xét nghiệm thay cho việc in giấy kể từ ngày 07/12/2025 (các hồ sơ chi tiết gửi kèm theo công văn này)

Bệnh viện Mắt Hà Nội – Đồng Nai kính đề nghị Cục Khoa Học Công Nghệ và Đào Tạo – Bộ Y Tế quan tâm, xem xét đăng tải thông tin về việc triển khai hồ sơ bệnh án điện tử của đơn vị trên Cổng thông tin điện tử của Bộ Y Tế

Xin trân trọng cảm ơn./.

*Nơi nhận*

- Như kính gửi
- Sở Y Tế Đồng Nai (để b/c)
- BHXH Đồng Nai
- Lưu: VT, KHTH-CNTT



## GIÁM ĐỐC

GIÁM ĐỐC  
BS CKI. Hoàng Vĩnh Hà

Số: 1624/QĐ-VNPT IT-ATTT-NCPT

Hà Nội, ngày 30 tháng 8 năm 2023

## QUYẾT ĐỊNH

Về việc Phê duyệt cấp độ an toàn thông tin đối với  
Hệ thống Phần mềm Bệnh án điện tử - VNPT EMR

### TỔNG GIÁM ĐỐC CÔNG TY

Căn cứ Luật An toàn thông tin mạng số 86/2015/QH13 ngày 01/07/2015;

Căn cứ Nghị định 85/2016/NĐ-CP ngày 01/07/2016 của Chính phủ về việc đảm bảo an toàn hệ thống thông tin theo cấp độ;

Căn cứ Thông tư số 12/2022/TT-BTTTT ngày 12/08/2022 của Bộ Thông tin và Truyền thông Quy định chi tiết và hướng dẫn một số điều của Nghị định số 85/2016/NĐ-CP ngày 01/07/2016 của Chính phủ về Bảo đảm an toàn hệ thống thông tin theo cấp độ;

Căn cứ Quyết định số 39/QĐ-VNPT-HĐTV-NL ngày 01/03/2018 của Hội đồng thành viên Tập đoàn Bưu chính Viễn thông Việt Nam về việc thành lập Công ty Công nghệ thông tin VNPT (VNPT-IT) – đơn vị trực thuộc Tập đoàn VNPT;

Căn cứ văn bản số 6174/VNPT-CN của Tập đoàn Bưu chính Viễn thông Việt Nam ngày 14/10/2022 v/v Triển khai đảm bảo an toàn thông tin theo cấp độ;

Căn cứ văn bản số 238/GUQ-VNPTIT-VP của Tổng Giám đốc Công ty Công nghệ thông tin VNPT ngày 19/01/2023 V/v Ủy quyền thực hiện phê duyệt cấp độ an toàn hệ thống thông tin;

Căn cứ văn bản số 2060/CV-ATTT-NCPT ngày 02/08/2023 V/v “Ý kiến thẩm định hồ sơ đề xuất cấp độ cho hệ thống VNPT EMR”;

Xét đề nghị của Giám đốc Trung tâm Giải pháp Y tế điện tử,

### QUYẾT ĐỊNH:

**Điều 1. Phê duyệt cấp độ an toàn thông tin đối với Hệ thống Phần mềm Bệnh án điện tử - VNPT EMR cụ thể như sau:**

1. Thông tin chung:

a) Tên hệ thống thông tin: **Hệ thống Phần mềm Bệnh án điện tử - VNPT EMR.**

b) Đơn vị vận hành hệ thống thông tin: Công ty Công nghệ thông tin VNPT (VNPT-IT) – CN Tập đoàn Bưu chính Viễn thông Việt Nam.

c) Địa chỉ: Số 57 Phố Huỳnh Thúc Kháng, Phường Láng Hạ, Quận Đống Đa, Thành phố Hà Nội, Việt Nam.



2. Cấp độ an toàn hệ thống thông tin: Cấp độ 3.

3. Phương án bảo đảm an toàn hệ thống thông tin:

Phương án bảo đảm an toàn thông tin trong thiết kế, quản lý và vận hành hệ thống trên tương ứng với cấp độ 3 là phù hợp với quy định tại Nghị định 85/2016/NĐ-CP ngày 01/07/2016 của Chính phủ, Thông tư số 12/2022/TT-BTTTT ngày 12/08/2022 của Bộ Thông tin và Truyền thông và Tiêu chuẩn quốc gia TCVN 11930:2017 về bảo đảm an toàn hệ thống thông tin theo cấp độ.

## **Điều 2. Tổ chức thực hiện**

1. Trung tâm Giải pháp Y tế điện tử (trực thuộc VNPT-IT) chịu trách nhiệm chủ trì tổ chức quản lý, vận hành, bảo đảm an toàn thông tin cho **Hệ thống Phần mềm Bệnh án điện tử - VNPT EMR** theo các yêu cầu tương ứng với Cấp độ 3 theo quy định tại Nghị định 85/2016/NĐ-CP ngày 01/07/2016 của Chính phủ, Thông tư số 12/2022/TT-BTTTT ngày 12/08/2022 của Bộ Thông tin và Truyền thông và Tiêu chuẩn quốc gia TCVN 11930:2017 về bảo đảm an toàn hệ thống thông tin theo cấp độ.

2. Trung tâm Điều hành IT, Trung tâm An toàn thông tin (trực thuộc VNPT-IT) có trách nhiệm phối hợp triển khai thực hiện các phương án bảo đảm an toàn thông tin tương ứng với cấp độ an toàn hệ thống thông tin theo quy định.

3. Ban Chất lượng sản phẩm (trực thuộc VNPT-IT) có trách nhiệm kiểm tra, giám sát việc thực hiện Quyết định này, báo cáo Tổng Giám đốc Công ty VNPT-IT theo quy định.

**Điều 3.** Quyết định này có hiệu lực thi hành kể từ ngày ký.

**Điều 4.** Các Ông (Bà) Chánh Văn phòng, Trưởng các Ban chức năng, Trưởng các đơn vị trực thuộc Công ty VNPT-IT chịu trách nhiệm thi hành quyết định này./.

### **Nơi nhận:**

- Như Điều 4;
- Lãnh đạo VNPT, Ban Công nghệ (để b/c);
- Ban TGD Cty VNPT-IT (để b/c);
- Lưu VT.

Số eOffice: 682195 - VBKS

**TUQ. TỔNG GIÁM ĐỐC**  
**GIÁM ĐỐC TT. AN TOÀN THÔNG TIN**



Nguyễn Ngọc Quân

Số: 596/QĐ-VNPT IT-ATTT

Hà Nội, ngày 24 tháng 4 năm 2024

## QUYẾT ĐỊNH

Về việc Phê duyệt cấp độ an toàn thông tin đối với  
Hệ thống dịch vụ VNPT-CA

### TỔNG GIÁM ĐỐC CÔNG TY

Căn cứ Luật An toàn thông tin mạng số 86/2015/QH13 ngày 01/07/2015;

Căn cứ Nghị định 85/2016/NĐ-CP ngày 01/07/2016 của Chính phủ về việc đảm bảo an toàn hệ thống thông tin theo cấp độ;

Căn cứ Thông tư số 12/2022/TT-BTTTT ngày 12/08/2022 của Bộ Thông tin và Truyền thông Quy định chi tiết và hướng dẫn một số điều của Nghị định số 85/2016/NĐ-CP ngày 01/07/2016 của Chính phủ về Bảo đảm an toàn hệ thống thông tin theo cấp độ;

Căn cứ Quyết định số 39/QĐ-VNPT-HĐTV-NL ngày 01/03/2018 của Hội đồng thành viên Tập đoàn Bưu chính Viễn thông Việt Nam về việc thành lập Công ty Công nghệ thông tin VNPT (VNPT-IT) – đơn vị trực thuộc Tập đoàn VNPT;

Căn cứ văn bản số 9610/VNPT-CN của Tập đoàn Bưu chính Viễn thông Việt Nam ngày 13/12/2023 v/v Triển khai đảm bảo an toàn theo cấp độ các hệ thống thông tin do VNPT IT chịu trách nhiệm vận hành;

Căn cứ văn bản số 2427/CV-ATTT-NCPT ngày 28/12/2023 v/v “Ý kiến thẩm định hồ sơ đề xuất cấp độ cho hệ thống VNPT-CA”;

Xét đề nghị của Giám đốc Trung tâm Giải pháp, Tích hợp hệ thống tại Tờ trình số 04/TTr-SI-QLSP ngày 05/01/2024 v/v “Phê duyệt cấp độ an toàn thông tin hệ thống VNPT CA”,

### QUYẾT ĐỊNH:

**Điều 1. Phê duyệt cấp độ an toàn thông tin đối với Hệ thống dịch vụ VNPT-CA cụ thể như sau:**

1. Thông tin chung:

a) Tên hệ thống thông tin: **Hệ thống dịch vụ VNPT-CA.**

b) Đơn vị vận hành hệ thống thông tin: Trung tâm Giải pháp, Tích hợp hệ thống - CN Công ty Công nghệ thông tin VNPT (VNPT-IT) – CN Tập đoàn Bưu chính Viễn thông Việt Nam.

c) Địa chỉ: Số 57 Phố Huỳnh Thúc Kháng, Phường Láng Hạ, Quận Đống Đa, Thành



phố Hà Nội, Việt Nam.

2. Cấp độ an toàn hệ thống thông tin: Cấp độ 3.

3. Phương án bảo đảm an toàn hệ thống thông tin:

Phương án bảo đảm an toàn thông tin trong thiết kế, quản lý và vận hành hệ thống trên tương ứng với cấp độ 3 là phù hợp với quy định tại Nghị định 85/2016/NĐ-CP ngày 01/07/2016 của Chính phủ, Thông tư 12/2022/TT-BTTTT ngày 12/08/2022 của Bộ Thông tin và Truyền thông và Tiêu chuẩn quốc gia TCVN 11930:2017 về bảo đảm an toàn hệ thống thông tin theo cấp độ.

## **Điều 2. Tổ chức thực hiện**

1. Trung tâm Giải pháp, Tích hợp hệ thống (trực thuộc VNPT-IT) chịu trách nhiệm chủ trì tổ chức quản lý, vận hành, bảo đảm an toàn thông tin cho **Hệ thống dịch vụ VNPT-CA** theo các yêu cầu tương ứng với Cấp độ 3 theo quy định tại Nghị định 85/2016/NĐ-CP ngày 01/07/2016 của Chính phủ, Thông tư số 12/2022/TT-BTTTT ngày 12/08/2022 của Bộ Thông tin và Truyền thông và Tiêu chuẩn quốc gia TCVN 11930:2017 về bảo đảm an toàn hệ thống thông tin theo cấp độ.

2. Trung tâm Điều hành IT, Trung tâm An toàn thông tin (trực thuộc VNPT-IT) có trách nhiệm phối hợp triển khai thực hiện các phương án bảo đảm an toàn thông tin tương ứng với cấp độ an toàn hệ thống thông tin theo quy định.

3. Ban Chất lượng sản phẩm (trực thuộc VNPT-IT) có trách nhiệm kiểm tra, giám sát việc thực hiện Quyết định này, báo cáo Tổng Giám đốc Công ty VNPT-IT theo quy định.

**Điều 3.** Quyết định này có hiệu lực thi hành kể từ ngày ký.

**Điều 4.** Các Ông (Bà) Chánh Văn phòng, Trưởng các Ban chức năng, Trưởng các đơn vị trực thuộc Công ty VNPT-IT chịu trách nhiệm thi hành quyết định này./.

### **Nơi nhận:**

- Như Điều 4;
- Tập đoàn VNPT (P.TGD Ngô Diên Hy), Ban Công nghệ (để b/c);
- Ban TGD Cty VNPT-IT (để b/c);
- Lưu VT.

Số eOffice: 264898 - VBKS

**KT. TỔNG GIÁM ĐỐC  
PHÓ TỔNG GIÁM ĐỐC**



**Hà Thái Bảo**

Số: 1494/QĐ-VNPT IT-ATTT-NCPT

Hà Nội, ngày 10 tháng 8 năm 2023

## **QUYẾT ĐỊNH**

**Về việc Phê duyệt cấp độ an toàn thông tin đối với  
Hệ thống Phần mềm chẩn đoán hình ảnh y khoa VNPT RIS/PACS**

### **TỔNG GIÁM ĐỐC CÔNG TY**

*Căn cứ Luật An toàn thông tin mạng số 86/2015/QH13 ngày 01/07/2015;*

*Căn cứ Nghị định 85/2016/NĐ-CP ngày 01/07/2016 của Chính phủ về việc đảm bảo an toàn hệ thống thông tin theo cấp độ;*

*Căn cứ Thông tư số 12/2022/TT-BTTTT ngày 12/08/2022 của Bộ Thông tin và Truyền thông Quy định chi tiết và hướng dẫn một số điều của Nghị định số 85/2016/NĐ-CP ngày 01/07/2016 của Chính phủ về Bảo đảm an toàn hệ thống thông tin theo cấp độ;*

*Căn cứ Quyết định số 39/QĐ-VNPT-HĐTV-NL ngày 01/03/2018 của Hội đồng thành viên Tập đoàn Bưu chính Viễn thông Việt Nam về việc thành lập Công ty Công nghệ thông tin VNPT (VNPT-IT) – đơn vị trực thuộc Tập đoàn VNPT;*

*Căn cứ văn bản số 6174/VNPT-CN của Tập đoàn Bưu chính Viễn thông Việt Nam ngày 14/10/2022 v/v Triển khai đảm bảo an toàn thông tin theo cấp độ;*

*Căn cứ văn bản số 238/GUQ-VNPTIT-VP của Tổng Giám đốc Công ty Công nghệ thông tin VNPT ngày 19/01/2023 V/v Ủy quyền thực hiện phê duyệt cấp độ an toàn hệ thống thông tin;*

*Căn cứ văn bản số 2079/CV-ATTT-NCPT ngày 08/08/2023 V/v “V/v Ý kiến thẩm định hồ sơ đề xuất cấp độ cho hệ thống VNPT RIS/PACS”;*

*Xét đề nghị của Giám đốc Trung tâm VNPT-IT Khu vực 3,*

### **QUYẾT ĐỊNH:**

**Điều 1. Phê duyệt cấp độ an toàn thông tin đối với Hệ thống Phần mềm chẩn đoán hình ảnh y khoa VNPT RIS/PACS cụ thể như sau:**

1. Thông tin chung:

a) Tên hệ thống thông tin: **Hệ thống Phần mềm chẩn đoán hình ảnh y khoa VNPT RIS/PACS.**

b) Đơn vị vận hành hệ thống thông tin: Công ty Công nghệ thông tin VNPT (VNPT-IT) – CN Tập đoàn Bưu chính Viễn thông Việt Nam.

c) Địa chỉ: Số 57 Phố Huỳnh Thúc Kháng, Phường Láng Hạ, Quận Đống Đa, Thành



phố Hà Nội, Việt Nam.

2. Cấp độ an toàn hệ thống thông tin: Cấp độ 3.

3. Phương án bảo đảm an toàn hệ thống thông tin:

Phương án bảo đảm an toàn thông tin trong thiết kế, quản lý và vận hành hệ thống trên tương ứng với cấp độ 3 là phù hợp với quy định tại Nghị định 85/2016/NĐ-CP ngày 01/07/2016 của Chính phủ, Thông tư 12/2022/TT-BTTTT ngày 12/08/2022 của Bộ Thông tin và Truyền thông và Tiêu chuẩn quốc gia TCVN 11930:2017 về bảo đảm an toàn hệ thống thông tin theo cấp độ.

## **Điều 2. Tổ chức thực hiện**

1. Trung tâm VNPT-IT Khu vực 3 (trực thuộc VNPT-IT) chịu trách nhiệm chủ trì tổ chức quản lý, vận hành, bảo đảm an toàn thông tin cho **Hệ thống Phần mềm chẩn đoán hình ảnh y khoa VNPT RIS/PACS** theo các yêu cầu tương ứng với Cấp độ 3 theo quy định tại Nghị định 85/2016/NĐ-CP ngày 01/07/2016 của Chính phủ, Thông tư số 12/2022/TT-BTTTT ngày 12/08/2022 của Bộ Thông tin và Truyền thông và Tiêu chuẩn quốc gia TCVN 11930:2017 về bảo đảm an toàn hệ thống thông tin theo cấp độ.

2. Trung tâm Điều hành IT, Trung tâm An toàn thông tin (trực thuộc VNPT-IT) có trách nhiệm phối hợp triển khai thực hiện các phương án bảo đảm an toàn thông tin tương ứng với cấp độ an toàn hệ thống thông tin theo quy định.

3. Ban Chất lượng sản phẩm (trực thuộc VNPT-IT) có trách nhiệm kiểm tra, giám sát việc thực hiện Quyết định này, báo cáo Tổng Giám đốc Công ty VNPT-IT theo quy định.

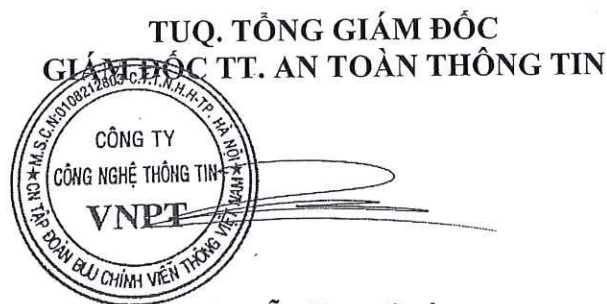
**Điều 3.** Quyết định này có hiệu lực thi hành kể từ ngày ký.

**Điều 4.** Các Ông (Bà) Chánh Văn phòng, Trưởng các Ban chức năng, Trưởng các đơn vị trực thuộc Công ty VNPT-IT chịu trách nhiệm thi hành quyết định này./.

### **Nơi nhận:**

- Như Điều 4;
- Lãnh đạo VNPT, Ban Công nghệ (để b/c);
- Ban TGD Cty VNPT-IT (để b/c);
- Lưu VT.

Số eOffice: 627465 - VBKS



**Nguyễn Ngọc Quân**

Số: 390/QĐ-VNPT IT-ATTT-NCPT

Hà Nội, ngày 02 tháng 3 năm 2023

## QUYẾT ĐỊNH

Về việc Phê duyệt cấp độ an toàn thông tin đối với Hệ thống quản lý  
xét nghiệm VNPT LIS

### TỔNG GIÁM ĐỐC CÔNG TY

Căn cứ Luật An toàn thông tin mạng số 86/2015/QH13 ngày 01/07/2015;

Căn cứ Nghị định 85/2016/NĐ-CP ngày 01/07/2016 của Chính phủ về việc đảm bảo an toàn hệ thống thông tin theo cấp độ;

Căn cứ Thông tư số 12/2022/TT-BTTTT ngày 12/08/2022 của Bộ Thông tin và Truyền thông Quy định chi tiết và hướng dẫn một số điều của Nghị định số 85/2016/NĐ-CP ngày 01/07/2016 của Chính phủ về Bảo đảm an toàn hệ thống thông tin theo cấp độ;

Căn cứ Quyết định số 39/QĐ-VNPT-HĐTV-NL ngày 01/03/2018 của Hội đồng thành viên Tập đoàn Bưu chính Viễn thông Việt Nam về việc thành lập Công ty Công nghệ thông tin VNPT (VNPT-IT) – đơn vị trực thuộc Tập đoàn VNPT;

Căn cứ văn bản số 6174/VNPT-CN của Tập đoàn Bưu chính Viễn thông Việt Nam ngày 14/10/2022 v/v Triển khai đảm bảo an toàn thông tin theo cấp độ;

Căn cứ văn bản số 238/GUQ-VNPTIT-VP của Tổng Giám đốc Công ty Công nghệ thông tin VNPT ngày 19/01/2023 V/v Ủy quyền thực hiện phê duyệt cấp độ an toàn hệ thống thông tin;

Căn cứ văn bản số 795/CV-ATTT-NCPT ngày 19/12/2022 v/v “Ý kiến thẩm định hồ sơ đề xuất cấp độ cho hệ thống VNPT LIS”;

Xét đề nghị của Giám đốc Trung tâm VNPT-IT khu vực 5,

### QUYẾT ĐỊNH:

**Điều 1. Phê duyệt cấp độ an toàn thông tin đối với Hệ thống quản lý xét nghiệm VNPT LIS cụ thể như sau:**

1. Thông tin chung:

- a) Tên hệ thống thông tin: Hệ thống quản lý xét nghiệm VNPT LIS.
- b) Đơn vị vận hành hệ thống thông tin: Công ty Công nghệ thông tin VNPT – Tập đoàn Bưu chính Viễn thông Việt Nam.
- c) Địa chỉ: 57 phố Huỳnh Thúc Kháng, phường Láng Hạ, Quận Đống Đa, TP Hà Nội, Việt Nam.



3. Phương án bảo đảm an toàn hệ thống thông tin:

Phương án bảo đảm an toàn thông tin trong thiết kế, quản lý và vận hành hệ thống trên tương ứng với cấp độ 3 là phù hợp với quy định tại Thông tư 12/2022/TT-BTTTT ngày 17/02/2022 của Bộ Thông tin và Truyền thông và Tiêu chuẩn quốc gia TCVN 11930:2017 về bảo đảm an toàn hệ thống thông tin theo cấp độ.

## Điều 2. Tổ chức thực hiện

1. Công ty Công nghệ thông tin VNPT (VNPT-IT) tổ chức quản lý, vận hành, bảo đảm an toàn thông tin cho Hệ thống quản lý xét nghiệm VNPT LIS theo quy định.
2. Trung tâm VNPT-IT khu vực 5, Trung tâm Điều hành IT, Trung tâm An toàn thông tin (trực thuộc VNPT-IT) có trách nhiệm:

Thực hiện các phương án bảo đảm an toàn thông tin tương ứng với Cấp độ 3 theo quy định tại Nghị định 85/2016/NĐ-CP ngày 01/07/2016 của Chính phủ và Thông tư số 12/2022/TT-BTTTT ngày 12/08/2022 của Bộ Thông tin và Truyền thông

3. Ban Chất lượng sản phẩm (trực thuộc VNPT-IT) có trách nhiệm:

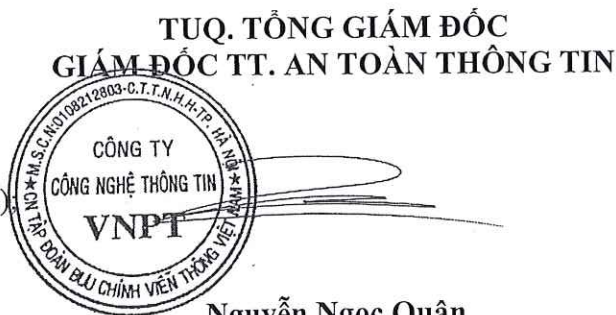
Kiểm tra, giám sát việc thực hiện Quyết định này, báo cáo Tổng Giám đốc Công ty VNPT-IT theo quy định.

**Điều 3.** Quyết định này có hiệu lực thi hành kể từ ngày ký.

**Điều 4.** Các Ông (Bà) Chánh Văn phòng, Trưởng các Ban chức năng, Trưởng các đơn vị trực thuộc Công ty VNPT-IT chịu trách nhiệm thi hành quyết định này./.

**Nơi nhân:**

- Lãnh đạo TĐ, Ban CN (đề b/c);
- Ban TGD Cty VNPT-IT (đề b/c);
- Ban CLgSP, Ban CLSP (đề t/h);
- TT: ITKV5, ĐHIT, ATTT, KTHT (đề t/h);
- Ban TTBH (đề biết);
- Lưu VT.



**Số eOffice: 162802 - VBĐT**

Nguyễn Ngọc Quân

Số: 846/QĐ-VNPT IT-ATTT-NCPT

Hà Nội, ngày 16 tháng 5 năm 2023

## QUYẾT ĐỊNH

### Về việc Phê duyệt cấp độ an toàn thông tin đối với Hệ thống VNPT HIS L2

#### TỔNG GIÁM ĐỐC CÔNG TY

Căn cứ Luật An toàn thông tin mạng số 86/2015/QH13 ngày 01/07/2015;

Căn cứ Nghị định 85/2016/NĐ-CP ngày 01/07/2016 của Chính phủ về việc đảm bảo an toàn hệ thống thông tin theo cấp độ;

Căn cứ Thông tư số 12/2022/TT-BTTTT ngày 12/08/2022 của Bộ Thông tin và Truyền thông Quy định chi tiết và hướng dẫn một số điều của Nghị định số 85/2016/NĐ-CP ngày 01/07/2016 của Chính phủ về Bảo đảm an toàn hệ thống thông tin theo cấp độ;

Căn cứ Quyết định số 39/QĐ-VNPT-HĐTV-NL ngày 01/03/2018 của Hội đồng thành viên Tập đoàn Bưu chính Viễn thông Việt Nam về việc thành lập Công ty Công nghệ thông tin VNPT (VNPT-IT) – đơn vị trực thuộc Tập đoàn VNPT;

Căn cứ văn bản số 6174/VNPT-CN của Tập đoàn Bưu chính Viễn thông Việt Nam ngày 14/10/2022 v/v Triển khai đảm bảo an toàn thông tin theo cấp độ;

Căn cứ văn bản số 238/GUQ-VNPTIT-VP của Tổng Giám đốc Công ty Công nghệ thông tin VNPT ngày 19/01/2023 V/v Ủy quyền thực hiện phê duyệt cấp độ an toàn hệ thống thông tin;

Căn cứ văn bản số 1007/CV-ATTT-NCPT ngày 10/4/2023 V/v “Ý kiến thẩm định hồ sơ đề xuất cấp độ cho hệ thống VNPT HIS L2”;

Xét đề nghị của Giám đốc Trung tâm Giải pháp Y tế điện tử,

#### QUYẾT ĐỊNH:

**Điều 1. Phê duyệt cấp độ an toàn thông tin đối với Hệ thống VNPT HIS L2 cụ thể như sau:**

1. Thông tin chung:

- Tên hệ thống thông tin: **Hệ thống Phần mềm quản lý bệnh viện VNPT HIS L2.**
- Đơn vị vận hành hệ thống thông tin: Công ty Công nghệ thông tin VNPT (VNPT-IT) – CN Tập đoàn Bưu chính Viễn thông Việt Nam.
- Địa chỉ: Số 57 Phố Huỳnh Thúc Kháng, Phường Láng Hạ, Quận Đống Đa, Thành phố Hà Nội, Việt Nam.



2. Cấp độ an toàn hệ thống thông tin: Cấp độ 3.

3. Phương án bảo đảm an toàn hệ thống thông tin:

Phương án bảo đảm an toàn thông tin trong thiết kế, quản lý và vận hành hệ thống trên tương ứng với cấp độ 3 là phù hợp với quy định tại Thông tư 12/2022/TT-BTTTT ngày 12/08/2022 của Bộ Thông tin và Truyền thông và Tiêu chuẩn quốc gia TCVN 11930:2017 về bảo đảm an toàn hệ thống thông tin theo cấp độ.

## **Điều 2. Tổ chức thực hiện**

1. Trung tâm Giải pháp Y tế điện tử (trực thuộc VNPT-IT) chịu trách nhiệm chủ trì tổ chức quản lý, vận hành, bảo đảm an toàn thông tin cho **Hệ thống Phần mềm quản lý bệnh viện VNPT HIS L2** theo các yêu cầu tương ứng với Cấp độ 3 theo quy định tại Nghị định 85/2016/NĐ-CP ngày 01/07/2016 của Chính phủ và Thông tư số 12/2022/TT-BTTTT ngày 12/08/2022 của Bộ Thông tin và Truyền thông.

2. Trung tâm Điều hành IT, Trung tâm An toàn thông tin (trực thuộc VNPT-IT) có trách nhiệm phối hợp triển khai thực hiện các phương án bảo đảm an toàn thông tin tương ứng với cấp độ an toàn hệ thống thông tin theo quy định.

3. Ban Chất lượng sản phẩm (trực thuộc VNPT-IT) có trách nhiệm kiểm tra, giám sát việc thực hiện Quyết định này, báo cáo Tổng Giám đốc Công ty VNPT-IT theo quy định.

**Điều 3.** Quyết định này có hiệu lực thi hành kể từ ngày ký.

**Điều 4.** Các Ông (Bà) Chánh Văn phòng, Trưởng các Ban chức năng, Trưởng các đơn vị trực thuộc Công ty VNPT-IT chịu trách nhiệm thi hành quyết định này./.

### **Nơi nhận:**

- Như Điều 4;
- Lãnh đạo VNPT, Ban Công nghệ (để b/c);
- Ban TGĐ Cty VNPT-IT (để b/c);
- Lưu VT.

