SỞ Y TẾ HÀ NỘI
TRUNG TÂM ĐÀO TẠO VÀ CHUYỂN GIAO CÔNG NGHỆ Y TẾ HÀ NỘI
CHUẨN HÓA NĂNG LỰC - KẾT NỐI CÔNG NGHỆ - CHUYỂN GIAO TRI THỨC - NHÂN RỘNG ĐỔI MỚI

Đơn vị đồng hành
TKM TECHNOLOGY COMPANY



AN TOÀN THÔNG TIN VÀ BẢO MẬT DỮ LIỆU TRONG BỆNH VIỆN

Tài liệu lớp tập huấn
ngày 29 tháng 10 năm 2026

Từ tuân thủ pháp luật đến quản trị rủi ro
và bảo vệ hoạt động khám bệnh chữa bệnh

Dành cho lãnh đạo bệnh viện và các bộ phận
chuyên môn công nghệ thông tin bảo hiểm y tế
quản lý chất lượng pháp chế tài chính

Đơn vị phối hợp chuyên môn
Công ty TKM và các chuyên gia

Hà Nội 2026

Lời giới thiệu và cách sử dụng

Bảo đảm an toàn thông tin trong bệnh viện gắn trực tiếp với việc tiếp tục cấp cứu, khám bệnh, điều trị và bảo vệ thông tin sức khỏe của người dân. Mỗi đơn vị cần biết hệ thống nào phải được bảo vệ, ai chịu trách nhiệm, làm gì khi xảy ra sự cố và dựa vào đâu để xác nhận hoạt động đã phục hồi an toàn.

Tập tài liệu phục vụ lớp tập huấn ngày 29 tháng 10 năm 2026 do Trung tâm Đào tạo và Chuyển giao công nghệ Y tế Hà Nội phối hợp với Công ty TKM và các chuyên gia tổ chức. Nội dung dùng cho học tập tại hội nghị và làm tài liệu thực hành tại bệnh viện. Địa điểm lớp tập huấn là Hội trường tầng 11 Trung tâm Kiểm soát bệnh tật Hà Nội, số 70 Nguyễn Chí Thanh, phường Láng, Hà Nội.

Sau lớp tập huấn, mỗi bệnh viện cần hình thành một bộ kết quả có thể kiểm tra được gồm danh mục hệ thống, bảng trách nhiệm, danh mục khoảng trống tuân thủ, phương án duy trì khám chữa bệnh, kế hoạch khắc phục và bằng chứng thử khôi phục dữ liệu.

Tìm nội dung theo nhiệm vụ

Người sử dụng	Nội dung ưu tiên	Sản phẩm mang về đơn vị
Giám đốc và ban giám đốc	Phát biểu định hướng; trách nhiệm quản trị; kế hoạch sau tập huấn	Quyết định phân công và kế hoạch khắc phục có nguồn lực
CNTT và đầu mối an toàn thông tin	Cấp độ; giám sát; ứng cứu; sao lưu và quản lý nhà cung cấp	Danh mục hệ thống, hồ sơ cấp độ, nhật ký và biên bản thử phục hồi
Kế hoạch tổng hợp và khoa chuyên môn	Duy trì khám chữa bệnh; nhận diện người bệnh; diễn tập	Quy trình dự phòng theo khoa, phòng và hồ sơ đối soát sau sự cố
BHYT và tài chính kế toán	An toàn dữ liệu liên thông; theo dõi lỗi và đối soát	Danh sách tồn đọng, chứng cứ truyền nhận và kết quả xử lý
Pháp chế và hành chính	Pháp luật; bảo vệ dữ liệu; hợp đồng; báo cáo	Bảng căn cứ áp dụng, đầu mối báo cáo và điều khoản trách nhiệm

Các nghĩa vụ pháp luật được dẫn bằng mã PL tại phần Văn bản và tài liệu tham khảo, cập nhật theo thời điểm 29/10/2026. Các biểu mẫu, chỉ số, kịch bản và mốc 30–60–90 ngày là công cụ hướng dẫn thực hành; đơn vị điều chỉnh, phê duyệt theo thẩm quyền và phải thực hiện đúng các thời hạn luật định có liên quan. Tình huống mô phỏng được ghi rõ; các chuyên đề bổ sung không phải kết luận về một bệnh viện cụ thể.

Bộ tài liệu được dùng xuyên suốt theo chu trình rà soát, giao việc, triển khai, kiểm chứng và cải tiến. Người đứng đầu cần xem kết quả thực tế, thay vì chỉ ghi nhận việc đã tham dự lớp hoặc đã ban hành văn bản.

Mục lục

Lời giới thiệu và cách sử dụng....2
Phần thứ nhất Phát biểu định hướng....4
Phát biểu khai mạc của lãnh đạo Sở Y tế....4
Phát biểu đề dẫn của Giám đốc Trung tâm....7
Phần thứ hai Chuyên đề quản trị và tổ chức thực hiện....10
Trách nhiệm pháp lý và trách nhiệm của người đứng đầu....10
Bảo vệ hệ thống thông tin theo cấp độ và quản trị rủi ro....13
Duy trì khám chữa bệnh và bảo đảm an toàn người bệnh khi có sự cố....17
Bảo vệ dữ liệu liên thông và bảo đảm quyền lợi bảo hiểm y tế....20
Phần thứ ba Chuyên đề kỹ thuật và kinh nghiệm thực hành....23
Đừng để máy tính trở thành bệnh nhân....23
Tổ chức SOC và giám sát an toàn thông tin trong bệnh viện....25
Sao lưu và phục hồi dữ liệu để duy trì khám chữa bệnh....27
Quản lý lỗ hổng ứng dụng và truy cập của nhà cung cấp....28
Bài học từ sự cố và thực hành xử lý tình huống....29
Phần thứ tư Bộ công cụ triển khai tại bệnh viện....31
Tổ chức thực hiện sau lớp tập huấn....31
Mẫu 01 Phiếu tự rà soát an toàn thông tin bệnh viện....32
Mẫu 02 Hồ sơ kiểm kê một hệ thống và các phụ thuộc....34
Mẫu 03 Sổ rủi ro và kế hoạch khắc phục....35
Mẫu 04 Danh bạ ứng cứu và bảng phân công....36
Mẫu 05 Báo cáo ban đầu và nhật ký xử lý sự cố....37
Mẫu 06 Biên bản thử khôi phục dữ liệu và dịch vụ....38
Mẫu 07 Kịch bản diễn tập gián đoạn hệ thống trong bốn giờ....39
Mẫu 08 Theo dõi lỗi liên thông và đối soát dữ liệu BHYT....41
Mẫu 09 Quản lý phiên hỗ trợ từ xa của nhà cung cấp....42
Mẫu 10 Báo cáo kết quả triển khai sau tập huấn....43
Phần thứ năm Văn bản và tài liệu tham khảo để triển khai....44
Danh mục văn bản gắn với trách nhiệm của bệnh viện....44
Những điểm pháp lý cần kiểm tra khi lập kế hoạch....46
Nguồn kỹ thuật và thuật ngữ sử dụng....48
Phần thứ sáu Các nền tảng và chương trình hỗ trợ của Trung tâm....50
Từ một lớp tập huấn đến năng lực chung của ngành....50
OHKE Nền tảng quản lý và điều phối nguồn lực khám sức khỏe....51
Medcap Hộ chiếu năng lực số ngành y tế....52
VTVL Cẩm nang điện tử và công cụ xây dựng đề án vị trí việc làm....53
MedCore và AI Agent dành cho lãnh đạo....53
MEDU và MedSurvey trong phát triển năng lực....54
Danh mục các lớp tập huấn và chương trình hỗ trợ....55
Đăng ký nhu cầu và đầu mối phối hợp với Trung tâm....57

Phần thứ nhất Phát biểu định hướng

Phát biểu khai mạc của lãnh đạo Sở Y tế

Lãnh đạo Sở Y tế Hà Nội

Kính thưa các chuyên gia, các vị đại biểu!

Thưa các đồng chí lãnh đạo bệnh viện và toàn thể học viên!

Hôm nay, thay mặt lãnh đạo Sở Y tế Hà Nội, tôi tới dự và khai mạc lớp tập huấn “An toàn thông tin bệnh viện năm 2026: Từ tuân thủ pháp luật đến quản trị rủi ro và bảo vệ hoạt động khám bệnh, chữa bệnh” do Trung tâm Đào tạo và Chuyển giao công nghệ Y tế Hà Nội phối hợp với Công ty TKM tổ chức. Đây là nội dung thiết thực, gắn trực tiếp với yêu cầu bảo đảm hoạt động an toàn, ổn định của các bệnh viện và bảo vệ quyền lợi của người bệnh.

Bệnh viện là đơn vị chuyên môn, hằng ngày phải tập trung nguồn lực cho cấp cứu, khám bệnh, điều trị và chăm sóc người bệnh. Trong điều kiện áp lực công việc lớn, nguồn lực còn hạn chế, sự quan tâm của lãnh đạo thường dành nhiều cho nhân lực, thuốc, trang thiết bị và phát triển kỹ thuật. Công tác an toàn, bảo mật thông tin và dự phòng sự cố công nghệ thông tin vì thế có lúc, có nơi chưa được quan tâm tương xứng; việc chuẩn bị phương án ứng phó còn được giao chủ yếu cho bộ phận kỹ thuật hoặc nhà cung cấp phần mềm.

Điều hành bệnh viện luôn đòi hỏi duy trì hoạt động khám bệnh, chữa bệnh liên tục. Khi công nghệ thông tin tham gia vào hầu hết các khâu, từ tiếp đón, chỉ định, xét nghiệm đến kê đơn và quản lý bệnh án, sự ổn định của hệ thống trở thành một điều kiện để bệnh viện vận hành. Người đứng đầu cần quan tâm đến an toàn thông tin ngay trong công tác quản trị hằng ngày.

Tôi muốn đặt ra một tình huống để các đồng chí cùng suy nghĩ: Nếu ngay lúc này, hệ thống công nghệ thông tin của bệnh viện bị xâm nhập, bị treo hoặc dữ liệu bị mã hóa, bệnh viện sẽ hoạt động như thế nào?

Người bệnh đang chờ sẽ được tiếp đón ra sao? Bác sĩ có truy cập được bệnh án, tiền sử dị ứng và các chỉ định đang thực hiện không? Kết quả xét nghiệm, chẩn đoán hình ảnh được chuyển đến khoa điều trị bằng cách nào? Việc cấp phát thuốc, thực hiện y lệnh và bàn giao giữa các ca trực có bảo đảm chính xác không? Nếu hệ thống ngừng hoạt động trong bốn giờ, một ngày hoặc lâu hơn, ai là người chỉ huy và phương án nào được kích hoạt để duy trì cấp cứu, điều trị?

Nếu dữ liệu người bệnh bị đánh cắp, hậu quả còn kéo dài ngay cả khi hệ thống vẫn hoạt động. Thông tin sức khỏe, thông tin cá nhân bị lộ có thể ảnh hưởng đến quyền riêng tư của người bệnh, uy tín bệnh viện và phát sinh trách nhiệm pháp lý. Một sự cố công nghệ thông tin có thể nhanh chóng trở thành sự cố trong hoạt động khám bệnh, chữa bệnh, làm gián đoạn phục vụ và tạo thêm nguy cơ mất an toàn cho người bệnh.

Bảo đảm an toàn thông tin phải được đặt trong cùng trách nhiệm bảo đảm an toàn người bệnh và duy trì hoạt động liên tục của bệnh viện. Giám đốc bệnh viện phải trực tiếp chỉ đạo, kiểm tra và chịu trách nhiệm về việc tổ chức thực hiện tại đơn vị mình.

Các quy định về bảo vệ dữ liệu cá nhân, bảo đảm an toàn hệ thống thông tin theo cấp độ và triển khai hồ sơ bệnh án điện tử cần được cụ thể hóa thành biện pháp thực hiện tại từng bệnh viện. Việc có quy chế, có hồ sơ phải đi liền với khả năng phát hiện rủi ro, ngăn ngừa sự cố và khôi phục hoạt động khi cần thiết. Kinh phí dành cho công tác này cần được xác định trong kế hoạch bảo đảm chất lượng và duy trì hoạt động của đơn vị.

Thay mặt lãnh đạo Sở Y tế, tôi biểu dương Trung tâm Đào tạo và Chuyển giao công nghệ Y tế Hà Nội đã chủ động phát huy vai trò của một đơn vị thuộc Sở, nhận diện nhu cầu thực tiễn của các bệnh viện, kết nối chuyên gia và phối hợp với Công ty TKM tổ chức lớp tập huấn này. Việc lựa chọn nội dung gắn với tuân thủ pháp luật, quản trị rủi ro và duy trì khám bệnh, chữa bệnh thể hiện hướng tiếp cận phù hợp, phục vụ trực tiếp yêu cầu quản lý của ngành.

Tôi trân trọng cảm ơn Công ty TKM và các chuyên gia đã phối hợp, đóng góp chuyên môn cho chương trình. Tôi mong các nội dung trao đổi hôm nay giúp lãnh đạo và cán bộ bệnh viện nhận diện được những điểm còn thiếu, biết cách tổ chức phòng ngừa và có cơ sở xây dựng phương án khắc phục phù hợp với điều kiện của đơn vị.

Thưa các đồng chí!

Để lớp tập huấn tạo ra chuyển biến cụ thể, tôi đề nghị các bệnh viện triển khai ngay sau hội nghị những nhiệm vụ sau:

Thứ nhất, tổ chức rà soát toàn diện thực trạng an toàn thông tin của đơn vị. Giám đốc bệnh viện trực tiếp chỉ đạo, huy động các khoa, phòng chuyên môn cùng tham gia; rà soát cả hệ thống do bệnh viện quản lý và dịch vụ thuê ngoài. Nội dung cần làm rõ gồm hệ thống trọng yếu, hồ sơ và phương án bảo đảm an toàn theo cấp độ, phân quyền truy cập, quản lý tài khoản, kết nối từ xa của nhà cung cấp, bảo vệ dữ liệu và những nguy cơ có thể gây gián đoạn hoạt động. Các hồ sơ thuộc diện phải phê duyệt cần được hoàn thiện, trình đúng thẩm quyền và tổ chức thực hiện theo quy định.

Thứ hai, xây dựng và thực tập phương án duy trì khám bệnh, chữa bệnh khi hệ thống gặp sự cố. Từng khoa, phòng phải biết công việc nào cần tiếp tục, sử dụng quy trình và biểu mẫu dự phòng nào, phối hợp với ai, báo cáo cho ai. Phương án phải ưu tiên cấp cứu và điều trị thiết yếu, bảo đảm nhận diện đúng người bệnh, thực hiện chính xác y lệnh, xét nghiệm và cấp phát thuốc; đồng thời quy định việc đối chiếu, cập nhật dữ liệu sau khi hệ thống được khôi phục. Cần diễn tập để kiểm chứng khả năng thực hiện.

Thứ ba, kiểm tra thực chất việc sao lưu và khả năng khôi phục dữ liệu. Bệnh viện cần có bản sao lưu được bảo vệ, tách biệt phù hợp với hệ thống đang vận hành; định kỳ thử khôi phục để xác định dữ liệu có sử dụng được hay không và cần bao lâu để phục hồi. Đồng thời, phải kiểm soát quyền truy cập, ghi nhận hoạt động trên hệ thống và làm rõ trách nhiệm bảo mật, hỗ trợ ứng cứu của các nhà cung cấp trong hợp đồng.

Thứ tư, lập kế hoạch khắc phục sau rà soát, xác định rõ việc cần làm, người chịu trách nhiệm, thời hạn hoàn thành và nguồn lực thực hiện. Các nguy cơ có thể ảnh hưởng trực tiếp đến hoạt động khám bệnh, chữa bệnh phải được ưu tiên xử lý. Những nội dung cần đầu tư, thuê dịch vụ hoặc hỗ trợ chuyên môn phải được đề xuất phù hợp, thực hiện đúng quy định. Khó khăn vượt thẩm quyền cần kịp thời báo cáo Sở Y tế để được hướng dẫn, phối hợp giải quyết.

