

Số: 631 /KH-BVDLTTNT

Khánh Hòa, ngày 21 tháng 9 năm 2026

KẾ HOẠCH

Triển khai thực hiện Quyết định số 515/QĐ-TTg ngày 30/3/2026 của Thủ tướng Chính phủ phê duyệt Đề án “Nâng cao năng lực hoạt động của lực lượng bảo vệ an ninh mạng quốc gia” tại Bệnh viện Da liễu – Tâm thần Ninh Thuận

Căn cứ Kế hoạch số 6756/KH-SYT ngày 28/8/2026 của Sở Y tế tỉnh Khánh Hòa về Triển khai thực hiện Quyết định số 515/QĐ-TTg ngày 30/3/2026 của Thủ tướng Chính phủ phê duyệt Đề án “Nâng cao năng lực hoạt động của lực lượng bảo vệ an ninh mạng quốc gia” trong ngành Y tế tỉnh Khánh Hòa;

Bệnh viện Da liễu – Tâm thần Ninh Thuận xây dựng kế hoạch Triển khai thực hiện Quyết định số 515/QĐ-TTg ngày 30/3/2026 của Thủ tướng Chính phủ phê duyệt Đề án “Nâng cao năng lực hoạt động của lực lượng bảo vệ an ninh mạng quốc gia” như sau:

I. CĂN CỨ VÀ THỰC TRẠNG

- Thực hiện Quyết định số 515/QĐ-TTg ngày 30/3/2026 của Thủ tướng Chính phủ, Kế hoạch số 10442/KH-UBND ngày 19/8/2026 của UBND tỉnh Khánh Hòa và Kế hoạch của Sở Y tế.

- Hiện nay, Bệnh viện đang vận hành hệ thống thông tin quản lý bệnh viện tích hợp (HIS, LIS, PACS, EMR và các phân hệ quản lý dược, viện phí, bảo hiểm y tế...).

- Hồ sơ xác định cấp độ an toàn hệ thống thông tin đang được hoàn thiện ở mức cấp độ 2, đã gửi Công an tỉnh và chờ thẩm định, phê duyệt. Công tác quản trị hệ thống, bảo đảm an toàn thông tin và ứng phó sự cố do bộ phận Công nghệ thông tin đảm nhiệm. Sao lưu dữ liệu đã được thực hiện định kỳ nhưng chưa có phương án chính thức được phê duyệt và diễn tập. Dữ liệu người bệnh thuộc chuyên khoa da liễu và tâm thần là dữ liệu nhạy cảm, cần được bảo vệ nghiêm ngặt.

- Trên cơ sở điều kiện thực tế, Bệnh viện xác định triển khai theo hướng từng bước, thiết thực, ưu tiên những việc bắt buộc và có thể thực hiện ngay.

II. MỤC TIÊU

1. Giai đoạn 2026 – 2027

- Hoàn thành trình phê duyệt Hồ sơ xác định cấp độ an toàn hệ thống thông tin Cấp độ 2 và triển khai đầy đủ phương án bảo vệ theo cấp độ được phê duyệt.

- Ban hành, hoàn thiện hệ thống quy chế, quy trình nội bộ về an toàn thông tin, bảo vệ dữ liệu người bệnh và ứng cứu sự cố

- Phân công rõ trách nhiệm: một lãnh đạo Bệnh viện phụ trách chung; bộ phận Công nghệ thông tin làm đầu mỗi kỹ thuật.

- 100% viên chức, người lao động được phổ biến kiến thức, kỹ năng cơ bản về an toàn thông tin, bảo vệ dữ liệu cá nhân/bệnh nhân và phòng chống lừa đảo trên không gian mạng.

2. Đến năm 2030

- Duy trì, cập nhật thường xuyên các phương án bảo vệ hệ thống thông tin, quy trình sao lưu và khôi phục dữ liệu.

- Định kỳ hằng năm tổ chức phổ biến kiến thức và cử cán bộ chuyên trách/kiêm nhiệm tham gia các lớp đào tạo, tập huấn chuyên sâu, diễn tập do Sở Y tế và Công an tỉnh tổ chức.

- Từng bước cải thiện hệ thống sao lưu dữ liệu và phương án duy trì hoạt động khi xảy ra sự cố.

III. NHIỆM VỤ VÀ GIẢI PHÁP

1. Hồ sơ cấp độ và quy chế

- Khẩn trương hoàn thiện Hồ sơ đề xuất cấp độ an toàn hệ thống thông tin (Cấp độ 2), phối hợp với lực lượng chức năng của Công an tỉnh để thẩm định và trình cấp có thẩm quyền phê duyệt.

- Bệnh viện đã ban hành đầy đủ các quy chế, quy trình liên quan gồm: Quy chế bảo đảm an toàn, an ninh mạng; Quy chế bảo mật thông tin và quyền riêng tư người bệnh; Quy trình xử lý sự cố an toàn thông tin; Quy trình sao lưu và phục hồi dữ liệu cùng các quyết định liên quan. Bộ phận Công nghệ thông tin tiếp tục rà soát, cập nhật khi có thay đổi hoặc yêu cầu mới.

2. Phân công trách nhiệm

- Giám đốc Bệnh viện chịu trách nhiệm toàn diện về công tác an ninh mạng tại đơn vị.

- Phân công 01 Đồng chí trong Ban Giám đốc trực tiếp phụ trách, chỉ đạo công tác an toàn thông tin, an ninh mạng.