Số eOffice: 371272 - VBKS

**TUQ. TỔNG GIÁM ĐỐC**  
**GIÁM ĐỐC TT. AN TOÀN THÔNG TIN**



**Nguyễn Ngọc Quân**

Số: 01 / QĐ-BVMHNĐNEMR

Đồng Nai, ngày 01 tháng 10 năm 2025

**QUYẾT ĐỊNH**

**Về việc ban hành Quy chế về hoàn thiện, quản lý  
và sử dụng bệnh án điện tử tại Bệnh viện Mắt Hà Nội – Đồng Nai**

**GIÁM ĐỐC BỆNH VIỆN MẮT HÀ NỘI – ĐỒNG NAI**

*Căn cứ Luật Khám bệnh, chữa bệnh ngày 09 tháng 01 năm 2023;*

*Căn cứ Luật An toàn thông tin mạng ngày 19 tháng 11 năm 2015*

*Căn cứ Luật Giao dịch điện tử ngày 22 tháng 06 năm 2023;*

*Căn cứ Luật căn cước số 26/2023/QH15 ngày 27 tháng năm 2023;*

*Căn cứ Nghị định số 96/NĐ-CP ngày 30/12/2023 của Chính phủ quy định chi tiết một số điều của Luật Khám bệnh, chữa bệnh;*

*Căn cứ Nghị định số 23/2025/NĐ-CP ngày 21/02/2025 của Chính phủ quy định về chữ ký điện tử và dịch vụ tin cậy;*

*Căn cứ Thông tư 32/2023/TT-BYT ngày 31/12/2023 của Bộ Y tế về Quy định chi tiết một số điều của Luật Khám bệnh, chữa bệnh;*

*Căn cứ Thông tư 13/2025/TT-BYT ngày 06/06/2025 của Bộ y tế Về Hướng dẫn triển khai hồ sơ bệnh án điện tử;*

*Căn cứ hướng dẫn tại Công văn số 365/TTYTQG-GPQLCL ngày 06/06/2025 của Trung tâm thông tin y tế Quốc Gia về Hướng dẫn yêu cầu kỹ thuật triển khai phần mềm hồ sơ bệnh án điện tử;*

*Xét đề nghị của Trưởng phòng Kế hoạch Tổng hợp.*

**QUYẾT ĐỊNH:**

**Điều 1.** Ban hành kèm theo Quyết định này “Quy chế về hoàn thiện, quản lý và sử dụng bệnh án điện tử tại Bệnh viện Mắt Hà Nội – Đồng Nai

**Điều 2.** Quyết định này có hiệu lực kể từ ngày ký.

**Điều 3.** Ban Giám đốc, Trưởng, phó khoa, phòng, Điều dưỡng trưởng, các tổ chức Đoàn thể và cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

**Nơi nhận:**

- Như Điều 3;
- Lưu VT, KHN.



**GIÁM ĐỐC**  
BS CKI. Hoàng Vĩnh Hà



SỞ Y TẾ ĐỒNG NAI  
BỆNH VIỆN MẮT  
HÀ NỘI – ĐỒNG NAI

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM  
Độc lập - Tự do - Hạnh phúc

## QUY CHẾ

### Quy chế về hoàn thiện, quản lý và sử dụng bệnh án điện tử tại Bệnh viện Mắt Hà Nội – Đồng Nai

(Ban hành kèm theo Quyết định số: 01 /QĐ-BVMHNDNEMR ngày 01 tháng 10 năm 2025  
của Giám đốc Bệnh viện Mắt Hà Nội – Đồng Nai)

## CHƯƠNG I

### QUY ĐỊNH CHUNG

#### Điều 1. Phạm vi điều chỉnh

Quy chế này quy định về việc lập, sử dụng, quản lý và chỉnh sửa hồ sơ bệnh án (sau đây gọi tắt là HSBA) điện tử tại Bệnh viện Mắt Hà Nội – Đồng Nai.

#### Điều 2. Giá trị pháp lý của HSBA điện tử

HSBA điện tử được lập, cập nhật, hiển thị, ký số, lưu trữ bằng phần mềm quản lý tổng thể bệnh viện đã đáp ứng các quy định của Thông tư 13/2025/TT-BYT ngày 06/06/2025 có giá trị pháp lý như HSBA giấy quy định tại Điều 69 Luật khám bệnh, chữa bệnh.

Khoản 1 điều 1 Thông tư 13/2025/TT-BYT quy định về giá trị pháp lý của Hồ sơ bệnh án điện tử tương đương khái niệm về Hồ sơ bệnh án tại điều khoản 17 điều 2 Luật 15/2023/QH15.

Điều 5 Thông tư 13/2025/TT-BYT quy định rõ về điều kiện chuyển tiếp cũng như công nhận giá trị pháp lý của HSBA điện tử.

#### Điều 3: Đối tượng áp dụng

Toàn thể cán bộ, nhân viên Bệnh viện Mắt Hà Nội – Đồng Nai có tài khoản trên Hệ thống phần mềm HIS của đơn vị, được cấp chữ ký số có chức năng, nhiệm vụ ký bệnh án và các giấy tờ, biểu mẫu phiếu y liên quan đến HSBA.

#### Điều 4. Mục đích sử dụng HSBA điện tử

1. Tận dụng và khai thác tối đa sức mạnh công nghệ thông tin trong việc xử lý, quản lý và lưu trữ HSBA điện tử, tăng tốc độ và hiệu quả; truy vấn và tham khảo dữ liệu.

2. Giúp người bệnh không phải lưu trữ và mang theo tất cả loại giấy tờ khi đi khám, chữa bệnh.

3. Bệnh án điện tử giúp quản lý thông tin sức khỏe liên tục, suốt đời của người dân, giúp người dân chủ động hơn trong phòng bệnh và chữa bệnh.

4. Việc đưa Bệnh án điện tử vào hoạt động cũng giảm thiểu thời gian chờ đợi và thủ tục rườm rà cho bệnh nhân và người nhà bệnh nhân.

5. Người bệnh không phải lo lắng nếu làm mất kết quả xét nghiệm, không phải hoang mang khi đọc chữ viết của bác sĩ.

6. Cung cấp thông tin, dữ liệu lâm sàng nhanh chóng, kịp thời giữa các cơ sở Khám, chữa bệnh. Khi thông tin về sức khỏe của người bệnh được thông suốt giữa các tuyến sẽ giúp việc chẩn đoán và phối hợp điều trị tốt hơn.

7. Các bác sĩ có thể truy cập HSBA điện tử từ bất kỳ nơi nào trên thế giới nếu có internet.

8. Tiết kiệm được chi phí duy trì các kho lưu trữ HSBA giấy.

9. Khi thông tin về Khám, chữa bệnh của người bệnh được minh bạch, giúp cho việc quản lý chi phí khám, chữa bệnh bảo hiểm y tế dễ dàng hơn, góp phần hạn chế việc lạm dụng thuốc và xét nghiệm nếu có.

10. Hồ sơ sức khỏe của người bệnh được bảo mật tuyệt đối và không bị rò rỉ thông tin sức khỏe qua bên ngoài.

#### **Điều 5. Nguyên tắc thực hiện thao tác trên HSBA điện tử**

1. Mỗi người bệnh khi nhập viện sẽ được cấp một mã số duy nhất dùng để quản lý, lưu trữ HSBA điện tử tại Bệnh viện Mắt Hà Nội – Đồng Nai đó là mã bệnh án, số vào viện hoặc số lưu trữ. Mã số này được cấp theo năm với cấu trúc như sau:

|                                          |
|------------------------------------------|
| <i>Số thứ tự / Mã khoa / Tháng / Năm</i> |
|------------------------------------------|

Ví dụ: 012345/K03/09/2024 là bệnh án số 01234 của Khoa nội (K03) tháng 09 năm 2024.

2. Khi thực hiện lập HSBA điện tử nhân viên y tế phải thực hiện đúng các yêu cầu sau đây:

a) Phải nhập liệu toàn bộ nội dung thông tin như HSBA giấy trên Hệ thống phần mềm HIS của đơn vị bao gồm tất cả các mẫu bệnh án đang được sử dụng tại Bệnh viện Mắt Hà Nội – Đồng Nai và các biểu mẫu khác có trong thành phần bệnh án được liệt kê ở Điều 7 theo Bộ Y tế và các biểu mẫu của đơn vị tự phát triển. Quy chế này theo đúng phân quyền truy cập thông tin (*các phiếu của bác sĩ thì tài khoản bác sĩ mới được tạo mới, tương tự đối với các phiếu của điều dưỡng, nữ hộ sinh, ...*)

b) Phải ký số và chịu trách nhiệm nội dung thông tin được nhập vào HSBA điện tử bao gồm các phiếu được quy định trong HSBA như các phiếu y, các phiếu kết quả cận lâm sàng, các bì bệnh án, phiếu điều trị.

c) Đối với các biểu mẫu phiếu y có 01 chữ ký khi lưu hệ thống phần mềm sẽ tự động ký số và không cho phép chỉnh sửa hoặc xóa khi chưa hủy ký số đối với nội dung phiếu vừa lưu.



d) Đối với các biểu mẫu phiếu y có từ 02 chữ ký trở lên thì phải ký số đầy đủ, nếu còn 01 người chưa ký thì xem như phiếu không hoàn tất, sẽ không thực hiện được khi lưu trữ HSBA .

e) Các sự kiện khám, chữa bệnh (*Khám bệnh, kê đơn, chỉ định dịch vụ, trả kết quả, đọc kết quả; Ghi chép của bác sĩ, điều dưỡng, nhân viên y tế, ...*) phải đảm bảo theo thời gian thực. Các trường hợp ngoại lệ:

+ Vô bệnh án (*không thuộc cấp cứu*) trong vòng 24 tiếng phải được hoàn thành.

+ Vô bệnh án thuộc cấp cứu trong vòng 48 tiếng phải được hoàn thành.

+ Tờ điều trị của bác sĩ cho phép lập phiếu trước không quá 12 tiếng so với thời gian thực.

+ Tờ chăm sóc của điều dưỡng cho phép lập phiếu trước không quá 12 tiếng so với thời gian thực.

f) Các bác sĩ thuộc các khoa Chẩn đoán hình ảnh, Nội soi, Xét nghiệm sử dụng chữ ký số để ký vào các phiếu kết quả chẩn đoán hình ảnh, thăm dò chức năng, xét nghiệm.

i) Đối với một số phiếu hoặc giấy tờ cần có chữ ký của người bệnh: nhân viên y tế sẽ hướng dẫn người bệnh ký tươi trên giấy cam đoan, cam kết phẫu thuật, phiếu đồng ý xét nghiệm HIV, bảng công khai thuốc đầu giường, kết quả xét nghiệm nồng độ cồn, ... Sau đó, các phiếu này sẽ được chụp ảnh thành bản điện tử và lưu trữ kèm theo HSBA điện tử, có chữ ký số xác nhận ảnh chụp của nhân viên y tế, đồng thời các phiếu bằng giấy này cũng phải được lưu trữ theo đúng quy định lưu trữ HSBA giấy.

j) Đối với bảng kê chi phí khám, chữa bệnh của bệnh nhân thực hiện đúng theo quyết định 6556/QĐ-BYT ngày 30/10/2018 phải có đầy đủ chữ ký bao gồm chữ ký bệnh nhân, chữ ký kế toán viện phí, và chữ ký nhân viên lập.

Đảm bảo bảng kê chi phí khám, chữa bệnh phải hoàn thiện khi kết thúc hồ sơ trên máy, tránh trường hợp hồ sơ đã trả về phòng Kế hoạch Tổng hợp và bảng kê chưa đầy đủ.

#### **Điều 6: Giải thích từ ngữ**

Trong Quy chế này, các từ ngữ dưới đây được hiểu như sau:

1. HIS là chữ viết tắt của cụm từ tiếng Anh “Hospital Information System” được dịch sang tiếng Việt là “Hệ thống thông tin bệnh viện”.

2. LIS là chữ viết tắt của cụm từ tiếng Anh “Laboratory Information System” được dịch sang tiếng Việt là “Hệ thống thông tin xét nghiệm”.

3. RIS là chữ viết tắt của cụm từ tiếng Anh “Radiology Information System” được dịch sang tiếng Việt là “Hệ thống thông tin chẩn đoán hình ảnh”.

4. PACS là chữ viết tắt của cụm từ tiếng Anh “Picture Archiving and Communication System” được dịch sang tiếng Việt là “Hệ thống lưu trữ và truyền tải hình ảnh”.

5. EMR là chữ viết tắt của cụm từ tiếng Anh “Electronic Medical Record” được dịch sang tiếng Việt là “Bệnh án điện tử”.

6. CDR là chữ viết tắt của cụm từ tiếng Anh “Clinical Data Repository” được dịch sang tiếng Việt là “Kho dữ liệu lâm sàng”.

7. CDSS là chữ viết tắt của cụm từ tiếng Anh “Clinical Decision Support System” được dịch sang tiếng Việt là “Hệ thống hỗ trợ quyết định lâm sàng”.

8. Tiêu chuẩn HL7 là chữ viết tắt của cụm từ tiếng Anh “Health Level 7 Standard” là tiêu chuẩn quốc tế cung cấp giao thức về quản lý, trao đổi và tích hợp thông tin y tế điện tử giữa các hệ thống thông tin y tế.

9. Tiêu chuẩn HL7 CDA chữ viết tắt của cụm từ tiếng Anh “Health Level 7 Clinical Document Architecture” là tài liệu có cấu trúc dựa trên định dạng XML quy định cấu trúc và ngữ nghĩa dữ liệu lâm sàng phục vụ mục tiêu trao đổi dữ liệu giữa các bên liên quan.

10. CCD là chữ viết tắt của cụm từ tiếng Anh “Continuity of Care Document” được dịch sang tiếng Việt là tập tin điện tử về tài liệu chăm sóc sức khỏe liên tục.

11. DICOM là chữ viết tắt của cụm từ tiếng Anh “Digital Imaging Communication in Medicine” là tiêu chuẩn quốc tế để truyền tải, lưu trữ, truy xuất, in ấn, xử lý và hiển thị thông tin hình ảnh y khoa.

12. Chữ ký số: là một dạng chữ ký điện tử được tạo ra bằng việc biến đổi một thông điệp dữ liệu sử dụng hệ thống mật mã không đối xứng theo người đó, có được thông điệp dữ liệu ban đầu và khóa công khai có thể xác định được chính xác.

*Chữ ký số sử dụng: Bệnh viện Mắt Hà Nội – Đồng Nai sử dụng chữ ký số được đăng ký bởi Tập đoàn Bưu chính Viễn thông Việt Nam (VNPT) được cung cấp trực tiếp bởi trung tâm VNPT-CA.*

## CHƯƠNG II

### HOÀN THIỆN, QUẢN LÝ VÀ SỬ DỤNG HỒ SƠ BỆNH ÁN ĐIỆN TỬ

#### Điều 7. Các loại và nội dung của HSBA điện tử

1. HSBA điện tử bao gồm HSBA nội trú, HSBA ngoại trú và các loại HSBA khác theo quy định tại về hồ sơ bệnh án tại khoản 17 Điều 2 Luật Khám bệnh.

2. Nội dung của HSBA điện tử gồm đầy đủ các trường thông tin theo mẫu của HSBA sử dụng trong cơ sở khám bệnh, chữa bệnh quy định tại Thông tư 32/2023/TT-BYT ngày 31/12/2023 của Bộ Y tế và Thông tư số 50/2017/TT-BYT ngày 29/12/2017 của Bộ trưởng Bộ Y tế sửa đổi, bổ sung các quy định liên quan đến thanh toán chi phí khám bệnh, chữa bệnh, Quyết định số 4604/QĐ-BYT ngày



29/11/2010 của Bộ trưởng Bộ Y tế Ban hành “Mẫu bệnh án Y học cổ truyền”, Quyết định số 999/QĐ-BYT ngày 05/04/2011 của Bộ trưởng Bộ Y tế về việc ban hành mẫu HSBA phá thai, Quyết định số 3443/QĐ-BYT ngày 22/09/2011 của Bộ trưởng Bộ Y tế về việc ban hành bổ sung mẫu HSBA và một số biểu mẫu hồ sơ chuyên khoa mắt, Quyết định số 1456/QĐ-BYT ngày 04/05/2012 của Bộ trưởng Bộ Y tế về việc ban hành mẫu HSBA bệnh tay chân miệng và các quy định khác có liên quan.

3. Danh sách các bệnh án, mẫu phiếu và hình thức ký sử dụng trong bệnh án điện tử của Bệnh viện Mắt Hà Nội – Đồng Nai được nêu ở Phụ lục kèm theo quyết định này.

### **Điều 8. Nhiệm vụ của Tổ kiểm tra HSBA**

- Chủ trì, phối hợp với phòng Kế hoạch Tổng hợp đảm bảo kiểm tra “đầu ra” về chất lượng HSBA trước khi gửi HSBA lên phòng Kế hoạch Tổng hợp để lưu trữ.

- Đảm bảo 100% HSBA trước khi lưu trữ được tổ kiểm tra đầy đủ về các nội dung: Hình thức, thủ tục hành chính; Các quy định pháp luật (biên bản phẫu thuật; lược trình phẫu thuật/thủ thuật; giấy cam đoan, ...); Nội dung chuyên môn.

- Những HSBA sau khi Tổ đã kiểm tra thì tích ô “xác nhận”. Chỉ những HSBA sau khi đã “xác nhận” mới được chuyển lên phòng Kế hoạch Tổng hợp để lưu trữ.

- Với những HSBA không đạt, Tổ kiểm tra có nhiệm vụ thông báo và chuyển về khoa lâm sàng để hoàn thiện.

### **Điều 9. Quy trình tiếp nhận, kiểm tra và lưu trữ HSBA**

1. Khoa lâm sàng tự kiểm tra việc hoàn thiện HSBA và gửi HSBA lên phòng Kế hoạch Tổng hợp để Tổ kiểm tra HSBA duyệt:

- Sau khi người bệnh ra viện trong vòng tối đa 3 -7 ngày khoa lâm sàng có nhiệm vụ hoàn thành HSBA (tổng kết HSBA) theo quy chế;

- Trưởng khoa lâm sàng kiểm tra tổng thể HSBA (hình thức; chất lượng nội dung; các loại giấy tờ; thủ tục hành chính, ...). Sau khi kiểm tra xong, Trưởng khoa (hoặc người được Giám đốc ủy quyền) xác nhận, ký chữ ký số đóng bệnh án và chuyển HSBA lên phòng Kế hoạch Tổng hợp;

- Đối với những HSBA chưa hoàn thiện hoặc còn thiếu mà bị Tổ kiểm tra HSBA trả về thì khoa/phòng phải có nhiệm vụ hoàn thiện, gửi lại lên phòng Kế hoạch Tổng hợp trong tối đa 48 giờ (trừ ngày lễ, ngày nghỉ).

2. Kiểm tra HSBA sau khi khoa lâm sàng chuyển lên phòng Kế hoạch Tổng hợp (Nhiệm vụ của Tổ kiểm tra HSBA, tại Điều 8):

Đối với những HSBA không đạt yêu cầu, Tổ kiểm tra HSBA có trách nhiệm gửi lại và thông báo cho khoa lâm sàng để sửa chữa, hoàn thiện.

3. Khắc phục HSBA chưa đạt yêu cầu:

- Thời gian khắc phục HSBA tối đa 48 giờ (trừ ngày lễ, ngày nghỉ) sau khi HSBA được trả về khoa. Nếu khoa lâm sàng không khắc phục, sửa chữa thì sẽ bị xử lý theo quy định.

- Đối với bệnh nhân được điều trị tại nhiều khoa, khoa cuối cùng có trách nhiệm hoàn thiện HSBA.

- Hàng tuần (sáng thứ 2), phòng Kế hoạch Tổng hợp thông báo những tồn tại và những HSBA khắc phục chậm của các khoa vào buổi giao ban cuối tuần.

#### 4. Cập nhật HSBA điện tử:

Thời gian cập nhật HSBA điện tử tối đa 12 giờ, kể từ khi có y lệnh khám bệnh, chữa bệnh. Trường hợp thời gian khám, chữa bệnh kéo dài trên 12 giờ hoặc có sự cố về công nghệ thông tin thì thời gian cập nhật HSBA điện tử tối đa không quá 24 giờ.

#### 5. Ký xác nhận HSBA để lưu trữ:

Giám đốc, các Phó Giám đốc hoặc người được Giám đốc ủy quyền (Trưởng khoa, trưởng phòng) được phép ký xác nhận (bằng chữ ký số) vào bìa HSBA đối với những HSBA đã được Tổ kiểm tra HSBA xác nhận “đạt”.

#### 6. Lưu trữ HSBA:

HSBA được lưu trữ sau khi Giám đốc, các Phó giám đốc hoặc người được Giám đốc ủy quyền ký xác nhận. HSBA được “tích” chuyển vào kho lưu trữ tại phần mềm HIS.

HSBA được lưu trữ tại Trung tâm dữ liệu của VNPT (IDC Nam Thăng Long) và lưu trữ dự phòng (backup) lưu trữ về hệ thống máy chủ tại *Bệnh viện Mắt Hà Nội – Đồng Nai*.

HSBA được sao lưu định kỳ theo quy chế sao lưu phục hồi dữ liệu của *Bệnh viện Mắt Hà Nội – Đồng Nai* đảm bảo theo quy định tại Điều 6 Thông tư 46/2018/TT-BYT ngày 28/12/2018 của Bộ Y tế.

### **Điều 10. Sử dụng và khai thác HSBA điện tử**

Việc sử dụng và khai thác HSBA điện tử phải tuân thủ đúng quy định tại Điều 69 Luật Khám chữa bệnh số 15/2023/QH15 ngày 09/01/2023 cụ thể như sau:

1. HSBA phải được lưu giữ và giữ bí mật theo quy định của pháp luật; trường hợp HSBA thuộc phạm vi bí mật nhà nước thì thực hiện theo quy định của pháp luật về bảo vệ bí mật nhà nước. Việc lưu trữ HSBA được thực hiện theo quy định của pháp luật về lưu trữ.

2. Việc khai thác HSBA đang trong quá trình điều trị được thực hiện như sau:

a) Học sinh, sinh viên, học viên, nghiên cứu viên của các cơ sở nghiên cứu, cơ sở đào tạo, người hành nghề, người trực tiếp tham gia điều trị người bệnh trong



cơ sở khám bệnh, chữa bệnh được đọc nhưng chỉ được sao chép khi có sự đồng ý của Ban giám đốc hoặc Trưởng phòng Kế hoạch Tổng hợp của Bệnh viện Mắt Hà Nội – Đồng Nai.

b) Người hành nghề của cơ sở khác được đọc, sao chép khi có sự đồng ý của Ban giám đốc hoặc Trưởng phòng Kế hoạch Tổng hợp của Bệnh viện Mắt Hà Nội – Đồng Nai.

3. Việc khai thác HSBA đã hoàn thành quá trình điều trị và được chuyển lưu trữ được thực hiện như sau:

a) Đại diện cơ quan quản lý nhà nước về y tế, cơ quan điều tra, viện kiểm sát, tòa án, thanh tra chuyên ngành y tế, tổ chức giám định pháp y, pháp y tâm thần, luật sư của người bệnh được tiếp cận, cung cấp HSBA để thực hiện nhiệm vụ theo quy định của pháp luật có liên quan;

b) Học sinh, sinh viên, học viên, nghiên cứu viên của các cơ sở nghiên cứu, cơ sở đào tạo, người hành nghề trong cơ sở khám bệnh, chữa bệnh được mượn HSBA tại chỗ để đọc hoặc sao chép phục vụ cho việc nghiên cứu hoặc công tác chuyên môn kỹ thuật khi có sự đồng ý của Ban giám đốc hoặc Trưởng phòng Kế hoạch Tổng hợp của Bệnh viện Mắt Hà Nội – Đồng Nai;

c) Đại diện cơ quan bảo hiểm xã hội, cơ quan giải quyết bồi thường nhà nước được mượn HSBA tại chỗ để đọc, ghi chép hoặc đề nghị cấp bản sao phục vụ nhiệm vụ được giao khi có sự đồng ý của Ban giám đốc hoặc Trưởng phòng Kế hoạch Tổng hợp của Bệnh viện Mắt Hà Nội – Đồng Nai;

d) Người bệnh hoặc người đại diện của người bệnh quy định tại điểm c và điểm d khoản 2 Điều 8 của Luật này được đọc, xem, sao chụp, ghi chép HSBA và được cung cấp bản tóm tắt HSBA khi có yêu cầu bằng văn bản;

đ) Người đại diện của người bệnh quy định tại điểm a và điểm d khoản 2 Điều 8 của Luật này được cung cấp bản tóm tắt HSBA khi có yêu cầu bằng văn bản.

4. Các đối tượng quy định tại khoản 2 và khoản 3 Điều này khi sử dụng thông tin trong HSBA phải giữ bí mật và chỉ được sử dụng đúng mục đích như đã đề nghị với Bệnh viện Mắt Hà Nội – Đồng Nai

### **CHƯƠNG III TỔ CHỨC THỰC HIỆN**

#### **Điều 11. Trách nhiệm của Bệnh viện Mắt Hà Nội – Đồng Nai**

1. Quản lý chặt chẽ hệ thống hạ tầng, đảm bảo hệ thống công nghệ thông tin của Bệnh viện hoạt động ổn định.

2. Chịu trách nhiệm cập mới, thu hồi, cấp lại các tài khoản có chữ ký điện tử, chữ ký số cho các cá nhân quản lý và sử dụng trong bệnh án điện tử.

3. Ban Giám đốc chỉ đạo Phòng Kế hoạch Tổng hợp, Tổ Công nghệ thông tin tổ chức tập huấn thường xuyên cho toàn nhân viên của đơn vị về quản lý, bảo mật và sử dụng HSBA điện tử.

### **Điều 12. Trách nhiệm cá nhân**

1. Cá nhân tự quản lý mật khẩu tài khoản, chữ ký số, chữ ký điện tử đang sử dụng trên phần mềm tại Bệnh viện Mắt Hà Nội – Đồng Nai.
2. Tham gia đào tạo và tập huấn về sử dụng hệ thống phần mềm HIS, chữ ký số, chữ ký điện tử.

### **Điều 13. Trách nhiệm của Tổ Công nghệ thông tin**

1. Chịu trách nhiệm cài đặt phần mềm quản lý tổng thể bệnh viện bao gồm các phân hệ HIS, LIS, PACS, EMR, chữ ký số, chữ ký điện tử. Cập nhật phiên bản phần mềm mới.
2. Tập huấn, hỗ trợ kỹ thuật cho nhân viên tại Bệnh viện Mắt Hà Nội – Đồng Nai trong quá trình sử dụng chữ ký số, chữ ký điện tử.
3. Tham mưu, giúp Ban Giám đốc kiểm tra, giám sát và đôn đốc việc quản lý và sử dụng HSBA điện tử.
4. Lập kế hoạch ứng phó sự cố, bản quản hệ thống dữ liệu thường xuyên.

### **Điều 14. Điều khoản thi hành**

1. Quy định này được áp dụng kể từ ngày 01/10/2025.
2. Trong quá trình thực hiện nếu có khó khăn, vướng mắc cần sửa đổi, bổ sung, các cá nhân phản ánh trực tiếp về Phòng Kế hoạch Tổng hợp để được hướng dẫn cụ thể.