Thứ năm, duy trì công tác phòng ngừa thường xuyên. Mỗi bệnh viện cần có đầu mối an toàn thông tin, quy trình tiếp nhận cảnh báo, báo cáo và phối hợp ứng cứu sự cố; tổ chức hướng dẫn cho nhân viên về bảo vệ tài khoản, sử dụng dữ liệu và nhận diện nguy cơ. Lãnh đạo bệnh viện cần định kỳ kiểm tra tiến độ khắc phục và khả năng vận hành phương án dự phòng.

Tôi đề nghị Trung tâm Đào tạo và Chuyển giao công nghệ Y tế Hà Nội tiếp tục tổng hợp nhu cầu, phối hợp với các phòng chuyên môn của Sở và các chuyên gia để hỗ trợ đào tạo, hướng dẫn các đơn vị theo chức năng, nhiệm vụ được giao. Trọng tâm là giúp bệnh viện có thêm năng lực tự rà soát, tổ chức thực hiện và duy trì kết quả sau tập huấn.

Đề nghị các đồng chí học viên tập trung trao đổi những tình huống thực tế tại đơn vị, đặt câu hỏi về những vấn đề còn vướng và chủ động chia sẻ kinh nghiệm. Sau hội nghị, mỗi bệnh viện cần xác định được các điểm yếu cần khắc phục, có kế hoạch hành động và tổ chức thực hiện để bảo đảm đơn vị hoạt động an toàn, ổn định, phục vụ người bệnh liên tục.

Với tinh thần đó, tôi tuyên bố khai mạc lớp tập huấn. Chúc các chuyên gia, các vị đại biểu và toàn thể các đồng chí sức khỏe; chúc chương trình thành công tốt đẹp.

Xin trân trọng cảm ơn!

Phát biểu đề dẫn của Giám đốc Trung tâm

PGS.TS. Doãn Ngọc Hải Giám đốc Trung tâm Đào tạo và Chuyển giao công nghệ Y tế Hà Nội

Kính thưa các đồng chí lãnh đạo bệnh viện, các chuyên gia, các vị đại biểu!

Kính thưa đại diện các cơ quan, đơn vị và các doanh nghiệp đồng hành cùng chương trình!

Trước hết, thay mặt Trung tâm Đào tạo và Chuyển giao công nghệ Y tế Hà Nội, tôi trân trọng cảm ơn các bệnh viện, các chuyên gia, Công ty TKM và toàn thể đại biểu đã tham dự, phối hợp tổ chức lớp tập huấn hôm nay.

Kính thưa các đồng chí!

Trong nhiều năm làm công tác quản lý y tế, từ cấp đơn vị đến cơ quan quản lý nhà nước, tôi nhận thấy một vấn đề đáng quan tâm: chúng ta dành nhiều nguồn lực phát triển chuyên môn, trang thiết bị, kỹ thuật mới và chuyển đổi số, nhưng chưa phải lúc nào cũng quan tâm tương xứng đến việc bảo đảm các hệ thống hoạt động an toàn, liên tục và có khả năng phục hồi khi xảy ra sự cố.

Qua thực tiễn công tác quản lý, nghiên cứu và đào tạo trong ngành y tế, tôi nhận thức rõ năng lực của hệ thống không chỉ thể hiện khi hoạt động bình thường, mà còn ở khả năng tổ chức, điều phối và duy trì dịch vụ thiết yếu trong tình huống bất thường. Đó cũng là lý do Trung tâm lựa chọn chủ đề tập huấn hôm nay là chuyển từ yêu cầu tuân thủ pháp luật đến quản trị rủi ro và bảo vệ hoạt động khám bệnh, chữa bệnh.

An toàn thông tin không chỉ là câu chuyện máy chủ, phần mềm hay thiết bị bảo mật. Đối với bệnh viện, đó còn là vấn đề quản trị, chất lượng khám chữa bệnh và trách nhiệm đối với người dân.

Tôi xin nêu một số ví dụ để thấy rõ tính chất nghiêm trọng của vấn đề. Tháng 10 năm 2026, cơ quan an ninh mạng Singapore cảnh báo về những lỗ hổng bảo mật nghiêm trọng trong PHP, công nghệ được sử dụng rộng rãi trên các máy chủ ứng dụng. Trong những điều kiện nhất định, lỗ hổng có thể bị khai thác để thực thi mã trái phép từ xa. Nếu các lớp bảo vệ khác không đủ hiệu quả, kẻ tấn công có thể xâm nhập sâu hơn, chiếm quyền điều khiển, đánh cắp dữ liệu, phá hoại hệ thống hoặc triển khai mã độc tống tiền. Nguồn cảnh báo kỹ thuật được dẫn tại [KT1].

Vụ tấn công vào Change Healthcare tại Mỹ tháng 2 năm 2024 đã làm gián đoạn các hệ thống thông tin y tế và thanh toán trên diện rộng. Cơ quan quản lý của Mỹ xác định sự cố ảnh hưởng trực tiếp đến hoạt động chăm sóc và quyền riêng tư của người bệnh. Bài học cần rút ra là một sự cố ở doanh nghiệp công nghệ cũng có thể lan sang hoạt động của nhiều cơ sở y tế [KT2].

Đối với bệnh viện, hậu quả có thể nghiêm trọng hơn bởi phía sau hệ thống thông tin là hoạt động cấp cứu, khám bệnh, điều trị và tính mạng người bệnh. Hãy hình dung HIS ngừng hoạt động, bác sĩ không truy cập được bệnh án điện tử, khoa xét nghiệm không chuyển được kết quả, khoa dược không nhận được đơn thuốc, các khoa điều trị không có đầy đủ thông tin thực hiện y lệnh. Hoặc một cuộc hội chẩn từ xa mất kết nối; một ứng dụng trí tuệ nhân tạo hỗ trợ chẩn đoán đưa ra kết quả không phù hợp do dữ liệu đầu vào thiếu hoặc sai lệch.

Vấn đề không chỉ là bao lâu thì sửa xong phần mềm, mà là trong thời gian chưa khôi phục, bệnh viện sẽ tổ chức khám chữa bệnh như thế nào để không ảnh hưởng đến tính mạng, sức khỏe và quyền lợi

người dân? Ai chỉ huy? Khoa cấp cứu tiếp nhận người bệnh bằng phương thức nào? Bác sĩ kiểm tra tiền sử dị ứng ra sao? Kết quả xét nghiệm nguy cấp được thông báo thế nào? Khi hệ thống hoạt động trở lại, ai đối chiếu dữ liệu để tránh nhầm lẫn?

Kính thưa các đồng chí!

Ngày 25 tháng 5 năm 2026, UBND thành phố Hà Nội ban hành Quyết định số 2644/QĐ-UBND thành lập Trung tâm Đào tạo và Chuyển giao công nghệ Y tế Hà Nội thuộc Sở Y tế; đồng thời ban hành Quyết định số 2645/QĐ-UBND quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Trung tâm. Trong bối cảnh sắp xếp bộ máy, tinh gọn đầu mối, việc thành lập Trung tâm cho thấy nhu cầu thực tiễn về năng lực đào tạo, chuyển giao công nghệ và hỗ trợ chuyển đổi số của ngành.

Ở đây tồn tại một khoảng trống cần giải quyết. Sở Y tế thực hiện chức năng quản lý nhà nước, tham mưu, hướng dẫn, phổ biến quy định, kiểm tra, đôn đốc theo thẩm quyền; không làm thay việc triển khai kỹ thuật và vận hành hệ thống của từng bệnh viện. Các bệnh viện có nhiệm vụ trọng tâm là khám chữa bệnh, trong khi không phải đơn vị nào cũng có đủ nhân lực chuyên sâu về đánh giá lỗ hổng, giám sát, ứng cứu sự cố và kiểm chứng khả năng phục hồi. Doanh nghiệp công nghệ có năng lực kỹ thuật, nhưng nếu chưa hiểu quy trình cấp cứu, điều trị, xét nghiệm, bệnh án và thanh toán BHYT, giải pháp có thể chưa phù hợp với thực tiễn chuyên môn.

Chính khoảng trống giữa yêu cầu quản lý nhà nước, năng lực thực hiện của bệnh viện và giải pháp của doanh nghiệp là vấn đề Trung tâm cần tham gia giải quyết. Trung tâm không làm thay chức năng của Sở, trách nhiệm của Giám đốc bệnh viện hay công việc của doanh nghiệp. Trung tâm kết nối các bên, chuyển tải yêu cầu quản lý và nhu cầu chuyên môn thành chương trình đào tạo, tài liệu hướng dẫn, phương pháp đánh giá và hoạt động chuyển giao công nghệ có thể áp dụng thực tế.

Chúng tôi mong muốn từng bước hình thành năng lực hỗ trợ chung cho toàn ngành, giúp các đơn vị tiếp cận kiến thức, công cụ và kinh nghiệm phù hợp, hạn chế tình trạng mỗi bệnh viện phải tự giải quyết những vấn đề giống nhau từ đầu. Giá trị Trung tâm hướng tới là đưa quy định và yêu cầu quản lý vào thực tiễn, nâng cao năng lực đơn vị và bảo vệ tốt hơn hoạt động phục vụ người dân.

Đó cũng là lý do Trung tâm phối hợp với TKM tổ chức lớp tập huấn này. Theo thông tin giới thiệu của doanh nghiệp, TKM hoạt động chuyên sâu về giải pháp an toàn, bảo mật thông tin mạng, rà quét lỗ hổng, phát hiện mã độc và kiểm thử hệ thống phần mềm. Nhóm giải pháp NOSC mà TKM giới thiệu bao gồm quản trị hạ tầng CNTT; đánh giá an ninh máy tính, thiết bị di động và hệ thống mạng; giám sát cổng thông tin điện tử, ứng dụng web và mạng LAN/WAN; phát hiện, cảnh báo điểm yếu và nguy cơ tấn công. Đây là những năng lực kỹ thuật có thể hỗ trợ các bệnh viện nhận diện nguy cơ, chủ động phòng ngừa và chuẩn bị phương án ứng cứu. Tuy nhiên, lựa chọn và triển khai giải pháp phải dựa trên khảo sát, đánh giá độc lập nhu cầu, đặc thù chuyên môn, mức độ rủi ro và quy định áp dụng tại từng đơn vị. Trung tâm phối hợp để kết nối năng lực chuyên môn y tế với năng lực công nghệ của doanh nghiệp, không giới thiệu một sản phẩm thay cho trách nhiệm đánh giá và quyết định của bệnh viện.

Kính thưa các đồng chí!

Tôi ủng hộ ứng dụng công nghệ mới, đặc biệt là trí tuệ nhân tạo, trong quản lý và chuyên môn y tế. Nhưng công nghệ càng tham gia sâu vào khám chữa bệnh, yêu cầu về an toàn, bảo mật, độ chính xác dữ liệu và duy trì hoạt động càng quan trọng. Chuyển đổi số không thể chỉ đánh giá bằng số lượng

phần mềm đã triển khai, mà phải đánh giá bằng chất lượng phục vụ, tính an toàn, hiệu quả và khả năng vận hành liên tục.

Trước hết, tuân thủ pháp luật là yêu cầu bắt buộc. Bệnh viện phải rà soát các quy định về an ninh mạng, an toàn thông tin, bảo vệ dữ liệu cá nhân, bảo mật bệnh án và an toàn hệ thống theo cấp độ. Tiếp đó, quản trị rủi ro phải trở thành một phần quản trị bệnh viện: Giám đốc phải biết hệ thống thiết yếu nào có thể gián đoạn, phương án dự phòng đã có hay chưa và khả năng phục hồi đã được kiểm chứng hay chưa. Cuối cùng, phải đặt người bệnh ở trung tâm mọi phương án ứng phó; không để người dân phải tự giải quyết khó khăn do sự cố nội bộ của bệnh viện.

Trong chương trình hôm nay, chúng ta sẽ cùng làm rõ trách nhiệm của người đứng đầu, yêu cầu bảo đảm an toàn thông tin theo cấp độ, phương án duy trì khám chữa bệnh khi hệ thống gián đoạn, đồng thời lắng nghe những tình huống tấn công mạng thực tế và các giải pháp phát hiện, ứng cứu, sao lưu, phục hồi dữ liệu. Điều quan trọng là mỗi đơn vị phải biết ai chịu trách nhiệm, cần làm gì trước, trong và sau sự cố.

Tôi mong sau lớp tập huấn, mỗi bệnh viện trả lời được ba câu hỏi: còn nguy cơ nào chưa được kiểm soát và yêu cầu pháp luật nào cần hoàn thiện; nếu hệ thống ngừng hoạt động ngay ngày mai thì có phương án tiếp tục phục vụ người bệnh hay chưa; và Giám đốc cần chỉ đạo việc gì, giao ai, phối hợp với ai, kiểm tra kết quả thế nào?

Một hệ thống y tế hiện đại phải có năng lực quản trị tốt, hoạt động an toàn, có khả năng ứng phó rủi ro và duy trì dịch vụ thiết yếu khi xảy ra sự cố. Đầu tư cho an toàn thông tin và phương án duy trì hoạt động không chỉ bảo vệ máy tính hay dữ liệu mà còn bảo vệ bệnh viện, người hành nghề và trước hết là sức khỏe, quyền lợi của người bệnh.

Tôi mong các phòng chuyên môn của Sở, các bệnh viện, Trung tâm và đối tác tiếp tục phối hợp để đưa nội dung tập huấn vào thực tiễn. Xin trân trọng cảm ơn lãnh đạo Sở Y tế, các đại biểu, chuyên gia và các đơn vị tham gia. Kính chúc các đồng chí sức khỏe và lớp tập huấn đạt kết quả thiết thực.

Xin trân trọng cảm ơn!

Phần thứ hai Chuyên đề quản trị và tổ chức thực hiện

Trách nhiệm pháp lý và trách nhiệm của người đứng đầu

Cơ sở pháp lý và phạm vi trách nhiệm

Tại ngày 29/10/2026, khung pháp lý về bảo vệ hệ thống phải đặt trên Luật An ninh mạng số 116/2025/QH15, có hiệu lực từ ngày 01/7/2026, và Nghị định số 331/2026/NĐ-CP, có hiệu lực từ ngày 19/8/2026. Theo Điều 44 của Luật, Luật An toàn thông tin mạng năm 2015 và Luật An ninh mạng năm 2018 đã hết hiệu lực. Các hồ sơ cũ cần được xem xét theo quy định chuyển tiếp, không sao chép nguyên căn cứ cũ cho hồ sơ mới [PL1, PL2].

Bệnh viện cần xác định đúng vai trò chủ quản hệ thống, đơn vị vận hành và các bên liên quan. Chức danh giám đốc bệnh viện không tự động đồng nghĩa với chủ quản của mọi nền tảng dùng tại bệnh viện; đối với nền tảng cấp ngành, trách nhiệm của bệnh viện phải được xác định trong mô hình quản lý và văn bản giao nhiệm vụ. Việc sử dụng dịch vụ thuê ngoài không loại bỏ trách nhiệm của đơn vị đối với dữ liệu và hoạt động thuộc phạm vi mình quản lý.

Đối với thông tin người bệnh, khoản 2 Điều 10 và Điều 69 Luật Khám bệnh, chữa bệnh quy định quyền giữ bí mật và việc lưu giữ, khai thác hồ sơ bệnh án. Luật Bảo vệ dữ liệu cá nhân số 91/2025/QH15 và Nghị định số 356/2025/NĐ-CP là căn cứ bổ sung cần áp dụng đồng thời. Cơ sở y tế phải tổ chức xử lý dữ liệu hợp pháp và bảo vệ dữ liệu trong suốt quá trình sử dụng [PL3–PL5].