- Bộ phận Công nghệ thông tin là đầu mối kỹ thuật, thực hiện nhiệm vụ: Quản trị hệ thống; sao lưu dữ liệu; tiếp nhận và xử lý ban đầu các sự cố; tham mưu các giải pháp bảo vệ dữ liệu bệnh nhân; duy trì kết nối 24/7 với Sở Y tế và lực lượng chuyên trách Công an tỉnh.

- Xây dựng và duy trì Danh bạ liên lạc khẩn cấp (Sở Y tế, Công an tỉnh, Đơn vị cung cấp giải pháp/phần mềm).

3. Đào tạo và phổ biến kiến thức

- Định kỳ hằng năm cử cán bộ phụ trách CNTT tham gia các chương trình đào tạo, bồi dưỡng nâng cao kỹ năng chuyên sâu và diễn tập do Sở Y tế, Công an tỉnh tổ chức.

- Tổ chức phổ biến, tuyên truyền kiến thức an ninh mạng cho toàn thể viên chức, người lao động (tối thiểu 01 lần/năm) lồng ghép qua các buổi giao ban, sinh hoạt khoa/phòng. Tập trung vào các nội dung: Phòng chống lừa đảo trực tuyến (Phishing), bảo vệ tài khoản cá nhân, bảo mật dữ liệu người bệnh, quy định không tự ý cài đặt phần mềm lạ hoặc sử dụng thiết bị lưu trữ ngoài chưa kiểm duyệt.

4. Sao lưu dữ liệu và ứng phó sự cố

- Duy trì nghiêm túc công tác sao lưu dữ liệu (Backup) định kỳ, tiến tới xây dựng phương án sao lưu dữ liệu độc lập, khép kín.

- Xây dựng Quy trình vận hành dự phòng nhằm bảo đảm hoạt động khám, chữa bệnh diễn ra liên tục, không bị gián đoạn khi hệ thống CNTT gặp sự cố nghiêm trọng..

- Khi xảy ra sự cố an toàn thông tin mạng, Bộ phận CNTT có trách nhiệm xử lý ban đầu và báo cáo ngay cho Lãnh đạo Bệnh viện, đồng thời thông báo về Sở Y tế để phối hợp xử lý kịp thời.

5. Phối hợp với các cơ quan liên quan

- Thực hiện nghiêm túc chế độ báo cáo định kỳ/đột xuất theo yêu cầu của Sở Y tế và Công an tỉnh.

- Chủ động chuẩn bị các điều kiện kỹ thuật cần thiết, sẵn sàng kết nối, chia sẻ dữ liệu/nhật ký hệ thống (log) về Trung tâm Giám sát an ninh mạng (SOC) của tỉnh theo lộ trình hướng dẫn của cấp trên.

- Tích cực tham gia các đợt diễn tập, rà quét lỗ hổng bảo mật do Sở Y tế và Công an tỉnh phối hợp tổ chức.

IV. KINH PHÍ

- Sử dụng nguồn ngân sách được giao, nguồn thu sự nghiệp và các nguồn hợp pháp khác.

- Ưu tiên bố trí cho việc hoàn thiện hồ sơ cấp độ, tập huấn và cải thiện thiết bị sao lưu dữ liệu.

- Không đặt chỉ tiêu cứng về tỷ lệ kinh phí nếu nguồn chưa bảo đảm.

V. TỔ CHỨC THỰC HIỆN

- Giám đốc Bệnh viện chịu trách nhiệm toàn diện việc triển khai Kế hoạch; phê duyệt quy chế và chỉ đạo xử lý sự cố. Lãnh đạo được phân công phụ trách theo dõi, đôn đốc thực hiện.

- Phòng Tổ chức - Hành chính – Kiểm soát nhiễm khuẩn theo dõi, tổng hợp báo cáo và quản lý bộ phận Công nghệ thông tin. Bộ phận Công nghệ thông tin (trực thuộc Phòng TCHC-KSNK) là đầu mối kỹ thuật, thực hiện hoàn thiện hồ sơ cấp độ, quản trị hệ thống, sao lưu dữ liệu, ứng phó sự cố, tham mưu và báo cáo.

- Phòng Kế hoạch – Tài chính – Điều dưỡng – Chỉ đạo tuyển bố trí kinh phí theo khả năng.

- Bộ phận CNTT Là đầu mối kỹ thuật, tham mưu hoàn thiện Hồ sơ cấp độ 2; duy trì quản trị, bảo mật hệ thống HIS, EMR...; sao lưu dữ liệu; tiếp nhận và phối hợp ứng cứu sự cố 24/7.

- Các khoa, phòng thực hiện quy định bảo vệ dữ liệu người bệnh, tham gia phổ biến kiến thức và kịp thời báo cáo khi có dấu hiệu bất thường.

Trên đây là Kế hoạch Triển khai thực hiện Quyết định số 515/QĐ-TTg ngày 30/3/2026 của Thủ tướng Chính phủ phê duyệt Đề án “Nâng cao năng lực hoạt động của lực lượng bảo vệ an ninh mạng quốc gia” tại đơn vị./.

Nơi nhận:

- Sở Y tế (b/c);
- Ban Lãnh đạo BV;
- Các khoa, phòng;
- Lưu: VT, TCHCKSNK.



GIÁM ĐỐC

Lê Văn Đồng