**GIÁM ĐỐC**  
BS CKI. Hoàng Vĩnh Hà



**PHỤ LỤC: DANH SÁCH CÁC BỆNH ÁN, MẪU PHIẾU VÀ HÌNH THỨC  
KÝ SỬ DỤNG TRONG BỆNH ÁN ĐIỆN TỬ  
CỦA BỆNH VIỆN MẮT HÀ NỘI – ĐỒNG NAI**

*(Ban hành kèm theo Quyết định số: 07 /QĐ-ĐNEMR ngày 01 tháng 10 năm 2025  
của Giám đốc Bệnh viện Mắt Hà Nội – Đồng Nai)*

| STT      | Tên mẫu phiếu, bệnh án                                   | Hình thức ký Nội trú                                           | Hình thức ký Ngoại trú | Ghi chú |
|----------|----------------------------------------------------------|----------------------------------------------------------------|------------------------|---------|
| <b>I</b> | <b>Mẫu giấy, Phiếu y</b>                                 |                                                                |                        |         |
| 1        | Đơn thuốc                                                | BS điều trị ký số                                              | BS phòng khám ký số    |         |
| 2        | Phiếu điều trị                                           | BS điều trị ký số                                              | BS điều trị ký số      |         |
| 3        | Phiếu chỉ định CDHA                                      | BS chỉ định ký số                                              |                        |         |
| 4        | Phiếu chỉ định xét nghiệm                                | BS chỉ định ký số                                              |                        |         |
| 5        | Phiếu chỉ định PTTT                                      | BS chỉ định ký số                                              |                        |         |
| 6        | Phiếu truyền máu                                         | Người làm xét nghiệm, ĐD thực hiện, BS điều trị (tất cả ký số) |                        |         |
| 7        | Phiếu khám chuyên khoa                                   | BS điều trị ký số                                              |                        |         |
| 8        | Phiếu chăm sóc                                           | ĐD ký điện tử                                                  |                        |         |
| 9        | Phiếu kế hoạch chăm sóc                                  | ĐD ký điện tử                                                  |                        |         |
| 10       | Phiếu theo dõi truyền dịch                               | ĐD ký điện tử, BS chỉ định ký số                               |                        |         |
| 11       | Phiếu thử phản ứng thuốc                                 | BS chỉ định; người thử; BS đọc kết quả ký số                   |                        |         |
| 12       | Giấy xác nhận bệnh nhân đang nằm viện                    | BS điều trị; Trưởng khoa ký số                                 |                        |         |
| 13       | Giấy ra viện                                             | Trưởng khoa, GD ký số                                          | BS ký số               |         |
| 14       | Giấy chứng nhận nghỉ việc hưởng BHXH                     | BS điều trị; Đại diện đơn vị (Ban giám đốc) ký số              |                        |         |
| 15       | Phiếu khám tiền mê                                       | BS ký số                                                       |                        |         |
| 16       | Phiếu đánh giá tình trạng dinh dưỡng (trưởng thành, trẻ, | BS ký số                                                       |                        |         |

| STT | Tên mẫu phiếu, bệnh án                                                        | Hình thức ký Nội trú                                    | Hình thức ký Ngoại trú | Ghi chú             |
|-----|-------------------------------------------------------------------------------|---------------------------------------------------------|------------------------|---------------------|
|     | sản, >18 tuổi không mang thai)                                                |                                                         |                        |                     |
| 17  | Phiếu kết quả xét nghiệm Giải phẫu bệnh                                       | BS ký số                                                |                        |                     |
| 18  | Phiếu kết quả xét nghiệm tế bào                                               | BS ký số                                                |                        |                     |
| 19  | Phiếu kết quả xét nghiệm PAP SMEAR                                            | BS ký số                                                |                        |                     |
| 20  | Phiếu kiểm gác và dụng cụ phẫu thuật                                          | ĐD vòng trong, ĐD vòng ngoài (tất cả ký số)             |                        |                     |
| 21  | Biên bản kiểm kê trước mổ                                                     | ĐD ký số                                                |                        |                     |
| 22  | Bảng kiểm chuẩn bị người bệnh trước phẫu thuật                                | ĐD ký số                                                |                        |                     |
| 23  | Phiếu theo dõi người bệnh sau mổ (trong 24 giờ đầu)                           | ĐD ký số                                                |                        |                     |
| 24  | Phiếu theo dõi và hồi sức người bệnh chưa mổ và sau mổ (từ giờ thứ 25 trở đi) | ĐD ký số                                                |                        |                     |
| 25  | Phiếu đánh giá trước khi cho người bệnh ra khỏi phòng hồi tỉnh                | Số hóa, in cho người bệnh ký, sau đó scan phiếu ký chốt |                        | Scan chuyển vào EMR |
| 26  | Phiếu bàn giao người bệnh và chuyển khoa hoặc chuyển phòng (BS)               | BS khoa giao, BS khoa nhận (tất cả ký số)               |                        |                     |
| 27  | Phiếu bàn giao người bệnh và chuyển khoa hoặc chuyển phòng (ĐD)               | BS khoa giao, BS khoa nhận (tất cả ký số)               |                        |                     |
| 28  | Biểu đồ chuyển dạ                                                             | ĐD ký số                                                |                        |                     |
| 29  | Phiếu điều trị sơ sinh (sau sinh)                                             | ĐD, BS, BS khám bệnh (ĐD ký điện tử, còn lại Ký số)     |                        |                     |



| STT | Tên mẫu phiếu, bệnh án                                            | Hình thức ký Nội trú                                    | Hình thức ký Ngoại trú | Ghi chú             |
|-----|-------------------------------------------------------------------|---------------------------------------------------------|------------------------|---------------------|
| 30  | Monitoring chỉ định                                               | Khai thác ghi tay, scan phiếu ký chốt                   |                        | Scan chuyển vào EMR |
| 31  | Monitoring kết quả                                                | Khai thác ghi tay, scan phiếu ký chốt                   |                        | Scan chuyển vào EMR |
| 32  | Bảng cho thuốc                                                    | Khai thác ghi tay, scan phiếu ký chốt                   |                        | Scan chuyển vào EMR |
| 33  | Phiếu kết quả nghiệm dung nạp 75gr glucose                        | Khai thác ghi tay, scan phiếu ký chốt                   |                        | Scan chuyển vào EMR |
| 34  | Giấy cam đoan chấp nhận phẫu thuật, thủ thuật và gây mê hồi sức   | Số hóa, in cho người bệnh ký, sau đó scan phiếu ký chốt |                        | Scan chuyển vào EMR |
| 35  | Cam kết phẫu thuật                                                | Số hóa, in cho người bệnh ký, sau đó scan phiếu ký chốt |                        | Scan chuyển vào EMR |
| 36  | Giấy cam kết chấp nhận gây mê hồi sức                             | Số hóa, in cho người bệnh ký, sau đó scan phiếu ký chốt |                        | Scan chuyển vào EMR |
| 37  | Giấy cam kết ra viện không theo chỉ định của BS (giấy xin về)     | Số hóa, in cho người bệnh ký, sau đó scan phiếu ký chốt |                        | Scan chuyển vào EMR |
| 38  | Giấy cung cấp thông tin và cam kết chung về nhập viện nội trú     | Số hóa, in cho người bệnh ký, sau đó scan phiếu ký chốt |                        | Scan chuyển vào EMR |
| 39  | Phiếu công khai thuốc                                             | Số hóa, in cho người bệnh ký, sau đó scan phiếu ký chốt |                        | Scan chuyển vào EMR |
| 40  | Từ chối sử dụng dịch vụ khám bệnh chữa bệnh                       | Số hóa, in cho người bệnh ký, sau đó scan phiếu ký chốt |                        | Scan chuyển vào EMR |
| 41  | Bảng kê sử dụng thuốc, VTYT, DVKT của bệnh nhân nội trú theo khoa | Số hóa, in cho người bệnh ký, sau đó scan phiếu ký chốt |                        | Scan chuyển vào EMR |
| 42  | Phiếu theo dõi chăm sóc cấp 1, Phiếu theo dõi chăm sóc (cấp 2-3)  | ĐD ký số                                                |                        |                     |

| STT | Tên mẫu phiếu, bệnh án                    | Hình thức ký Nội trú                                                | Hình thức ký Ngoại trú                                  | Ghi chú                 |
|-----|-------------------------------------------|---------------------------------------------------------------------|---------------------------------------------------------|-------------------------|
| 43  | Phiếu theo dõi chức năng sống             | ĐD ký số                                                            |                                                         |                         |
| 44  | Đánh giá người bệnh nhập viện             | BS ký số                                                            |                                                         |                         |
| 45  | Phiếu kết quả xét nghiệm                  | KTV xét nghiệm (người thực hiện); Trưởng khoa xét nghiệm ký số      |                                                         | Thực hiện trên LIS      |
| 46  | Phiếu kết quả CDHA_Xquang, CT             | Người đọc kết quả ký số                                             |                                                         | Thực hiện trên RIS/PACS |
| 47  | Phiếu kết quả CDHA Siêu âm, nội soi       | Người đọc kết quả ký số                                             |                                                         | Thực hiện trên RIS/PACS |
| 48  | Trích biên bản hội chẩn                   | Chủ tọa, thư ký, thành viên tham gia (từ 1 - 4 người); tất cả ký số |                                                         |                         |
| 49  | Phiếu gây mê hồi sức                      | BS ký số                                                            |                                                         |                         |
| 50  | Phiếu chứng nhận PTTT                     | Trưởng khoa, GD ký số                                               | BS ký số                                                |                         |
| 51  | Giấy hẹn khám lại                         | Bác sĩ điều trị; Đại diện đơn vị (Ban giám đốc) ký số               |                                                         |                         |
| 52  | Phiếu theo dõi tại phòng hồi tỉnh         | Khai thác ghi tay, scan phiếu ký chốt                               |                                                         | Scan chuyển vào EMR     |
| 53  | Phiếu công khai vật tư                    | Số hóa, in cho người bệnh ký, sau đó scan phiếu ký chốt             |                                                         | Scan chuyển vào EMR     |
| 54  | Phiếu công khai dịch vụ                   | Số hóa, in cho người bệnh ký, sau đó scan phiếu ký chốt             |                                                         | Scan chuyển vào EMR     |
| 55  | Phiếu công khai thuốc                     | Số hóa, in cho người bệnh ký, sau đó scan phiếu ký chốt             |                                                         | Scan chuyển vào EMR     |
| 56  | Bảng kê Ngoài BHYT của bệnh nhân nội trú  | Số hóa, in cho người bệnh ký, sau đó scan phiếu ký chốt             | Số hóa, in cho người bệnh ký, sau đó scan phiếu ký chốt | Scan chuyển vào EMR     |
| 57  | Bảng kê BHYT của bệnh nhân khám ngoại trú | Số hóa, in cho người bệnh ký, sau đó scan phiếu ký chốt             | Số hóa, in cho người bệnh ký, sau                       | Scan chuyển vào EMR     |



| STT       | Tên mẫu phiếu, bệnh án                       | Hình thức ký Nội trú                                    | Hình thức ký Ngoại trú                                  | Ghi chú             |
|-----------|----------------------------------------------|---------------------------------------------------------|---------------------------------------------------------|---------------------|
|           |                                              |                                                         | đó scan phiếu ký chốt                                   |                     |
| 58        | Bảng kê BHYT của bệnh nhân bệnh án ngoại trú | Số hóa, in cho người bệnh ký, sau đó scan phiếu ký chốt | Số hóa, in cho người bệnh ký, sau đó scan phiếu ký chốt | Scan chuyển vào EMR |
| 59        | Bảng kê BHYT của bệnh nhân nội trú           | Số hóa, in cho người bệnh ký, sau đó scan phiếu ký chốt | Số hóa, in cho người bệnh ký, sau đó scan phiếu ký chốt | Scan chuyển vào EMR |
| <b>II</b> | <b>Phiếu nhận từ nơi khác chuyển đến</b>     |                                                         |                                                         |                     |
| 1         | Giấy chuyển viện từ nơi khác đến             |                                                         |                                                         | Scan chuyển vào EMR |

SỞ Y TẾ TỈNH ĐỒNG NAI  
BỆNH VIỆN MẮT HÀ NỘI – ĐỒNG NAI

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM  
Độc lập - Tự do - Hạnh phúc

Số: 01 /QĐ-ĐNEMR

Đồng Nai, ngày 01 tháng 10 năm 2025

## QUYẾT ĐỊNH

**Về việc ban hành Quy định quản lý, sử dụng hệ thống Camera giám sát trong Bệnh viện Mắt Hà Nội – Đồng Nai**

### GIÁM ĐỐC BỆNH VIỆN

*Căn cứ Luật Công nghệ thông tin ngày 29/06/2006;*

*Căn cứ Luật An toàn thông tin ngày 19/11/2015;*

*Căn cứ Luật An ninh mạng ngày 12/06/2018;*

*Căn cứ Nghị định số 64/2007/NĐ-CP ngày 10/04/2007 của Chính phủ về việc ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước;*

*Căn cứ Nghị định số 47/2020/NĐ-CP ngày 09/04/2020 của Chính phủ về quản lý, kết nối và chia sẻ dữ liệu số của cơ quan nhà nước;*

*Xét đề nghị của Trưởng phòng Tổ chức – Hành chính, Trưởng phòng Kế hoạch – Nghiệp vụ - Điều dưỡng,*

### QUYẾT ĐỊNH:

**Điều 1.** Ban hành kèm theo Quyết định này Quy định quản lý, sử dụng hệ thống Camera giám sát tại Bệnh viện Mắt Hà Nội – Đồng Nai

**Điều 2.** Bản “Quy định quản lý, sử dụng hệ thống Camera giám sát” ban hành kèm theo Quyết định này được áp dụng tại các Khoa, Phòng thuộc Bệnh viện Mắt Hà Nội – Đồng Nai

**Điều 3.** Quyết định này có hiệu lực thi hành kể từ ngày ký.

**Điều 4.** Các ông (bà) Trưởng phòng Hành chính – Kế Toán; Trưởng phòng Kế hoạch tổng hợp; Trưởng các Khoa, Phòng trực thuộc Bệnh viện và các cá nhân, đơn vị liên quan chịu trách nhiệm thi hành Quyết định này./.

#### Nơi nhận:

- Như Điều 4;
- GD và các Phó GD TTYT;
- Lưu VT, TCHC.



**GIÁM ĐỐC**  
BS CKI. Hoàng Vinh Hà



## **QUY ĐỊNH QUẢN LÝ, SỬ DỤNG HỆ THỐNG CAMERA GIÁM SÁT TRONG BỆNH VIỆN MẮT HÀ NỘI – ĐỒNG NAI**

*(Ban hành kèm theo Quyết định số: 01 /ĐNEMR, ngày 01 tháng 10 năm 2025  
của Giám đốc Bệnh viện Mắt Hà Nội – Đồng Nai)*

### **Điều 1: Mục đích, phạm vi áp dụng**

1. Văn bản này quy định về việc quản lý và sử dụng hệ thống Camera giám sát hỗ trợ công tác đảm bảo an ninh, an toàn tại Bệnh viện Mắt Hà Nội – Đồng Nai

2. Đối tượng áp dụng của Quy định này bao gồm toàn thể cán bộ, viên chức, người lao động và người dân đến khám và điều trị tại Bệnh viện.

### **Điều 2: Quy định chung**

1. Hệ thống Camera giám sát được xác định là công cụ hỗ trợ cho công tác quản lý an ninh, trật tự và được truy xuất dữ liệu khi có chỉ đạo của Giám đốc.

2. Hệ thống Camera giám sát là tài sản của Bệnh viện Mắt Hà Nội – Đồng Nai, giao cho Phòng Kế hoạch tổng hợp trực tiếp quản lý và sử dụng phục vụ cho công tác kiểm tra, giám sát và chịu trách nhiệm trước Giám đốc.

3. Việc lưu trữ hình ảnh, dữ liệu giám sát bằng Camera được lưu trữ theo quy định của đơn vị, sử dụng ổ đĩa máy vi tính hoặc thiết bị lưu trữ chuyên dụng khác theo quy định.

4. Trường hợp xảy ra sự cố, hư hỏng, Phòng Kế hoạch tổng hợp xử lý ngay tùy sự cố kỹ thuật, không tiếp tục cho thiết bị hoạt động để hạn chế thấp nhất hư hỏng. Báo cáo Ban giám đốc, đề xuất sửa chữa, thay thế phục vụ công tác.

5. Thực hiện chế độ bảo trì, bảo dưỡng định kỳ, đề xuất sửa chữa thay thế những thiết bị hư hỏng, kiểm tra hiệu chuẩn thiết bị đúng quy định; phân công cán bộ chịu trách nhiệm quản lý, sử dụng, vệ sinh sau khi sử dụng, bảo quản, lưu giữ thiết bị theo yêu cầu của nhà sản xuất, kiểm tra các chức năng hoạt động của thiết bị đảm bảo sẵn sàng phục vụ công tác.

6. Về kiểm tra tình trạng sử dụng trang thiết bị: Định kỳ vào cuối năm hoặc đột xuất theo yêu cầu. Sau khi kiểm tra tình trạng sử dụng trang thiết bị, Phòng Kế hoạch tổng hợp tiến hành đề xuất phương án.

### **Điều 3: Quy định cụ thể**

1. Phân quyền khai thác và sử dụng:
  - Ban Giám đốc: Giám đốc, Phó giám đốc.
  - Phòng Kế hoạch tổng hợp: trực tiếp quản lý và sử dụng.
  - Lãnh đạo thường xuyên kiểm tra, nhắc nhở nhân viên, người lao động thực hiện đúng trình tự quản lý, sử dụng, vận hành thiết bị.

2. Đối với nhân viên được phân công quản lý, sử dụng truy xuất dữ liệu hình ảnh

- Nhân viên được phân công chịu trách nhiệm kiểm tra, khởi động và vận hành thiết bị, thực hiện thao tác từ khởi động đến kết thúc theo đúng trình tự đã được tập huấn, theo hướng dẫn của nhà sản xuất.

- Nhân viên được phân công chịu trách nhiệm theo dõi hình ảnh Camera quan sát hoặc đề xuất kiểm tra dữ liệu của Camera, nếu có thông tin cảnh báo hoặc phát hiện có nghi vấn cần xử lý tại hiện trường thì chụp ảnh, in ảnh, báo cáo lãnh đạo xử lý theo thẩm quyền, thực hiện ghi nhận tình hình kiểm tra vào hồ sơ và ghi nhận đồng thời vào sổ theo dõi quản lý việc sử dụng.

Thực hiện các bước cơ bản sau:

- + Đăng nhập hệ thống.
- + Chọn hệ thống Camera, khu vực đặt Camera theo yêu cầu quan sát.
- + Thực hiện ghi hình theo yêu cầu quản lý: Ghi theo ngày/giờ hoặc ghi theo sự kiện.

- + Tìm kiếm, truy xuất dữ liệu bằng cách: chọn Camera muốn truy xuất hoặc chọn ngày/giờ muốn truy xuất để kiểm tra, tìm kiếm dữ liệu.

- Trường hợp có sự cố về hệ thống máy tính, chương trình hoặc Camera không hoạt động thì báo cáo lãnh đạo để chỉ đạo cán bộ quản trị mạng xử lý kịp thời các sự cố, vướng mắc phát sinh liên quan đến hệ thống Camera.

- Hình ảnh, dữ liệu do Camera ghi lại là cơ sở để xem xét xử lý các vụ việc có liên quan.

#### **Điều 4: Kiểm tra khai thác dữ liệu**

1. Phòng Kế hoạch tổng hợp chịu trách nhiệm tổ chức lưu trữ và bảo mật các dữ liệu hình ảnh của hệ thống Camera giám sát.

2. Ban Giám đốc được quyền yêu cầu xem, kiểm tra những hình ảnh đã được lưu trữ trong hệ thống Camera giám sát.

3. Các đơn vị, cá nhân có nhu cầu xem, kiểm tra những hình ảnh đã được lưu trữ trong hệ thống Camera phải có đề nghị bằng văn bản và được sự đồng ý của Ban Giám đốc hoặc Trưởng phòng Kế hoạch tổng hợp.

#### **Điều 5: Các hành vi nghiêm cấm**

1. Để lộ hoặc cung cấp tài khoản truy cập hệ thống cho người khác, đơn vị khác.

2. Kết nối, cài cắm trái phép các thiết bị khác vào hệ thống Camera.

3. Can thiệp, ngăn chặn, truy cập trái phép hoặc làm vô hiệu quá tính năng kỹ thuật của hệ thống Camera.

4. Thay đổi, ngăn chặn, truy cập trái phép đường truyền nhận, ghi hình ảnh của hệ thống Camera.

5. Xoá, thay đổi, sao chép hoặc tiết lộ trái phép các dữ liệu hình ảnh được lưu trữ trên hệ thống Camera.

#### **Điều 6: Xử lý vi phạm**



1. Dữ liệu hình ảnh do Camera ghi lại là cơ sở làm chứng cứ truy cứu trách nhiệm và xem xét xử lý các vụ việc vi phạm cụ thể của cá nhân và đơn vị có liên quan.

2. Đơn vị, cá nhân vi phạm quy định này thì tùy theo tính chất, mức độ vi phạm mà xử lý kỷ luật. Nếu gây thiệt hại thì phải bồi thường theo quy định.

**Điều 7: Tổ chức thực hiện**

- Quy định này có hiệu lực kể từ ngày ký.
- Trong quá trình triển khai, thực hiện, nếu phát sinh vướng mắc thì tập hợp ý kiến gửi về Phòng Kế hoạch tổng hợp làm cơ sở trình Ban Giám đốc hướng xử lý, giải quyết./.

**GIÁM ĐỐC**



**GIÁM ĐỐC**  
BS CKI. Hoàng Vĩnh Hà

Mẫu văn bản đề nghị xem, kiểm tra hình ảnh trong hệ thống Camera

**BỆNH VIỆN MẮT HÀ NỘI – ĐỒNG NAI**  
KHOA/PHÒNG .....

**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM**  
**Độc lập - Tự do - Hạnh phúc**

*Đồng Nai, ngày 01 tháng 10 năm 2025*

**GIẤY ĐỀ NGHỊ XEM, KIỂM TRA HÌNH ẢNH**  
**TRONG HỆ THỐNG CAMERA AN NINH TẠI BỆNH VIỆN**

Kính gửi:

- Ban giám đốc Bệnh viện.
- Trưởng phòng kế hoạch tổng hợp.

Tôi tên là: ..... hiện đang làm việc tại Khoa, phòng ..... của Bệnh viện mắt Hà Nội – Đồng Nai có nhu cầu xem, kiểm tra hình ảnh trong Hệ thống Camera của Bệnh viện.

Lý do đề nghị xem, kiểm tra: .....

Thời gian đề nghị kiểm tra:

Từ ..... giờ ..... phút, ngày .....

Đến ..... giờ ..... phút, ngày .....

Vị trí camera đề nghị kiểm tra: .....

**NGƯỜI ĐỀ NGHỊ**  
(ký, ghi rõ họ tên)

**CÁN BỘ TRÍCH XUẤT**  
**CAMERA**

**LÃNH ĐẠO KHOA, PHÒNG**

(ký, ghi rõ họ tên)

*BS. Nguyễn Thị Hồng*

**LÃNH ĐẠO BỆNH VIỆN**



**GIÁM ĐỐC**  
*BS CKI. Hoàng Vĩnh Hà*



Số: 02 /QĐ-ĐNEMR

Đồng Nai, ngày 01 tháng 10 năm 2025

## QUYẾT ĐỊNH

**Ban hành các Giải pháp, Phương án, Kịch bản phòng ngừa khắc phục sự cố gây mất an toàn thông tin tại Bệnh viện Mắt Hà Nội – Đồng Nai**

### GIÁM ĐỐC BỆNH VIỆN MẮT HÀ NỘI – ĐỒNG NAI

*Căn cứ Luật giao dịch điện tử ngày 22 tháng 6 năm 2023;*

*Căn cứ Luật Công nghệ thông tin ngày 29 tháng 6 năm 2006;*

*Căn cứ Luật An toàn thông tin mạng ngày 19 tháng 11 năm 2015;*

*Căn cứ Nghị định số 85/2016/NĐ-CP ngày 01/07/2016 của Chính phủ về đảm bảo an toàn hệ thống thông tin theo cấp độ;*

*Căn cứ thông tư số 03/2017/TT-BTTTT ngày 24/04/2017 của Bộ trưởng Bộ thông tin và Truyền thông về Quy định chi tiết và hướng dẫn một số điều của Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;*

*Căn cứ thông tư số 20/2017/TT-BTTTT ngày 12/09/2017 của Bộ Thông tin và Truyền thông quy định về điều phối, ứng cứu sự cố an toàn thông tin mạng trên toàn quốc;*

*Căn cứ quyết định số 4159/QĐ-BYT, ngày 13/10/2014 của Bộ Y tế về Ban hành quy định về đảm bảo an toàn thông tin Y tế điện tử tại các đơn vị trong ngành Y tế;*

*Căn cứ Thông tư số 54/TT-BYT ngày 29/12/2017 của Bộ Y tế về việc Ban hành Bộ tiêu chí ứng dụng công nghệ thông tin tại các cơ sở khám bệnh, chữa bệnh;*

*Căn cứ Thông tư 13/2025/TT-BYT ngày 06 tháng 06 năm 2025 của Bộ y tế Vv Hướng dẫn triển khai hồ sơ bệnh án điện tử;*

*Căn cứ Văn bản số 365/TTYTQG-GPQLCL ngày 06 tháng 06 năm 2025 của Trung tâm thông tin y tế Quốc Gia về Hướng dẫn yêu cầu kỹ thuật triển khai phần mềm hồ sơ bệnh án điện tử;*

*Căn cứ Kế hoạch triển khai Hồ sơ bệnh án điện tử tại [Bệnh viện/TTYT];*

*Xét đề nghị của Trưởng phòng Kế hoạch*

**QUYẾT ĐỊNH:**

**Điều 1.** Ban hành kèm theo Quyết định này các Giải pháp, Phương án, Kịch bản phòng ngừa khắc phục sự cố gây mất an toàn thông tin tại Bệnh viện Mắt Hà Nội – Đồng Nai, cụ thể như sau:

1.1. Kịch bản phòng ngừa khắc phục sự cố hệ thống tại Bệnh viện Mắt Hà Nội – Đồng Nai (có kịch bản kèm theo);

1.2. Quy trình sao lưu và phục hồi dữ liệu tại Bệnh viện Mắt Hà Nội – Đồng Nai (có quy trình kèm theo);

1.3. Phương án cảnh báo và phòng chống tấn công có chủ đích đối với các hệ thống cung cấp dịch vụ qua internet của tại Bệnh viện Mắt Hà Nội – Đồng Nai (có phương án kèm theo);

1.4. Phương án chống tấn công xâm nhập từ xa (DOS, DDOS) cơ chế chống tấn công từ chối dịch vụ trên hệ thống của tại Bệnh viện Mắt Hà Nội – Đồng Nai (có phương án kèm theo);

**Điều 2.** Quyết định này có hiệu lực kể từ ngày ký.

**Điều 3.** Tổ CNTT phòng Kế hoạch tổng hợp, các khoa, phòng, các tập thể, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

**Nơi nhận:**

- Như Điều 3;
- GD và các PGD;
- Lưu: VT, KHNV.

## GIÁM ĐỐC



GIÁM ĐỐC  
BS CKI. Hoàng Vĩnh Hà



SỞ Y TẾ TỈNH ĐỒNG NAI  
**BỆNH VIỆN MẮT  
HÀ NỘI – ĐỒNG NAI**  
Số: 03 /QĐ-ĐNEMR

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM  
Độc lập – Tự do – Hạnh phúc

Đồng Nai, ngày 01 tháng 10 năm 2025

### **QUYẾT ĐỊNH**

**Ban hành Quy chế bảo đảm an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin của Bệnh viện Mắt Hà Nội – Đồng Nai**

#### **GIÁM ĐỐC BỆNH VIỆN MẮT HÀ NỘI – ĐỒNG NAI**

*Căn cứ Luật An toàn thông tin mạng ngày 19/11/2015;*

*Căn cứ Luật An ninh mạng ngày 12/6/2018;*

*Căn cứ Luật Khám bệnh, chữa bệnh ngày 09/01/2023;*

*Căn cứ Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;*

*Căn cứ Nghị định số 53/2022/NĐ-CP ngày 15/8/2022 của Chính phủ quy định chi tiết một số điều của Luật An ninh mạng;*

*Căn cứ Quyết định số 4159/QĐ-BYT, ngày 13/10/2014 của Bộ Y tế về ban hành quy định về đảm bảo an toàn thông tin Y tế điện tử tại các đơn vị trong ngành Y tế;*

*Căn cứ Thông tư số 53/2014/TT-BYT ngày 29/12/2014 của Bộ Y tế quy định điều kiện hoạt động y tế trên môi trường mạng;*

*Căn cứ Thông tư số 46/2018/TT-BYT ngày 28/12/2018 của Bộ Y tế quy định hồ sơ bệnh án điện tử;*

*Căn cứ Quyết định số 874/QĐ-BTTTT ngày 17/6/2021 của Bộ Thông tin Truyền thông quyết định về việc ban hành bộ quy tắc ứng xử trên mạng xã hội;*

*Căn cứ Thông tư số 12/2022/TT-BTTTT ngày 12/08/2022 của Bộ Thông tin và Truyền thông quy định chi tiết và hướng dẫn một số điều của Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;*

*Theo đề nghị của Trưởng phòng Kế hoạch Tổng hợp.*

## QUYẾT ĐỊNH:

**Điều 1.** Ban hành kèm theo Quyết định này Quy chế bảo đảm an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin của Bệnh viện Mắt Hà Nội – Đồng Nai.

**Điều 2.** Quyết định này có hiệu lực thi hành kể từ ngày ký.

**Điều 3.** Ban Giám đốc và Trưởng các khoa, phòng, các tập thể, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

**Nơi nhận:**

- Như Điều 3;
- Lưu: VT, KH-CĐT

**GIÁM ĐỐC**



**GIÁM ĐỐC**  
BS CKI. Hoàng Vinh Hà



SỞ Y TẾ TỈNH ĐỒNG NAI  
**Bệnh viện Mắt**  
**Hà Nội – Đồng Nai**

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM  
Độc lập – Tự do – Hạnh phúc

## **QUY CHẾ**

**Bảo đảm an toàn, an ninh thông tin trong hoạt động  
ứng dụng công nghệ thông tin của  
Bệnh viện Mắt Hà Nội – Đồng Nai**

*(Kèm theo Quyết định số 03/QĐ-ĐNEMR ngày 01 tháng 10 năm 2025  
của Bệnh viện Mắt Hà Nội – Đồng Nai)*

### **Chương I** **QUY ĐỊNH CHUNG**

#### **Điều 1. Phạm vi điều chỉnh, đối tượng áp dụng**

##### **1. Phạm vi điều chỉnh**

Quy chế này quy định về công tác đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin của Bệnh viện Mắt Hà Nội – Đồng Nai.

##### **2. Đối tượng áp dụng**

a) Các đơn vị trực thuộc Bệnh viện Mắt Hà Nội – Đồng Nai bao gồm: Khoa, Phòng (gọi tắt là các đơn vị trực thuộc Bệnh viện).

b) Cán bộ, công chức, viên chức, người lao động, thực tập sinh, sinh viên đang làm việc, học tập tại Bệnh viện Mắt Hà Nội – Đồng Nai.

c) Các cơ quan, tổ chức, cá nhân cung cấp dịch vụ viễn thông, công nghệ thông tin và an toàn thông tin có tham gia vào các hoạt động ứng dụng công nghệ thông tin tại Bệnh viện Mắt Hà Nội – Đồng Nai.

#### **Điều 2. Giải thích từ ngữ**

Trong quy chế này, các từ ngữ dưới đây được hiểu như sau:

1. *Bảo mật* là sử dụng kỹ thuật mật mã hoặc các phương tiện kỹ thuật, nghiệp vụ khác để che giấu, không cho người không có trách nhiệm biết được nội dung thông tin.

2. *An ninh thông tin (ANTT)* là việc bảo đảm thông tin trên mạng không gây

phương hại đến an ninh quốc gia, trật tự an toàn xã hội, bí mật nhà nước, quyền và lợi ích hợp pháp của tổ chức, cá nhân.