Theo chức năng quản lý nhà nước được giao tại Quyết định số 5066/QĐ-UBND ngày 09/10/2025, Sở Y tế hướng dẫn, tổ chức thực hiện và kiểm tra các nội dung thuộc lĩnh vực quản lý; các nội dung thuộc cơ quan chuyên trách được phối hợp theo thẩm quyền. Bệnh viện phải duy trì được đầu mối tiếp nhận chỉ đạo và giải quyết vướng mắc [PL9].

Trách nhiệm của bệnh viện và người đứng đầu

Trước hết, người đứng đầu bệnh viện phải tổ chức phân công trách nhiệm rõ ràng đối với các hệ thống thông tin và dữ liệu do đơn vị quản lý. Trách nhiệm này bao gồm việc chỉ đạo xây dựng quy chế nội bộ, bố trí đầu mối, xem xét nguồn lực, tổ chức kiểm tra việc thực hiện và xử lý các tồn tại được phát hiện. Việc thuê phần mềm, hạ tầng hoặc dịch vụ kỹ thuật không làm mất đi trách nhiệm quản lý của bệnh viện đối với hoạt động và dữ liệu thuộc phạm vi của mình.

Bệnh viện cần lập danh mục hệ thống, xác định chủ quản và đơn vị vận hành, loại dữ liệu, kết nối bên ngoài và nhà cung cấp. Trên cơ sở đó, phối hợp thực hiện việc đề xuất, thẩm định, phê duyệt cấp độ theo đúng trường hợp áp dụng; tổ chức triển khai và kiểm tra các biện pháp đã được phê duyệt [PL2]. Minh chứng quản trị nên bao gồm cả hồ sơ pháp lý lẫn kết quả vận hành thực tế.

Thứ ba, đối với dữ liệu cá nhân, bệnh viện cần quy định ai được tiếp cận thông tin, phục vụ mục đích nào, được phép chia sẻ cho ai và theo quy trình nào. Việc cấp tài khoản phải gắn với nhiệm vụ; thay đổi vị trí công tác hoặc chấm dứt hợp đồng phải kéo theo rà soát quyền truy cập. Hoạt động khai thác dữ liệu, đặc biệt dữ liệu bệnh án và thông tin sức khỏe, cần có cơ chế ghi nhận và kiểm tra phù hợp. Không được sử dụng dữ liệu bệnh nhân cho mục đích ngoài phạm vi được phép chỉ vì hệ thống kỹ thuật cho phép truy cập.

Thứ tư, các hợp đồng với đơn vị cung cấp phần mềm, lưu trữ, bảo trì và hỗ trợ kỹ thuật phải làm rõ trách nhiệm bảo mật, phạm vi truy cập, xử lý sự cố, bàn giao dữ liệu và hỗ trợ khôi phục. Khi nhà cung cấp có quyền truy cập từ xa, bệnh viện cần có cơ chế cấp phép, giám sát và thu hồi quyền truy cập. Đây là nội dung quản trị hợp đồng và quản trị rủi ro, không chỉ là vấn đề cấu hình kỹ thuật.

Trách nhiệm khi xảy ra sự cố

Một sự cố mạng tại bệnh viện có thể đồng thời ảnh hưởng đến bảo mật thông tin, khả năng truy cập bệnh án, hoạt động cấp cứu, điều trị và quyền lợi của người bệnh. Vì vậy, bệnh viện phải có cơ chế phát hiện, báo cáo, chỉ huy và phối hợp xử lý sự cố; xác định đầu mối tiếp nhận, người quyết định kích hoạt phương án dự phòng và kênh thông tin đến các khoa, phòng. Các nghĩa vụ thông báo, báo cáo đến cơ quan có thẩm quyền phải thực hiện theo loại sự cố và quy định pháp luật tương ứng.

Khi có dấu hiệu lộ lọt dữ liệu, đơn vị cần kịp thời bảo toàn thông tin, ghi nhận thời điểm phát hiện, phạm vi hệ thống ảnh hưởng, loại dữ liệu liên quan và các biện pháp đã áp dụng. Không nên tự kết luận nguyên nhân khi chưa có căn cứ; cũng không được trì hoãn các biện pháp bảo vệ cần thiết trong khi chờ kết quả xác minh. Việc cung cấp thông tin ra bên ngoài phải thống nhất đầu mối, bảo đảm đúng thẩm quyền và không làm lộ thêm dữ liệu cá nhân.

Đối với tình huống hệ thống dừng hoạt động, bệnh viện phải ưu tiên duy trì hoạt động khám bệnh, chữa bệnh an toàn. Các khoa cần có quy trình dự phòng cho tiếp đón, nhận diện người bệnh, chỉ định, kết quả xét nghiệm, cấp phát thuốc và lưu trữ thông tin. Khi hệ thống được phục hồi, cần đối chiếu, nhập bổ sung và kiểm tra tính nhất quán của dữ liệu để hạn chế sai sót chuyên môn. Nội dung kỹ thuật của phương án sẽ được các báo cáo viên chuyên môn trao đổi trong các phần tiếp theo.

Yêu cầu về tổ chức thực hiện và chế độ thông tin, báo cáo

Các bệnh viện cần sau lớp tập huấn tổ chức rà soát các văn bản quản lý nội bộ, phân công trách nhiệm, danh mục hệ thống và hồ sơ pháp lý liên quan; kiểm tra việc thực hiện bảo vệ dữ liệu cá nhân; rà soát hợp đồng với nhà cung cấp và phương án tiếp nhận, xử lý, báo cáo sự cố. Những nội dung còn thiếu cần được lập thành kế hoạch khắc phục, nêu rõ đầu mối, sản phẩm phải hoàn thành, thời hạn và nguồn lực. Các mốc thời gian cụ thể sẽ thực hiện theo chỉ đạo của Sở Y tế và quy định có liên quan, không tự đặt thành thời hạn pháp luật.

Về chế độ thông tin, bệnh viện cần báo cáo trung thực tình trạng thực hiện và khó khăn phát sinh, phân biệt rõ nội dung đã hoàn thành, đang triển khai và chưa có đủ điều kiện thực hiện. Đối với sự cố, thông tin ban đầu cần được chuyển nhanh qua đầu mối đã xác định; báo cáo tiếp theo phải cập nhật diễn biến, ảnh hưởng và kết quả xử lý. Trường hợp cần phối hợp với cơ quan chuyên môn hoặc nhà cung cấp, đơn vị phải chủ động liên hệ, lưu vết yêu cầu và theo dõi đến khi có kết quả.

Văn phòng Sở, trong phạm vi nhiệm vụ được lãnh đạo Sở phân công, phối hợp tiếp nhận, tổng hợp, tham mưu chuyển xử lý và theo dõi việc thực hiện các chỉ đạo liên quan. Các vấn đề kỹ thuật, chuyên môn khám chữa bệnh, bảo hiểm y tế và kiểm tra chuyên ngành được chuyển đến phòng, cơ quan có thẩm quyền tương ứng. Cách phối hợp này nhằm bảo đảm thông tin thông suốt, không chồng lấn chức năng giữa các đơn vị.

Vai trò của Sở Y tế trong phổ biến pháp luật, hướng dẫn, kiểm tra và đôn đốc thực hiện

Về trách nhiệm quản lý nhà nước, Sở Y tế là cơ quan chuyên môn thuộc Ủy ban nhân dân Thành phố, thực hiện chức năng tham mưu, giúp Ủy ban nhân dân Thành phố quản lý nhà nước về y tế theo phạm vi được giao. Trong đó, việc hướng dẫn cơ sở khám bệnh, chữa bệnh tuân thủ pháp luật, bảo vệ thông tin người bệnh và bảo đảm hoạt động khám bệnh, chữa bệnh an toàn phải được triển khai trong phạm vi thẩm quyền của Sở; các vấn đề thuộc thẩm quyền cơ quan chuyên trách về an ninh mạng, an toàn thông tin được phối hợp, chuyển xử lý theo quy định.

Sở Y tế tổ chức phổ biến, hướng dẫn và đôn đốc thực hiện các quy định liên quan trong phạm vi chức năng được giao. Nội dung cần phù hợp từng nhóm: lãnh đạo nắm trách nhiệm tổ chức; nhân viên chuyên môn nắm cách bảo vệ hồ sơ bệnh án; đầu mối CNTT nắm yêu cầu quản lý hệ thống và phối hợp ứng cứu. Bệnh viện tổ chức phổ biến lại cho khoa, phòng và lưu hồ sơ thực hiện [PL9].

Thứ hai, Sở Y tế hướng dẫn các đơn vị tự rà soát, xác định nội dung phải tuân thủ và những khó khăn cần giải quyết. Nội dung rà soát cần gắn với hồ sơ quản lý hệ thống thông tin, việc phân công trách nhiệm, bảo vệ dữ liệu cá nhân, quản lý nhà cung cấp, phương án ứng cứu sự cố và duy trì hoạt động khám bệnh, chữa bệnh. Sở có thể ban hành hướng dẫn, biểu mẫu tổng hợp, yêu cầu báo cáo theo thẩm quyền; không thay thế trách nhiệm tự tổ chức thực hiện của giám đốc bệnh viện.

Thứ ba, công tác kiểm tra và đôn đốc phải dựa trên kế hoạch, thẩm quyền và sự phân công cụ thể. Sở Y tế tổng hợp kết quả tự rà soát, lựa chọn nội dung cần kiểm tra, phối hợp với cơ quan chuyên môn có thẩm quyền khi cần thiết. Khi kiểm tra, cần đối chiếu hồ sơ với thực tế: hệ thống có được quản lý đúng phương án đã phê duyệt hay không; quyền truy cập có được kiểm soát hay không; phương án dự phòng có khả năng triển khai hay không. Kết quả kiểm tra cần chỉ rõ tồn tại, đơn vị chịu trách nhiệm, thời hạn khắc phục và phương thức báo cáo kết quả; việc xử lý vi phạm chỉ thực hiện theo đúng thẩm quyền, trình tự pháp luật.

Thứ tư, Sở Y tế theo dõi việc khắc phục sau kiểm tra. Đơn vị được yêu cầu khắc phục phải báo cáo bằng kết quả và tài liệu chứng minh, không chỉ báo cáo đã ban hành kế hoạch. Với khó khăn vượt thẩm quyền của bệnh viện, Sở tiếp nhận, tổng hợp và phối hợp với cơ quan liên quan để hướng dẫn giải quyết; những vấn đề vượt thẩm quyền của Sở được báo cáo cấp có thẩm quyền. Việc theo dõi chỉ kết thúc khi đã xác định được kết quả xử lý hoặc có quyết định, hướng dẫn tiếp theo của cơ quan có thẩm quyền.

Đối với Văn phòng Sở, nhiệm vụ phù hợp là tham mưu về công tác phổ biến pháp luật, phối hợp tổng hợp thông tin, theo dõi văn bản chỉ đạo và đôn đốc thực hiện theo phân công của lãnh đạo Sở. Các phòng chuyên môn của Sở chịu trách nhiệm tham mưu nội dung nghiệp vụ thuộc lĩnh vực được giao. Sự phối hợp này bảo đảm một yêu cầu thống nhất: bệnh viện được hướng dẫn rõ việc phải làm, được tiếp nhận và giải quyết vướng mắc, đồng thời chịu trách nhiệm về kết quả thực hiện tại đơn vị.

Kết luận

Bảo đảm an ninh mạng, an toàn thông tin và bảo vệ dữ liệu cá nhân tại bệnh viện là yêu cầu pháp lý gắn trực tiếp với trách nhiệm quản lý, điều hành và chất lượng phục vụ người bệnh. Việc tuân thủ cần được thể hiện bằng quy chế, hồ sơ, phân công, biện pháp thực tế, khả năng xử lý sự cố và kết quả kiểm tra, chứ không chỉ bằng cam kết chung.

Đề nghị lãnh đạo các bệnh viện trực tiếp chỉ đạo rà soát, xác định rõ những việc phải làm và tổ chức khắc phục các tồn tại thuộc trách nhiệm của đơn vị; đồng thời chủ động báo cáo, đề xuất đối với những vấn đề vượt thẩm quyền.

Điều kiện thông báo vi phạm bảo vệ dữ liệu cá nhân

Khoản 1 Điều 23 Luật Bảo vệ dữ liệu cá nhân yêu cầu bên kiểm soát dữ liệu, bên kiểm soát và xử lý dữ liệu, bên thứ ba thông báo cho cơ quan chuyên trách chậm nhất 72 giờ kể từ khi phát hiện vi phạm thuộc các trường hợp gây tổn hại được quy định trong điều này. Bên xử lý dữ liệu phải thông báo kịp thời cho bên kiểm soát hoặc bên kiểm soát và xử lý dữ liệu. Điều 28 Nghị định 356/2025/NĐ-CP quy định việc thông báo theo Mẫu số 08 [PL4, PL5].

Trong tổ chức ứng cứu của bệnh viện, đầu mối pháp chế cần cùng người phụ trách dữ liệu đánh giá nghĩa vụ thông báo ngay khi phát hiện. Việc lập báo cáo ban đầu, bảo vệ người bệnh và khoanh vùng hệ thống được tiến hành đồng thời; không chờ xác định toàn bộ nguyên nhân mới xem xét nghĩa vụ pháp lý. Các yêu cầu báo cáo sự cố mạng và chỉ đạo của cơ quan quản lý cần được kiểm tra riêng theo loại sự cố.

Bảo vệ hệ thống thông tin theo cấp độ và quản trị rủi ro

Yêu cầu quản lý đặt ra đối với bệnh viện

Trong phạm vi chức năng tham mưu về quản lý bảo hiểm y tế và công nghệ thông tin, Chuyên đề tập trung vào hai nhóm vấn đề: thực hiện quy định về an toàn hệ thống thông tin theo cấp độ và bảo đảm an toàn dữ liệu trong quá trình kết nối, liên thông phục vụ khám bệnh, chữa bệnh bảo hiểm y tế.

Trong bệnh viện, hệ thống thông tin phục vụ nhiều khâu liên tiếp: đăng ký khám, tiếp nhận, lập hồ sơ, chỉ định cận lâm sàng, tiếp nhận kết quả, kê đơn, cấp phát thuốc, lưu trữ bệnh án, tổng hợp chi phí và chuyển dữ liệu thanh toán. Các hệ thống có thể do bệnh viện tự vận hành, thuê dịch vụ hoặc kết nối với đơn vị khác. Vì vậy, quản lý an toàn thông tin không thể giới hạn ở việc cài đặt phần mềm bảo vệ trên máy tính; trước hết phải xác định rõ hệ thống nào đang được sử dụng, ai chịu trách nhiệm và mức độ ảnh hưởng khi hệ thống bị gián đoạn.

Yêu cầu của cơ quan quản lý nhà nước là các đơn vị thực hiện đúng quy định pháp luật, tổ chức kiểm tra và lưu giữ được hồ sơ, bằng chứng thực hiện. Bệnh viện phải biết tình trạng tuân thủ của mình, những nguy cơ còn tồn tại và biện pháp khắc phục. Nội dung chuyên đề không thay thế hoạt động thẩm định, phê duyệt cấp độ hoặc đánh giá chuyên môn kỹ thuật theo thẩm quyền.

Hệ thống văn bản cần đối chiếu khi tổ chức thực hiện

Căn cứ trung tâm về phân loại và bảo vệ hệ thống tại thời điểm lớp tập huấn là Điều 9, Điều 10 Luật An ninh mạng số 116/2025/QH15 và Nghị định số 331/2026/NĐ-CP. Nghị định quy định tiêu chí, thủ tục, thẩm quyền và trách nhiệm liên quan đến cấp độ. Khi rà soát hồ sơ, cần phân biệt hồ sơ mới với hệ thống đã có cấp độ hoặc đang đầu tư trước ngày 01/7/2026 thuộc diện chuyển tiếp [PL1, PL2].

Ngoài cấp độ hệ thống, đơn vị cần đối chiếu các quy định về hồ sơ bệnh án, bảo vệ dữ liệu cá nhân và bệnh án điện tử. Nghĩa vụ bảo vệ thông tin và nghĩa vụ duy trì phục vụ người bệnh cần được thực hiện đồng thời [PL3–PL7].

Việc xác định phạm vi cần phản ánh đúng chức năng, cấu trúc, luồng dữ liệu và quan hệ phụ thuộc của hệ thống. Một bệnh viện có thể khai thác nhiều hệ thống với chủ quản và cấp độ khác nhau. Các thành phần liên thông không được tách hình thức để giảm yêu cầu bảo vệ; đồng thời không gộp tùy tiện toàn bộ thiết bị vào một hồ sơ thiếu căn cứ [PL2].

Công việc thứ nhất kiểm kê và phân loại hệ thống thông tin

Các bệnh viện cần bắt đầu bằng danh mục hệ thống thông tin thực tế đang khai thác. Danh mục cần thể hiện tên hệ thống, chức năng, bộ phận sử dụng, đơn vị quản lý và vận hành, dữ liệu xử lý, các kết nối chính, hình thức triển khai và đầu mối phụ trách. Ngoài các hệ thống quản lý bệnh viện, xét nghiệm, chẩn đoán hình ảnh và bệnh án điện tử, cần xem xét hệ thống cổng thông tin, thư điện tử, hạ tầng mạng, máy chủ, lưu trữ, sao lưu và các hệ thống liên quan khác theo phạm vi áp dụng.

Việc kiểm kê phải đi kèm xác định những khâu chuyên môn phụ thuộc vào hệ thống. Ví dụ, khi hệ thống quản lý xét nghiệm không sử dụng được, bệnh viện phải biết khoa nào không nhận được kết quả, quy trình thông báo kết quả khẩn thực hiện bằng cách nào và ai xác nhận việc bàn giao. Đây là cơ sở để phân tích mức độ ảnh hưởng và ưu tiên bảo vệ, chứ không chỉ là danh sách thiết bị.

Sau kiểm kê, bệnh viện xác định hệ thống thuộc phạm vi quản lý của mình và phối hợp với chủ quản hệ thống để thực hiện việc đề xuất, thẩm định, phê duyệt cấp độ theo đúng trình tự, thẩm quyền. Cấp độ phải căn cứ tiêu chí pháp luật và tính chất hệ thống; không tự ấn định cấp độ chỉ dựa vào tên gọi HIS, LIS, PACS hoặc bệnh án điện tử. Đối với hệ thống chưa có hồ sơ cần thiết, đơn vị phải xác định nguyên nhân, trách nhiệm và lộ trình hoàn thiện.

Công việc thứ hai hồ sơ cấp độ phải đi liền với biện pháp bảo vệ

Một nội dung cần được kiểm tra là tính thống nhất giữa hồ sơ đề xuất cấp độ, quyết định phê duyệt, phương án bảo đảm an toàn và thực tế triển khai. Hồ sơ đã được phê duyệt không có nghĩa là các biện pháp đã được thực hiện đầy đủ. Cần đối chiếu các yêu cầu áp dụng với cấu hình, quy trình vận hành, phân công nhân sự, công tác kiểm tra và hồ sơ ghi nhận kết quả.

Đề nghị mỗi bệnh viện chuẩn bị được bộ hồ sơ để xuất trình khi cơ quan có thẩm quyền kiểm tra: danh mục hệ thống; hồ sơ xác định cấp độ và văn bản phê duyệt theo diện áp dụng; phương án bảo đảm an toàn; quy chế vận hành; kế hoạch kiểm tra, đánh giá; kết quả rà soát và biện pháp khắc phục. Với nội dung chưa đáp ứng, cần có danh mục tồn tại và người chịu trách nhiệm xử lý.

Cần phân biệt ba việc: xây dựng hồ sơ, được phê duyệt theo thẩm quyền và tổ chức triển khai biện pháp bảo vệ. Ba việc có liên hệ nhưng không thay thế nhau. Khi báo cáo kết quả, bệnh viện cần nêu rõ đã hoàn thành đến bước nào, có tài liệu chứng minh gì và nội dung nào còn phải thực hiện.

Công việc thứ ba kiểm soát tài khoản, quyền truy cập và dữ liệu người bệnh

Dữ liệu sức khỏe là thông tin cần được bảo vệ nghiêm ngặt. Đề nghị rà soát toàn bộ quy trình tạo, cấp, thay đổi và thu hồi tài khoản. Mỗi nhóm người sử dụng chỉ được tiếp cận thông tin phù hợp nhiệm vụ;

phải có cơ chế quản lý tài khoản quản trị, tài khoản dùng chung nếu còn tồn tại, tài khoản nhân viên đã chuyển công tác và quyền truy cập từ xa của đơn vị cung cấp dịch vụ.

Khi bác sĩ, điều dưỡng, nhân viên tiếp đón, kế toán hoặc nhân viên công nghệ thông tin cùng làm việc trên một hệ thống, trách nhiệm của từng nhóm không giống nhau. Vì vậy, phân quyền phải dựa trên chức năng thực tế, đồng thời lưu được dấu vết cần thiết để xác định ai đã xem, cập nhật hoặc thay đổi dữ liệu theo yêu cầu áp dụng. Các hoạt động truy cập bất thường cần có đầu mối tiếp nhận, kiểm tra và xử lý.

Bệnh viện cần xem xét cơ sở pháp lý của việc thu thập, sử dụng và chia sẻ dữ liệu, mục đích xử lý, thời hạn lưu trữ, trách nhiệm bảo mật và việc chuyển giao dữ liệu cho bên thứ ba. Việc ký hợp đồng với doanh nghiệp cung cấp phần mềm không làm mất đi trách nhiệm của bệnh viện đối với dữ liệu thuộc phạm vi quản lý. Các điều khoản hợp đồng cần làm rõ quyền truy cập, phạm vi xử lý dữ liệu, nghĩa vụ bảo mật, thông báo sự cố, bàn giao và xóa hoặc hoàn trả dữ liệu khi chấm dứt dịch vụ theo quy định.

Công việc thứ tư ứng cứu sự cố và duy trì khám chữa bệnh

Một hệ thống có thể bị gián đoạn do lỗi kỹ thuật, mất điện, mất kết nối, thao tác sai hoặc sự cố an toàn thông tin. Điều quan trọng với Giám đốc bệnh viện là phải có phương án chỉ huy, phối hợp và duy trì các hoạt động thiết yếu. Bộ phận công nghệ thông tin xử lý hệ thống, nhưng các khoa, phòng chuyên môn chịu trách nhiệm thực hiện quy trình khám chữa bệnh an toàn trong thời gian gián đoạn.

Đề nghị bệnh viện xây dựng kịch bản tối thiểu cho trường hợp không truy cập được hồ sơ bệnh án, không nhận được kết quả xét nghiệm điện tử, không truyền được đơn thuốc hoặc không gửi được dữ liệu phục vụ thanh toán. Kịch bản phải xác định ai ra quyết định kích hoạt, bộ phận nào được thông báo, biểu mẫu dự phòng nào được sử dụng, cách xác nhận danh tính người bệnh, kiểm tra y lệnh, cấp phát thuốc và bàn giao giữa các ca trực.

Khi hệ thống hoạt động trở lại, không chỉ khôi phục máy chủ mà còn phải kiểm tra tính toàn vẹn và đối chiếu dữ liệu phát sinh trong thời gian xử lý thủ công. Phải có đầu mối kiểm tra để tránh nhập thiếu, nhập trùng hoặc ghi nhận sai thông tin chuyên môn. Nội dung diễn tập cần có biên bản, đánh giá điểm chưa đạt và phương án điều chỉnh. Tần suất và hình thức thực hiện căn cứ quy định áp dụng, mức độ rủi ro và kế hoạch của đơn vị.

Công việc thứ năm sao lưu, thử phục hồi và quản lý nhà cung cấp

Việc có bản sao lưu không đồng nghĩa với việc chắc chắn khôi phục được dữ liệu. Đề nghị bệnh viện kiểm tra danh mục dữ liệu cần sao lưu, lịch sao lưu, nơi lưu giữ, quyền truy cập, cơ chế bảo vệ bản sao và quy trình phục hồi. Cần tổ chức thử khôi phục trong điều kiện phù hợp, ghi nhận kết quả, thời gian cần thiết và những vấn đề phát hiện để khắc phục.

Đối với dịch vụ thuê ngoài, bệnh viện cần xác định trong hợp đồng trách nhiệm bảo vệ hệ thống, quản lý truy cập từ xa, phối hợp ứng cứu, hỗ trợ khôi phục, bảo mật dữ liệu, chế độ báo cáo và bàn giao khi kết thúc hợp đồng. Khi có sự cố, phải biết rõ số điện thoại hoặc kênh liên hệ, người có thẩm quyền yêu cầu hỗ trợ và cách ghi nhận quá trình xử lý.

Đề nghị Giám đốc bệnh viện định kỳ xem xét báo cáo về các nguy cơ trọng yếu và khả năng phục hồi hoạt động. Những vấn đề cần kinh phí phải được tổng hợp trong kế hoạch của đơn vị theo quy định; không nhất thiết mọi bệnh viện phải mua cùng một sản phẩm, nhưng đều phải chứng minh được biện pháp bảo vệ tương ứng với nghĩa vụ và rủi ro của mình.

Trách nhiệm của người đứng đầu và yêu cầu sau hội nghị

Trách nhiệm quản lý của Giám đốc bệnh viện thể hiện ở việc tổ chức thực hiện: giao đầu mối, phân công nhiệm vụ, ban hành hoặc chỉ đạo ban hành quy trình thuộc thẩm quyền, bố trí nguồn lực, kiểm tra kết quả và xử lý tồn tại. Giám đốc không cần trực tiếp thực hiện cấu hình kỹ thuật, nhưng cần biết hệ thống trọng yếu nào chưa đáp ứng yêu cầu, phương án dự phòng có hoạt động được hay không và ai chịu trách nhiệm khi xảy ra sự cố.

Các bệnh viện cần sau tập huấn tổ chức rà soát theo năm nhóm: hệ thống và cấp độ; tài khoản và dữ liệu; sao lưu và khôi phục; ứng cứu và duy trì khám chữa bệnh; hợp đồng, nhân sự và kiểm tra nội bộ. Mỗi nội dung cần ghi tình trạng, hồ sơ chứng minh, điểm chưa đáp ứng, biện pháp xử lý và người phụ trách.

Việc tổng hợp, báo cáo và hướng dẫn tiếp theo sẽ thực hiện theo chỉ đạo của lãnh đạo Sở Y tế và chức năng, nhiệm vụ của các đơn vị liên quan. Đối với các vấn đề vượt thẩm quyền, bệnh viện cần báo cáo đúng đầu mối để được hướng dẫn. Mục tiêu là nâng cao khả năng tuân thủ và quản trị rủi ro trên cơ sở kiểm tra được, không dừng ở việc nghe phổ biến quy định.

Làm rõ cấp độ và mức ưu tiên lâm sàng

Cấp độ pháp lý của hệ thống và mức ưu tiên phục hồi chuyên môn là hai thông tin cần quản lý song song. Cấp độ được xác định theo pháp luật; thứ tự phục hồi còn phụ thuộc nguy cơ đối với người bệnh và quan hệ giữa các dịch vụ. Bệnh viện cần đánh giá cả trường hợp dữ liệu vẫn còn nhưng không truy cập được và trường hợp hệ thống vẫn chạy nhưng dữ liệu đã bị sửa hoặc lộ.

Tình huống cần phân tích	Dữ liệu cần kiểm chứng	Đầu ra quản lý
Hệ thống đồng thời đáp ứng tiêu chí ở nhiều cấp độ	Phạm vi và các tiêu chí tại Nghị định 331/2026/NĐ-CP	Chọn cấp độ cao nhất trong các tiêu chí cùng đáp ứng theo khoản 2 Điều 8
Hệ thống đã có quyết định cấp độ trước ngày 01/7/2026	Quyết định, phạm vi cũ và hiện trạng thay đổi	Xác định trường hợp giữ cấp độ, cập nhật biện pháp hoặc phải xác định lại
HIS không sử dụng được nhưng máy xét nghiệm còn hoạt động	Luồng chỉ định, nhận diện mẫu, thông báo kết quả nguy cấp	Quy trình bàn giao thủ công và thứ tự khôi phục các dịch vụ phụ thuộc
Thuê máy chủ hoặc phần mềm của doanh nghiệp	Chủ quản, đơn vị vận hành, quyền truy cập và hợp đồng	Bảng trách nhiệm chung và quy trình phối hợp xử lý sự cố

Điểm kiểm tra sau chuyên đề: lãnh đạo đơn vị phải chỉ ra được phạm vi từng hệ thống, người chịu trách nhiệm, hồ sơ cấp độ hiện có, các biện pháp còn thiếu và bằng chứng vận hành cần kiểm chứng. Việc ghi đơn giản “đã thuê bảo mật” không đủ để quản trị các nội dung này.

Duy trì khám chữa bệnh và bảo đảm an toàn người bệnh khi có sự cố

Trách nhiệm quản lý nhà nước về chuyên môn khám bệnh, chữa bệnh

Sở Y tế thực hiện quản lý nhà nước về khám bệnh, chữa bệnh theo chức năng được giao. Tại bệnh viện, bộ phận kế hoạch tổng hợp, quản lý chất lượng, điều dưỡng và các khoa chuyên môn phải cùng tham gia xây dựng phương án khi hệ thống số gián đoạn. Mục tiêu là duy trì chăm sóc an toàn và bảo vệ quyền của người bệnh, đồng thời tổ chức xử lý kỹ thuật [PL3, PL9].

Trong chuyên đề này, yêu cầu quản lý nhà nước được đặt từ phía người bệnh: khi hệ thống thông tin gặp sự cố, người dân vẫn phải được tiếp cận sơ cứu, cấp cứu và các dịch vụ khám chữa bệnh cần thiết một cách kịp thời, an toàn; được giải thích rõ tình trạng phục vụ và được bảo vệ thông tin sức khỏe. Sự cố kỹ thuật không được trở thành lý do để bệnh viện buông lỏng trách nhiệm chuyên môn hoặc để người bệnh tự xoay xở giữa các khoa, phòng.

Các nghĩa vụ tổ chức sơ cứu, cấp cứu, khám chữa bệnh, thực hiện quy định chuyên môn và bảo vệ quyền người bệnh theo Luật Khám bệnh, chữa bệnh vẫn phải được thực hiện khi sử dụng quy trình dự phòng. Hồ sơ phát sinh cần được ghi nhận, đối chiếu và lưu giữ đúng quy định [PL3].

Yêu cầu các bệnh viện chủ động bảo đảm hoạt động chuyên môn

Trước hết, Giám đốc bệnh viện phải chỉ đạo xây dựng và phê duyệt phương án duy trì khám bệnh, chữa bệnh khi hệ thống thông tin bị gián đoạn, phù hợp với cơ cấu tổ chức và phạm vi hoạt động của đơn vị. Phương án cần xác định người chỉ huy, người thay thế, đầu mối liên lạc, điều kiện kích hoạt, thứ tự ưu tiên và trách nhiệm từng khoa, phòng. Đây là biện pháp tổ chức thực hiện nghĩa vụ bảo đảm khám chữa bệnh an toàn, không phải một thủ tục cấp phép mới.