3. *An toàn thông tin (ATTT)* là bao gồm các hoạt động quản lý, nghiệp vụ và kỹ thuật đối với hệ thống thông tin nội bộ nhằm bảo vệ, khôi phục các hệ thống, các dịch vụ và nội dung thông tin đối với nguy cơ tự nhiên hoặc do con người gây ra. Việc bảo vệ thông tin, tài sản và con người trong hệ thống thông tin nội bộ nhằm bảo đảm cho các hệ thống thực hiện đúng chức năng, phục vụ đúng đối tượng một cách sẵn sàng, chính xác và tin cậy. An toàn thông tin bao hàm các nội dung bảo vệ và bảo mật thông tin, an toàn dữ liệu, an toàn máy tính và an toàn mạng, đặc biệt an toàn thông tin bệnh nhân.

4. *Mạng* là khái niệm chung dùng để chỉ mạng LAN, mạng viễn thông cố định, di động và mạng Internet.

5. *Phần mềm độc hại* là phần mềm có khả năng gây ra hoạt động không bình thường, cho một hay một phần hay toàn bộ hệ thống thông tin hoặc thực hiện sao chép, sửa đổi, xóa bỏ trái phép thông tin lưu trữ trong hệ thống thông tin của bệnh viện.

6. *Phần mềm gián điệp (spyware)* là một loại phần mềm độc hại được thiết kế để thu thập thông tin từ máy tính hoặc thiết bị di động mà không được sự đồng ý của người dùng. Phần mềm này có thể theo dõi hoạt động trực tuyến, thu thập thông tin cá nhân, như lịch sử duyệt web, mật khẩu và dữ liệu tài chính.

7. *Tính sẵn sàng* là bảo đảm những người được cấp quyền có thể truy nhập thông tin và các tài sản liên quan ngay khi có nhu cầu.

8. *Cổng giao tiếp (Port)* là để định danh các ứng dụng gửi và nhận dữ liệu, mỗi ứng dụng sẽ tương ứng với một cổng giao tiếp, những ứng dụng phổ biến được đặt với số hiệu cổng định trước, nhằm định danh duy nhất các ứng dụng đó.

Khi máy tính sử dụng dịch vụ nào thì cổng giao tiếp tương ứng với dịch vụ đó sẽ mở.

9. *Giao thức* là tập hợp các quy tắc, quy ước hệ thống của mạng mà tất cả các thực thể tham gia hệ thống phải tuân theo.

10. *Bản ghi nhật ký hệ thống (Logfile)* là mỗi tập tin được tạo ra trên mỗi thiết bị của hệ thống thông tin như: Tường lửa, cân bằng tải, máy chủ ứng dụng...



có chứa tất cả các thông tin về các hoạt động xảy ra trên thiết bị đó. Bản ghi nhật ký hệ thống dùng để phân tích những sự kiện đã xảy ra, nguồn gốc và các kết quả để có các biện pháp xử lý thích hợp.

11. *Sự cố an toàn thông tin* là một hoặc một chuỗi các sự kiện ATTT không mong muốn có khả năng làm tổn hại các hoạt động nghiệp vụ và đe dọa ATTT.

12. *Virus* là một loại phần mềm độc hại (malware) được thiết kế để tự nhân bản và lây lan từ máy tính này sang máy tính khác. Một virus thường cần một chương trình hoặc tệp hợp lệ để lây nhiễm, và khi người dùng mở tệp hoặc chạy chương trình bị nhiễm, virus sẽ được kích hoạt và bắt đầu hoạt động.

13. *Bí mật nhà nước* là thông tin có nội dung quan trọng do người đứng đầu cơ quan, tổ chức có thẩm quyền xác định căn cứ vào quy định Luật Bảo vệ bí mật nhà nước 2018, chưa công khai, nếu bị lộ, bị mất có thể gây nguy hại đến lợi ích quốc gia, dân tộc.

14. *Bộ phận chuyên trách về an toàn thông tin* là bộ phận do chủ quản hệ thống thông tin thành lập hoặc chỉ định để thực thi nhiệm vụ bảo đảm an toàn thông tin và ứng cứu sự cố an toàn thông tin mạng.

## **Chương II**

### **TRÁCH NHIỆM VÀ TỔ CHỨC ĐẢM BẢO AN TOÀN, AN NINH THÔNG TIN TRONG BỆNH VIỆN**

#### **Điều 3. Trách nhiệm của Giám đốc bệnh viện, trưởng các khoa phòng.**

##### **1. Giám đốc bệnh viện.**

a) Chịu trách nhiệm cao nhất về ATTT trong bệnh viện.

b) Chỉ đạo các đơn vị tăng cường công tác đảm bảo ATTT - ANTT trong hoạt động ứng dụng CNTT và ưu tiên đầu tư các thiết bị phần cứng, phần mềm liên quan đến công tác đảm bảo ATTT.

c) Lãnh đạo, chỉ đạo làm tốt công tác tuyển chọn, điều động, thẩm định tiêu chuẩn chính trị và quản lý chính trị nội bộ đối với nhân viên làm việc tại các vị trí trọng yếu, nhạy cảm liên quan ATTT - ANTT và bí mật nhà nước.

##### **2. Trưởng khoa phòng thuộc bệnh viện**

a) Chịu trách nhiệm cao nhất về ATTT trong khoa phòng.

b) Tổ chức triển khai, đôn đốc việc thực thi các chính sách, quy trình, quy

định, tiêu chuẩn, hướng dẫn và các giải pháp kỹ thuật nhằm đảm bảo ATTT - ANTT trong khoa phòng.

c) Thông báo và phối hợp với Nhân viên CNTT khi xảy ra sự cố.

d) Chịu trách nhiệm toàn diện trước Giám đốc Bệnh viện trong công tác đảm bảo ATTT - ANTT tại khoa phòng.

e) Tổ chức quán triệt, hướng dẫn cho nhân viên trong khoa phòng nâng cao ý thức trách nhiệm bảo vệ ATTT - ANTT và bí mật nhà nước.

#### **Điều 4. Trách nhiệm của Phòng Kế hoạch Tổng hợp**

1. Phòng Kế hoạch Tổng hợp có cán bộ chuyên trách về ATTT cho hệ thống; tham mưu và chịu trách nhiệm trước Giám đốc bệnh viện về việc triển khai công tác đảm bảo ATTT.

2. Hàng năm xây dựng dự toán, kế hoạch, tổng hợp kinh phí, báo cáo định kỳ hoặc đột xuất về triển khai công tác ATTT trình Lãnh đạo bệnh viện.

3. Chủ trì, phối hợp với các khoa phòng liên quan thành lập đoàn kiểm tra, tiến hành kiểm tra định kỳ hoặc đột xuất khi phát hiện có các dấu hiệu, hành vi vi phạm ATTT - ANTT; báo cáo cấp trên để có biện pháp xử lý kỷ luật đối với cán bộ, nhân viên (CBNV) khi có vi phạm theo quy định của pháp luật.

4. Tham mưu cho Ban giám đốc triển khai các chương trình đào tạo, bồi dưỡng, hội nghị tuyên truyền ATTT - ANTT trong toàn bệnh viện; thông báo, hướng dẫn, khuyến cáo cho các đơn vị trực thuộc bệnh viện, người dùng biết để có biện pháp phòng ngừa, ngăn chặn các nguy cơ mất ATTT - ANTT do virus, phần mềm độc hại, phần mềm gián điệp,... gây ra; hỗ trợ khoa phòng, người dùng giải quyết sự cố khi có yêu cầu.

5. Ban hành các quy trình vận hành hệ thống công nghệ thông tin bao gồm: Quy trình khởi động, đóng hệ thống, quy trình sao lưu, phục hồi dữ liệu, quy trình xử lý sự cố, quy trình giám sát và ghi nhật ký hoạt động của hệ thống... Trong đó phải xác định rõ phạm vi, trách nhiệm của người sử dụng, vận hành hệ thống; kiểm soát sự thay đổi của phiên bản phần mềm, cấu hình phần cứng, quy trình vận hành, ghi chép lại các thay đổi; lập kế hoạch, thực hiện kiểm tra, thử nghiệm sự thay đổi, báo cáo kết quả và phải được phê duyệt trước khi áp dụng chính thức. Có phương án dự phòng cho việc phục hồi hệ thống trong trường hợp thực hiện



thay đổi không thành công hoặc gặp các sự cố không có khả năng dự tính trước.

6. Định kỳ 01 năm hoặc khi có thay đổi Quy chế bảo đảm an toàn, an ninh thông tin, tổ chức rà soát, kiểm tra tính phù hợp của Quy chế này với các quy định của pháp luật về ATTT - ANTT và các quy định, tiêu chuẩn liên quan; kiểm tra tính đáp ứng của Quy chế này với yêu cầu thực tế của bệnh viện; báo cáo Lãnh đạo bệnh viện về việc sửa đổi, bổ sung Quy chế trong trường hợp cần thiết.

7. Cử nhân sự tham gia các hoạt động, công tác bảo đảm an toàn, an ninh thông tin khi có yêu cầu của tổ chức có thẩm quyền.

### **Điều 5. Trách nhiệm của toàn bộ nhân viên trong bệnh viện**

1. Nghiêm chỉnh chấp hành các quy trình, quy định, chính sách, hướng dẫn về ATTT - ANTT trong quá trình thực hiện nhiệm vụ được giao.

2. Tham gia vào việc triển khai các giải pháp, kế hoạch nhằm đảm bảo ATTT - ANTT tại bệnh viện; tham gia quá trình phản ứng sự cố ATTT theo sự điều phối của Phòng Kế hoạch Tổng hợp Bệnh viện, tuân theo các quy định và quy trình liên quan; trong quá trình làm nhiệm vụ nếu phát hiện mất ATTT yêu cầu CBNV phải báo cáo ngay với quản lý đơn vị và Phòng Kế hoạch Tổng hợp để kịp thời ngăn chặn, xử lý.

3. Chịu trách nhiệm nếu vi phạm các chính sách, quy trình, quy định, hướng dẫn ATTT - ANTT.

### **Điều 6. Tổ chức, phân công chức năng, nhiệm vụ ATTT trong bệnh viện**

1. Khối tham mưu: Phòng Kế hoạch Tổng hợp, có chức năng, nhiệm vụ liên quan đến công tác ATTT như sau:

a) Đầu mối với các cơ quan quản lý nhà nước, các đơn vị ngoài bệnh viện về hoạt động thuộc lĩnh vực ATTT.

b) Nghiên cứu, tham mưu, xây dựng tầm nhìn chiến lược, xây dựng mô hình tổ chức, mục tiêu, kế hoạch hành động ATTT trong toàn bệnh viện.

c) Chủ trì xây dựng, đề xuất, ban hành văn bản chính sách, chủ trì xây dựng cơ chế vận hành ATTT, đảm bảo tuân thủ các quy định có liên quan của pháp luật; chủ trì xây dựng tiêu chuẩn ATTT cho các yêu cầu đảm bảo ATTT theo các quy định trong Quy chế này.

d) Điều hành, hướng dẫn và đôn đốc các khoa phòng trực thuộc bệnh viện thực hiện tuân thủ các quy định của pháp luật và bệnh viện về công tác ATTT; kiểm tra, giám sát và đánh giá việc thực hiện công tác ATTT tại các khoa phòng trực thuộc bệnh viện; đề xuất xử lý theo thẩm quyền các vi phạm qui định, quy trình, hướng dẫn về ATTT tại bệnh viện.

e) Chủ trì, quy hoạch và triển khai các giải pháp kỹ thuật đảm bảo ATTT cấp bệnh viện; chủ trì phối hợp với các khoa phòng xây dựng các bài toán về ATTT trong bệnh viện; định kỳ hàng năm tổ chức phổ biến, tuyên truyền nâng cao nhận thức và ATTT - ANTT cho người sử dụng.

f) Xây dựng định hướng, kế hoạch đào tạo, kiểm tra đánh giá nhân sự về ATTT.

g) Điều phối, trực tiếp tham gia xử lý các sự cố ATTT.

2. Các khoa phòng thuộc bệnh viện có chức năng, nhiệm vụ sau:

a) Tiếp nhận và triển khai các văn bản chính sách ATTT - ANTT do bộ phận ATTT của bệnh viện hoặc do các cơ quan có thẩm quyền ban hành.

b) Phối hợp triển khai các giải pháp kỹ thuật phục vụ công tác ATTT; thực hiện khắc phục các điểm yếu, lỗ hổng và lỗi ATTT được cảnh báo do bộ phận ATTT của bệnh viện hướng dẫn; sẵn sàng, chủ động phối hợp trong công tác ứng cứu sự cố ATTT.

c) Chủ động đề xuất các ý kiến, giải pháp để cải thiện tình hình ATTT của đơn vị và toàn bệnh viện.

### **Chương III**

## **AN TOÀN THÔNG TIN TRONG QUẢN LÝ NGUỒN NHÂN LỰC**

### **Điều 7. Đảm bảo ATTT trước khi tuyển dụng hoặc phân công nhiệm vụ**

1. Phòng Kế hoạch Tổng hợp xác định trách nhiệm về an toàn, bảo mật thông tin của vị trí cần tuyển dụng hoặc phân công.

2. Phòng Kế hoạch Tổng hợp thực hiện kiểm tra lý lịch, xem xét đánh giá nghiêm ngặt tư cách đạo đức, trình độ chuyên môn khi tuyển dụng, phân công CBNV làm việc tại các vị trí trọng yếu như: Quản trị hệ thống, vận hành hệ thống,



quản trị hệ thống an ninh bảo mật, quản trị cơ sở dữ liệu...

3. Trong Quyết định giao nhiệm vụ hoặc hợp đồng lao động phải có các điều khoản về trách nhiệm đảm bảo an toàn, bảo mật thông tin của người được giao nhiệm vụ trong và sau khi làm việc tại đơn vị. Đối với những trường hợp tuyển dụng trước thời điểm quy chế được ban hành phải có bản cam kết.

#### **Điều 8. Đảm bảo ATTT trong thời gian làm việc**

1. Các khoa phòng thuộc bệnh viện có trách nhiệm phổ biến và cập nhật các quy định về an toàn, bảo mật thông tin cho CBNV; có trách nhiệm yêu cầu và kiểm tra việc thi hành các quy định về an toàn, bảo mật thông tin của cá nhân thuộc đơn vị tối thiểu một lần mỗi năm.

2. Các khoa phòng thuộc bệnh viện có trách nhiệm áp dụng các biện pháp kỷ luật hoặc đề xuất kỷ luật đối với CBNV của đơn vị, vi phạm qui định an toàn, bảo mật thông tin.

#### **Điều 9. Đảm bảo ATTT trong trường hợp nhân viên nghỉ hoặc thay đổi công việc**

1. Khi CBNV đã nghỉ việc hoặc thay đổi công việc, khoa phòng thuộc bệnh viện phải xác định rõ trách nhiệm của CBNV và các bên liên quan trong sử dụng hệ thống công nghệ thông tin của bệnh viện.

2. Khoa phòng thuộc bệnh viện có trách nhiệm yêu cầu bộ phận ATTT thu hồi hoặc thay đổi, điều chỉnh quyền truy cập hệ thống, các thông tin được lưu trên các phương tiện lưu trữ, các trang thiết bị máy móc, phần cứng, phần mềm và các tài sản khác thuộc sở hữu của bệnh viện; cán bộ phụ trách hành chính phải báo với cán bộ phụ trách CNTT vô hiệu hóa tất cả các quyền ra, vào, truy cập tài nguyên, quản trị hệ thống sau khi cán bộ thôi việc.

3. Việc thu hồi hoặc thay đổi quyền truy cập phải có xác nhận của lãnh đạo khoa phòng bệnh viện.

4. Khoa phòng thuộc bệnh viện có trách nhiệm chủ trì, theo dõi, đảm bảo thực thi điều này.

**Chương IV****QUY ĐỊNH VỀ AN NINH, AN TOÀN THÔNG TIN ĐỐI VỚI CBNV****Điều 10. Quy định bảo vệ thông tin, dữ liệu**

1. Nghiêm cấm CBNV thu thập, cung cấp, trao đổi, làm lộ, làm mất, chiếm đoạt, mua bán, tiêu hủy trái phép các thông tin về chủ trương, kế hoạch, chiến lược phát triển, số liệu, dữ liệu về nhân sự, tài chính, thông tin về dữ liệu khách hàng, tài liệu nội bộ ... dưới bất kỳ hình thức nào. Trường hợp đặc biệt phải được phê duyệt của Giám đốc bệnh viện.

2. Nghiêm cấm tất cả các trường hợp tải lên (upload), chia sẻ tài liệu/dữ liệu nội bộ bệnh viện, mã nguồn phần mềm (source code), tài sản phần mềm bệnh viện trên các trang mạng internet (mediafile, 4share, gmail, yahoo mail, dropbox, google drive...) hoặc tải trên các ứng dụng xã hội như: facebook, zalo, viber, telegram ... chỉ được sử dụng chức năng chia sẻ dữ liệu trên các kênh công cụ do bệnh viện cấp phát và có phê duyệt.

**Điều 11. Quy định về việc truy cập, sử dụng máy tính an toàn**

1. Nghiêm cấm CBNV truy cập các website không lành mạnh, các website có nội dung vi phạm pháp luật, các website chứa mã độc, chứa nội dung bẻ khóa...

2. Nghiêm cấm truy cập internet trên các máy tính của bệnh viện thông qua các thiết bị USB - 3G cá nhân và các thiết bị không thuộc bệnh viện hoặc Phòng Kế hoạch Tổng hợp quản lý. Trường hợp đặc biệt cần phải có sự phê duyệt của bộ phận ATTT và Lãnh đạo đơn vị.

3. Không mở trực tiếp các file đính kèm, các đường link lạ không rõ nguồn gốc.

**Điều 12. Quy tắc ứng xử trên mạng xã hội**

1. Tìm hiểu và tuân thủ các điều khoản hướng dẫn sử dụng của nhà cung cấp dịch vụ mạng xã hội trước khi đăng ký, tham gia mạng xã hội.

2. Thực hiện biện pháp tự quản lý, bảo mật tài khoản mạng xã hội và nhanh chóng thông báo tới các cơ quan chức năng, nhà cung cấp dịch vụ khi tài khoản bị mất quyền kiểm soát, bị giả mạo, lợi dụng và sử dụng vào mục đích không lành mạnh, ảnh hưởng đến an ninh quốc gia và trật tự an toàn xã hội, ảnh hưởng đến



quyền và lợi ích hợp pháp của tổ chức, cá nhân.

3. Chia sẻ những thông tin có nguồn chính thống, đáng tin cậy.

4. Có các hành vi, ứng xử phù hợp với những giá trị đạo đức, văn hóa, truyền thống của dân tộc Việt Nam; không sử dụng từ ngữ gây thù hận, kích động bạo lực, phân biệt vùng miền, giới tính, tôn giáo.

5. Không đăng tải những nội dung vi phạm pháp luật, các thông tin xúc phạm danh dự, nhân phẩm ảnh hưởng đến quyền và lợi ích hợp pháp của các tổ chức, cá nhân khác; thông tin gây phương hại đến an ninh quốc gia, trật tự an toàn xã hội, bí mật nhà nước; sử dụng ngôn ngữ phản cảm, vi phạm thuần phong mỹ tục; tung tin giả, tin sai sự thật; quảng cáo, kinh doanh dịch vụ trái phép.

6. Khuyến khích sử dụng mạng xã hội để tuyên truyền, quảng bá về đất nước - con người, văn hóa tốt đẹp của Việt Nam, chia sẻ thông tin tích cực, những tấm gương người tốt, việc tốt.

### **Điều 13. Các hành vi khác bị nghiêm cấm theo quy định của pháp luật**

1. Theo Điều 7 Luật An toàn thông tin mạng số 86/2015/QH13 ban hành ngày 19/11/2015.

2. Theo Điều 8 Luật An ninh mạng số 24/2018/QH14 ban hành ngày 12/06/2018.

## **Chương V QUY ĐỊNH VỀ TÀI KHOẢN**

### **Mục 1 QUY ĐỊNH VỀ TRÁCH NHIỆM QUẢN LÝ VÀ SỬ DỤNG TÀI KHOẢN**

#### **Điều 14. Trách nhiệm của Phòng Kế hoạch Tổng hợp**

1. Chịu trách nhiệm xây dựng giải pháp, thực hiện khai báo chính sách quản lý tài khoản/mật khẩu theo đúng quy định trên hệ thống do đơn vị quản lý đúng quy định và quy trình về việc cấp phát, phân quyền, thu hồi tài khoản.

2. Thẩm định các yêu cầu cấp phát tài khoản đối với các hệ thống do đơn vị

sử dụng.

3. Lập và duy trì hồ sơ theo dõi việc cấp phát, thu hồi, thay đổi thông tin tài khoản, thông tin nhóm quyền trên các hệ thống. Đảm bảo tất cả các tài khoản, nhóm quyền khai báo trên hệ thống đều hợp lệ so với hồ sơ theo dõi, không tồn tại trên hệ thống những tài khoản không rõ cá nhân/đơn vị sử dụng hoặc đã hết hạn.

4. Thông báo cho người sử dụng về các quyền truy cập, thời gian sử dụng tài khoản, yêu cầu người sử dụng xác nhận quyền truy cập của mình khi được cấp/thay đổi thông tin tài khoản.

5. Phải thực hiện thủ tục thu hồi, thay đổi tài khoản theo quy trình đã ban hành đối với các cá nhân thay đổi công tác (chuyển đơn vị, nghỉ việc).

6. Đối với các tài khoản được cấp ngắn hạn để thực hiện kế hoạch, khi thực hiện xong kế hoạch, đơn vị quản lý gửi yêu cầu Phòng Kế hoạch Tổng hợp tiến hành thu hồi/vô hiệu hóa/hủy tài khoản.

7. Định kỳ hàng tháng kiểm tra, rà soát công tác cấp phát, phân quyền, thu hồi tài khoản trên các hệ thống do đơn vị quản lý. Thực hiện thu hồi các tài khoản đã hết hạn sử dụng.

### **Điều 15. Trách nhiệm cá nhân**

1. Thiết lập chính sách mật khẩu mạnh cho các tài khoản được cấp theo đúng quy định về chính sách mật khẩu mạnh.

2. Chịu trách nhiệm trước Giám đốc bệnh viện trong việc quản lý, sử dụng, bảo mật tài khoản được cấp.

3. Phải cam kết sử dụng tài khoản đúng mục đích công việc, không được lạm dụng quyền được cấp vào các mục đích cá nhân, trường hợp tài khoản được cấp quyền vượt quá chức năng nhiệm vụ, người sử dụng có trách nhiệm thông báo cho người quản lý tài khoản.

4. Đảm bảo tính bảo mật thông tin tài khoản được cấp, không in ra giấy, ghi ra file không mã hóa, không được cho mượn, chia sẻ tài khoản, mật khẩu cho người khác, hoặc sử dụng chung tài khoản của người khác; trường hợp đặc biệt phải có sự phê duyệt của lãnh đạo, sau đó phải đổi lại mật khẩu.



5. Khi bị lộ mật khẩu, hoặc nghi ngờ mật khẩu bị lộ phải đổi ngay mật khẩu, trong trường hợp không thể tự đổi phải làm thủ tục khôi phục mật khẩu theo quy trình quản lý cấp phát tài khoản tương ứng.

6. Khi được cung cấp mật khẩu mới hoặc được khôi phục mật khẩu, cần phải đổi ngay mật khẩu mới.

7. Người sử dụng không sử dụng chức năng mặc định lưu trữ các thông tin về mật khẩu trên trình duyệt web và các công cụ (SQL navigator ...) kết nối vào mạng lưới, hệ thống/ứng dụng, Database của bệnh viện, ngoại trừ trong trường hợp sử dụng Master Password hay các phần mềm chuyên dụng có mã hóa để bảo vệ mật khẩu.

## Mục 2

### QUY ĐỊNH VỀ TÀI KHOẢN

#### **Điều 16. Phân loại tài khoản**

1. Tài khoản cấp cho cá nhân: Tài khoản cấp cho cá nhân sử dụng, phục vụ theo nhiệm vụ được giao (tài khoản đăng nhập máy tính, tài khoản email, truy cập ứng dụng ...).

2. Tài khoản quản trị hệ thống CNTT (tài khoản quản trị thiết bị bảo mật, tài khoản truy cập hệ thống máy chủ, camera, thiết bị mạng, thiết bị bảo mật, cơ sở dữ liệu (Database), tài khoản quản trị phần mềm (admin) ...

3. Tài khoản cấp cho ứng dụng CNTT: Tài khoản được dùng cho ứng dụng CNTT tự động, kết nối vào hệ thống để phục vụ các hoạt động nghiệp vụ của ứng dụng. Tài khoản cấp cho ứng dụng phải cấp cho người chịu trách nhiệm quản lý cụ thể, và chỉ được dùng thông qua ứng dụng CNTT.

#### **Điều 17. Quy định đặt tên tài khoản**

1. Quy định đặt tên tài khoản cấp cho các cá nhân: Tên tài khoản được đặt đảm bảo được yếu tố định danh được cá nhân.

2. Quy định đặt tên tài khoản cấp ứng dụng CNTT: Tên tài khoản được đặt đảm bảo yếu tố định danh được ứng dụng sử dụng tài khoản.

3. Quy định đặt tên tài khoản cấp cho nhân viên, đối tác/nhân viên thực tập:

Tên tài khoản được đặt phải đảm bảo yếu tố định danh được nhân sự sử dụng tài khoản.

### **Điều 18. Đối tượng được cấp tài khoản**

1. Các cá nhân thuộc bệnh viện sử dụng theo nhiệm vụ được phân cấp (trực tiếp sử dụng tài khoản hoặc quản lý tài khoản cấp cho các ứng dụng).

2. Chỉ xem xét cấp tài khoản cho đối tác, đơn vị, cá nhân bên ngoài trong một số trường hợp đặc biệt được sự đồng ý của Ban Giám đốc/Phòng Kế hoạch Tổng hợp bệnh viện và đơn vị đầu mối xin cấp tài khoản cho đối tác phải chịu trách nhiệm trong trường hợp tài khoản bị sử dụng sai mục đích.

## **Mục 3 QUY ĐỊNH VỀ CẤP PHÁT, PHÂN QUYỀN VÀ THU HỒI TÀI KHOẢN**

### **Điều 19. Quy định về cấp phát tài khoản**

1. Phòng Kế hoạch Tổng hợp chịu trách nhiệm xây dựng, ban hành quy trình quản lý, cấp phát tài khoản truy cập các hệ thống.

2. Tài khoản được cấp phải có cá nhân chịu trách nhiệm quản lý và sử dụng theo nhiệm vụ được phân công; không cấp tài khoản dùng chung, kể cả tài khoản chỉ có quyền giám sát.

3. Với tài khoản cấp cho nhân sự đối tác phải có cam kết của đối tác sử dụng tài khoản đúng mục đích.

4. Tài khoản xin cấp và được cấp phát cho cá nhân dựa trên nguyên tắc đảm bảo quyền hạn tối thiểu, vừa đủ cho với công việc ứng với vị trí làm việc. Người xin cấp phát tài khoản phải xác định thời hạn hiệu lực của tài khoản được cấp phát (ngày, tháng, năm, thời gian hiệu lực).

### **Điều 20. Quy định về quản lý nhóm quyền, phân quyền cho tài khoản.**

1. Các nhóm quyền quản trị hệ thống phải được phân công và phê duyệt từ Phòng Kế hoạch Tổng hợp.

2. Các nhóm quyền trên các hệ thống phải được định nghĩa chi tiết, bao gồm: Tên nhóm quyền, mục đích của nhóm quyền, các quyền được thực hiện, đối tượng được cấp tài khoản thuộc nhóm quyền đã định nghĩa.



3. Đơn vị phải quản lý thông tin nhóm quyền (lưu thông tin đồng thời bằng văn bản được phê duyệt và trên hệ thống phân quyền), chỉ được phân quyền tài khoản theo các nhóm quyền đã được định nghĩa.

### **Điều 21. Quy định về thu hồi tài khoản**

1. Các tài khoản đến thời điểm hết hiệu lực, đơn vị phải yêu cầu phòng Kế hoạch Tổng hợp thu hồi hoặc xóa bỏ trên hệ thống.

2. Đơn vị có nhân sự thay đổi nhiệm vụ, vị trí công tác, nghỉ việc ... đơn vị phải làm thủ tục đề nghị phòng Kế hoạch Tổng hợp thu hồi/hủy tài khoản.

3. Định kỳ hàng tháng, đơn vị phải rà soát các hệ thống do đơn vị quản lý và yêu cầu phòng Kế hoạch Tổng hợp thu hồi các tài khoản hết hiệu lực, cấp phát sai qui định.

## **Mục 4**

### **CÔNG TÁC KIỂM SOÁT, GIÁM SÁT TRUY CẬP**

#### **Điều 22. Kiểm soát truy cập**

1. Phòng Kế hoạch Tổng hợp phải xác định và lập danh sách các hệ thống quan trọng, các tài khoản có đặc quyền, tài khoản có quyền thực hiện các chức năng quan trọng trong hệ thống (tài khoản quan trọng).

2. Không dùng các kết nối truy cập trực tiếp từ internet đến máy tính, hệ thống mạng nội bộ, các công cụ hỗ trợ truy cập Ultraview, Teamviewer, VNC, Anydesk ... Sử dụng công cụ truy cập từ xa do Phòng Kế hoạch Tổng hợp quy định.