Tại khoa Khám bệnh và khoa Cấp cứu, phải có quy trình tiếp nhận dự phòng, nhận diện đúng người bệnh, phân loại ưu tiên, ghi nhận thời điểm tiếp nhận và chuyển giao thông tin cho bộ phận chuyên môn. Không để người bệnh cấp cứu phải chờ khôi phục phần mềm mới được đánh giá, xử trí. Với người bệnh ngoại trú, bệnh viện cần công khai hướng dẫn tại nơi tiếp đón, tổ chức phân luồng và giải thích thời gian chờ, không để người bệnh đi lại nhiều lần chỉ vì sự cố nội bộ.

Tại khoa lâm sàng, cần có biểu mẫu dự phòng để ghi chép diễn biến, chỉ định, y lệnh, thực hiện thuốc, theo dõi và bàn giao ca. Trước khi thực hiện can thiệp, nhân viên y tế phải kiểm tra danh tính, thông tin dị ứng, chỉ định và các yếu tố nguy cơ bằng những nguồn thông tin đáng tin cậy còn sẵn có. Trường hợp không đủ thông tin để thực hiện một kỹ thuật không cấp cứu an toàn, người có thẩm quyền chuyên môn phải đánh giá, quyết định và giải thích phù hợp cho người bệnh.

Tại khoa Xét nghiệm, Chẩn đoán hình ảnh, Dược và các bộ phận hỗ trợ, phải xác định cách tiếp nhận chỉ định, gắn mã hoặc nhận diện mẫu, thông báo kết quả quan trọng, cấp phát thuốc và đối chiếu chứng từ trong thời gian hệ thống gián đoạn. Những bước kiểm tra nhằm tránh nhầm người bệnh, nhầm mẫu, nhầm thuốc hoặc bỏ sót kết quả bất thường phải được duy trì.

Trách nhiệm của người đứng đầu và bảo vệ quyền lợi người bệnh

Giám đốc bệnh viện chịu trách nhiệm tổ chức hoạt động khám bệnh, chữa bệnh của đơn vị theo pháp luật; không thể giao toàn bộ trách nhiệm duy trì hoạt động cho phòng công nghệ thông tin hoặc nhà

cung cấp phần mềm. Lãnh đạo bệnh viện phải biết các khâu chuyên môn nào có thể dừng, khâu nào bắt buộc duy trì; ai có quyền quyết định điều chỉnh luồng người bệnh, huy động nhân lực hoặc chuyển tuyến khi vượt khả năng đáp ứng.

Bệnh viện cần thông tin kịp thời, dễ hiểu cho người bệnh và người nhà về việc thay đổi quy trình, thời gian chờ và đầu mối giải quyết vướng mắc. Việc thông báo phải tránh công bố dữ liệu cá nhân hoặc thông tin sức khỏe không cần thiết. Cơ sở phải có cơ chế tiếp nhận phản ánh của người dân trong thời gian sự cố; xử lý ngay những trường hợp có nguy cơ ảnh hưởng đến tính mạng, sức khỏe hoặc quyền được khám chữa bệnh.

Khi hệ thống phục hồi, không được mặc nhiên coi hoạt động đã trở lại bình thường. Các khoa, phòng phải đối chiếu hồ sơ giấy và dữ liệu điện tử, kiểm tra y lệnh, kết quả xét nghiệm, thuốc đã cấp, thủ thuật đã thực hiện và thông tin bàn giao; phân công người kiểm tra trước khi cập nhật bổ sung. Việc cập nhật, lưu trữ và bảo vệ hồ sơ bệnh án phải phù hợp Điều 69 Luật Khám bệnh, chữa bệnh và các quy định liên quan.

Sở y tế hướng dẫn, theo dõi, kiểm tra và đôn đốc thực hiện

Trên cơ sở chức năng quản lý nhà nước được giao, Phòng Nghiệp vụ Y tham mưu Sở Y tế hướng dẫn các cơ sở rà soát nguy cơ gián đoạn hoạt động chuyên môn, xây dựng phương án dự phòng, phân công trách nhiệm và tổ chức thực hành tình huống. Việc hướng dẫn phải dựa trên yêu cầu chuyên môn và an toàn người bệnh, có tính đến sự khác nhau giữa bệnh viện đa khoa, chuyên khoa, quy mô giường bệnh và mức độ ứng dụng công nghệ thông tin.

Sở Y tế cần yêu cầu các bệnh viện thuộc phạm vi quản lý báo cáo kết quả rà soát theo nội dung thống nhất: phương án đã được ban hành hay chưa; khoa, phòng nào đã có quy trình dự phòng; ai chịu trách nhiệm kích hoạt; cách duy trì cấp cứu, điều trị, xét nghiệm, cấp phát thuốc; phương án thông tin cho người bệnh; kết quả diễn tập và các tồn tại cần khắc phục. Đây là đề xuất nội dung chỉ đạo, triển khai bằng văn bản của cấp có thẩm quyền, không phải chế độ báo cáo mới đã được pháp luật ấn định.

Đối với đơn vị chưa có phương án hoặc phương án không thể vận hành trên thực tế, Sở Y tế theo thẩm quyền hướng dẫn, đôn đốc khắc phục, xác định mốc hoàn thành và theo dõi kết quả. Khi phát hiện dấu hiệu vi phạm quy định chuyên môn hoặc ảnh hưởng quyền lợi người bệnh, Phòng Nghiệp vụ Y tổng hợp, báo cáo lãnh đạo Sở để xem xét chỉ đạo kiểm tra, phối hợp Phòng Kiểm tra lĩnh vực Y tế và các cơ quan có thẩm quyền theo đúng phân công. Phòng Nghiệp vụ Y không tự nhận thẩm quyền xử phạt hoặc thanh tra ngoài nhiệm vụ được giao.

Nếu sự cố phát sinh từ hạ tầng, phần mềm hoặc kết nối ngoài khả năng xử lý của bệnh viện, đơn vị vẫn phải bảo đảm hoạt động chuyên môn trong khả năng cho phép, lưu nhận diễn biến sự cố và phối hợp với Phòng Quản lý Bảo hiểm y tế và Công nghệ thông tin, nhà cung cấp và cơ quan liên quan. Việc chưa xác định được bên gây lỗi không phải căn cứ để ngừng chăm sóc người bệnh; các vướng mắc vượt thẩm quyền cần báo cáo Sở để phối hợp giải quyết.

Các tình huống rủi ro chuyên môn và yêu cầu dự phòng

Những tình huống sau đây là ví dụ giả định để các bệnh viện tự đánh giá khả năng ứng phó, không phải kết luận về sự cố đã xảy ra tại một cơ sở cụ thể. Ngay cả khi đã thực hiện đầy đủ các biện pháp an

toàn thông tin, bệnh viện vẫn phải dự liệu nguy cơ mất điện, lỗi phần mềm, lỗi đường truyền, hỏng thiết bị, sai lệch dữ liệu hoặc sự cố từ nhà cung cấp.

Thứ nhất, đối với hệ thống quản lý bệnh viện HIS. Nếu HIS ngừng hoạt động vào giờ cao điểm, việc tiếp đón, xác minh người bệnh, xem lịch sử khám, chỉ định và cấp phát thuốc có thể bị gián đoạn. Nếu nhân viên sử dụng thông tin ghi tay nhưng không có quy trình kiểm tra hai yếu tố nhận diện, có thể phát sinh nhầm người bệnh hoặc nhầm chỉ định. Bệnh viện cần quy định rõ thời điểm chuyển sang chế độ dự phòng, bộ biểu mẫu sử dụng, người duyệt chỉ định, cách đối chiếu thuốc và trách nhiệm nhập bù, kiểm tra trùng lặp sau khi hệ thống phục hồi. Không được để người bệnh cấp cứu phải chờ hệ thống hoạt động trở lại mới được đánh giá và xử trí.

Thứ hai, đối với xét nghiệm và chẩn đoán hình ảnh. Khi LIS, RIS hoặc PACS không nhận được chỉ định hoặc không trả được kết quả, mẫu bệnh phẩm có nguy cơ không được theo dõi đầy đủ, kết quả có thể đến chậm hoặc bị gắn sai hồ sơ nếu khâu nhận diện thủ công không chặt chẽ. Đặc biệt, các kết quả nguy cấp phải có kênh thông báo trực tiếp, ghi nhận người nhận, thời điểm nhận và xác nhận đã xử trí; không phụ thuộc duy nhất vào thông báo tự động. Các khoa phải thống nhất quy trình cấp mã, bàn giao mẫu, trả kết quả có xác nhận và đối chiếu dữ liệu sau sự cố.

Thứ ba, đối với khám chữa bệnh từ xa (telehealth). Khi mất đường truyền, âm thanh hoặc hình ảnh không bảo đảm chất lượng, bác sĩ có thể không thu thập được đầy đủ dấu hiệu lâm sàng hoặc không tiếp cận được kết quả cận lâm sàng. Bệnh viện phải có tiêu chí tạm dừng hội chẩn hoặc khám từ xa khi điều kiện kỹ thuật không đáp ứng, phương thức liên lạc thay thế bảo đảm bảo mật phù hợp, đầu mối hỗ trợ tại cơ sở đang có người bệnh và phương án chuyển sang thăm khám trực tiếp hoặc chuyển tuyến khi cần. Không tiếp tục đưa ra quyết định chuyên môn chỉ dựa trên dữ liệu thiếu hoặc không xác thực.

Thứ tư, đối với các công cụ trí tuệ nhân tạo hỗ trợ chẩn đoán, cảnh báo nguy cơ hoặc gợi ý điều trị. Dữ liệu đầu vào thiếu, sai hoặc không được cập nhật có thể làm cho kết quả gợi ý không phù hợp; hệ thống có thể ngừng hoạt động hoặc cho kết quả khác với đánh giá lâm sàng. Vì vậy, bệnh viện cần xác định rõ phạm vi sử dụng, người chịu trách nhiệm thẩm định kết quả, cơ chế kiểm tra độc lập đối với quyết định có nguy cơ cao, quy trình ngừng sử dụng công cụ khi có dấu hiệu bất thường và phương án thực hành chuyên môn không phụ thuộc vào AI. AI là công cụ hỗ trợ trong phạm vi được phép; không thay thế trách nhiệm chuyên môn của người hành nghề.

Từ các tình huống trên, yêu cầu đặt ra không chỉ là có bản sao lưu dữ liệu hoặc hợp đồng bảo trì. Mỗi bệnh viện cần lập danh mục các quy trình khám chữa bệnh phụ thuộc hệ thống số; xác định mức gián đoạn có thể chấp nhận về mặt chuyên môn, thứ tự ưu tiên khôi phục, nguồn lực dự phòng và người ra quyết định. Phương án phải được tập huấn cho ca trực, thực hành tình huống và cập nhật sau mỗi lần thử nghiệm hoặc xảy ra sự cố. Việc thử nghiệm phải tránh ảnh hưởng đến người bệnh đang được điều trị.

Phòng Nghiệp vụ Y tham mưu Sở Y tế yêu cầu các bệnh viện thuộc phạm vi quản lý rà soát những nguy cơ nêu trên, hoàn thiện quy trình dự phòng theo đặc thù chuyên môn và báo cáo các vướng mắc vượt thẩm quyền. Khi kiểm tra, đôn đốc, trọng tâm không chỉ là bệnh viện có văn bản hay không, mà là nhân viên có biết thực hiện, người bệnh có tiếp tục được phục vụ an toàn và các sai lệch phát sinh có được phát hiện, khắc phục hay không.

Nội dung cần thực hiện sau tập huấn

Các bệnh viện cần tổ chức họp lãnh đạo và các khoa, phòng liên quan để kiểm tra lại phương án duy trì khám chữa bệnh; hoàn thiện danh mục hoạt động thiết yếu và biểu mẫu dự phòng; giao trách nhiệm cụ thể cho từng đầu mối; thử nghiệm tình huống gián đoạn hệ thống trong ca trực; ghi nhận điểm chưa phù hợp và tổ chức khắc phục. Đơn vị cần lưu bằng chứng triển khai để phục vụ tự đánh giá và công tác quản lý theo thẩm quyền.

Các bộ phận liên quan tổng hợp vấn đề vượt thẩm quyền và báo cáo lãnh đạo đơn vị để đề nghị Sở Y tế hướng dẫn, phối hợp xử lý. Kết quả triển khai cần được kiểm tra bằng thực hành của ca trực và khả năng phục vụ thực tế.

Bảo vệ dữ liệu liên thông và bảo đảm quyền lợi bảo hiểm y tế

Dữ liệu liên thông là một khâu trong quá trình khám chữa bệnh

Chuyên đề tập trung vào yêu cầu bảo vệ dữ liệu khi bệnh viện kết nối và trao đổi thông tin phục vụ quản lý, giám định và thanh toán bảo hiểm y tế. Dữ liệu không hình thành riêng ở bộ phận bảo hiểm y tế mà bắt đầu từ tiếp đón, khám bệnh, chỉ định, thực hiện dịch vụ kỹ thuật, kê đơn, cấp thuốc và tổng hợp chi phí.

Vì vậy, một lỗi định danh, một dữ liệu chuyên môn chưa được xác nhận hoặc một thao tác sửa đổi không được kiểm soát có thể ảnh hưởng đến chất lượng dữ liệu liên thông. Việc quản lý cần đồng thời đáp ứng ba yêu cầu: thông tin đúng với thực tế khám chữa bệnh; quá trình truyền nhận có kiểm soát; và dữ liệu được bảo vệ trong toàn bộ quá trình sử dụng.

Bệnh viện phải thực hiện các quy định hiện hành của Luật Bảo hiểm y tế và văn bản hướng dẫn, Luật Khám bệnh, chữa bệnh, các quy định về dữ liệu điện tử phục vụ giám định, thanh toán BHYT và các quy định về bảo vệ dữ liệu cá nhân. Khi áp dụng biểu mẫu, chuẩn dữ liệu hoặc thời hạn gửi, đơn vị phải đối chiếu quy định và hướng dẫn kỹ thuật đang có hiệu lực của cơ quan có thẩm quyền.

Kiểm soát dữ liệu từ nguồn phát sinh đến khi gửi đi

Khâu thứ nhất là kiểm soát thông tin đầu vào. Bệnh viện cần có quy trình xác thực và đối chiếu thông tin người bệnh, thông tin về quyền lợi BHYT, hồ sơ khám chữa bệnh, mã dịch vụ, thuốc, vật tư và chi phí. Mỗi khoa, phòng chịu trách nhiệm về dữ liệu do mình tạo lập hoặc xác nhận theo chức năng được giao. Bộ phận phụ trách BHYT phối hợp kiểm tra tính đầy đủ, hợp lệ và nhất quán trước khi gửi dữ liệu.

Khâu thứ hai là kiểm soát quyền sửa đổi và phê duyệt. Cần xác định rõ ai được nhập, ai được sửa, ai được xác nhận và ai được truyền dữ liệu. Việc sửa thông tin phải tuân thủ quy trình chuyên môn, nghiệp vụ và lưu được dấu vết theo yêu cầu áp dụng. Không nên để tài khoản chung hoặc quyền quản trị không được kiểm soát trở thành cách xử lý thường xuyên các lỗi dữ liệu.

Khâu thứ ba là kiểm soát quá trình truyền nhận. Bệnh viện cần theo dõi trạng thái gửi, nhận, phản hồi, dữ liệu bị từ chối hoặc chưa được ghi nhận; phân công bộ phận xử lý và đối soát. Đối với lỗi liên quan đến kết nối hoặc hệ thống của bên ngoài, cần lưu chứng cứ kỹ thuật và phối hợp với đầu mối có thẩm quyền để xác minh, tránh suy đoán nguyên nhân.

Bảo vệ quyền lợi người bệnh khi có gián đoạn

Khi hệ thống liên thông hoặc phần mềm của bệnh viện không hoạt động, nhiệm vụ trước hết là tổ chức tiếp nhận và khám chữa bệnh theo quy định chuyên môn, đặc biệt đối với cấp cứu. Việc xử lý hồ sơ và thanh toán BHYT phải căn cứ quy định hiện hành và hướng dẫn của cơ quan có thẩm quyền; không tự đặt thêm điều kiện làm ảnh hưởng quyền lợi hợp pháp của người bệnh.

Các bệnh viện cần xây dựng phương án dự phòng phù hợp, trong đó phân công rõ bộ phận tiếp đón, khoa lâm sàng, phòng tài chính kế toán, bộ phận BHYT và CNTT. Trong thời gian gián đoạn cần ghi nhận thông tin, chứng từ, thời điểm phát sinh và người thực hiện để có cơ sở đối chiếu khi hệ thống được khôi phục. Không được tự ý sử dụng kênh truyền dữ liệu thiếu kiểm soát hoặc chia sẻ thông tin sức khỏe qua các tài khoản cá nhân không phù hợp quy định.

Sau khi hệ thống phục hồi, bệnh viện tổ chức rà soát dữ liệu chưa gửi, dữ liệu gửi lỗi, dữ liệu trùng và các thông tin cần cập nhật. Việc bổ sung phải có người phụ trách và bước kiểm tra, đối chiếu với hồ sơ chuyên môn gốc. Nếu có vướng mắc về thời hạn, quy trình hoặc quyền lợi BHYT, cần tổng hợp tình huống cụ thể, chứng từ liên quan và báo cáo cơ quan có thẩm quyền để được hướng dẫn.

Trách nhiệm phối hợp và nội dung kiểm tra của bệnh viện

Giám đốc bệnh viện cần chỉ đạo cơ chế phối hợp giữa bộ phận BHYT, công nghệ thông tin, tài chính kế toán và các khoa chuyên môn. Bộ phận BHYT không thể tự bảo đảm chất lượng dữ liệu nếu dữ liệu nguồn chưa được kiểm soát; bộ phận CNTT cũng không thể tự quyết định tính đúng đắn của một chỉ định hoặc khoản chi phí. Trách nhiệm phải gắn với từng bước hình thành và sử dụng dữ liệu.

Đề nghị kiểm tra định kỳ ít nhất các nội dung quản lý sau theo kế hoạch đơn vị: quy trình định danh và kiểm tra quyền lợi; phân quyền nhập, sửa, duyệt và gửi dữ liệu; nhật ký truyền nhận; danh sách lỗi và kết quả xử lý; quy trình đối soát; phương án dự phòng khi mất kết nối; và hồ sơ phối hợp với đơn vị cung cấp phần mềm, cơ quan liên quan. Tần suất cụ thể thực hiện theo quy định áp dụng và đánh giá rủi ro của đơn vị.

Kết quả rà soát cần được báo cáo cho lãnh đạo bệnh viện bằng những nội dung có thể kiểm chứng: số lượng và loại lỗi cần xử lý, tình trạng tồn đọng, nguyên nhân đã xác định, biện pháp khắc phục và trách nhiệm thực hiện. Không nên chỉ báo cáo chung rằng hệ thống đang hoạt động ổn định nếu chưa kiểm tra khả năng khôi phục, tính đầy đủ của dữ liệu và việc xử lý lỗi truyền nhận.

Thực hiện hướng dẫn liên thông dữ liệu và xử lý vướng mắc ngoài phạm vi bệnh viện

Liên thông dữ liệu khám bệnh, chữa bệnh bảo hiểm y tế không phải là hoạt động tự nguyện hoặc chỉ thực hiện khi điều kiện kỹ thuật thuận lợi. Đây là yêu cầu thực hiện theo quy định về cung cấp, chuyển dữ liệu điện tử phục vụ quản lý, giám định và thanh toán bảo hiểm y tế. Sở Y tế đã có văn bản hướng dẫn các cơ sở khám bệnh, chữa bệnh triển khai liên thông dữ liệu. Các bệnh viện cần rà soát, thực hiện đầy đủ các yêu cầu tại văn bản của Sở cùng với quy định, chuẩn dữ liệu và hướng dẫn hiện hành của cơ quan có thẩm quyền; không coi việc đã cài đặt phần mềm hoặc đã gửi dữ liệu một lần là hoàn thành trách nhiệm.

Trách nhiệm của bệnh viện là bảo đảm dữ liệu phát sinh từ hoạt động khám bệnh, chữa bệnh được lập đúng, kiểm tra, ký hoặc xác nhận theo quy định, truyền đúng đầu mối, theo dõi kết quả tiếp nhận và

khắc phục các lỗi thuộc phạm vi quản lý. Trách nhiệm này cần được giao cụ thể cho bộ phận chuyên môn, bộ phận bảo hiểm y tế và bộ phận công nghệ thông tin. Người đứng đầu bệnh viện chỉ đạo, kiểm tra tiến độ và xử lý các vướng mắc vượt quá thẩm quyền của từng bộ phận.

Trong thực tế, dữ liệu có thể không liên thông được vì nhiều nguyên nhân khác nhau: thông tin định danh không khớp; mã danh mục, cấu trúc hoặc định dạng dữ liệu chưa phù hợp; hồ sơ chuyên môn chưa hoàn tất; lỗi phần mềm hoặc đường truyền tại bệnh viện; lỗi kết nối, tiếp nhận hoặc phản hồi từ hệ thống bên ngoài; hoặc chưa thống nhất cách xử lý một tình huống nghiệp vụ. Không nên mặc nhiên quy tất cả các lỗi cho bộ phận công nghệ thông tin của bệnh viện, cũng không mặc nhiên cho rằng lỗi thuộc hệ thống bên ngoài khi chưa có căn cứ.

Khi phát sinh vướng mắc, bệnh viện cần xác định rõ lỗi ở khâu nào và có thuộc phạm vi kiểm soát của mình hay không. Hồ sơ xử lý cần ghi nhận thời điểm, mã giao dịch hoặc mã hồ sơ phù hợp, thông báo lỗi, nhật ký truyền nhận, ảnh chụp màn hình khi cần thiết, kết quả kiểm tra tại đơn vị và các lần trao đổi với bên liên quan. Việc cung cấp chứng cứ phải tuân thủ quy định bảo vệ dữ liệu cá nhân, không gửi tràn lan thông tin người bệnh qua kênh không được phép.

Nếu nguyên nhân thuộc bệnh viện hoặc nhà cung cấp phần mềm do bệnh viện thuê, đơn vị phải chủ động khắc phục, yêu cầu nhà cung cấp thực hiện nghĩa vụ theo hợp đồng và kiểm tra lại kết quả. Nếu đã có căn cứ cho thấy nguyên nhân không thuộc phạm vi bệnh viện, cần có văn bản hoặc yêu cầu qua kênh chính thức gửi đúng đầu mối quản lý, vận hành, tiếp nhận dữ liệu hoặc cơ quan bảo hiểm xã hội có liên quan, nêu rõ lỗi, bằng chứng, tác động và nội dung cần phối hợp xử lý. Bệnh viện phải theo dõi, đôn đốc, trao đổi và báo cáo cấp có thẩm quyền khi cần thiết cho đến khi có kết quả xử lý và xác nhận dữ liệu được tiếp nhận, đối soát theo quy định; không dừng ở việc thông báo rằng hệ thống bên ngoài bị lỗi.

Đối với các lỗi kéo dài, ảnh hưởng đến quyền lợi người bệnh hoặc công tác giám định, thanh toán, bệnh viện cần tổng hợp theo từng nhóm nguyên nhân, số hồ sơ bị ảnh hưởng, thời gian tồn đọng, đơn vị đã liên hệ và kết quả xử lý để báo cáo Sở Y tế theo phân cấp và hướng dẫn. Trong thời gian chờ giải quyết, phải tiếp tục bảo đảm khám bệnh, chữa bệnh, lưu giữ chứng từ và xử lý dữ liệu theo phương án hợp pháp được cơ quan có thẩm quyền hướng dẫn. Chỉ kết thúc một vướng mắc khi đã kiểm tra kết quả thực tế, không chỉ khi nhận được phản hồi rằng lỗi đã được sửa.

Kết luận của phần báo cáo

Mục tiêu của quản lý dữ liệu liên thông là bảo đảm thông tin đúng, có kiểm soát, có thể truy vết và không bỏ sót quyền lợi hợp pháp của người bệnh. Kết quả cần được chứng minh bằng hồ sơ nguồn, trạng thái tiếp nhận, biên bản đối soát và danh mục lỗi đã xử lý. Khi thực hiện, đối chiếu Nghị định 188/2025/NĐ-CP, Thông tư 12/2026/TT-BTC và các chuẩn dữ liệu hiện hành theo trường hợp áp dụng [PL8, PL12].

Đơn vị cần duy trì cơ chế phối hợp giữa chuyên môn, BHYT, CNTT, tài chính kế toán và đầu mối bên ngoài. Các vướng mắc kéo dài phải có người theo dõi đến khi dữ liệu được tiếp nhận, đối soát và có kết quả xử lý thực tế.

Phần thứ ba Chuyên đề kỹ thuật và kinh nghiệm thực hành

Đừng để máy tính trở thành bệnh nhân

Chuyên đề biên tập từ đề cương chuẩn bị cho chuyên gia Hà Văn Triệu

Một máy tính trong bệnh viện có thể là điểm truy cập vào hồ sơ bệnh án, chỉ định thuốc, kết quả xét nghiệm, lịch phẫu thuật hoặc dữ liệu thanh toán. Do đó, đánh giá hậu quả của sự cố phải đi từ công việc bị ảnh hưởng và người bệnh đang cần được phục vụ. Một máy chủ đã được khởi động lại chưa đồng nghĩa hoạt động khám chữa bệnh đã an toàn.

Nhận diện các đường xâm nhập thường gặp

Đường thứ nhất là lừa đảo lấy tài khoản. Email có thể giả danh đối tác gửi bảng đối soát BHYT, tài liệu hội nghị, hóa đơn hoặc kết quả xét nghiệm. Người dùng truy cập trang đăng nhập giả hoặc chấp nhận yêu cầu xác thực không do mình khởi tạo. Tài khoản có quyền rộng làm hậu quả lan nhanh. Cách phòng ngừa là kiểm tra nguồn gửi, xác nhận yêu cầu bất thường qua kênh khác, dùng tài khoản riêng và triển khai xác thực đa yếu tố phù hợp.

Đường thứ hai là ứng dụng web và thành phần phần mềm chưa được cập nhật. Một website, cổng đặt lịch hoặc thành phần PHP của sản phẩm bên thứ ba có thể trở thành điểm vào. Mức độ khai thác phụ thuộc phiên bản, cấu hình, quyền và lớp bảo vệ. Rà soát phải bao gồm phần mềm do nhà thầu vận hành, không chỉ máy chủ mà bệnh viện tự quản lý.

Đường thứ ba là kết nối hỗ trợ từ xa. Nếu nhà cung cấp dùng tài khoản chung, duy trì quyền quản trị thường trực hoặc không ghi nhận phiên làm việc, bệnh viện khó xác định ai đã can thiệp và vào thời điểm nào. Cần cấp quyền theo yêu cầu công việc, giới hạn thời gian, có người giám sát và thu hồi quyền sau khi hoàn tất.

Đường thứ tư là thiết bị đầu cuối và thiết bị kết nối mạng. Máy tính dùng chung, USB, phần mềm cài ngoài quy trình, thiết bị cũ và mạng khách không tách biệt đều có thể tạo đường lan truyền. Đối với thiết bị y tế, thay đổi cấu hình, quét hoặc cài phần mềm bảo vệ phải được đánh giá tương thích và phối hợp với đơn vị có trách nhiệm về thiết bị.

Tác động đối với hoạt động y tế

Hệ thống hoặc quy trình	Nguy cơ cần kiểm soát	Chuẩn bị của khoa phòng
HIS và bệnh án điện tử	Không tra cứu được dị ứng, diễn biến, y lệnh; phát sinh hồ sơ trùng	Quy trình nhận diện, ghi nhận thủ công và đối chiếu sau khôi phục
Xét nghiệm	Chỉ định, mẫu và kết quả không khớp; chậm báo kết quả nguy cấp	Sổ bàn giao mẫu; mã nhận diện; kênh báo và xác nhận kết quả
Chẩn đoán hình ảnh	Không truy xuất được ảnh hoặc báo cáo đúng người bệnh	Quy trình tiếp nhận, đọc và trả kết quả dự phòng có kiểm soát

Hệ thống hoặc quy trình	Nguy cơ cần kiểm soát	Chuẩn bị của khoa phòng
Dược	Không nhận được đơn hoặc không đối chiếu được thuốc đã cấp	Phiếu cấp phát dự phòng, kiểm tra và ký nhận theo quy trình
Telehealth và AI	Mất kết nối, đầu vào thiếu hoặc gợi ý sai lệch	Tiêu chí dừng công cụ; đánh giá độc lập của người có trách nhiệm

Sáu hành động đầu tiên khi nghi có sự cố

• Báo đầu mối chỉ huy theo danh bạ ứng cứu; ghi thời điểm phát hiện và mô tả ngắn dấu hiệu quan sát được.

• Đánh giá ảnh hưởng đối với người bệnh và kích hoạt phương án dự phòng ở các khoa liên quan.

• Khoanh vùng thiết bị hoặc tài khoản nghi bị xâm nhập theo phương án đã phê duyệt và hướng dẫn của đội ứng cứu.

• Bảo toàn nhật ký, cảnh báo và dấu vết cần thiết; ghi lại mọi thao tác có thể làm thay đổi hệ thống.

• Thực hiện thông tin, báo cáo qua đúng đầu mối; đánh giá nghĩa vụ thông báo dữ liệu cá nhân và phối hợp cơ quan có thẩm quyền.

• Khôi phục theo thứ tự ưu tiên sau khi đã kiểm tra môi trường, bản sao lưu và dữ liệu; có xác nhận của cả kỹ thuật và chuyên môn.

Nhân viên không tự ý xóa log, cài lại máy chủ, đăng ảnh bệnh án lên nhóm chat hoặc thương lượng với đối tượng tống tiền. Đội kỹ thuật không ngắt đồng loạt hệ thống lâm sàng mà chưa đánh giá tác động, trừ tình huống khẩn cấp đã có quy định và thẩm quyền xử lý. An toàn người bệnh và ngăn chặn tấn công phải được tổ chức đồng thời.

Sáu ưu tiên phòng ngừa tại đơn vị

Bệnh viện cần có danh mục tài sản số; quy trình tiếp nhận và xử lý cảnh báo lỗ hổng; tài khoản và quyền được quản lý; phân vùng mạng theo chức năng; sao lưu được thử phục hồi; diễn tập có khoa chuyên môn tham gia. Các biện pháp phải có người phụ trách và bằng chứng duy trì. Danh mục đầu tư chỉ nên được xây dựng sau khi xác định khoảng trống và yêu cầu cần đáp ứng.

Tại cuộc giao ban quản trị, giám đốc có thể yêu cầu báo cáo ngắn về hệ thống thiết yếu, ba rủi ro đang ưu tiên, tiến độ khắc phục, bản sao lưu đã thử gần nhất và kết quả diễn tập. Một câu trả lời có ngày kiểm tra, người xác nhận và minh chứng sử dụng được giúp lãnh đạo quyết định tốt hơn một báo cáo chung rằng hệ thống đang ổn định.

Tổ chức SOC và giám sát an toàn thông tin trong bệnh viện

Chuyên đề kỹ thuật phục vụ phối hợp giữa bệnh viện và đơn vị cung cấp dịch vụ

SOC là năng lực tổ chức giám sát, phát hiện, phân tích và phối hợp xử lý sự cố. Năng lực này cần con người, quy trình và công cụ; không chỉ là một màn hình cảnh báo. Mô hình tại bệnh viện có thể gồm đầu mối nội bộ kết hợp nhà cung cấp dịch vụ, với phạm vi dữ liệu và trách nhiệm được thống nhất bằng văn bản.