3. Đối với các tài khoản quan trọng trong hệ thống, chỉ được thực hiện kết nối, tác động từ địa chỉ IP đã được đăng ký.

4. Phòng Kế hoạch Tổng hợp phải lưu hồ sơ quản lý các địa chỉ IP được phép kết nối, tác động đến các hệ thống quan trọng. Định kỳ hàng tháng rà soát danh sách địa chỉ IP được phép truy cập tới các hệ thống quan trọng.

#### **Điều 23. Giám sát truy cập**

1. . Phòng Kế hoạch Tổng hợp phải có các giải pháp kỹ thuật để kiểm soát, giám sát các tài khoản có thể kết nối đến các hệ thống quan trọng.

2. Phải thực hiện ghi nhật ký (log) tác động, log thực hiện các chức năng quan trọng trên hệ thống. Thời gian lưu log tối thiểu 6 tháng, được lãnh đạo . Phòng Kế hoạch Tổng hợp phê duyệt đảm bảo đáp ứng theo yêu cầu nghiệp vụ của từng hệ thống, chức năng cụ thể.

## **Chương VI**

### **QUY ĐỊNH VỀ AN TOÀN THÔNG TIN ĐỐI VỚI MẠNG MÁY TÍNH/ THIẾT BỊ VĂN PHÒNG**

**Điều 24. Quy định an toàn thông tin trên thiết bị, máy tính, thiết bị di động người dùng cuối**

Tất cả các thiết bị di động, máy tính người dùng cuối sử dụng trong bệnh viện phải đảm bảo các tiêu chuẩn ATTT theo tiêu chuẩn về ATTT trên các loại thiết bị, máy tính người dùng cuối.

**Điều 25. Quy định đảm bảo ATTT đối với mạng bệnh viện**

1. Mạng LAN trong toàn bệnh viện phải đảm bảo đáp ứng ATTT.
2. Tất cả các giải pháp, thiết bị mạng văn phòng có dây hoặc không dây phải triển khai, cấu hình đảm bảo ATTT theo tiêu chuẩn ATTT.

## **Chương VII**

### **QUY ĐỊNH VỀ ATTT KHI LÀM VIỆC VỚI ĐỐI TÁC**

**Điều 26. ATTT khi làm việc với đối tác**

1. Hợp đồng với các đối tác có kết nối đến hệ thống thông tin, cung cấp triển khai các ứng dụng cho bệnh viện phải bao gồm các điều khoản và nghĩa vụ về ATTT, cam kết không tiết lộ thông tin, trách nhiệm xử lý, vá lỗi hỏng phần mềm, điều khoản xử phạt trong trường hợp đối tác vi phạm quy định an toàn, bảo mật thông tin và trách nhiệm phải bồi thường thiệt hại do đối tác gây ra. Quy định này áp dụng cho cá nhân, tổ chức liên quan của đối tác bao gồm nhân viên của đối tác và các nhà thầu phụ của đối tác trong trường hợp đối tác ký kết hợp đồng với nhà thầu phụ.

2. Đơn vị đầu mối làm việc với các đối tác phải lập hồ sơ nhật ký giám sát dịch vụ của đối tác cung cấp, bao gồm tối thiểu các thông tin sau:



- Tên đối tác
- Dịch vụ cung cấp
- Ngày thực hiện
- Các vấn đề ATTT (sự cố gây gián đoạn, mất hay lộ thông tin, lỗ hổng phần mềm, thời gian khắc phục lỗ hổng ...)
- Các thay đổi trong dịch vụ/nhân sự (nếu có)

#### **Điều 27. Tiêu chuẩn ATTT cho đối tác**

1. Tất cả các hệ thống, dịch vụ, sản phẩm do đối tác cung cấp chuyên giao cho bệnh viện phải đáp ứng các tiêu chuẩn ATTT của bệnh viện ban hành.
2. Tất cả các hợp đồng hợp tác với đối tác phải có điều khoản cam kết của đối tác phải đáp ứng các tiêu chuẩn ATTT theo các tiêu chuẩn ATTT do bệnh viện ban hành. Điều khoản cam kết phải nêu rõ trách nhiệm, phương án, thời gian xử lý với các vi phạm tiêu chuẩn ATTT của đối tác.

### **Chương VIII**

#### **QUY ĐỊNH QUẢN LÝ ATTT THIẾT BỊ CÓ KHẢ NĂNG LƯU TRỮ THÔNG TIN DỮ LIỆU**

Các quy định trong mục này áp dụng cho việc cấp phát, quản lý vào/ra, luân chuyển thu hồi tất cả các thiết bị điện tử, CNTT, viễn thông có chứa hoặc có khả năng lưu trữ thông tin quan trọng ( bao gồm chủ trương, kế hoạch, chiến lược phát triển, số liệu, dữ liệu về bệnh nhân, nhân sự, tài chính ....).

#### **Mục 1**

#### **QUẢN LÝ CÁC PHƯƠNG TIỆN LƯU TRỮ DI ĐỘNG**

##### **Điều 28. Quy định sử dụng thiết bị lưu trữ cá nhân**

Nghiêm cấm CBNV trong bệnh viện sử dụng USB, thẻ nhớ, bộ nhớ trong smartphone, ổ cứng di động, ổ cứng ngoài cá nhân để chép dữ liệu từ máy tính

nội bộ của bệnh viện. Trong trường hợp đặc biệt phải được sự phê duyệt cho phép theo quy định của . Phòng Kế hoạch Tổng hợp bệnh viện.

**Điều 29. Quy định đối với các thiết bị lưu trữ của đơn vị được cấp phép**

1. Các phương tiện lưu trữ di động (ổ cứng, USB, thẻ nhớ...) sử dụng tại bệnh viện phải được dán nhãn nhận biết phương tiện được phép sử dụng, phải chỉ định cá nhân quản lý và chịu trách nhiệm.

2. Trường hợp sử dụng các phương tiện lưu trữ di động với các máy chủ, phương tiện phải được kiểm tra mã độc trước khi sử dụng.

**Mục 2**

**AN TOÀN KHI THU HỒI, LUÂN CHUYỂN, THANH LÝ  
THIẾT BỊ/HỆ THỐNG**

**Điều 30. An toàn khi thu hồi, luân chuyển, thanh lý thiết bị/hệ thống**

1. Các thiết bị (máy tính, phương tiện lưu trữ...) khi thu hồi, luân chuyển, thanh lý bộ phận đang sử dụng/quản lý phải xóa dữ liệu, ghi đè hoặc phá hủy vật lý (đảm bảo không khôi phục được).

2. Đối với các phương tiện lưu trữ có chứa dữ liệu quan trọng, phương án xử lý và ghi đè dữ liệu phải được Phòng Kế hoạch Tổng hợp phê duyệt.

3. Trường hợp bàn giao thiết bị mạng: Phòng Kế hoạch Tổng hợp loại bỏ hoàn toàn các cấu hình hiện tại trên thiết bị, khôi phục về trạng thái mặc định của nhà sản xuất trước khi thay đổi mục đích sử dụng/bàn giao.

4. Trường hợp bàn giao/luân chuyển máy chủ.

a) Đối với máy chủ thay đổi mục đích sử dụng, bộ phận quản trị máy chủ phải thực hiện hủy (xóa) hết các dữ liệu trên máy chủ cũ trước khi thay đổi mục đích sử dụng (bao gồm: các file, thư mục cấu hình ứng dụng, mã nguồn ...).

b) Tất cả các thiết bị ra/vào cơ quan đều phải có sự phê duyệt và kiểm soát theo qui định.

5. Trường hợp kết thúc vận hành, khai thác, thanh lý, hủy bỏ hệ thống



a) Phải được bộ phận chuyên trách an toàn thông tin thực hiện kiểm tra, đánh giá bảo đảm an toàn thông tin.

b) Quá trình xử lý thông tin trên hệ thống phải được thực hiện khi thay đổi mục đích sử dụng hoặc gỡ bỏ theo phương án kỹ thuật được lãnh đạo bệnh viện phê duyệt.

## **Chương IX**

### **QUY ĐỊNH ĐẢM BẢO ATTT CHO SẢN PHẨM PHẦN MỀM/THIẾT BỊ**

#### **Mục 1**

#### **QUY ĐỊNH VỀ TIÊU CHUẨN ATTT CHO CÁC SẢN PHẨM PHẦN MỀM/ THIẾT BỊ**

##### **Điều 31. Tiêu chuẩn ATTT cho các sản phẩm phần mềm/ thiết bị**

1. Các sản phẩm phần mềm/thiết bị bao gồm tất cả các sản phẩm phần mềm, thiết bị do bệnh viện triển khai ứng dụng, sản xuất, hợp tác, mua sắm sử dụng, các sản phẩm phần mềm/thiết bị của đối tác nhưng được hợp tác triển khai, ứng dụng, hoạt động trong nội bộ bệnh viện.

2. Tất cả các sản phẩm phần mềm/thiết bị phải đảm bảo theo tiêu chuẩn ATTT cho các loại sản phẩm phần mềm/thiết bị do bệnh viện ban hành (bao gồm ứng dụng web, mobile...).

#### **Mục 2**

#### **QUY ĐỊNH KIỂM SOÁT, ĐÁNH GIÁ ATTT TRƯỚC KHI TRIỂN KHAI, NÂNG CẤP, SỬ DỤNG SẢN PHẨM PHẦN MỀM/THIẾT BỊ**

##### **Điều 32. Quy định đánh giá ATTT trước khi triển khai, nâng cấp, sử dụng**

Tất cả các sản phẩm phần mềm/thiết bị trước khi triển khai, nâng cấp hay đưa vào sử dụng đều phải đáp ứng các tiêu chuẩn ATTT do bệnh viện ban hành.

### Mục 3

## QUY ĐỊNH THỬ NGHIỆM VÀ NGHIỆM THU ĐƯA VÀO SỬ DỤNG SẢN PHẨM PHẦN MỀM/THIẾT BỊ

### Điều 33: Quy định thử nghiệm và nghiệm thu trước khi đưa vào sử dụng

1. Bên triển khai xây dựng kế hoạch, nội dung thử nghiệm hệ thống, trình cấp có thẩm quyền phê duyệt, trước khi thực hiện thử nghiệm và nghiệm thu hệ thống.
2. Hệ thống phải được thực hiện kiểm thử hệ thống trước khi đưa vào vận hành, khai thác sử dụng theo nội dung, kế hoạch, quy trình thử nghiệm và nghiệm thu hệ thống được phê duyệt.
3. Giao cho bộ phận chuyên trách an toàn thông tin là đầu mối thực hiện hoặc phối hợp thực hiện với các đơn vị triển khai trong quá trình thử nghiệm và nghiệm thu hệ thống.

### Chương X

## QUY ĐỊNH ĐẢM BẢO ATTT CHO HỆ THỐNG CÔNG NGHỆ THÔNG TIN

Các quy định trong mục này áp dụng cho các hoạt động vận hành, khai thác các hệ thống CNTT (như quy hoạch, triển khai, quản trị, tác động, đóng mở kết nối...) nhằm đảm bảo ATTT cho tất cả các hệ thống công nghệ thông tin của bệnh viện.

### Mục 1

## QUY ĐỊNH VỀ TIÊU CHUẨN ATTT CHO CÁC HỆ THỐNG CÔNG NGHỆ THÔNG TIN

### Điều 34. Tiêu chuẩn ATTT cho các hệ thống công nghệ thông tin

1. Các hệ thống công nghệ thông tin (bao gồm tất cả các thiết bị mạng lõi, truyền dẫn, tài nguyên vật lý, hệ thống máy chủ, hệ điều hành, cơ sở dữ liệu...) được triển khai, ứng dụng trong bệnh viện cho mục đích quản lý khám, chữa bệnh.
2. Tất cả các hệ thống công nghệ thông tin trong bệnh viện phải được thiết kế, triển khai, thiết lập, cấu hình bảo mật đảm bảo ATTT tương ứng với từng loại



tiêu chuẩn ATTT cho hệ thống, thiết bị, giải pháp, dịch vụ do bệnh viện ban hành (như tiêu chuẩn ATTT cho máy chủ, hệ điều hành, cơ sở dữ liệu...).

3. Khi có thay đổi thiết kế, đánh giá lại tính phù hợp của phương án thiết kế đối với các yêu cầu an toàn đặt ra đối với hệ thống thông tin.

## **Mục 2**

### **QUY ĐỊNH ĐẢM BẢO ATTT TRONG QUY HOẠCH HỆ THỐNG CNTT**

#### **Điều 35. Yêu cầu về tài liệu, văn bản vận hành, triển khai theo kế hoạch.**

1. Tất cả hệ thống mạng phải có tài liệu quy hoạch được cấp lãnh đạo tương ứng phê duyệt.

2. Tất cả các máy chủ/thiết bị phải được lắp đặt, triển khai và vận hành theo các tài liệu quy hoạch đã được Phòng Kế hoạch Tổng hợp phê duyệt.

3. Tất cả các hệ thống phải có tài liệu, hồ sơ mô tả và quản lý hệ thống, tài liệu hồ sơ này phải được cập nhật ngay khi có sự thay đổi thông tin, bao gồm:

- Mô hình kết nối của các thiết bị mạng, máy chủ, mô hình mạng bao gồm cả sơ đồ luận lý và vật lý.
- Thông tin quản lý thiết bị mạng trong hệ thống (tên/loại/mục đích sử dụng/cấu hình phần cứng... thiết bị).
- Thông tin quản lý các máy chủ (tên/ loại/chức năng/cấu hình vật lý/hệ điều hành/các phần mềm/dịch vụ... máy chủ).
- Thông tin quản lý ứng dụng (tên/loại/module... ứng dụng).
- Thông tin quản lý sự cố (tên/thời điểm xảy ra/biện pháp xử lý... sự cố).
- Thông tin quản lý rủi ro hệ thống (loại rủi ro gây ảnh hưởng, lỗ hổng...)
- Thông tin liên lạc của những cá nhân quản lý/chịu trách nhiệm về hệ thống, ứng dụng.
- Các tài liệu, quy trình, hướng dẫn khai thác, vận hành hệ thống.

## **Mục 3**

## **QUY ĐỊNH VỀ CHÍNH SÁCH TRUY CẬP, ĐỊNH TUYẾN MẠNG**

### **Điều 36. Quy định chung về việc phê duyệt, sử dụng chính sách truy cập, định tuyến mạng**

1. Tất cả các chính sách truy nhập phải được Phòng Kế hoạch Tổng hợp phê duyệt trước khi triển khai. Nội dung phê duyệt phải đầy đủ thông tin về mục đích sử dụng và thông tin triển khai chi tiết.

2. Tất cả các chính sách truy nhập sau khi phê duyệt đưa vào sử dụng phải được sử dụng đúng mục đích phê duyệt, không sử dụng cho các mục đích khác.

### **Điều 37. Quy định quản lý chính sách truy nhập tường lửa**

1. Tất cả các chính sách truy cập tường lửa trong bệnh viện đều phải đảm bảo theo tiêu chuẩn cấu hình chính sách (policy) cho hệ thống các tường lửa do bệnh viện ban hành.

2. Nhân sự quản trị tường lửa phải thực hiện lưu hồ sơ theo dõi các chính sách được thiết lập trên tường lửa. Thể hiện đầy đủ các thông tin sau: Địa chỉ IP nguồn, địa chỉ IP đích, cổng sử dụng dịch vụ, thời hạn hiệu lực chính sách yêu cầu, mô tả mục đích sử dụng.

## **Mục 4**

## **QUY ĐỊNH CÀI ĐẶT, TRIỂN KHAI, CẤU HÌNH, CẬP NHẬT PHIÊN BẢN, BẢN VÁ CHO HỆ THỐNG/THIẾT BỊ**

### **Điều 38. Quy định về đảm bảo ATTT sau khi cài đặt, triển khai máy chủ/thiết bị**

1. Bộ phận triển khai hệ thống phải cài đặt hệ thống/thiết bị theo hướng dẫn đã được đơn vị ban hành. Các hướng dẫn triển khai phải được cập nhật đầy đủ khi có sự thay đổi (ví dụ: cập nhật thêm bản vá lỗi máy chủ...).

2. Sau khi triển khai/cài đặt bộ phận ATTT phải kiểm tra và ký xác nhận đảm bảo hệ thống, thiết bị đảm bảo các tiêu chuẩn ATTT do bệnh viện ban hành.

### **Điều 39. Quy định quản lý phiên bản và bản vá trên máy chủ/thiết bị/ứng dụng**

1. Bộ phận quản trị các hệ thống, thiết bị khi triển khai nâng cấp, cập nhật bản vá phải quản lý thông tin lịch sử các phiên bản ứng dụng, hệ thống được đưa



lên khai thác, có tài liệu mô tả rõ ràng sự thay đổi ứng dụng mỗi lần cập nhật.

2. Bộ phận quản trị có trách nhiệm nâng cấp, cập nhật bản vá cho hệ thống/thiết bị với các lỗ hổng ATTT do đối tác cung cấp, các khuyến cáo của nhà sản xuất hoặc các đơn vị chuyên trách quản lý về ATTT cảnh báo.

## **Mục 5**

### **QUY ĐỊNH VỀ CÔNG TÁC QUẢN TRỊ HỆ THỐNG CNTT**

#### **Điều 40. Quy định về công tác quản trị**

1. Tất cả các truy cập để quản trị trên thiết bị đều phải được đặt mật khẩu bảo vệ (cổng console...).

2. Không thực hiện quản trị hệ thống, máy chủ, thiết bị mạng, tường lửa, thiết bị chuyển mạch, thiết bị định tuyến, trang quản trị nội dung từ ngoài internet hoặc trực tiếp từ các máy tính cá nhân. Tất cả các thao tác quản trị phải thực hiện trên hệ thống/máy tính đã được quy hoạch/đánh giá ATTT và phê duyệt.

3. Riêng với hệ thống công khai (public), hosting ngoài internet yêu cầu phải sử dụng giải pháp mạng riêng ảo (VPN), hệ thống truy cập từ xa do bộ phận ATTT cung cấp để thực hiện công tác quản trị từ xa nếu cần thiết.

4. Đơn vị quản trị thiết bị phải thực hiện sao lưu định kỳ (ngày/tuần/tháng) theo kế hoạch phê duyệt của Phòng Kế hoạch Tổng hợp. Nội dung sao lưu gồm: hệ điều hành, file cấu hình thiết bị...

5. Bộ phận quản trị thiết bị phải xây dựng phương án khôi phục cấu hình thiết bị.

#### **Điều 41. Quy định quản lý rủi ro**

Đối với các hệ thống chưa được thực hiện cấu hình ATTT đầy đủ theo hướng dẫn và quy định của bệnh viện, còn tồn tại các lỗ hổng/điểm yếu đã được cảnh báo, bộ phận quản trị của hệ thống phải thực hiện các biện pháp theo dõi và quản lý rủi ro hệ thống bị tấn công khai thác cụ thể:

1. Cập nhật các lỗ hổng/điểm yếu, lỗi chưa được xử lý vào hồ sơ quản lý hệ thống. Chuyển trạng thái hệ thống sang tình trạng còn tồn tại rủi ro và nguy cơ bị khai thác, tấn công.

2. Thực hiện các biện pháp tăng cường giám sát đối với hệ thống bằng các

công cụ tự động và giám sát thủ công (kiểm tra log hệ thống...). Trường hợp hệ thống còn tồn tại các lỗi, điểm yếu/lỗ hổng ở mức cao, cần thực hiện kiểm tra xem xét log hệ thống, phân tích các dấu hiệu tấn công định kỳ hàng ngày.

3. Phân tích, lựa chọn và thiết lập các biện pháp kiểm soát tạm thời nhằm giảm thiểu nguy cơ bị khai thác trong từng trường hợp cụ thể (cài đặt tường lửa, cô lập hệ thống có lỗi đối với các hệ thống quan trọng để hạn chế bị tấn công leo thang...).

## **Mục 6**

### **GIÁM SÁT VẬN HÀNH, TÁC ĐỘNG HỆ THỐNG**

#### **Điều 42. Ghi Log vận hành và quản trị hệ thống, ứng dụng**

Bộ phận quản trị phải bật tính năng ghi log nhằm lưu vết của hệ điều hành, log dịch vụ, log cơ sở dữ liệu, log hệ thống đảm bảo ATTT, log ứng dụng theo các tiêu chuẩn ATTT tương ứng cho từng đối tượng do bệnh viện ban hành.

#### **Điều 43. Xử lý log lỗi**

1. Các log sai, lỗi của hệ thống đều phải được bộ phận quản trị và ATTT xem xét, phân tích nguyên nhân và đưa ra biện pháp xử lý và cải tiến.
2. Lưu hồ sơ xem xét hành động đã xử lý.

## **Chương XI**

### **QUY ĐỊNH QUẢN LÝ SỰ CỐ ATTT**

#### **Điều 44. Phát hiện, cảnh báo, xử lý sự cố ATTT**

Tất cả các sự cố ATTT trong bệnh viện phải được phát hiện, xử lý theo quy trình, kịch bản xử lý sự cố ATTT do bệnh viện ban hành.

## **Chương XII**

### **KIỂM TRA, KHẮC PHỤC LỖ HỔNG ATTT, BÁO CÁO ĐÁNH GIÁ CÔNG TÁC AN TOÀN THÔNG TIN**

#### **Điều 45. Kiểm tra theo kế hoạch**

1. Phòng Kế hoạch Tổng hợp lập kế hoạch và thực hiện kiểm tra định kỳ (tối thiểu 1 lần/ quý) việc chấp hành về các quy định về ATTT tại các khoa phòng thuộc bệnh viện.



2. Khi tiến hành kiểm tra phải có biên bản kiểm tra được ký bởi các bên, ghi đúng hiện trạng và đầy đủ nội dung kiểm tra.

#### **Điều 46. Kiểm tra đột xuất**

1. Phòng Kế hoạch Tổng hợp tin thực hiện kiểm tra theo yêu cầu của Giám đốc bệnh viện.

2. Phòng Kế hoạch Tổng hợp tiến hành kiểm tra đột xuất các cá nhân, đơn vị trực thuộc bệnh viện có dấu hiệu vi phạm quy định về ATTT.

#### **Điều 47. Chế độ báo cáo**

1. Báo cáo định kỳ

a) Nhân sự phụ trách ATTT thực hiện báo cáo định kỳ hàng quý về cho phòng Kế hoạch Tổng hợp.

b) Nội dung báo cáo định kỳ gồm: Kết quả thực hiện công tác ATTT trong quý, kế hoạch công tác ATTT quý tiếp theo. Phòng Kế hoạch Tổng hợp có trách nhiệm ban hành các hướng dẫn chi tiết, biểu mẫu, thông tin cần báo cáo phù hợp với định hướng quản lý công tác ATTT trong bệnh viện.

c) Thời gian gửi báo cáo: Gửi trước ngày 25 hàng quý.

2. Báo cáo đột xuất

Nhân sự phụ trách ATTT báo cáo đột xuất theo yêu cầu của trưởng Phòng Kế hoạch Tổng hợp, Giám đốc bệnh viện hoặc theo công việc đột xuất cần xử lý, hỗ trợ.

### **Chương XIII QUY ĐỊNH BẢO MẬT VÀ TÍNH RIÊNG TƯ CỦA HỒ SƠ BỆNH ÁN ĐIỆN TỬ**

#### **Điều 48. Bảo mật và tính riêng tư của hồ sơ bệnh án điện tử**

Thực hiện theo qui định tại Điều 10 Thông tư số 46/2018/TT – BHYT ngày 28/12/2018 và các qui định khác của Bộ Y tế.

#### **Điều 49. Bảo vệ thông tin sức khỏe người bệnh**

1. Những thông tin sức khỏe được bảo vệ là những thông tin bao gồm dữ liệu nhân khẩu học giúp nhận dạng được cá nhân đó liên quan đến.

a) Thông tin về sức khỏe hoặc tình trạng sức khỏe thể chất hoặc tinh thần

trong quá khứ, hiện tại hoặc tương lai.

b) Thông tin về cung cấp dịch vụ chăm sóc sức khỏe cho cá nhân.

c) Thông tin thanh toán trong quá khứ, hiện tại hoặc tương lai cho việc cung cấp dịch vụ chăm sóc sức khỏe cá nhân.

d) Tên, tất cả các số nhận dạng địa lý, số điện thoại, số fax, địa chỉ email, số an sinh xã hội, số hồ sơ bệnh án, số bảo hiểm y tế, số tài khoản ngân hàng, số chứng chỉ, giấy phép, số nhận dạng xe và seri (bao gồm cả biển số xe), số định danh thiết bị và số seri, định danh sinh trắc học, hình ảnh đầy đủ khuôn mặt và bất kỳ hình ảnh nào giúp nhận dạng, bất kỳ số nhận dạng, đặc điểm nhận dạng...

2. Có thể sử dụng hình ảnh cá nhân mà không cần sự đồng ý của người có hình ảnh hoặc người đại diện theo pháp luật của họ, bao gồm: hình ảnh được sử dụng vì lợi ích quốc gia, dân tộc, lợi ích công cộng, hình ảnh được sử dụng từ các hoạt động công cộng, bao gồm hội nghị, hội thảo, hoạt động thi đấu thể thao, biểu diễn nghệ thuật và hoạt động công cộng khác mà không làm tổn hại đến danh dự, nhân phẩm, uy tín của người có hình ảnh.

#### **Điều 50. Bí mật hồ sơ bệnh án**

1. Hồ sơ bệnh án phải được lưu giữ và giữ bí mật theo quy định của pháp luật; trường hợp hồ sơ bệnh án thuộc phạm vi bí mật nhà nước thì thực hiện theo quy định của pháp luật về bảo vệ bí mật nhà nước. Việc lưu trữ hồ sơ bệnh án được thực hiện theo quy định của pháp luật về lưu trữ.

2. Những thông tin của người bệnh trong hồ sơ bệnh án chỉ được phép công bố khi người bệnh đồng ý hoặc trong trường hợp khác được pháp luật qui định.

#### **Điều 51. Chủ thể được quyền tiếp cận, khai thác hồ sơ bệnh án**

Theo qui định tại Điều 69 Luật Khám bệnh, chữa bệnh ngày 09/01/2023.

1. Khai thác hồ sơ bệnh án trong quá trình điều trị.

a) Học sinh, sinh viên, học viên, nghiên cứu viên của các cơ sở nghiên cứu, cơ sở đào tạo, người hành nghề, người trực tiếp tham gia điều trị người bệnh trong cơ sở khám bệnh, chữa bệnh được đọc nhưng chỉ được sao chép khi có sự đồng ý của cơ sở khám bệnh, chữa bệnh.

b) Người hành nghề của cơ sở khác được đọc, sao chép khi có sự đồng ý của cơ sở khám bệnh, chữa bệnh.

2. Khai thác hồ sơ bệnh án đã hoàn thành quá trình điều trị và được chuyển



lưu trữ.

a) Đại diện cơ quan quản lý nhà nước về y tế, cơ quan điều tra, viện kiểm sát, tòa án, thanh tra chuyên ngành y tế, tổ chức giám định pháp y, pháp y tâm thần, luật sư của người bệnh được tiếp cận, cung cấp hồ sơ bệnh án để thực hiện nhiệm vụ theo quy định của pháp luật có liên quan.

b) Học sinh, sinh viên, học viên, nghiên cứu viên của các cơ sở nghiên cứu, cơ sở đào tạo, người hành nghề trong cơ sở khám bệnh, chữa bệnh được mượn hồ sơ bệnh án tại chỗ để đọc hoặc sao chép phục vụ cho việc nghiên cứu hoặc công tác chuyên môn kỹ thuật khi có sự đồng ý của cơ sở khám bệnh, chữa bệnh.

c) Đại diện cơ quan bảo hiểm xã hội, cơ quan giải quyết bồi thường nhà nước được mượn hồ sơ bệnh án tại chỗ để đọc, ghi chép hoặc đề nghị cấp bản sao phục vụ nhiệm vụ được giao khi có sự đồng ý của cơ sở khám bệnh, chữa bệnh.

d) Người bệnh hoặc người đại diện theo ủy quyền hoặc người đại diện theo pháp luật của người bệnh hoặc người đại diện theo pháp luật của pháp nhân hoặc người được pháp nhân phân công mà pháp nhân đó chịu trách nhiệm quản lý, chăm sóc, nuôi dưỡng người bệnh theo quy định của Bộ luật Dân sự ngày 24/11/2015 được đọc, xem, sao chụp, ghi chép hồ sơ bệnh án và được cung cấp bản tóm tắt hồ sơ bệnh án khi có yêu cầu bằng văn bản.

e) Người do người bệnh là người thành niên tự lựa chọn hoặc người đại diện theo pháp luật của pháp nhân hoặc người được pháp nhân phân công mà pháp nhân đó chịu trách nhiệm quản lý, chăm sóc, nuôi dưỡng người bệnh theo quy định của Bộ luật Dân sự ngày 24/11/2015 được cung cấp bản tóm tắt hồ sơ bệnh án khi có yêu cầu bằng văn bản.

3. Khi sử dụng thông tin trong hồ sơ bệnh án phải giữ bí mật và chỉ được sử dụng đúng mục đích như đã đề nghị với cơ sở khám bệnh, chữa bệnh.

## **Chương XIV** **KHEN THƯỞNG, KỶ LUẬT**

### **Điều 52. Khen thưởng**

Định kỳ (hàng năm) Phòng Kế hoạch Tổng hợp tin chịu trách nhiệm theo dõi và đề xuất khen thưởng, hình thức khen thưởng cho các cá nhân, tập thể có thành

tích tốt trong công tác đảm bảo ATTT.