Các chức năng cần hiểu trước khi lựa chọn giải pháp

Thành phần tham chiếu	Chức năng	Minh chứng sử dụng được
SIEM	Thu thập, chuẩn hóa và tương quan nhật ký	Có nguồn log, thời gian đồng bộ và cảnh báo đã kiểm chứng
SOAR	Điều phối quy trình, mở phiếu và tự động hóa có kiểm soát	Có điểm phê duyệt trước thao tác ảnh hưởng dịch vụ lâm sàng
Threat Intelligence	Cập nhật thông tin chỉ dấu và phương thức tấn công	Có quy trình đánh giá, áp dụng và theo dõi hiệu quả quy tắc
Giám sát hạ tầng và dịch vụ	Theo dõi trạng thái máy chủ, mạng, ứng dụng và hàng đợi	Phân biệt được mất dịch vụ với dấu hiệu tấn công để xử lý
DLP	Phát hiện, hạn chế xuất dữ liệu ngoài phạm vi cho phép	Có chính sách dữ liệu, phân quyền và cách xử lý cảnh báo
NAC và quản lý thiết bị	Kiểm soát thiết bị truy cập mạng	Nhận diện được thiết bị và có phương án xử lý thiết bị lạ

Các thành phần trên là chức năng tham chiếu. Một giải pháp có thể đáp ứng nhiều chức năng; không có yêu cầu của tài liệu này buộc bệnh viện mua từng sản phẩm riêng biệt. Yêu cầu triển khai phải xuất phát từ hồ sơ cấp độ, rủi ro, quy mô và khả năng tổ chức vận hành.

Chọn nguồn giám sát theo rủi ro

Ưu tiên các nguồn có thể giúp phát hiện truy cập quản trị bất thường, mất dịch vụ thiết yếu, truy cập dữ liệu vượt nhiệm vụ, thay đổi cấu hình và tác động tới sao lưu. Nguồn thường cần xem xét gồm hệ thống danh tính, VPN, firewall, máy chủ HIS hoặc EMR, cơ sở dữ liệu, máy trạm quan trọng và nền tảng sao lưu. Danh sách thực tế phải có người phụ trách, phương thức thu thập, quyền truy cập và mục đích sử dụng rõ ràng.

Log có thể chứa dữ liệu cá nhân hoặc thông tin nội bộ nhạy cảm. Việc chuyển log cho nhà cung cấp cần được giới hạn theo nhu cầu, phân quyền, bảo vệ đường truyền, xác định nơi lưu và thời gian lưu theo quy định áp dụng. Không thu thập toàn bộ bệnh án chỉ để phục vụ một cảnh báo đăng nhập.

Từ cảnh báo đến hành động

Bước xử lý	Người hoặc nhóm phụ trách	Kết quả phải lưu
Tiếp nhận và xác minh	Đầu mối trực hoặc SOC	Mã sự kiện, nguồn cảnh báo, thời điểm và mức độ tin cậy
Phân loại tác động	CNTT cùng lãnh đạo chuyên môn	Dịch vụ bị ảnh hưởng, phạm vi dữ liệu, nguy cơ đối với người bệnh
Kích hoạt chỉ huy	Người có thẩm quyền theo phương án	Quyết định kích hoạt và người thay thế khi cần
Ngăn chặn và xử lý	Đội ứng cứu với các đơn vị liên quan	Nhật ký thao tác, quyết định cô lập, chứng cứ và thay đổi đã thực hiện
Phục hồi và xác nhận	CNTT, nhà cung cấp và khoa sử dụng	Kết quả kiểm thử, đối soát dữ liệu và quyết định đưa vào khai thác
Cải tiến	Lãnh đạo đơn vị và nhóm quản trị rủi ro	Nguyên nhân đã xác minh, biện pháp phòng ngừa và người theo dõi

Kiểm soát tự động hóa

Một kịch bản tự động khóa tài khoản hoặc cô lập máy có thể giảm thời gian ứng phó nhưng cũng có thể làm mất khả năng sử dụng dịch vụ thiết yếu. Trước khi áp dụng, bệnh viện cần xác định hệ thống được phép tự động xử lý, điều kiện kích hoạt, cấp phê duyệt, cách khôi phục và phương án thông báo cho khoa chuyên môn. Kịch bản phải thử trong môi trường phù hợp, có khả năng dừng và ghi nhật ký.

Nghiệm thu dịch vụ bằng tình huống

Việc nghiệm thu nên kiểm tra một cảnh báo thử đã được cho phép: log có đến đúng nơi không, ai nhận cảnh báo, khi nào có người xác minh, thông tin có đủ để ra quyết định và phiếu xử lý được đóng bằng bằng chứng nào. Bệnh viện cần kiểm tra cả trường hợp mất kết nối với SOC, ngoài giờ làm việc và đầu mối chính không có mặt.

Chỉ số gợi ý	Cách hiểu để tránh báo cáo hình thức
Tỷ lệ hệ thống trọng yếu có giám sát	Tính trên danh mục đã phê duyệt; xác nhận log hoặc tín hiệu vẫn đến và sử dụng được
Thời gian phát hiện	Đo từ dấu mốc sự kiện có thể xác định tới khi cảnh báo được phát hiện
Thời gian tiếp nhận và phản ứng	Tách thời điểm nhận cảnh báo, xác minh, quyết định và thực hiện biện pháp
Sự cố tái diễn	Đối chiếu nguyên nhân và biện pháp đã khắc phục, không chỉ đếm số phiếu
Chất lượng đóng cảnh báo	Có người xác nhận kết quả, tác động và minh chứng phục hồi

Các giá trị mục tiêu phải được bệnh viện thống nhất theo mức rủi ro và hợp đồng. Không dùng một ngưỡng thời gian mặc định cho mọi hệ thống. NIST SP 800-61 Rev.3 khuyến nghị tích hợp chuẩn bị, phát hiện, ứng phó và phục hồi vào quản trị rủi ro thường xuyên; nội dung vận dụng tại đây được điều chỉnh theo quy trình của bệnh viện [KT3].

Sao lưu và phục hồi dữ liệu để duy trì khám chữa bệnh

Chuyên đề thực hành bổ sung

Mục tiêu của sao lưu là tạo được dữ liệu và môi trường có thể sử dụng để phục hồi dịch vụ. Tệp sao lưu tồn tại hoặc màn hình hiển thị tác vụ thành công chưa chứng minh được bệnh viện sẽ hoạt động trở lại. Đơn vị phải thử khôi phục, kiểm tra nội dung và đo thời gian thực tế.

Xác định phục hồi cái gì và phục hồi đến thời điểm nào

Danh mục phục hồi cần bao gồm cơ sở dữ liệu, tệp bệnh án và ảnh, cấu hình ứng dụng, tài khoản dịch vụ, khóa và chứng thư cần thiết, phiên bản phần mềm, cấu hình kết nối, danh mục dùng chung và hướng dẫn thao tác. Nếu chỉ sao lưu cơ sở dữ liệu nhưng thiếu phiên bản ứng dụng hoặc khóa truy cập, thời gian đưa dịch vụ trở lại có thể kéo dài.

RTO là mục tiêu về thời gian khôi phục dịch vụ; RPO là mục tiêu về điểm dữ liệu có thể phục hồi, thể hiện khoảng dữ liệu có nguy cơ mất giữa hai thời điểm. Đây là mục tiêu quản trị do đơn vị xác định trên cơ sở yêu cầu áp dụng và tác động nghiệp vụ. Giá trị phải được khoa chuyên môn hiểu, người có thẩm quyền phê duyệt và kiểm chứng bằng thử nghiệm.

Ví dụ minh họa: bệnh viện đặt mục tiêu phục hồi một dịch vụ trong 2 giờ và chấp nhận khoảng mất dữ liệu tối đa 15 phút. Thử nghiệm mất 5 giờ hoặc chỉ phục hồi đến bản sao của ngày trước cho thấy mục tiêu chưa được đáp ứng. Các con số ví dụ không phải tiêu chuẩn chung cho hệ thống bệnh viện.

Tạo bản sao có khả năng sống sót sau tấn công

CISA khuyến nghị duy trì bản sao lưu được mã hóa, tách khỏi khả năng truy cập thông thường và thử độ sẵn sàng, toàn vẹn. Đồng bộ đám mây có thể đồng bộ cả tệp bị mã hóa; vì vậy cần kiểm tra cơ chế phiên bản, bảo vệ xóa và khả năng phục hồi, thay vì mặc nhiên coi đồng bộ là sao lưu [KT4].

Cách vận dụng tại bệnh viện là tách tài khoản quản trị sao lưu, kiểm soát quyền xóa, bảo vệ khóa, lưu bản sao ở miền lỗi phù hợp và có quy trình lấy bản sao khi hệ thống danh tính chính bị ảnh hưởng. Có thể tham khảo nguyên tắc nhiều bản sao, nhiều phương tiện và một bản tách biệt; phương án cụ thể phải được thiết kế theo rủi ro và khả năng phục hồi của từng đơn vị.

Thử phục hồi theo quy trình có người xác nhận

- Chọn phạm vi thử và mục tiêu rõ ràng; sử dụng môi trường cách ly phù hợp để không gây ảnh hưởng người bệnh đang được điều trị.
- Ghi nhận bản sao sử dụng, thời điểm dữ liệu, phiên bản phần mềm, tài nguyên và các phụ thuộc cần thiết.

- Khôi phục theo hướng dẫn; ghi thời gian từng công đoạn, lỗi và biện pháp xử lý.
- Kiểm tra tính toàn vẹn kỹ thuật, trạng thái ứng dụng và các kết nối liên quan; không cho kết nối tràn sang hệ thống đang nghi bị xâm nhập.
- Để khoa sử dụng kiểm tra hồ sơ mẫu, truy xuất ảnh hoặc kết quả và các chức năng cần thiết theo phạm vi thử.
- Đối chiếu RTO và RPO mục tiêu với kết quả thực tế; lập biên bản, phân công khắc phục và xác định lần thử tiếp theo.

Khôi phục sau sự cố mã độc

Đội ứng cứu cần đánh giá nguyên nhân, dấu hiệu còn tồn tại và độ tin cậy của bản sao. Không đưa toàn bộ dữ liệu vừa phục hồi vào cùng mạng nghi bị xâm nhập mà chưa có kiểm soát. Việc đưa dịch vụ trở lại phải có quyết định theo phương án, giám sát tăng cường và kênh nhận phản ánh của người dùng.

Sau khi kỹ thuật hoạt động, khoa chuyên môn đối chiếu hồ sơ phát sinh trong thời gian dự phòng. Cần phát hiện chỉ định trùng, kết quả chưa chuyển, thuốc đã cấp nhưng chưa ghi nhận và sai lệch danh tính. Ký xác nhận hoàn tất phục hồi phải bao gồm phạm vi đã kiểm tra và phần việc còn tồn, không chỉ xác nhận máy chủ đã chạy.

Quản lý lỗ hổng ứng dụng và truy cập của nhà cung cấp

Chuyên đề thực hành bổ sung

Biến cảnh báo thành nhiệm vụ có kết quả

Ngày 21/10/2026, Cơ quan An ninh mạng Singapore công bố cảnh báo PHP2Shell và cập nhật ngày 23/10/2026 về nguy cơ thực thi mã từ xa. Cảnh báo yêu cầu nhận diện các nơi có PHP, kể cả thành phần trong ứng dụng bên thứ ba, ưu tiên hệ thống tiếp xúc Internet và triển khai cập nhật theo hướng dẫn chính thức [KT1].

Bài học quản trị cho bệnh viện là phải biết phiên bản phần mềm nào đang được sử dụng, ai vận hành và ai nhận cảnh báo. Danh sách website công khai có thể chỉ là một phần của phạm vi; ứng dụng đặt lịch, cổng tra cứu và công cụ nội bộ cũng cần được kiểm kê. Cảnh báo phải được giao cho một người xác minh, xác định mức ảnh hưởng và báo cáo kết quả xử lý.

Quy trình xử lý một lỗ hổng

Bước	Câu hỏi cần trả lời	Minh chứng
Nhận diện	Thành phần và phiên bản bị ảnh hưởng có trong hệ thống không	Kết quả kiểm kê hoặc xác nhận có căn cứ của nhà cung cấp
Đánh giá	Có tiếp xúc Internet, chứa dữ liệu nhạy cảm hay ảnh hưởng dịch vụ thiết yếu không	Phiếu đánh giá phạm vi và mức ưu tiên

Bước	Câu hỏi cần trả lời	Minh chứng
Chuẩn bị	Có bản vá, biện pháp tạm thời, bản sao và phương án quay lại không	Kế hoạch thay đổi và người phê duyệt
Thử nghiệm	Ứng dụng và kết nối chuyên môn có hoạt động sau thay đổi không	Biên bản thử trong môi trường được phép
Triển khai	Khi nào thực hiện và thông báo ai	Nhật ký triển khai, cấu hình hoặc phiên bản mới
Xác nhận	Đã loại bỏ điểm yếu và kiểm tra dấu hiệu xâm nhập chưa	Kết quả xác minh và quyết định đóng nhiệm vụ

Không thực hiện quét xâm nhập hoặc thử khai thác trên hệ thống đang phục vụ người bệnh nếu chưa có phạm vi, thẩm quyền, thời gian và phương án bảo vệ được thống nhất. Đối với thiết bị y tế hoặc phần mềm đặc thù, cần có ý kiến của đơn vị chịu trách nhiệm về tương thích và bảo hành trước khi thay đổi.

Điều khoản cần có khi làm việc với nhà cung cấp

Hợp đồng và quy trình phối hợp nên xác định phạm vi hệ thống, người chịu trách nhiệm từng lớp, quyền tiếp cận dữ liệu, cơ chế truy cập từ xa, hỗ trợ khi có sự cố, thời gian phản hồi, quản lý bản vá, nghĩa vụ báo khi phát hiện nguy cơ, xuất trả dữ liệu và hỗ trợ chuyển đổi khi chấm dứt dịch vụ. Các cam kết phải có cách kiểm tra và tiêu chí nghiệm thu.

Mỗi phiên hỗ trợ từ xa cần gắn với yêu cầu được duyệt, tài khoản phù hợp, thời hạn truy cập và nhật ký thay đổi. Người tiếp nhận kết quả phải kiểm tra ứng dụng sử dụng được và quyền đã thu hồi hoặc trở về trạng thái quy định. Khi nhà cung cấp đổi nhân sự, bệnh viện cần nhận được cập nhật đầu mối và rà soát lại quyền.

Đối với thuê dịch vụ giám sát, không mặc nhiên chuyển toàn bộ dữ liệu khám chữa bệnh cho bên ngoài. Phạm vi log, nơi lưu, quyền truy cập, việc sử dụng nhà thầu phụ và cách hoàn trả hoặc xử lý dữ liệu phải được xác định trước theo căn cứ pháp lý áp dụng.

Bài học từ sự cố và thực hành xử lý tình huống

Tổng hợp tài liệu chuyên môn trong nước và quốc tế

Sự cố của bên cung cấp dịch vụ có thể ảnh hưởng nhiều cơ sở y tế

Trong thư ngày 13/3/2024, cơ quan quản lý quyền dân sự thuộc Bộ Y tế và Dịch vụ Nhân sinh Hoa Kỳ ghi nhận vụ tấn công vào Change Healthcare cuối tháng 2/2024 làm gián đoạn các hệ thống thông tin y tế và thanh toán trên toàn quốc. Cơ quan này nhấn mạnh tác động tới chăm sóc người bệnh và quyền riêng tư [KT2].

Vận dụng vào bệnh viện, việc đánh giá nhà cung cấp cần bao gồm phụ thuộc vận hành và phương án thay thế. Nếu hệ thống bên ngoài mất kết nối, đơn vị phải có cách giữ chứng từ, theo dõi dữ liệu chưa

gửi, phối hợp khắc phục và phục vụ người bệnh trong khả năng cho phép. Đăng ký một yêu cầu hỗ trợ chưa phải kết quả cuối cùng; cần xác nhận dịch vụ và dữ liệu đã thực sự phục hồi.