### **Điều 53. Kỷ luật**

Đối với các cá nhân, khoa, phòng, để xảy ra các sự cố ATTT ảnh hưởng đến hoạt động bệnh viện, ảnh hưởng đến uy tín, hình ảnh và thương hiệu của bệnh viện Phòng Kế hoạch Tổng hợp đề xuất biện pháp xử lý theo chế tài xử lý khi xảy ra sự cố mất ATTT cho phòng Tổ chức – Tài chính và Ban Giám Đốc bệnh viện.

## **Chương XV TỔ CHỨC THỰC HIỆN**

### **Điều 54. Tổ chức thực hiện**

1. Phòng Kế hoạch Tổng hợp phối hợp với các khoa phòng trong bệnh viện xây dựng, hoàn thiện các tiêu chuẩn đảm bảo ATTT cho các đối tượng, hoạt động cụ thể, ban hành theo tình hình thực tế.

2. Phòng Kế hoạch Tổng hợp tin có trách nhiệm phối hợp với các phòng chức năng thường xuyên tổ chức kiểm tra công tác thực thi quy chế này.

3. Trong quá trình thực hiện, nếu có các vấn đề vướng mắc, phát sinh các khoa phòng thuộc bệnh viện phản ánh kịp thời về Phòng Kế hoạch Tổng hợp để tổng hợp, báo cáo Ban Giám đốc xem xét, điều chỉnh cho phù hợp.

4. Quy chế này được phổ biến đến tất cả các nhân viên và được đăng tải trên trang thông tin điện tử của bệnh viện.

5. Trưởng các khoa phòng thuộc bệnh viện có trách nhiệm tổ chức thực hiện các qui định tại Quy chế này. Quán triệt Quy chế này đến toàn thể CBNV trong khoa phòng thực hiện nghiêm túc. Các cá nhân chịu trách nhiệm trước Giám đốc bệnh viện và pháp luật về việc thực hiện Quy chế này.

6. Các nội dung nào không được đề cập trong Quy chế này thì thực hiện theo quy định của pháp luật./.

### **Phụ lục**

## **CHÍNH SÁCH, TIÊU CHUẨN AN TOÀN THÔNG TIN**

(Kèm theo Quyết định số 03 /QĐ-ĐNEMR ngày 01 tháng 10 năm 2025 của Bệnh viện Mắt Hà Nội – Đồng Nai )



**CHÍNH SÁCH MẬT KHẨU MẠNH**

| <b>TT</b> | <b>Chính sách</b>                                   | <b>Yêu cầu</b>                                                                 | <b>Ghi chú</b>                                                                                                              |
|-----------|-----------------------------------------------------|--------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------|
| 1         | Độ dài mật khẩu tối thiểu.                          | $\geq 8$ ký tự                                                                 |                                                                                                                             |
| 2         | Độ phức tạp của mật khẩu.                           | Mật khẩu bao gồm: Chữ hoa, chữ thường, số và ký tự đặc biệt.                   |                                                                                                                             |
| 3         | Số lần đặt mật khẩu không được trùng nhau.          | 3 lần                                                                          | Mật khẩu lần sau phải khác với mật khẩu lần trước.                                                                          |
| 4         | Đổi mật khẩu cho lần đăng nhập đầu tiên.            | Có                                                                             | Người dùng tự thay đổi mật khẩu và thay đổi mật khẩu mạnh.                                                                  |
| 5         | Thời hạn hiệu lực của mật khẩu.                     | $\leq 90$ ngày                                                                 | Định kỳ (tối đa 90 ngày ) người sử dụng phải thực hiện đổi mật khẩu.                                                        |
| 6         | Số lần đăng nhập không thành công liên tiếp tối đa. | $\leq 5$ lần                                                                   | Hệ thống thực hiện bật captcha hoặc khóa đăng nhập sau khoảng thời gian nếu thực hiện đăng nhập liên tiếp không thành công. |
| 7         | Lưu trữ thông tin tài khoản và mật khẩu.            | Thông tin tài khoản và mật khẩu được lưu dưới dạng mã hóa, không viết ra giấy. |                                                                                                                             |

|   |                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                                                                                                       |
|---|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------|
| 8 | Mật khẩu không dễ đoán. | <ul style="list-style-type: none"> <li>- Mật khẩu không được bao gồm thông tin cá nhân (tài khoản, số điện thoại, họ tên, ngày tháng năm sinh, mã nhân viên).</li> <li>- Mật khẩu không được bao gồm các thông tin thông dụng như tên phòng ban, đơn vị, ngày tháng năm thiết lập mật khẩu.</li> <li>- Mật khẩu không được bao gồm các chuỗi ký tự liên tiếp (từ 4 ký tự trở lên), chuỗi các ký tự giống nhau (từ 4 ký tự trở lên).</li> <li>- Không đặt mặc định mật khẩu quy định chung/ mặc định.</li> </ul> | <p>Ví dụ mật khẩu không được phép:</p> <p>1234566a@</p> <p>12345678@</p> <p>Abc12345@</p> <p>....</p> |
|---|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------|

## Phần II

### CHÍNH SÁCH QUẢN LÝ AN TOÀN MẠNG

#### 2.1. Quản lý, vận hành hoạt động bình thường của hệ thống.

a) Thực hiện việc quản lý và kiểm soát mạng nhằm ngăn ngừa các nguy cơ, rủi ro và duy trì an toàn cho các máy tính, ứng dụng sử dụng mạng:

- Có sơ đồ logic và vật lý về hệ thống mạng, tổ chức quản lý định danh, xác thực đối với người sử dụng nhằm mục đích quản lý hệ thống chặt chẽ, bảo đảm an toàn và bảo mật.

- Sử dụng thiết bị tường lửa, thiết bị phát hiện và kiểm soát truy cập từ bên ngoài mạng và phân chia hệ thống mạng thành các vùng mạng quản lý theo chính sách an toàn thông tin (ATTT) riêng; kiểm soát truy cập từ bên trong mạng; kết



nói về hệ thống giám sát tập trung; phòng chống xâm nhập giữa các vùng mạng; phòng chống phần mềm độc hại trên môi trường mạng.

b) Thiết lập, cấu hình đầy đủ các tính năng của thiết bị mạng. Thường xuyên, kiểm tra phiên bản hệ điều hành của thiết bị mạng để cập nhật, vá lỗi khi cần thiết. Sử dụng các công cụ để dò tìm và phát hiện kịp thời các điểm yếu, lỗ hổng bảo mật và các truy cập bất hợp pháp vào hệ thống mạng. Thường xuyên kiểm tra, phát hiện những kết nối, trang thiết bị, phần mềm cài đặt bất hợp pháp vào mạng.

c) Xác định và ghi rõ các tính năng an toàn, các mức độ bảo mật của dịch vụ và yêu cầu quản lý trong các thỏa thuận về dịch vụ mạng do bên thứ ba cung cấp.

d) Mạng không dây (WIFI), thiết lập các thông số an toàn nhằm tăng cường công tác bảo mật.

- Sử dụng mã hóa WPA2 hoặc cao hơn.
- Mật khẩu ít nhất 12-16 ký tự bao gồm các chữ hoa, chữ thường, số và ký tự đặc biệt.
- Thay đổi mật khẩu định kỳ 3 tháng một lần.
- Giới hạn quyền truy cập đối với một số vị trí cần thiết thông qua lọc địa chỉ MAC thiết bị.

## **2.2. Cập nhật, sao lưu dự phòng và khôi phục sau khi xảy ra sự cố.**

a) Sử dụng tối thiểu 2 đường truyền Internet của tối thiểu 2 nhà cung cấp dịch vụ khác nhau, các đường truyền trên trục lõi và các thiết bị quan trọng có tối thiểu 2 đường truyền vật lý. Các thiết bị quan trọng của hệ thống đảm bảo cơ chế High availability (VRRP, Stack Switch...), các thiết bị còn lại có cơ chế mua sắm dự phòng trong trường hợp hư hỏng đột xuất, đảm bảo tính sẵn sàng đáp ứng yêu cầu hoạt động của hệ thống mạng.

b) Các thông tin cấu hình thiết bị mạng, kết nối, định danh trong mạng được backup định kỳ, được lưu trữ đảm bảo không bị ảnh hưởng và khôi phục nhanh chóng sau khi xảy ra sự cố; thiết lập kịch bản ứng phó, khôi phục sau khi sự cố xảy ra.

c) Thường xuyên kiểm tra và cập nhật firmware.

### **2.3. Chính sách truy cập và quản lý cấu hình hệ thống**

a) Cán bộ quản lý, nhân viên vận hành truy cập, khai thác thông tin theo trách nhiệm và phân quyền được quy định; việc khai thác thông tin phải bảo đảm nguyên tắc bảo mật, không được tự ý cung cấp thông tin ra bên ngoài.

b) Cán bộ quản lý, nhân viên vận hành có trách nhiệm theo dõi và phát hiện các trường hợp truy cập hệ thống trái phép hoặc thao tác vượt quá giới hạn, báo cáo cho cán bộ quản lý để tiến hành ngăn chặn, thu hồi, khóa quyền truy cập của các tài khoản vi phạm.

c) Cấu hình tối ưu, tăng cường bảo mật cho thiết bị hệ thống (cứng hóa) trước khi đưa vào vận hành, khai thác.

d) Quy trình kết nối thiết bị đầu cuối của người sử dụng vào hệ thống mạng; truy nhập và quản lý cấu hình hệ thống; cấu hình tối ưu, tăng cường bảo mật cho thiết bị mạng, bảo mật (cứng hóa) trong hệ thống và thực hiện quy trình trước khi đưa hệ thống vào vận hành khai thác.

## **Phần III**

### **CHÍNH SÁCH QUẢN LÝ AN TOÀN MÁY CHỦ VÀ ỨNG DỤNG**

#### **3.1. Quản lý, vận hành hoạt động bình thường của hệ thống máy chủ và dịch vụ**

a) Bảo đảm cho hệ điều hành, phần mềm cài đặt trên máy chủ hoạt động liên tục, ổn định và an toàn.

b) Thường xuyên kiểm tra cấu hình, các file nhật ký hoạt động của hệ điều hành, phần mềm nhằm kịp thời phát hiện và xử lý những sự cố nếu có.

c) Quản lý các thay đổi cấu hình kỹ thuật của hệ điều hành, phần mềm.

- Thường xuyên cập nhật các bản vá lỗi hệ điều hành, phần mềm từ nhà cung cấp.

- Loại bỏ các thành phần của hệ điều hành, phần mềm không cần thiết hoặc không còn nhu cầu sử dụng.



- Các bản quyền phần mềm được thống kê, quản lý thời gian hạn phục vụ cho việc gia hạn.

### **3.2. Truy cập mạng của máy chủ**

a) Bảo đảm các kết nối mạng trên máy chủ hoạt động liên tục, ổn định và an toàn.

b) Cấu hình, kiểm soát các kết nối, các cổng dịch vụ từ bên trong đi ra cũng nhưng bên ngoài vào hệ thống.

### **3.3. Truy cập và quản trị máy chủ và ứng dụng**

a) Thay đổi các tài khoản, mật khẩu mặc định ngay khi đưa hệ điều hành, phần mềm vào sử dụng.

b) Cấp quyền quản lý truy cập của người sử dụng trên máy chủ cài đặt hệ điều hành; thiết lập phương thức xác thực mạnh, mật khẩu mạnh, ưu tiên các phương thức xác thực đa yếu tố (MFA); thiết lập quyền truy cập theo nguyên tắc quyền tối thiểu và phân vai truy cập.

c) Toàn bộ máy chủ và thiết bị công nghệ thông tin (CNTT) không phải máy tính ngoại trừ các hệ thống bắt buộc phải có giao tiếp với Internet (các hệ thống phục vụ truy cập Internet; cung cấp giao diện ra Internet của trang tin điện tử, thư điện tử...; phục vụ cập nhật bản vá hệ điều hành, mẫu mã độc, mẫu điểm yếu, mẫu tấn công; phục vụ backup từ cloud) không được kết nối Internet.

d) Cán bộ chuyên trách về CNTT của bệnh viện chịu trách nhiệm cài đặt, gỡ bỏ hệ điều hành, dịch vụ, phần mềm trên hệ thống máy chủ và ứng dụng. Cán bộ chuyên trách về CNTT của bệnh viện chịu trách nhiệm cài đặt phần mềm cho máy tính phục vụ công việc. Người dùng không được can thiệp vào các phần mềm đã cài đặt trên máy tính (thay đổi, gỡ bỏ...) khi chưa được sự đồng ý của Cán bộ CNTT của bệnh viện.

e) Kết nối và gỡ bỏ hệ thống máy chủ và dịch vụ khỏi hệ thống

- Cấu hình tối ưu và tăng cường bảo mật (cứng hóa) cho hệ thống máy chủ trước khi đưa vào vận hành, khai thác.

- Lập kế hoạch gỡ bỏ một cách an toàn, bao gồm việc xóa sạch dữ liệu và thông tin nhạy cảm để đảm bảo rằng không có thông tin nào bị lộ ra ngoài.

f) Các máy chủ trước khi đưa vào vận hành khai thác cần triển khai một số yêu cầu tối ưu và tăng cường bảo mật (cứng hóa) như:

- Sử dụng hệ điều hành bảo đảm ATTT.
- Loại bỏ hoặc tắt tất cả các dịch vụ, cổng mở không cần thiết.
- Sử dụng các phiên bản phần mềm an toàn.
- Thường xuyên kiểm tra, cập nhật bản phiên bản và bản vá lỗi cho hệ thiều hành, phần mềm ứng dụng.

g) Kiểm soát truy cập và ghi nhận lại hoạt động (log) của tất cả các dịch vụ. Cấm tất cả các truy cập từ bên ngoài vào hệ thống, chỉ cấp quyền truy cập xác đáng cho các người dùng tin cậy.

h) Kiểm soát truy cập ở cấp người dùng cho mỗi dịch vụ.

### **3.4 Cập nhật, sao lưu dự phòng và khôi phục sau khi xảy ra sự cố**

a) Triển khai hệ thống/phương tiện lưu trữ độc lập với hệ thống lưu trữ trên các máy chủ dịch vụ để sao lưu dự phòng.

b) Phân loại và quản lý thông tin, dữ liệu được lưu trữ theo từng loại/nhóm thông tin được gán nhãn khác nhau.

c) Thực hiện sao lưu, dự phòng các thông tin, dữ liệu cơ bản sau: tập tin cấu hình hệ thống, ảnh hệ điều hành máy chủ, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ...

d) Thiết lập kịch bản ứng phó, khôi phục sau khi sự cố xảy ra.

## **Phần IV**

### **CHÍNH SÁCH QUẢN LÝ AN TOÀN DỮ LIỆU**

#### **4.1. Yêu cầu an toàn đối với phương pháp mã hóa**



a) Bệnh viện xây dựng và áp dụng quy định sử dụng các phương thức mã hóa thích hợp theo các chuẩn quốc gia hoặc quốc tế đã được công nhận để bảo vệ thông tin.

b) Phải có biện pháp quản lý khóa mã hóa thích hợp để hỗ trợ việc sử dụng các kỹ thuật mã hóa.

c) Phân loại, quản lý và sử dụng khóa bí mật và dữ liệu mã hóa.

d) Cơ chế mã hóa và kiểm tra tính nguyên vẹn của dữ liệu.

#### **4.2. Trao đổi dữ liệu qua môi trường mạng và phương tiện lưu trữ**

a) Ban hành quy định về trao đổi thông tin tối thiểu gồm: Phân loại thông tin theo mức độ nhạy cảm; quyền và trách nhiệm của cá nhân khi tiếp cận thông tin; biện pháp đảm bảo tính toàn vẹn, bảo mật khi truyền nhận, xử lý, lưu trữ thông tin; chế độ bảo quản thông tin; Các thông tin, tài liệu, dữ liệu nhạy cảm phải được mã hóa trước khi trao đổi, truyền nhận qua mạng máy tính.

b) Thực hiện các biện pháp quản lý, giám sát và kiểm soát chặt chẽ các trang, các kết nối dữ liệu cung cấp thông tin, dịch vụ, giao dịch trực tuyến cho các tổ chức, cá nhân bên ngoài.

c) Thực hiện biện pháp bảo vệ trang thiết bị, phần mềm phục vụ trao đổi thông tin nội bộ nhằm hạn chế việc xâm nhập, khai thác bất hợp pháp các thông tin nhạy cảm.

d) Sao lưu dự phòng và khôi phục dữ liệu (tần suất sao lưu dự phòng, phương tiện lưu trữ, thời gian lưu trữ; nơi lưu trữ, phương thức lưu trữ và phương thức lấy dữ liệu ra khỏi phương tiện lưu trữ).

- Lập danh sách các dữ liệu, phần mềm cần được sao lưu, có phân loại theo thời gian lưu trữ, thời gian sao lưu, phương pháp sao lưu và thời gian kiểm tra phục hồi hệ thống từ dữ liệu sao lưu.

- Xây dựng tài liệu, quy trình hướng dẫn sao lưu/phục hồi dữ liệu của hệ thống: Bộ phận quản trị hệ thống thực hiện xây dựng Tài liệu hướng dẫn sao lưu cụ thể đối với từng hệ thống cung cấp dịch vụ, hệ thống điều hành, quản lý.

#### **4.3. Cập nhật đồng bộ thông tin, dữ liệu giữa hệ thống sao lưu dự phòng chính và hệ thống phụ.**

a) Định kỳ hoặc khi có thay đổi cấu hình trên hệ thống thực hiện quy trình sao lưu dự phòng: tập tin cấu hình hệ thống, dữ liệu, thông tin nghiệp vụ và các thông tin, dữ liệu quan trọng khác trên hệ thống (nếu có).

b) Thực hiện sao lưu dữ liệu định kỳ: Cán bộ phụ trách sao lưu thực hiện sao lưu định kỳ theo phương án sao lưu đã được phê duyệt.

c) Kiểm tra định kỳ: Dữ liệu sao lưu phải được lưu trữ an toàn và được kiểm tra thường xuyên đảm bảo sẵn sàng cho việc sử dụng khi cần. Kiểm tra, phục hồi hệ thống từ dữ liệu sao lưu.

### **Phần V**

## **CHÍNH SÁCH QUẢN LÝ AN TOÀN THIẾT BỊ VÀ NGƯỜI DÙNG ĐẦU CUỐI**

### **5.1. Chính sách về quản lý an toàn thiết bị đầu cuối**

a) Thông tin về thiết bị đầu cuối (tên, chủng loại, địa chỉ MAC, địa chỉ IP) phải được quản lý và cập nhật.

b) Các thiết bị đầu cuối phải được quản lý khi kết nối vào hệ thống mạng theo địa chỉ MAC, IP.

c) Thực hiện việc kiểm tra, đánh giá, từ đó xử lý những điểm yếu ATTT cho thiết bị đầu cuối định kỳ và trước khi bắt đầu đưa vào sử dụng.

d) Khi truy cập và sử dụng thiết bị đầu cuối từ xa phải có cơ chế xác thực và sử dụng giao thức mạng an toàn.

e) Lập kế hoạch bảo trì định kỳ cho thiết bị để kiểm tra, bảo trì phần cứng và nâng cấp phần mềm, nhằm đảm bảo thiết bị luôn hoạt động ở hiệu suất tối ưu. Theo dõi tuổi thọ thiết bị và thay thế những thiết bị đã lỗi thời hoặc không còn đáp ứng yêu cầu công việc, nhằm đảm bảo hiệu suất và bảo mật.



f) Việc cấu hình, kết nối, triển khai và gỡ bỏ thiết bị đầu cuối trong hệ thống phải được cho phép bởi người có thẩm quyền và thực hiện theo quy trình được phê duyệt.

## **5.2. Chính sách về quản lý an toàn người sử dụng đầu cuối**

a) Quản lý truy cập, sử dụng tài nguyên nội bộ.

- Người sử dụng khi truy cập, sử dụng tài nguyên nội bộ, truy cập mạng và tài nguyên trên Internet phải tuân thủ các quy định của pháp luật về bảo đảm ATTT và các quy định của bệnh viện.

- Khi cài đặt, kết nối máy tính/thiết bị đầu cuối phải thực hiện theo hướng dẫn/quy trình dưới sự giám sát của bộ phận chuyên trách về ATTT.

- Máy tính/thiết bị đầu cuối phải được xử lý điểm yếu ATTT, cấu hình cứng hóa bảo mật trước khi kết nối vào hệ thống.

- Các máy tính thuộc sở hữu cá nhân (máy xách tay của cá nhân, thiết bị di động thông minh) muốn sử dụng mục đích phục vụ công việc theo yêu cầu của bệnh viện, muốn kết nối vào hệ thống thông tin của bệnh viện phải được bộ phận quản lý ATTT kiểm tra trước khi đưa vào sử dụng.

- Việc sử dụng các thiết bị lưu trữ ngoài như ổ cứng di động, các loại thẻ nhớ, thiết bị lưu trữ USB,... phải thường xuyên quét mã độc trước khi đọc hoặc sao chép dữ liệu.

b) Quản lý truy cập mạng và tài nguyên trên Internet

- Nghiêm túc chấp hành các quy chế, quy trình nội bộ và các quy định khác của pháp luật về ATTT mạng. Chịu trách nhiệm bảo đảm an toàn thông tin mạng trong phạm vi trách nhiệm và quyền hạn được giao.

- Có trách nhiệm tự quản lý, bảo quản thiết bị, tài khoản, ứng dụng mà mình được giao sử dụng.

- Khi phát hiện nguy cơ hoặc sự cố mất an toàn thông tin mạng phải báo cáo ngay với cấp trên và bộ phận phụ trách công nghệ thông tin của bệnh viện để kịp thời ngăn chặn và xử lý.

- Tham gia các chương trình đào tạo, hướng dẫn về ATTT mạng được bệnh viện hoặc cơ quan có chuyên môn tổ chức.

## **Phần VI**

### **CHÍNH SÁCH QUẢN LÝ RỦI RO AN TOÀN THÔNG TIN**

#### **6.1. Xác định mức rủi ro**

- Nhận biết tài sản thông qua xác định và thu thập thông tin đầy đủ về tài sản của mình đang quản lý, đặc biệt là các thông tin liên quan đến đặc điểm, nơi lưu trữ, mức độ quan trọng và giá trị, đặc thù của tài sản. Đánh giá các nguy cơ, điểm yếu đối với tài sản đó, từ đó có thể đánh giá xem mỗi tài sản khi gặp rủi ro thì sẽ gây ra hậu quả, mức độ ảnh hưởng thế nào đối với bệnh viện.

- Phân loại nhóm các điểm yếu: Nhóm các điểm yếu liên quan đến tồn tại lỗ hổng, điểm yếu ATTT trong hệ thống; nhóm các điểm yếu liên quan đến thiếu hoặc không đáp ứng các biện pháp quản lý: không có quy định về sử dụng mật khẩu an toàn; không có quy định về lưu trữ có mã hóa, không có quy định về quy trình xử lý sự cố, không có quy định về bảo đảm ATTT phía người sử dụng...; nhóm các điểm yếu liên quan đến thiếu hoặc không đáp ứng các biện pháp kỹ thuật: Không có biện pháp phòng chống xâm nhập, không có biện pháp phòng chống mã độc, không có biện pháp phòng chống tấn công...; nhóm các điểm yếu khác liên quan đến các nguy cơ mất ATTT từ bên thứ ba.

- Phân loại các mối đe dọa: Nhóm các mối đe dọa từ việc tồn tại, điểm yếu, lỗ hổng trong hệ thống; nhóm các mối đe dọa từ việc thiếu hoặc không đáp ứng các biện pháp quản lý; nhóm các mối đe dọa từ việc thiếu hoặc không đáp ứng các biện pháp kỹ thuật.

- Đánh giá hậu quả và khả năng xảy ra sự cố, xác định mức rủi ro bao gồm các mức thấp, trung bình, cao, rất cao, cực cao.

**6.2. Xây dựng quy trình đánh giá và quản lý rủi ro:** bao gồm 04 bước: (1) Thiết lập bối cảnh; (2) Đánh giá rủi ro; (3) Xử lý rủi ro; (4) Chấp nhận rủi ro và



02 quá trình cần thực hiện song song: Truyền thông và tư vấn rủi ro, Giám sát và soát xét rủi ro.

**6.3. Biện pháp kiểm soát rủi ro:** được thực hiện theo yêu cầu an toàn cơ bản trong Hồ sơ đề xuất cấp độ của Hệ thống thông tin được cấp có thẩm quyền phê duyệt.

## **Phần VII**

### **CHÍNH SÁCH QUẢN LÝ SỰ CỐ AN TOÀN THÔNG TIN**

a) Phân nhóm sự cố an toàn thông tin mạng theo quy định tại Quyết định số 05/2017/QĐ-TTg của Thủ tướng Chính phủ ngày 16/3/2017 quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia; Xây dựng phương án tiếp nhận, phát hiện, phân loại và xử lý ban đầu sự cố an toàn thông tin mạng, ứng phó sự cố an toàn thông tin mạng.

b) Xây dựng quy trình ứng cứu sự cố an toàn thông tin mạng thông thường và nghiêm trọng theo quy định tại Điều 13,14 Quyết định số 05/2017/QĐ-TTg.

c) Xây dựng và triển khai kế hoạch ứng phó sự cố an toàn thông tin theo quy định tại Điều 16 Quyết định số 05/2017/QĐ-TTg.

d) Xây dựng và triển khai phương án giám sát, phát hiện và cảnh báo sự cố an toàn thông tin trong quy trình ứng cứu sự cố an toàn thông tin mạng nhằm khắc phục sự cố về ATTT; Hỗ trợ, phối hợp và hướng dẫn các cơ quan khắc phục sự cố mất ATTT; Yêu cầu ngưng hoạt động một phần hoặc toàn bộ các hệ thống thông tin của các cơ quan nhằm phục vụ công tác khắc phục sự cố về ATTT; Phối hợp với đơn vị chức năng trong điều tra các nguyên nhân gây ra sự cố mất an toàn thông tin theo chỉ đạo của Lãnh đạo.

e) Liên hệ, phối hợp với các cơ quan, tổ chức trong công tác hỗ trợ điều phối xử lý sự cố an toàn thông tin: Tùy theo mức độ sự cố, phối hợp Tổ ứng cứu sự cố an toàn thông tin của huyện hoặc Đội ứng cứu sự cố an toàn thông tin mạng tỉnh và các đơn vị có liên quan hướng dẫn xử lý, ứng cứu các sự cố an toàn thông tin mạng.

### **Phần VIII**

#### **TIÊU CHUẨN ATTT CHO CÁC SẢN PHẨM PHẦN MỀM**

a) Tùy theo đề xuất cấp độ của hệ thống thông tin được áp dụng các tiêu chuẩn theo Quyết định số 742/QĐ-BTTTT ngày 22/4/2022 của Bộ Thông tin Truyền thông ban hành an toàn cơ bản đối với phần mềm nội bộ.

b) Có biên bản, hợp đồng và các cam kết đối với bên thuê khoán các nội dung liên quan đến việc phát triển phần mềm thuê khoán; yêu cầu các nhà phát triển cung cấp mã nguồn phần mềm cho bệnh viện.

### **Phần IX**

#### **TIÊU CHUẨN AN TOÀN THÔNG TIN CHO HỆ THỐNG CAMERA**

Áp dụng các tiêu chí theo Quyết định số 724/QĐ-BTTTT ngày 07/5/2024 của Bộ Thông tin Truyền thông ban hành bộ tiêu chí về yêu cầu an toàn thông tin cơ bản cho camera giám sát.

### **Phần X**

#### **TIÊU CHUẨN AN TOÀN THÔNG TIN CHO THIẾT BỊ IOT**

Áp dụng các tiêu chí theo Quyết định số 736/QĐ-BTTTT ngày 31/5/2021 của Bộ Thông tin Truyền thông ban hành danh mục yêu cầu cơ bản bảo đảm ATTT mạng cho thiết bị IOT tiêu dùng.

### **Phần XI**

#### **TIÊU CHUẨN AN TOÀN THÔNG TIN CHO THIẾT BỊ ÂM THANH SỬ DỤNG MẠNG IP**

Áp dụng một số tiêu chí trong Thông tư số 39/2020/TT-TT-BTTTT ngày 24/11/2020 của Bộ Thông tin Truyền thông quy định về quản lý đài truyền thanh cấp xã ứng dụng công nghệ thông tin - viễn thông.



Số: 04 / QĐ-ĐNEMR

Đồng Nai, ngày 01 tháng 10 năm 2025

**QUYẾT ĐỊNH**  
**Về việc ban hành quy chế Bảo mật thông tin**  
**và Quyền riêng tư của người bệnh**

**GIÁM ĐỐC BỆNH VIỆN MẮT HÀ NỘI – ĐỒNG NAI**

*Căn cứ Luật Công nghệ thông tin 67/2006/QH11 ngày 29/06/2006;*  
*Căn cứ Luật Khám bệnh, chữa bệnh 15/2023/QH15 ngày 09/01/2023;*  
*Căn cứ Nghị định số 13/2023/NĐ-CP ngày 17/04/2023 của Chính phủ về bảo vệ dữ liệu cá nhân;*  
*Căn cứ Luật giao dịch điện tử số 20/2023/QH15 ngày 22/06/2023 ;*  
*Căn cứ Luật căn cước số 26/2023/QH15 ngày 27/11/2023;*  
*Căn cứ Nghị định số 137/2024/NĐ-CP ngày 23/10/2024 của Chính Phủ Quy định về giao dịch điện tử của cơ quan nhà nước và hệ thống thông tin phục vụ giao dịch điện tử;*  
*Căn cứ Thông tư số 54/2017/TT-BYT ngày 29/12/2017 của Bộ Y tế ban hành Bộ tiêu chí ứng dụng công nghệ thông tin tại các cơ sở khám chữa bệnh;*  
*Căn cứ Thông tư 13/2025/TT-BYT ngày 06 tháng 06 năm 2025 của Bộ y tế Vv Hướng dẫn triển khai hồ sơ bệnh án điện tử;*  
*Căn cứ Văn bản số 365/TTYTQG-GPQLCL ngày 06 tháng 06 năm 2025 của Trung tâm thông tin y tế Quốc Gia về Hướng dẫn yêu cầu kỹ thuật triển khai phần mềm hồ sơ bệnh án điện tử;*  
*Xét đề nghị của Trưởng phòng Kế hoạch Tổng hợp,*

**QUYẾT ĐỊNH:**

**Điều 1.** Ban hành kèm theo Quyết định này Quy chế Bảo mật thông tin và Quyền riêng tư của người bệnh tại Bệnh viện Mắt Hà Nội – Đồng Nai.

**Điều 2.** Quy chế này áp dụng thống nhất toàn Bệnh viện Mắt Hà Nội – Đồng Nai.

**Điều 3.** Quyết định này có hiệu lực kể từ ngày ký.

**Điều 4.** Trưởng các đơn vị trực thuộc, các cá nhân có liên quan đến công tác khám chữa bệnh của Bệnh viện Mắt Hà Nội – Đồng Nai chịu trách nhiệm thi hành Quyết định này./.

**Nơi nhận:**

- Như Điều 4;
- GĐ và các PGĐ TTYT;
- Lưu: VT, KHN.V.



**GIÁM ĐỐC**

**GIÁM ĐỐC**  
**BS CKI. Hoàng Vĩnh Hà**

## QUY CHẾ

### **Bảo mật thông tin và Quyền riêng tư của người bệnh**

*(Ban hành kèm theo Quyết định số: 04 /QĐ-ĐNEMR, ngày 01 tháng 10 năm 2025  
của Bệnh viện Mắt Hà Nội – Đồng Nai)*

## CHƯƠNG I QUY ĐỊNH CHUNG

### **Điều 1: Phạm vi điều chỉnh**

Quy chế này quy định về Bảo mật thông tin và quyền riêng tư của người bệnh có bệnh án điện tử tại Bệnh viện Mắt Hà Nội – Đồng Nai.

### **Điều 2: Đối tượng áp dụng**

Toàn thể cán bộ, nhân viên Bệnh viện Mắt Hà Nội – Đồng Nai có sử dụng bệnh án điện tử trong khám, chữa bệnh cho người bệnh.

## CHƯƠNG II BẢO MẬT THÔNG TIN VÀ QUYỀN RIÊNG TƯ CỦA NGƯỜI BỆNH

### **Điều 3. Bệnh viện thực hiện bảo mật hồ sơ bệnh án điện tử như sau**

1. Kiểm soát truy cập của người dùng gồm xác thực người dùng, phân quyền người dùng theo từng vai trò công việc, thiết lập khoảng thời gian giới hạn cho phép người dùng truy cập vào phần mềm;
2. Bảo vệ, ngăn chặn việc truy cập trái phép vào hồ sơ bệnh án điện tử;
3. Có phương án hoặc quy trình phục hồi dữ liệu trong trường hợp có sự cố;
4. Có phương án phòng ngừa, phát hiện, ngăn chặn và loại bỏ phần mềm độc hại.

### **Điều 4: Việc truy cập, chia sẻ thông tin trong hồ sơ bệnh án điện tử**

Các cơ quan, tổ chức, cá nhân có quyền tiếp cận, tham khảo dữ liệu hồ sơ bệnh án điện tử theo các phạm vi như sau:

1. Các tổ chức, cá nhân sau được truy cập, tham khảo tại chỗ hồ sơ bệnh án điện tử sau khi có sự cho phép của Giám đốc Bệnh viện.
  - a) Sinh viên thực tập, nghiên cứu viên, người hành nghề trong cơ sở khám bệnh, chữa bệnh được mượn hồ sơ bệnh án tại chỗ để đọc hoặc sao chép phục vụ cho việc nghiên cứu hoặc công tác chuyên môn kỹ thuật;



b) Đại diện cơ quan quản lý nhà nước về y tế trực tiếp quản lý cơ sở khám bệnh, chữa bệnh, cơ quan điều tra, viện kiểm sát, tòa án, thanh tra chuyên ngành y tế, cơ quan bảo hiểm, tổ chức giám định pháp y, pháp y tâm thần, luật sư được mượn hồ sơ bệnh án tại chỗ để đọc hoặc sao chép phục vụ nhiệm vụ được giao theo thẩm quyền cho phép;

c) Người bệnh hoặc người đại diện của người bệnh được nhận bản tóm tắt hồ sơ bệnh án theo quy định tại khoản 1 Điều 12 của Luật Khám bệnh, chữa bệnh.

2. Các tổ chức, cá nhân khi truy cập, tham khảo các bệnh án điện tử phải giữ bí mật và chỉ được sử dụng đúng mục đích như đã đề nghị với người đứng đầu cơ sở khám bệnh, chữa bệnh.

### **Điều 5. Liên thông, trao đổi dữ liệu hồ sơ bệnh án điện tử giữa các cơ sở khám bệnh, chữa bệnh.**

Tập đoàn bưu chính Viễn thông Việt Nam bảo đảm việc lưu trữ hồ sơ bệnh án điện tử của Bệnh viện Mắt Hà Nội – Đồng Nai tại Trung tâm hạ tầng IDC- Chi nhánh Công ty Công nghệ thông tin VNPT (IDC Nam Thăng Long –Hà Nội) và lưu trữ dự phòng (cloud) tại Trung tâm hạ tầng IDC- Chi nhánh Công ty Công nghệ thông tin VNPT ( IDC Tân Thận- Thành phố Hồ chí Minh) đáp ứng tiêu chuẩn theo quy định của Bộ trưởng Bộ Khoa học và Công nghệ.

Các bệnh án điện tử đã được mã hóa sẽ được trao đổi dữ liệu của Bệnh viện Mắt Hà Nội – Đồng Nai với các cơ sở y tế khác theo yêu cầu chuyên môn và được Giám đốc Bệnh viện Mắt Hà Nội – Đồng Nai đồng ý. Dữ liệu được trao đổi ở dạng mã hóa theo đúng hướng dẫn của Bộ Y tế.

Dữ liệu Hồ sơ bệnh án điện tử phải kết nối số định danh cá nhân của công dân Việt Nam và người nước ngoài đã được cấp tài khoản định danh điện tử theo quy định pháp luật về căn cước ( Khoản 3, điều 1, TT13/TT-BYT).

Phần mềm có khả năng kết xuất được thông tin hồ sơ bệnh án điện tử theo chuẩn định dạng của Bộ y tế phục vụ liên thông dữ liệu, chia sẻ bệnh án điện tử.

### **Điều 6. Ghi vết các giao dịch, tương tác trên hồ sơ bệnh án điện tử:**

Khi bệnh án điện tử chưa được ký số, chưa được chuyển về Trung tâm dữ liệu: phần mềm bệnh án điện tử có khả năng ghi vết tất cả các giao dịch, tương tác của người dùng trên phần mềm hồ sơ bệnh án điện tử bao gồm ngày, thời gian khi xem, nhập mới, chỉnh sửa, hủy, khôi phục dữ liệu, thông tin trong hồ sơ bệnh án điện tử.

Khi bệnh án điện tử đã được ký số, đã được lưu tại server tại Trung tâm hạ tầng IDC- Chi nhánh Công ty Công nghệ thông tin VNPT (IDC Nam Thăng Long –Hà Nội) và lưu trữ dự phòng (cloud) tại Trung tâm hạ tầng IDC- Chi nhánh Công ty Công nghệ thông tin VNPT ( IDC Tân Thận- Thành phố Hồ chí Minh): phần mềm khóa toàn bộ và không cho phép bất cứ thay đổi nào thực hiện trên các bệnh án điện tử.



### **CHƯƠNG III**

## **NỘI DUNG BẢO MẬT THÔNG TIN VÀ QUYỀN RIÊNG TƯ CỦA NGƯỜI BỆNH CÓ HỒ SƠ BỆNH ÁN ĐIỆN TỬ**

### **Điều 7. Nguyên tắc bảo vệ thông tin cá nhân trên mạng**

1. Cá nhân tự bảo vệ thông tin cá nhân của mình và tuân thủ quy định của pháp luật về cung cấp thông tin cá nhân khi sử dụng dịch vụ trên mạng.
2. Tổ chức, cá nhân xử lý thông tin cá nhân có trách nhiệm đảm bảo an toàn thông tin đối với thông tin do mình xử lý.
3. Tổ chức, cá nhân xử lý thông tin cá nhân phải xây dựng và công bố công khai biện pháp xử lý, bảo vệ thông tin cá nhân của Tổ chức, cá nhân mình.
4. Việc bảo vệ thông tin cá nhân thực hiện theo quy định của Luật an toàn thông tin mạng ngày 19/11/2015 và Nghị định 13/2023/NĐ-CP ngày 17/4/2023 của Chính phủ về Bảo vệ dữ liệu cá nhân.
5. Việc xử lý thông tin cá nhân phục vụ mục đích đảm bảo quốc phòng, an ninh quốc gia, trật tự, an toàn xã hội hoặc không nhằm mục đích thương mại được thực hiện theo quy định khác của pháp luật có liên quan.

### **Điều 8. Thu thập và sử dụng thông tin cá nhân**

1. Tổ chức, cá nhân xử lý thông tin cá nhân có trách nhiệm sau đây:
  - a) Tiến hành thu thập thông tin cá nhân sau khi có sự đồng ý của chủ thể thông tin cá nhân về phạm vi, mục đích của việc thu thập và sử dụng thông tin đó;
  - b) Chỉ sử dụng thông tin cá nhân đã thu thập vào mục đích khác mục đích ban đầu sau khi có sự đồng ý của chủ thể thông tin cá nhân;
  - c) Không được cung cấp, chia sẻ, phát tán thông tin cá nhân mà mình đã thu thập, tiếp cận, kiểm soát cho bên thứ ba, trừ trường hợp có sự đồng ý của chủ thể thông tin cá nhân đó theo yêu cầu của cơ quan Nhà nước có thẩm quyền.
2. Cơ quan Nhà nước chịu trách nhiệm bảo mật, lưu trữ thông tin cá nhân do mình thu thập.
3. Chủ thể thông tin cá nhân có quyền yêu cầu tổ chức, cá nhân xử lý thông tin cá nhân cung cấp thông tin cá nhân của mình mà tổ chức, cá nhân đó đã thu thập, lưu trữ.

### **Điều 9. Cập nhật, sửa đổi và huỷ bỏ thông tin cá nhân**

1. Chủ thể thông tin cá nhân có quyền yêu cầu tổ chức, cá nhân xử lý thông tin cá nhân cập nhật, sửa đổi, huỷ bỏ thông tin cá nhân của mình mà tổ chức, cá nhân đó đã thu thập, lưu trữ hoặc ngừng cung cấp thông tin cá nhân của mình cho bên thứ ba.
2. Ngay khi nhận được yêu cầu của chủ thể thông tin cá nhân về việc cập nhật, sửa đổi, huỷ bỏ thông tin cá nhân hoặc đề nghị ngừng cung cấp thông tin cá nhân cho bên thứ ba, tổ chức, cá nhân xử lý thông tin cá nhân có trách nhiệm sau đây:

a) Thực hiện yêu cầu và thông báo cho chủ thể thông tin cá nhân hoặc cung cấp cho chủ thể thông tin cá nhân quyền tiếp cận để tự cập nhật, sửa đổi, huỷ bỏ thông tin cá nhân của mình.

b) Áp dụng biện pháp phù hợp để bảo vệ thông tin cá nhân; thông báo cho chủ thể thông tin cá nhân đó trong trường hợp chưa thực hiện được yêu cầu do yếu tố kỹ thuật hoặc yếu tố khác.

3. Tổ chức, cá nhân xử lý thông tin cá nhân phải huỷ bỏ thông tin cá nhân đã được lưu trữ khi đã hoàn thành mục đích sử dụng hoặc hết thời hạn lưu trữ và thông báo cho chủ thể thông tin cá nhân biết, trừ trường hợp pháp luật có khác.

#### **Điều 10. Bảo đảm an toàn thông tin cá nhân trên mạng**

1. Tổ chức, cá nhân xử lý thông tin cá nhân phải áp dụng biện pháp quản lý, kỹ thuật phù hợp để bảo vệ thông tin cá nhân do mình thu thập, lưu trữ; tuân thủ các tiêu chuẩn, quy chuẩn kỹ thuật về bảo đảm an toàn thông tin mạng.

2. Thông tin khoản 1 Điều này chỉ được phép công bố khi người bệnh đồng ý hoặc để chia sẻ thông tin, kinh nghiệm nhằm nâng cao chất lượng chẩn đoán, chăm sóc, điều trị người bệnh giữa những người hành nghề trong nhóm trực tiếp điều trị cho người bệnh hoặc trong trường hợp khác được pháp luật quy định.

#### **Điều 12. Quyền được cung cấp thông tin về hồ sơ bệnh án và chi phí khám bệnh, chữa bệnh của người bệnh**

Theo Luật khám, chữa bệnh số 15/2023/QH15 ngày 09/01/2023, người bệnh được đọc, xem, sao chụp, ghi chép hồ sơ bệnh án và cung cấp tóm tắt hồ sơ bệnh án theo quy định của Luật này; được cung cấp và giải thích chi tiết về các khoản chi trả dịch vụ khám bệnh, chữa bệnh khi có yêu cầu.

### **CHƯƠNG IV TỔ CHỨC THỰC HIỆN**

#### **Điều 13. Trách nhiệm của Bệnh viện Mắt Hà Nội – Đồng Nai**

- Đầu tư đầy đủ các trang thiết bị phần cứng, phần mềm đảm bảo việc bảo mật thông tin và quyền riêng tư của người bệnh .

- Có trách nhiệm ký hợp đồng với cơ sở cung cấp Trung tâm dữ liệu đáp ứng đầy đủ các tiêu chuẩn của Bộ Khoa học và Công nghệ và các phương án đảm bảo an toàn dữ liệu theo khuyến nghị, hướng dẫn của Bộ y tế .

- Thực hiện tập huấn cho các nhân viên trong Bệnh viện các nội dung trong quy chế, và triển khai thực hiện theo các nội dung trong quy chế.

#### **Điều 14. Trách nhiệm cá nhân**

Cá nhân có trách nhiệm thực hiện đầy đủ các nội dung đã quy định trong quy chế.

#### **Điều 15. Trách nhiệm của Công nghệ thông tin**



Chịu trách nhiệm triển khai các giải pháp bảo đảm bảo mật thông tin bệnh án và quyền riêng tư của người bệnh.

- Hỗ trợ các nhân sự của Bệnh viện khi gặp các sự cố trong khi triển khai các nội dung theo quy chế.

- Tham mưu, giúp ban Giám đốc kiểm tra, giám sát và đôn đốc việc triển khai các giải pháp bảo đảm bảo mật và quyền riêng tư của người bệnh khi triển khai bệnh án điện tử tại Bệnh viện.

#### **Điều 16. Điều khoản thi hành**

Trong quá trình thực hiện nếu có khó khăn, vướng mắc cần sửa đổi, bổ sung, các Khoa, Phòng của Bệnh viện và các cá nhân phản ánh trực tiếp về phòng Phòng Kế hoạch Tổng hợp để được hướng dẫn cụ thể./.



**GIÁM ĐỐC**

**GIÁM ĐỐC**  
*BS CKI. Hoàng Vinh Hà*

Số: 05 /QĐ-ĐNEMR

Đồng Nai, ngày 01 tháng 10 năm 2025

### QUYẾT ĐỊNH

V/v: Ban hành Quy chế quản lý, sử dụng chứng thư số, chữ ký điện tử,  
chữ ký số và sinh trắc học (dấu vân tay)  
tại Bệnh viện Mắt Hà Nội – Đồng Nai

### GIÁM ĐỐC BỆNH VIỆN MẮT HÀ NỘI – ĐỒNG NAI

*Căn cứ Luật Khám bệnh, chữa bệnh ngày 09 tháng 01 năm 2023;*

*Căn cứ Luật An toàn thông tin mạng ngày 19 tháng 11 năm 2015;*

*Căn cứ Luật giao dịch điện tử ngày 22 tháng 06 năm 2023;*

*Căn cứ Nghị định 23/2025/NĐ-CP ngày 21/02/2025 của Chính phủ quy định về chữ ký điện tử và dịch vụ đáng tin cậy;*

*Căn cứ Thông tư 13/2025/TT-BYT ngày 06/06/2025 của Bộ y tế Về Hướng dẫn triển khai hồ sơ bệnh án điện tử;*

*Căn cứ hướng dẫn tại Công văn số 365/TTYTQG-GPQLCL ngày 06/06/2025 của Trung tâm thông tin y tế Quốc Gia về Hướng dẫn yêu cầu kỹ thuật triển khai phần mềm hồ sơ bệnh án điện tử;*

*Xét đề nghị của Trưởng phòng Kế hoạch Tổng hợp,*

### QUYẾT ĐỊNH:

**Điều 1.** Ban hành kèm theo Quyết định này “Quy chế quản lý, sử dụng chứng thư số, chữ ký, chữ ký điện tử và sinh trắc học (dấu vân tay) tại Bệnh viện Mắt Hà Nội – Đồng Nai”.

**Điều 2.** Quyết định này có hiệu lực thi hành kể từ ngày ký.

**Điều 3.** Ban giám đốc, Trưởng các đơn vị trực thuộc Bệnh viện và các cá nhân có liên quan đến công tác khám chữa bệnh của Bệnh viện Mắt Hà Nội – Đồng Nai chịu trách nhiệm thi hành Quyết định này./.

#### Nơi nhận:

- Sở Y tế (để b/c);
- Như Điều 3;
- Lưu: VT, KHN.V.



**GIÁM ĐỐC**  
BS CKI. Hoàng Vinh Hà



## QUY CHẾ

### Quản lý, sử dụng chứng thư số, chữ ký số, chữ ký điện tử và sinh trắc học (dấu vân tay) tại Bệnh viện Mắt Hà Nội – Đồng Nai

(Ban hành kèm theo Quyết định số: 05 /QĐ-ĐNEMR, ngày 01 tháng 10 năm 2025  
của Bệnh viện Mắt Hà Nội – Đồng Nai)

## CHƯƠNG I QUY ĐỊNH CHUNG

### Điều 1. Phạm vi điều chỉnh

Quy chế này quy định về việc quản lý, sử dụng chứng thư số, chữ ký số, chữ ký điện tử và sinh trắc học (dấu vân tay) trong việc trao đổi sử dụng văn bản điện tử, Hồ sơ bệnh án điện tử tại Bệnh viện Mắt Hà Nội – Đồng Nai.

### Điều 2. Đối tượng áp dụng

Quy chế này áp dụng cho toàn thể cán bộ, nhân viên (CBNV) trong Bệnh viện Mắt Hà Nội – Đồng Nai và cơ quan, đơn vị, cá nhân liên quan tham gia khai thác, sử dụng chứng thư số, chữ ký số, chữ ký điện tử và sử dụng sinh trắc học (dấu vân tay) đã được cấp, bàn giao chữ ký số và tài khoản đăng nhập trên hệ thống phần mềm tại Bệnh viện Mắt Hà Nội – Đồng Nai.

Quy chế này được áp dụng đối với người bệnh, người đại diện cho người bệnh đến khám và chữa bệnh tại Bệnh viện Mắt Hà Nội – Đồng Nai sử dụng sinh trắc học (dấu vân tay) trong hồ sơ bệnh án điện tử.

### Điều 3. Giải thích từ ngữ

Trong Quy chế này, các từ ngữ dưới đây được hiểu như sau:

1. **Chứng thư số:** là một dạng chứng thư điện tử do tổ chức cung cấp dịch vụ chứng thực chữ ký số chuyên dùng phục vụ các cơ quan Đảng, Nhà nước, tổ chức chính trị - xã hội cấp.

2. **Chữ ký điện tử:** là dạng chữ ký được tạo lập dưới dạng từ, chữ, số, ký hiệu, âm thanh hoặc các hình thức khác bằng phương tiện điện tử, gắn liền hoặc kết hợp một cách logic với thông điệp dữ liệu, có khả năng xác nhận người ký thông điệp dữ liệu và xác nhận sự chấp thuận của người đó đối với nội dung thông điệp dữ liệu được ký (theo Luật Giao dịch điện tử).

3. **Chữ ký số:** là một dạng chữ ký số điện tử được tạo ra bằng việc biến đổi một thông điệp dữ liệu sử dụng hệ thống mật mã không đối xứng theo người đó có được thông điệp dữ liệu ban đầu và khóa công khai có thể xác định được chính xác:

a) Việc biến đổi nêu trên được tạo ra bằng đúng khóa bí mật tương ứng với khóa công khai trong cùng một cặp khóa;

b) Sự toàn vẹn nội dung của thông điệp dữ liệu kể từ khi thực hiện việc biến đổi nêu trên.

(Theo nghị định 130/2018/NĐ-CP ngày 27/08/2024 quy định chi tiết thi hành Luật giao dịch điện tử về chữ ký số và dịch vụ chứng thực chữ ký số của Chính phủ).

#### **4. Mục đích sử dụng chữ ký số, chữ ký điện tử:**

- Chữ ký số là chứng thư số được cấp cho cá nhân, được sử dụng để ký văn bản điện tử thay cho chữ ký tay, được chứng thực bởi các cơ quan quản lý nhà nước;

- Chữ ký điện tử là số hóa chữ ký thực tế của người dùng dưới định dạng hình ảnh và không được chứng thực bởi các cơ quan quản lý nhà nước.

5. **Thuê bao:** là tổ chức, cá nhân được cấp chứng thư số, chấp nhận chứng thư số và giữ khóa bí mật tương ứng với khóa công khai ghi trên chứng thư số được cấp.

6. **Thiết bị lưu khóa bí mật:** là thiết bị vật lý chứa chứng thư số và khóa bí mật tương ứng với khóa công khai ghi trên chứng thư số của thuê bao.

7. **Chữ ký số chuyên dùng:** là chữ ký số được cấp bởi Ban cơ yếu chính phủ.

8. **Văn bản điện tử được ký số:** là văn bản điện tử có gắn kèm theo các chữ ký số của chính văn bản đó.

9. **Bệnh án điện tử được ký số:** là các chỉ định, các kết quả cận lâm sàng, các tờ điều trị, các biểu chăm sóc, chức năng sống, ... theo đúng yêu cầu tại điều 3 của Thông tư số 13/2025/TT-BYT ngày 06/06/2025 quy định về ký, xác nhận điện tử trong hồ sơ bệnh án điện tử.

10. **Chứng thư số cá nhân:** là một chứng thư số được cấp cho cá nhân, được tạo lập bởi khóa bí mật trên phần mềm ký số, được sử dụng để ký văn bản điện tử thay cho chữ ký tay, được chứng thực bởi các cơ quan quản lý nhà nước.

11. **Chứng thư số của tổ chức:** là một chứng thư số được cấp cho tổ chức, được tạo lập bởi khóa bí mật trên phần mềm ký số, được sử dụng để ký văn bản điện tử thay cho con dấu của tổ chức đó (con dấu điện tử).

12. **Chữ ký số hợp lệ:** là chữ ký số được Hệ thống thống chứng thực do Cục Chứng thực số và Bảo mật thông tin cung cấp xác thực đảm bảo tính hợp lệ của các yếu tố sau: Người ký, loại chứng thư số, hiệu lực của chứng thư số, thời gian ký, tính toàn vẹn của nội dung sau khi ký.

13. **Công nghệ sinh trắc học (quét dấu vân tay):** là một công nghệ bảo mật sử dụng dấu vân tay của một người để xác định danh tính của người đó.

### **Điều 3: Nguyên tắc chung**

1. Chữ ký số được sử dụng rộng rãi cho tất cả các loại văn bản điện tử, hồ sơ bệnh án điện tử trong Bệnh viện cũng như trong cơ quan nhà nước; không áp dụng



đổi với các văn bản mật, tuyệt mật, tối mật và các văn bản khác theo quy định của pháp luật.

2. Việc áp dụng chữ ký số, chữ ký điện tử được thực hiện từng bước theo lộ trình thích hợp để đạt hiệu quả tốt nhất trong các giao dịch điện tử, bệnh án điện tử.

3. Triển khai sử dụng chữ ký số phù hợp với thực tiễn, không làm ngưng trệ công tác văn thư lưu trữ, hành chính, công tác khám chữa bệnh khi thực hiện áp dụng chữ ký số.

4. Việc quản lý, sử dụng chữ số, chữ ký điện tử, sinh trắc học (dấu vân tay) phải đảm bảo an toàn, an ninh thông tin trong mọi hoạt động của Bệnh viện.

#### **Điều 4. Nguyên tắc định dạng văn bản, gửi, nhận và giá trị pháp lý của văn bản điện tử, bệnh án điện tử**

1. Thể thức và kỹ thuật trình bày văn bản điện tử được thực hiện theo quy định tại Thông tư số 01/2019/TT-BNV ngày 24/1/2019 của Bộ Nội vụ về quy định quy trình trao đổi, lưu trữ xử lý tài liệu điện tử trong công tác văn thư, các chức năng cơ bản của hệ thống quản lý tài liệu điện tử trong quá trình xử lý công việc của các cơ quan tổ chức; Nguyên tắc quản lý, triển khai hồ sơ bệnh án điện tử đáp ứng theo quy định tại điều 1 thông tư 13/2025/TT-BYT ngày 06/06/2025 của Bộ y tế về Hướng dẫn triển khai hồ sơ bệnh án điện tử;

2. Văn bản điện tử, bệnh án điện tử được ký số với loại chữ ký số của cá nhân đã được xác thực hợp lệ thì có giá trị tương đương với văn bản có chữ ký tay của cá nhân đó.

3. Văn bản điện tử, bệnh án điện tử được ký số với loại chữ ký số của Bệnh viện Mắt Hà Nội – Đồng Nai đã được xác thực hợp lệ thì có giá trị tương đương với văn bản giấy có đóng dấu của Bệnh viện Mắt Hà Nội – Đồng Nai.

4. Bệnh án điện tử được ký số với loại chữ ký số của cá nhân là Lãnh đạo hoặc người được lãnh đạo ủy quyền, chữ ký số hoặc chữ ký điện tử của cán bộ, nhân viên Bệnh viện được cấp phát theo quy định, xác nhận dấu vân tay của người bệnh hoặc đại diện người bệnh đã được xác thực hợp lệ, thì có giá trị tương đương như bệnh án giấy có chữ ký tay và đóng dấu.

5. Văn bản điện tử, bệnh án điện tử sau khi áp dụng chữ ký số hợp lệ tại Khoản 2, Khoản 3, Khoản 4, Khoản 5 điều này được ban hành, phát hành, lưu trữ qua hệ thống thông tin chung của Bộ Y tế, Tỉnh Đồng Nai, Sở Y tế Đồng Nai, Bệnh viện Mắt Hà Nội – Đồng Nai và các cơ quan quản lý khác theo quy định.

#### **Điều 5. Các hành vi bị nghiêm cấm**

1. Cản trở các tổ chức, cá nhân thuộc quản lý của Bệnh viện sử dụng chữ ký số, chữ ký điện tử.

2. Cản trở hoặc ngăn chặn trái phép quá trình truyền, gửi, nhận, lưu trữ văn bản điện tử, bệnh án điện tử đã được ký số.

3. Tạo ra hoặc phát tán chương trình phần mềm làm rối loạn, thay đổi, phá

hoại hệ thống điều hành hoặc có hành vi khác nhằm phá hoại hạ tầng công nghệ về giao dịch điện tử tại Bệnh viện Mắt Hà Nội – Đồng Nai.

4. Trực tiếp hoặc gián tiếp phá hoại hoặc cản trở hệ thống cung cấp dịch vụ chứng thực chữ ký số của tổ chức cung cấp dịch vụ chứng thực chữ ký số, trực tiếp hoặc gián tiếp làm giả chứng thư số.

5. Trộm cắp, gian lận, làm giả, chiếm đoạt hoặc sử dụng trái phép chữ ký số của cá nhân, của tổ chức thuộc Bệnh viện.

6. Sử dụng chữ ký số gây mất an ninh, trật tự, an toàn xã hội hoặc các hoạt động khác trái với quy định của pháp luật.

7. Trộm cắp, gian lận, chiếm đoạt hoặc sử dụng trái phép thiết bị lưu khóa bí mật của tổ chức, cá nhân thuộc Bệnh viện Mắt Hà Nội – Đồng Nai.

## **CHƯƠNG II**

### **QUẢN LÝ, SỬ DỤNG CHỨNG THƯ SỐ, CHỮ KÝ SỐ, CHỮ KÝ ĐIỆN TỬ VÀ SINH TRẮC HỌC (DẤU VÂN TAY)**

#### **Điều 6. Người quản lý thuê bao**

Giám đốc Bệnh viện chịu trách nhiệm chỉ đạo việc quản lý, khai thác sử dụng chứng thư số, chữ ký số, chữ ký điện tử, sinh trắc học (dấu vân tay) cấp cho các tổ chức, cá nhân là cán bộ nhân viên thuộc Bệnh viện Mắt Hà Nội – Đồng Nai.

#### **Điều 7. Các loại văn bản bắt buộc áp dụng chữ ký số tại Bệnh viện**

1. Các văn bản điện tử phù hợp với các quy định tại Khoản 1 điều này được trao đổi trên các hệ thống thông tin của Bệnh viện được xem là thông tin chính thức và có giá trị pháp lý như văn bản giấy; Các cơ quan, đơn vị không cần gửi bản giấy khi phát hành văn bản.

2. Hồ sơ bệnh án điện tử áp dụng chữ ký số, chữ ký điện tử, sinh trắc học (dấu vân tay) được quy định tại Điều 3 của Thông tư 13/2025/TT-BYT ngày 06/06/2025 của Bộ y tế Vv Hướng dẫn triển khai hồ sơ bệnh án điện tử (có phụ lục 02 đính kèm); Các biểu mẫu trong bệnh án điện tử bắt buộc ký tại Quyết định số 1895/1997/QĐ-BYT ngày 19/9/1997 của Bộ Y tế về việc Ban hành Quy chế Bệnh viện.

#### **Điều 8. Quy trình ký số trên văn bản điện tử và bệnh án điện tử**

##### **1. Quy trình ký số trên văn bản điện tử:**

Thực hiện theo Thông tư 01/2019/TT-BNV ngày 24/01/2019 của Bộ Nội vụ về hướng dẫn quản lý văn bản điện tử, cụ thể như sau:

- ✓ *Hình thức chữ ký của người có thẩm quyền ký ban hành văn bản*

- Vị trí ký số: Tại vị trí của người có thẩm quyền ký ban hành văn bản trên văn bản giấy;

- Hình ảnh: Chữ ký của người có thẩm quyền trên văn bản giấy, màu xanh,



định dạng (.png).

✓ *Hình thức chữ ký của cơ quan, tổ chức ban hành văn bản*

- Vị trí ký: Trùm lên khoảng 1/3 chữ ký của người có thẩm quyền về phía bên trái;

- Hình ảnh: Dấu của cơ quan tổ chức, ban hành văn bản, màu đỏ, kích thước bằng kích thước thực tế của con dấu, định dạng (.png);

- Thông tin: Tên cơ quan, tổ chức, thời gian ký (ngày, tháng, năm, giờ, phút, giây, múi giờ Việt Nam theo tiêu chuẩn ISO 8601);

**Bước 1:** Lãnh đạo sử dụng chứng thư số của cá nhân mình để ký số trên văn bản chuyên viên (Trưởng khoa/phòng, đơn vị) trình phát hành (*theo hình thức chữ ký của người có thẩm quyền ký ban hành văn bản*);

**Bước 2:** Chuyển Văn thư phát hành văn bản (*Qua hệ thống quản lý văn bản điện tử của tỉnh*);

**Bước 3:** Văn thư sử dụng chức năng “Chờ phát hành” chọn văn bản cần phát hành; Văn thư kiểm tra lại cập nhật đầy đủ thông tin Số ký hiệu, ngày tháng phát hành, Người ký văn bản, đơn vị soạn thảo; Sau đó ấn nút “Ký CA” và dùng chứng thư số của Bệnh viện để ký lên văn bản điện tử đính kèm sau đó ấn phát hành văn bản;

## ***2. Quy trình ký số trên Hồ sơ bệnh án điện tử***

**Bước 1:** Nhân viên Y tế (Trưởng khoa, phó khoa, bác sĩ điều trị, kỹ thuật viên, điều dưỡng, ...) sử dụng chữ ký số, chữ ký điện tử để ký hồ sơ bệnh án điện tử;

Người bệnh hoặc đại diện người bệnh sử dụng sinh trắc học (dấu vân tay) để ký trong hồ sơ bệnh án điện tử;

Sau khi hoàn thành các khoa chuyển về Phòng Kế hoạch Tổng hợp.

**Bước 2:** Phòng Kế hoạch Tổng hợp rà soát kiểm tra bệnh án điện tử:

+ Nếu Hồ sơ bệnh án điện tử đạt yêu cầu thì nhân viên phòng Kế hoạch Tổng hợp hoặc Trưởng phòng Kế hoạch Tổng hợp chuyển Giám đốc hoặc người được Giám đốc ủy quyền (Phó giám đốc; Trưởng phòng Kế hoạch Tổng hợp, Trưởng khoa, ...) ký số xác thực bệnh án điện tử và chuyển lưu trữ Kế hoạch Tổng hợp;

+ Nếu Hồ sơ bệnh án điện tử chưa đạt yêu cầu, nhân viên phòng Kế hoạch Tổng hợp trả lại các khoa phòng để bổ sung hoàn thiện (*Sau khi bổ sung hoàn thiện xong các khoa gửi lại Tổ kiểm soát bệnh án để kiểm tra*).

\* *Hình thức ký số trong hồ sơ bệnh án điện tử đối với Lãnh đạo Bệnh viện hoặc người được Lãnh đạo Bệnh viện phân công, ủy quyền:*

Giám đốc Bệnh viện hoặc Phó Giám đốc Bệnh viện, Trưởng phòng Kế hoạch tổng hợp, Trưởng các khoa lâm sàng được ủy quyền sử dụng chữ ký số để ký vào hồ sơ bệnh án điện tử sau khi tổng kết toàn bộ quá trình điều trị cho người bệnh và hoàn chỉnh hồ sơ bệnh án điện tử.

- Vị trí ký: tại vị trí dành cho Lãnh đạo Bệnh viện hoặc người được Lãnh đạo Bệnh viện phân công ủy quyền ký như trên bệnh án giấy;

*\* Hình thức ký số trong hồ sơ bệnh án điện tử đối với cán bộ nhân viên y tế:*

Nhân viên y tế (Trưởng khoa, phó khoa, bác sĩ điều trị, kỹ thuật viên, điều dưỡng, ...) sử dụng chữ ký số, chữ ký điện tử để ký hồ sơ bệnh án điện tử:

- Vị trí ký: tại vị trí dành cho cán bộ, nhân viên ký như trên bệnh án giấy;

- Hình ảnh: chữ ký điện tử, chữ ký số của người được giao ký trên bệnh án điện tử, màu xanh, định dạng (JPG).

*\* Hình thức ký số trong hồ sơ bệnh án điện tử đối với người bệnh hoặc người đại diện cho người bệnh:*

Đối với người bệnh hoặc người đại diện cho người bệnh sử dụng dấu vân tay để ký xác nhận trên hồ sơ bệnh án điện tử:

- Hình thức ký: ký bằng quét dấu vân tay;

- Vị trí ký: tại vị trí dành cho người bệnh ký như trên bệnh án giấy;

- Hình ảnh: dấu vân tay của người bệnh hoặc người đại diện cho người bệnh.

### **Điều 9. Xác thực chữ ký số**

Khi nhận được văn bản điện tử được ký từ số, hồ sơ bệnh án điện tử ký số thì văn thư hoặc cán bộ tiếp nhận văn bản, cán bộ quản lý hồ sơ Bệnh án điện tử thì phải thực hiện việc xác thực chữ ký như sau:

1. Kiểm tra tính hợp lệ của chữ ký số, bao gồm kiểm tra các yếu tố: Người ký, tính hợp lệ của chứng thư số, thời gian ký, tính toàn vẹn của nội dung. Khi các yếu tố kiểm tra trên đều hợp lệ thì chữ ký số là hợp lệ.

2. Nếu chữ ký số không hợp lệ thì thông báo lại với đơn vị gửi văn bản, bệnh án điện tử biết để ký và gửi lại, đồng thời xóa văn bản, bệnh án không hợp lệ đó.

3. Nếu văn bản điện tử, bệnh án điện tử được ký bởi chữ ký số hợp lệ thì tiếp nhận, xử lý, lưu trữ theo đúng quy định tại Thông tư 01/2019/TT-BNV về quản lý lưu trữ văn bản điện tử, Thông tư 13/2025/TT-BYT ngày 06/06/2025 về hồ sơ bệnh án điện tử.

4. Các văn bản điện tử có chữ ký số lấy từ các trang thông tin điện tử hoặc các nguồn khác phải được xác thực chữ ký số trước khi sử dụng.

### **Điều 10. Lưu trữ, khai thác sử dụng văn bản điện tử, bệnh án điện tử đã ký số**

1. Trường hợp nhận văn bản đến bằng văn bản điện tử có sử dụng chữ ký số, các cơ quan, tổ chức phải thực hiện ngay việc đưa văn bản đến vào hệ thống quản lý văn bản đi, đến (*hệ thống quản lý văn bản và điều hành*) của đơn vị mình, chuyển xử lý trong nội bộ cơ quan, tổ chức mà không cần thực hiện in văn bản ra giấy và đóng dấu đến.

2. Văn bản điện tử, bệnh án điện tử được ký số khi lưu trữ phải là dạng



nguyên bản, không bị thay đổi sai lệch theo quy định của pháp luật về giao dịch điện tử.

3. Văn bản điện tử, bệnh án điện tử được ký số phải được lưu trữ có tổ chức, khoa học bảo đảm cho việc tìm kiếm, tra cứu được dễ dàng, thuận tiện.

4. Sau khi gửi, nhận các văn bản điện tử, Bệnh án điện tử được ký số phải thực hiện lưu trữ trên hệ thống máy chủ, định kỳ hàng tháng sao lưu sang các thiết bị lưu trữ chuyên dùng để đảm bảo an toàn, an ninh thông tin.

5. Đối với hồ sơ Bệnh án điện tử được ký số việc lưu trữ và khai thác sử dụng thực hiện theo 1 Thông tư 13/2025/TT-BYT ngày 06/06/2025 của Bộ y tế về Hướng dẫn triển khai hồ sơ bệnh án điện tử; Quy chế khai thác sử dụng bệnh án điện tử tại Bệnh viện Mắt Hà Nội – Đồng Nai.

### **Điều 11. Đăng ký cấp mới, gia hạn, thay đổi thông tin, thu hồi, cấp lại chứng thư số**

1. Điều kiện, trình tự, thủ tục, thời gian thực hiện đăng ký mới, gia hạn, cấp lại, thay đổi thông tin chứng thư số được thực hiện theo các quy định tại các Điều 13, Điều 14, Điều 15, Điều 16, Điều 17, Điều 18, Điều 20, Điều 22, Điều 23 Thông tư 08/2016/TT-BQP ngày 01/02/2016 của Bộ Quốc phòng quy định về cung cấp, quản lý, sử dụng dịch vụ chứng thực chữ ký số chuyên dùng phục vụ các cơ quan Đảng, Nhà nước, tổ chức chính trị - xã hội (sau đây gọi tắt là Thông tư số 08/2016/TT-BQP).

2. Phòng Kế hoạch Tổng hợp là đầu mối tiếp nhận đăng ký mới, gia hạn, cấp lại, thay đổi thông tin chứng thư số của các tổ chức, cá nhân thuộc Bệnh viện trình Giám đốc Bệnh viện xem xét trình các cấp có thẩm quyền cấp phát, hoặc đơn vị cung cấp dịch vụ chữ ký số cấp phát theo quy định.

### **Điều 12. Thu hồi, khôi phục thiết bị lưu khóa bí mật (USB Token)**

1. Điều kiện, trình tự, thủ tục, thời gian thực hiện thu hồi thiết bị lưu khóa bí mật sau khi chứng thư số hết hạn sử dụng hoặc chứng thư số bị thu hồi được thực hiện theo quy định tại Điều 21 Thông tư số 08/2016/TT-BQP.

2. Khôi phục thiết bị lưu khóa bí mật trong trường hợp thiết bị lưu khóa bí mật bị khóa do nhập sai mật khẩu quá số lần quy định (do Cục Chứng thực số và Bảo mật thông tin thiết lập) được thực hiện theo quy định tại Điều 24 Thông tư số 08/2016/TT-BQP.

### **Điều 13. Quản lý thiết bị lưu khóa bí mật**

1. Việc quản lý thiết bị lưu khóa bí mật được thực hiện theo các quy định tại Điều 25 Thông tư số 08/2016/TT-BQP.

2. Thiết bị USB Token của cơ quan, tổ chức được ủy quyền cho văn thư quản lý và sử dụng. Việc bảo quản, lưu giữ được thực hiện như với con dấu của đơn vị. Người được giao quản lý thiết bị lưu khóa bí mật của cơ quan, đơn vị chịu trách nhiệm trong việc quản lý và sử dụng thiết bị lưu khóa để tạo ra chữ ký số của cơ quan, đơn vị mình. Khi thay đổi người quản lý thiết bị lưu khóa bí mật phải lập



Biên bản bàn giao. Biên bản bàn giao thiết bị lưu khóa bí mật được lập theo Mẫu 13 của Phụ lục kèm theo Thông tư số 08/2016/TT-BQP.

3. Thiết bị lưu khóa của cá nhân do chính cá nhân đó bảo quản, lưu giữ và sử dụng và chịu hoàn toàn trách nhiệm về thiết bị lưu khóa, chữ ký số của mình trước Giám đốc Bệnh viện, trước pháp luật theo đúng quy định. Trong quá trình sử dụng tuyệt đối không được tiết lộ mật khẩu, hoặc để người khác sử dụng thiết bị của mình để ký số trên các văn bản điện tử.

### **CHƯƠNG III**

#### **TỔ CHỨC THỰC HIỆN**

#### **Điều 14. Trách nhiệm của lãnh đạo Bệnh viện, Lãnh đạo các Khoa, Phòng, Đơn vị**

1. Tổ chức khai thác, sử dụng có hiệu quả chứng thư số của Bệnh viện, và các chứng thư số cá nhân, dịch vụ, thiết bị phần mềm thuộc thẩm quyền quản lý theo quy định; thực hiện việc áp dụng chữ ký số trong việc gửi nhận văn bản điện tử giữa các cơ quan, đơn vị, nội bộ Bệnh viện và Hồ sơ bệnh án điện tử đúng lộ trình theo chỉ đạo của Giám đốc Bệnh viện.

2. Có trách nhiệm phân công và cử cán bộ phòng tiếp nhận chứng thư số, tiếp nhận chuyển giao cài đặt phần mềm ký số và đào tạo hướng dẫn sử dụng ký số tại Bệnh viện.

3. Đối với chứng thư số cấp cho tổ chức Bệnh viện, phải có biên bản giao thiết bị lưu khóa bí mật cho người được phân công làm nhiệm vụ Văn thư khai thác sử dụng để ký số các văn bản điện tử, bệnh án điện tử; đảm bảo an toàn việc sử dụng thiết bị lưu khóa bí mật tại Bệnh viện.

4. Thường xuyên kiểm tra việc quản lý và sử dụng chữ ký số, chứng thư số của cơ quan, tổ chức mình và các cá nhân đảm bảo thực hiện theo đúng các quy định của Quy chế này và các quy định khác có liên quan.

5. Trang bị hệ thống thông tin đáp ứng yêu cầu để thực hiện ký số, lưu trữ văn bản điện tử, Bệnh án điện tử, phục vụ khai thác và sử dụng văn bản điện tử, Bệnh án điện tử theo quy định.

6. Thực hiện báo cáo kết quả sử dụng chữ ký số, chứng thư số của các cá nhân thuộc các phòng, khoa, đơn vị trong Bệnh viện theo yêu cầu của Lãnh đạo Bệnh viện và các đơn vị cấp trên.

#### **Điều 15: Trách nhiệm của Phòng Kế hoạch Tổng hợp, Phòng Tổ chức – Hành chính.**

1. Chủ trì, hướng dẫn, triển khai thực hiện Quy chế này và các quy định hiện hành của Nhà nước có liên quan đến công tác quản lý, sử dụng chứng thư số, chữ ký số trong Bệnh viện Mắt Hà Nội – Đồng Nai.

2. Phòng Tổ chức - Hành chính phối hợp với Sở Y tế, Sở Thông tin và truyền thông tỉnh Đồng Nai, và đơn vị cung cấp dịch vụ chữ ký số, xây dựng kế hoạch đào tạo, tập huấn hướng dẫn quản lý và sử dụng chữ ký số, chứng thư



số, chữ ký điện tử cho nhân viên trong Bệnh viện;

3. Thường xuyên đôn đốc, kiểm tra việc sử dụng chữ ký số, chứng thư số, thiết bị lưu khóa bí mật và việc thực hiện các quy định trong Quy chế này của các cá nhân trong phạm vi thẩm quyền quản lý tại Bệnh viện.

4. Hằng năm, chủ trì, phối hợp với các khoa phòng và các đơn vị liên quan rà soát, tổng hợp nhu cầu xây dựng kế hoạch, bổ sung và xin cấp mới chứng thư số để đáp ứng nhu cầu khai thác và sử dụng chữ ký số của Bệnh viện, trình Sở Y tế, Sở Thông tin và Truyền thông tỉnh Đồng Nai, Ban cơ yếu Chính phủ, Công ty cung cấp chữ ký số cấp phát.

5. Thống kê, theo dõi việc sử dụng chứng thư số trong Bệnh viện, thực hiện báo cáo định kỳ, đột xuất cho Ban Giám đốc Bệnh viện và các cơ quan liên quan.

**Điều 16. Trách nhiệm của các cá nhân được cấp chứng thư số, chữ ký số, chữ ký điện tử.**

1. Cung cấp chính xác và đầy đủ các thông tin, hồ sơ liên quan đến việc cấp, gia hạn, thu hồi chứng thư số, chữ ký số, chữ ký điện tử.

2. Thông báo kịp thời cho cơ quan quản lý trực tiếp thuê bao những thông tin liên quan đến thiết bị lưu khóa bí mật trong các trường hợp như: Bị mất, bị hỏng vật lý, bị khóa thiết bị do nhập sai mật khẩu theo quy định và các trường hợp mất an toàn, an ninh khác.

3. Tham gia các khóa đào tạo, tập huấn liên quan đến việc quản lý và sử dụng chữ ký số, chứng thư số trong Bệnh viện do Bệnh viện tổ chức.

4. Quản lý thiết bị lưu khóa bí mật theo quy định tại Điều 10 Quy chế này và tuân thủ các quy định của pháp luật về quản lý và sử dụng chữ ký số, chứng thư số.

5. Sử dụng chứng thư số đúng mục đích và tuân thủ các quy trình, quy định của Quy chế này và các văn bản pháp luật có liên quan về quản lý, sử dụng chữ ký số, chứng thư số và dịch vụ chứng thực chữ ký số.

6. Có trách nhiệm cung cấp thông tin theo quy định và khi có yêu cầu của cơ quan có thẩm quyền.

**Điều 17. Trách nhiệm của cán bộ làm công tác Văn thư tại Bệnh viện**

1. Thực hiện ký số văn bản điện tử và phát hành văn bản điện tử đã ký số qua mạng theo các quy định trong Quy chế này và các quy định khác có liên quan.

2. Thực hiện lưu trữ văn bản điện tử theo quy định hiện hành.

3. Thực hiện xác thực chữ ký số trên các văn bản đến của các cơ quan, đơn vị khác gửi đến, phản ánh với cơ quan, đơn vị đó nếu chữ ký số không hợp lệ.

4. Chịu trách nhiệm tiếp nhận, quản ký và sử dụng chứng thư số, thiết bị lưu khóa bí mật của tổ chức (Bệnh viện) khi được phân công, đảm bảo đúng các quy định trong Quy chế này và các quy định khác có liên quan.

**Điều 18. Điều khoản thi hành**





SỞ Y TẾ ĐỒNG NAI  
BỆNH VIỆN MẮT  
HÀ NỘI – ĐỒNG NAI

Số: 06 /QĐ-ĐNEMR

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM  
Độc lập – Tự do – Hạnh phúc

Đồng Nai, ngày 01 tháng 10 năm 2025

### QUYẾT ĐỊNH

Về việc bàn giao sử dụng, quản lý chữ ký số, chữ ký điện tử cho nhân viên y tế sử dụng trên phần mềm Quản lý bệnh viện và hồ sơ bệnh án điện tử tại Bệnh viện Mắt Hà Nội – Đồng Nai

### GIÁM ĐỐC BỆNH VIỆN MẮT HÀ NỘI – ĐỒNG NAI

Căn cứ Luật Giao dịch điện tử số: 20/2023/QH15 ngày 22 tháng 06 năm 2023 của Quốc hội;

Căn cứ Luật Công nghệ thông tin số: 67/2006/QH11 ngày 29 tháng 06 năm 2006 của Quốc hội;

Căn cứ Luật Khám bệnh, chữa bệnh số: 15/2023/QH15 ngày 09 tháng 01 năm 2023 của Quốc hội;

Căn cứ Thông tư số: 46/2018/TT-BYT ngày 28/12/2018 của Bộ Y tế về việc Quy định hồ sơ bệnh án điện tử;

Căn cứ Thông tư số: 32/2023/TT – BHYT ngày 31/12/2023 của Bộ Y tế về việc Quy định chi tiết một số điều của Luật khám bệnh, chữa bệnh;

Theo đề nghị của Phòng Kế hoạch Tổng hợp.

### QUYẾT ĐỊNH:

**Điều 1.** Bàn giao sử dụng, quản lý chữ ký số, chữ ký điện tử cho nhân viên y tế của Bệnh viện Mắt Hà Nội – Đồng Nai sử dụng trên phần mềm Quản lý Bệnh viện và hồ sơ bệnh án điện tử.

**Điều 2.** Mỗi cá nhân chỉ được sử dụng 01 mẫu chữ ký số, chữ ký điện tử đã được phê duyệt để thao tác trên phần mềm quản lý bệnh viện và Hồ sơ bệnh án điện tử, phần mềm quản lý văn bản theo đúng chức năng, nhiệm vụ và quyền hạn được giao, tuân thủ các quy định về quản lý chữ ký số, chữ ký điện tử ban hành tại Quyết định số: .

Trường hợp có thay đổi mẫu chữ ký số vì lý do bất khả kháng, phải được sự đồng ý và phê duyệt của Ban giám đốc Bệnh viện.

Cá nhân có trách nhiệm sử dụng và quản lý chữ ký số, ký điện tử đúng các quy trình, quy định và phải chịu trách nhiệm trước Ban Giám đốc, cơ quan pháp luật về hậu quả do không tuân thủ quy định tại Điều 2.

**Điều 3.** Quyết định này có hiệu lực kể từ ngày ký.

Trưởng/phụ trách các khoa, phòng trong Bệnh viện và cá nhân có tên tại Điều 1 chịu trách nhiệm thi hành Quyết định này.

**Nơi nhận:**

- Như điều 3;
- BGD, Các khoa phòng;
- Lưu VT, KH-CĐT.

**GIÁM ĐỐC**



**GIÁM ĐỐC**  
BS CKI. Hoàng Vĩnh Hà



Số: 68/BBVMEMR

Đồng Nai, ngày 20 tháng 11 năm 2025

### QUYẾT ĐỊNH

V/v Thành lập Hội đồng chuyên môn đánh giá Bệnh án điện tử để quyết định việc sử dụng và lưu trữ hồ sơ Bệnh án điện tử thay thế cho Bệnh án giấy, lưu trữ và truyền tải hình ảnh y tế thay cho in phim, lưu trữ thông tin xét nghiệm thay cho việc in giấy của Bệnh viện Mắt Hà Nội – Đồng Nai

### GIÁM ĐỐC BỆNH VIỆN MẮT HÀ NỘI – ĐỒNG NAI

*Căn cứ Luật Khám bệnh, chữa bệnh số 15/2023/QH15 ngày 09/01/2023;*

*Căn cứ Luật giao dịch điện tử số 20/2023/QH15 ngày 22/06/2023 ;*

*Căn cứ Luật căn cước số 26/2023/QH15 ngày 27/11/2023;*

*Căn cứ Luật An toàn thông tin mạng số 86/2015/QH13 ngày 19/11/2015;*

*Căn cứ Luật Công nghệ thông tin 67/2006/QH11 ngày 29/06/2006;*

*Căn cứ Nghị định 96/NĐ-CP ngày 30/12/2023 của Chính phủ quy định Chi tiết một số điều của Luật khám bệnh, chữa bệnh;*

*Căn cứ Thông tư 32/2023/TT-BYT ngày 31/12/2023 của Bộ Y tế về Quy định chi tiết một số điều của Luật Khám bệnh, chữa bệnh;*

*Căn cứ Nghị định số 137/2024/NĐ-CP ngày 23/10/2024 của Chính Phủ Quy định về giao dịch điện tử của cơ quan nhà nước và hệ thống thông tin phục vụ giao dịch điện tử;*

*Căn cứ Thông tư số 53/2014/TT-BYT ngày 29/12/2014 của Bộ Y tế về Ban hành Quy định điều kiện hoạt động y tế trên môi trường mạng;*

*Căn cứ Thông tư số 48/2017/TT-BYT ngày 28/12/2017 của Bộ Y tế về Ban hành Quy định trích chuyển dữ liệu điện tử trong quản lý và thanh toán chi phí khám bệnh, chữa bệnh bảo hiểm y tế;*

*Căn cứ Thông tư số 54/TT-BYT ngày 29/12/2017 của Bộ Y tế về việc Ban hành Bộ tiêu chí ứng dụng công nghệ thông tin tại các cơ sở khám bệnh, chữa bệnh;*

*Căn cứ Thông tư số 32/TT-BYT ngày 31/12/2023 của Bộ Y tế về Quy định chi tiết một số điều của Luật Khám bệnh, chữa bệnh;*

*Căn cứ Thông tư 13/2025/TT-BYT ngày 06 tháng 06 năm 2025 của Bộ Y tế Về Hướng dẫn triển khai hồ sơ bệnh án điện tử;*

*Căn cứ Thông tư số 33/2025/TT-BYT ngày 01/07/2025 của Bộ Y tế về quy định hạn lưu trữ Hồ sơ, tài liệu Ngành y tế;*

*Căn cứ Văn bản số 365/TTYTQG-GPQLCL ngày 06 tháng 06 năm 2025 của Trung tâm thông tin y tế Quốc Gia về Hướng dẫn yêu cầu kỹ thuật triển khai phần mềm hồ sơ bệnh án điện tử;*

*Xét đề nghị của Trưởng phòng Kế hoạch Tổng hợp,*

### **QUYẾT ĐỊNH:**

**Điều 1.** Thành lập Hội đồng chuyên môn đánh giá việc sử dụng và lưu trữ hồ sơ bệnh án điện tử thay cho hồ sơ bệnh án giấy, lưu trữ và truyền tải hình ảnh y tế thay cho in phim và lưu trữ thông tin xét nghiệm thay cho việc in giấy tại Bệnh viện Mắt Hà Nội – Đồng Nai (*Chi tiết theo danh sách đính kèm*).

**Điều 2.** Hội đồng chuyên môn có trách nhiệm:

- Thẩm định các điều kiện đảm bảo triển khai bệnh án điện tử tại Bệnh viện Mắt Hà Nội – Đồng Nai;

- Quyết định sử dụng và lưu trữ trên hồ sơ bệnh án điện tử thay cho bệnh án giấy, lưu trữ và truyền tải hình ảnh y tế thay cho in phim và lưu trữ thông tin xét nghiệm thay cho việc in giấy.

**Điều 3.** Hội đồng hoạt động theo nguyên tắc thảo luận tập thể, quyết định theo đa số và tự giải thể khi hoàn thành nhiệm vụ.

**Điều 4.** Quyết định có hiệu lực từ ngày ký.

Trưởng các Khoa, Phòng liên quan, các thành viên Hội đồng có tên tại Điều 1 và các đơn vị có liên quan căn cứ Quyết định thi hành./.

**Nơi nhận:**

- Sở Y tế Đồng Nai (để b/c);
- Như điều 4 (để t/h);
- Lưu: VT, CNTT.



**TRẦN THẾ THẮNG**



## DANH SÁCH

**Hội đồng chuyên môn quyết định sử dụng và lưu trữ hồ sơ bệnh án điện tử  
thay thế cho hồ sơ giấy, lưu trữ và truyền tải hình ảnh y tế thay cho in phim  
và lưu trữ thông tin xét nghiệm thay cho việc in giấy**

*(Ban hành kèm theo Quyết định số: 68/BBVMMEMR ngày 20 tháng 11 năm 2025)*

| STT | Họ tên             | Chức vụ                       | Chức danh<br>trong hội đồng |
|-----|--------------------|-------------------------------|-----------------------------|
| 1   | Hoàng Vĩnh Hà      | Giám đốc chuyên môn Bệnh viện | Chủ tịch thường<br>trực     |
| 2   | Trần Ngọc Hưng     | Phó Giám Đốc chuyên môn       | Phó chủ tịch<br>thường trực |
| 3   | Nguyễn Thị Hồng    | TP Kế hoạch tổng hợp          | Thư ký                      |
| 4   | Bùi Thái Đạt       | Trưởng khoa Mắt tổng hợp      | Ủy viên                     |
| 5   | Nguyễn Mai Anh     | Trưởng khoa Dược              | Ủy viên                     |
| 6   | Nguyễn Thị Diễm    | Trưởng khoa Xét nghiệm        | Ủy viên                     |
| 7   | Ngô Hoàng Anh Kiệt | Kế toán trưởng                | Ủy viên                     |