Lỗ hổng đã được công bố cần được kiểm tra tại hệ thống thực tế

Một thông báo cảnh báo chỉ có giá trị khi dẫn đến việc xác định đúng phạm vi bị ảnh hưởng, hành động giảm rủi ro và xác nhận kết quả. Với ví dụ PHP ở chuyên đề trước, yêu cầu gửi nhà thầu có thể là cung cấp danh mục thành phần, phiên bản, đánh giá ảnh hưởng, kế hoạch cập nhật và bằng chứng kiểm tra sau thay đổi. Không dùng nhận định chung rằng website vẫn mở được làm căn cứ kết luận an toàn.

Bài tập một Website bị thay đổi nội dung

Tình huống mô phỏng: người dùng báo website công khai của đơn vị xuất hiện nội dung lạ. Hệ thống tiếp đón vẫn hoạt động. Nhóm học viên xác định chủ quản và đơn vị vận hành website; kiểm tra dấu hiệu phạm vi ảnh hưởng; phân công bảo toàn chứng cứ; xem xét kết nối và tài khoản có liên quan hệ thống nội bộ; tổ chức thông tin chính thức và lập nhiệm vụ phục hồi. Không suy đoán website bị thay đổi đồng nghĩa toàn bộ dữ liệu bệnh án đã bị lấy cắp, cũng không kết luận dữ liệu an toàn khi chưa đánh giá.

Bài tập hai Hệ thống chạy nhưng dữ liệu có dấu hiệu sai lệch

Tình huống mô phỏng: một khoa phát hiện kết quả xét nghiệm hiển thị không khớp phiếu xác nhận. Nhóm học viên xác định phạm vi hồ sơ có thể bị ảnh hưởng, kênh báo chuyên môn, biện pháp kiểm tra độc lập và cách bảo toàn các phiên bản dữ liệu. Việc điều trị tiếp theo do người có trách nhiệm chuyên môn quyết định trên cơ sở thông tin đã được kiểm chứng; đội kỹ thuật hỗ trợ truy vết và kiểm soát việc sửa dữ liệu.

Bài tập ba Sao lưu thành công nhưng không phục hồi được

Tình huống mô phỏng: màn hình sao lưu báo thành công trong nhiều tuần, nhưng khi thử phục hồi thì thiếu khóa giải mã và giấy phép phần mềm. Nhóm học viên chỉ rõ nguyên nhân quản trị, dữ liệu và phụ thuộc cần bổ sung; ai nhận bàn giao; ai kiểm tra độc lập và bằng chứng nào để nghiệm thu lại. Kết quả bài tập là một kế hoạch khắc phục có người phụ trách và ngày thử lại.

Các nhóm trình bày câu trả lời theo cùng một mẫu gồm tác động, người quyết định, hành động đầu tiên, bằng chứng cần giữ và điều kiện đóng sự cố. Cách trình bày này giúp lãnh đạo nhìn rõ quyết định cần đưa ra và trách nhiệm tiếp theo của từng bộ phận.

Phần thứ tư Bộ công cụ triển khai tại bệnh viện

Tổ chức thực hiện sau lớp tập huấn

Sau lớp tập huấn, bệnh viện cần chuyển nội dung học thành một kế hoạch có người phụ trách, thời hạn, sản phẩm và minh chứng. Ban giám đốc nên tổ chức một cuộc làm việc với CNTT, kế hoạch tổng hợp, điều dưỡng, quản lý chất lượng, BHYT, tài chính và bộ phận pháp chế để thống nhất danh mục việc cần làm và nguy cơ phải xử lý trước.

Các việc cần bắt đầu ngay

- Xác nhận đầu mối chỉ huy, người thay thế và danh bạ liên hệ ngoài giờ; chuyển thông tin này tới các ca trực.
- Kiểm kê hệ thống trọng yếu, dịch vụ phụ thuộc và tình trạng hồ sơ cấp độ; nhận diện các nghĩa vụ chuyển tiếp cần thực hiện.
- Kiểm tra tài khoản quản trị, tài khoản nghỉ việc và quyền truy cập từ xa đang mở; xử lý quyền không còn phù hợp theo quy trình.
- Xác định bản sao lưu có thể sử dụng, người có quyền lấy bản sao và lần thử khôi phục gần nhất.
- Rà soát bộ biểu mẫu dự phòng và khả năng thực hiện tại cấp cứu, xét nghiệm, dược, chẩn đoán hình ảnh và khoa lâm sàng.
- Ghi thành nhiệm vụ các nguy cơ ảnh hưởng trực tiếp tới người bệnh, dữ liệu nhạy cảm và khả năng phục hồi; phân công người theo dõi tới kết quả.

Lộ trình thực hành 30 60 90 ngày

Mốc đề xuất	Công việc trọng tâm	Điều kiện xác nhận kết quả
Trong 30 ngày	Kiểm kê; tự rà soát; giao đầu mối; đánh giá khoảng trống hồ sơ và quy trình; lập kế hoạch	Có danh mục được xác nhận, rủi ro ưu tiên, người chịu trách nhiệm và nguồn lực dự kiến
Trong 60 ngày	Triển khai kiểm soát ưu tiên; thử khôi phục; hoàn thiện quy trình dự phòng và quản lý nhà thầu	Có minh chứng thay đổi, biên bản thử, tồn tại và nhiệm vụ khắc phục tiếp theo
Trong 90 ngày	Diễn tập liên bộ phận; kiểm tra độc lập; đánh giá hiệu quả và điều chỉnh	Có biên bản diễn tập, kết quả đối soát, nhiệm vụ chưa đạt và quyết định cải tiến

Lộ trình này là gợi ý tổ chức thực hành. Nguy cơ cấp bách cần được xử lý ngay; nghĩa vụ pháp luật và chỉ đạo có thời hạn ngắn hơn phải được ưu tiên. Không chờ đủ 30 ngày để báo cáo một sự cố đang diễn ra hoặc để xem xét việc bảo vệ người bệnh.

Mẫu 01 Phiếu tự rà soát an toàn thông tin bệnh viện

Tên bệnh viện: .....

Ngày rà soát: ..... Nhóm thực hiện: .....

Người xác nhận: ..... Phạm vi rà soát: .....

Ghi trạng thái theo một trong bốn mức: Đầy đủ, Một phần, Chưa có, Không áp dụng. Trường hợp Không áp dụng phải có lý do và người xác nhận. Trạng thái Đầy đủ cần kèm minh chứng đã kiểm tra; không suy ra mức độ tuân thủ tổng thể chỉ bằng số ô đã đánh dấu.

Mã	Nội dung đối chiếu	Trạng thái	Minh chứng hoặc tồn tại
01	Danh mục hệ thống, dữ liệu và kết nối được cập nhật		
02	Chủ quản, đơn vị vận hành và người phụ trách được xác định		
03	Cấp độ hiện có và trường hợp chuyển tiếp được đối chiếu		
04	Hồ sơ đề xuất, thẩm định, phê duyệt thuộc diện áp dụng được quản lý		
05	Biện pháp bảo vệ được đối chiếu với phương án đã phê duyệt		
06	Tài khoản cá nhân, đặc quyền và quy trình thu hồi được kiểm soát		
07	Quyền truy cập từ xa và tài khoản nhà cung cấp được rà soát		
08	Máy chủ, ứng dụng và thành phần phần mềm có đầu mối quản lý bản vá		
09	Mạng khách, mạng thiết bị và mạng nghiệp vụ được kiểm soát phù hợp		
10	Có nguồn log và đầu mối tiếp nhận, xác minh cảnh báo		
11	Phạm vi sử dụng, chia sẻ và bảo vệ dữ liệu người bệnh được quy định		
12	Nghĩa vụ bảo vệ dữ liệu cá nhân và hồ sơ cần thiết được rà soát		
13	Bản sao lưu được bảo vệ và có người chịu trách nhiệm		
14	Đã thử khôi phục và đối chiếu dữ liệu với mục tiêu đã phê duyệt		

Mã	Nội dung đối chiếu	Trạng thái	Minh chứng hoặc tồn tại
15	Có danh bạ ứng cứu, người chỉ huy và người thay thế		
16	Có quy trình báo cáo, phối hợp và đánh giá nghĩa vụ thông báo		
17	Các khoa có biểu mẫu và quy trình khám chữa bệnh dự phòng		
18	Có quy trình nhập bổ sung, kiểm tra và đối soát sau phục hồi		
19	Hợp đồng quy định truy cập, bảo mật, ứng cứu và bàn giao dữ liệu		
20	Có kế hoạch khắc phục, diễn tập và theo dõi kết quả thực tế		

Ba nguy cơ ưu tiên: .....

Việc cần quyết định ngay: .....

Tài liệu kèm theo và nơi quản lý: .....

Mẫu 02 Hồ sơ kiểm kê một hệ thống và các phụ thuộc

Mỗi hệ thống lập một phiếu; liên kết với danh mục tài sản và hồ sơ cấp độ của đơn vị.

Trường thông tin	Thông tin cần điền
Tên và mã hệ thống	.....
Chức năng và khoa phòng sử dụng	.....
Chủ quản và căn cứ xác định	.....
Đơn vị vận hành và nhà cung cấp	.....
Phụ trách kỹ thuật và người thay thế	.....
Dữ liệu xử lý và nhóm chủ thể dữ liệu	.....
Phạm vi phục vụ và số chủ thể dữ liệu có căn cứ	.....
Cấp độ và quyết định hiện có	.....
Trường hợp cần cập nhật hoặc xác định lại	.....
Vị trí triển khai và phương thức kết nối	.....
Kết nối tới hệ thống ngoài bệnh viện	.....
Tài khoản và quyền đặc biệt cần quản lý	.....
Sao lưu và lần thử khôi phục gần nhất	.....

Phụ thuộc cần thiết để dịch vụ hoạt động

Ghi hệ thống danh tính, mạng, điện, cơ sở dữ liệu, chứng thư, khóa, thiết bị, phần mềm hoặc dịch vụ bên ngoài. Chỉ lưu sơ đồ chi tiết và thông tin truy cập trong hồ sơ nội bộ được bảo vệ; không ghi mật khẩu vào phiếu.

Phụ thuộc	Ảnh hưởng nếu mất	Người phối hợp và phương án thay thế
.....	.....	.....
.....	.....	.....
.....	.....	.....

Người lập: ..... Người kiểm tra: .....

Ngày cập nhật và lý do thay đổi: .....

Mẫu 03 Sổ rủi ro và kế hoạch khắc phục

Bệnh viện: ..... Kỳ theo dõi: .....

Ưu tiên xử lý theo ảnh hưởng tới an toàn người bệnh, nghĩa vụ pháp lý, nguy cơ lộ hoặc sai dữ liệu, phạm vi lan truyền và khả năng phục hồi. Phân loại dưới đây là cách quản lý nội bộ, không thay thế cấp độ pháp lý của hệ thống.

Mã và ưu tiên	Tồn tại và tác động	Việc cần làm và sản phẩm	Người và hạn hoàn thành	Minh chứng và trạng thái
R01 Khẩn	Ví dụ: chưa thử phục hồi dữ liệu của dịch vụ trọng yếu	Thử phục hồi cách ly; xác nhận dữ liệu và thời gian	Đơn vị tự phân công và phê duyệt	Ghi kết quả thực tế; chưa coi là đạt nếu chưa kiểm tra
R02	....	....	....	....
R03	....	....	....	....
R04	....	....	....	....
R05	....	....	....	....

Nội dung lãnh đạo cần quyết định

Nguồn lực cần bố trí: .....

Nội dung cần phối hợp ngoài đơn vị: .....

Rủi ro chưa thể khắc phục và biện pháp tạm thời: .....

Người chấp thuận phương án tạm thời và thời hạn xem xét lại: .....

Chỉ đóng nhiệm vụ khi sản phẩm đã được người có trách nhiệm kiểm tra. Nếu giải pháp chưa đạt, ghi rõ phần còn thiếu, trách nhiệm và mốc xử lý tiếp theo; không đóng chỉ vì đã gửi email hoặc nhận thông báo nhà cung cấp đã sửa.

Mẫu 04 Danh bạ ứng cứu và bảng phân công

Phiên bản: ..... Ngày kiểm tra liên lạc: ..... Người quản lý: .....

Vai trò	Họ tên và kênh liên hệ công vụ	Người thay thế và giờ trực
Chỉ huy sự cố	.....	.....
Lãnh đạo chuyên môn	.....	.....
Đầu mối CNTT và an toàn thông tin	.....	.....
Kế hoạch tổng hợp và điều dưỡng	.....	.....
Cấp cứu và hồi sức	.....	.....
Xét nghiệm và chẩn đoán hình ảnh	.....	.....
Dược	.....	.....
BHYT và tài chính kế toán	.....	.....
Pháp chế và phụ trách dữ liệu	.....	.....
Truyền thông và tiếp nhận phản ánh	.....	.....
Nhà cung cấp HIS hoặc EMR	.....	.....
Nhà cung cấp hạ tầng hoặc SOC	.....	.....
Đầu mối Sở và cơ quan chuyên trách theo phân cấp	.....	.....

Quyết định và trách nhiệm cần xác định trước

Người được quyền kích hoạt phương án dự phòng: .....

Người quyết định cô lập hệ thống trọng yếu: .....

Người quyết định thông tin ra bên ngoài: .....

Người xác nhận phục hồi kỹ thuật và chuyên môn: .....

Nơi lưu bản danh bạ ngoại tuyến và cách cập nhật: .....

Danh bạ phải dùng được khi mất thư điện tử hoặc mạng nội bộ. Thông tin liên hệ cá nhân được bảo vệ phù hợp; không công khai toàn bộ danh bạ ứng cứu trên cổng thông tin.

Mẫu 05 Báo cáo ban đầu và nhật ký xử lý sự cố

Mẫu thực hành nội bộ. Không thay thế biểu mẫu, kênh và thời hạn thông báo pháp luật quy định, trong đó có Mẫu số 08 tại Nghị định 356/2025/NĐ-CP nếu thuộc diện áp dụng.

Thông tin ban đầu

Mã sự cố: ..... Đơn vị hoặc hệ thống: .....
Thời điểm phát hiện: ..... Người phát hiện: .....
Dấu hiệu quan sát được: .....
Thời điểm bắt đầu ảnh hưởng nếu đã xác minh: .....
Dịch vụ và khoa phòng bị ảnh hưởng: .....
Ảnh hưởng người bệnh đang được ghi nhận: .....
Dữ liệu có thể liên quan và mức xác minh: .....
Người chỉ huy và đầu mối kỹ thuật: .....
Phương án dự phòng đã kích hoạt: .....
Biện pháp khoanh vùng và người phê duyệt: .....
Chứng cứ đã bảo toàn và người quản lý: .....

Theo dõi báo cáo và phối hợp

Đầu mối nhận	Thời điểm và kênh	Nội dung và người gửi	Kết quả tiếp nhận
.....	.....	.....	.....
.....	.....	.....	.....
.....	.....	.....	.....

Nghĩa vụ thông báo đã xem xét, căn cứ và thời điểm tính hạn: .....
Thông tin còn cần xác minh và người thực hiện: .....

Nhật ký hành động

Thời điểm	Người thực hiện	Hành động và phê duyệt	Kết quả và chứng cứ
.....	.....	.....	.....
.....	.....	.....	.....
.....	.....	.....	.....
.....	.....	.....	.....

Báo cáo tiếp theo dự kiến lúc: ..... Người lập: .....

Mẫu 06 Biên bản thử khôi phục dữ liệu và dịch vụ

Hệ thống và phạm vi thử: .....
Môi trường thử và biện pháp cách ly: .....
Người phê duyệt: ..... Nhóm thực hiện: .....

Chỉ tiêu hoặc thành phần	Mục tiêu hoặc thông tin	Kết quả thực tế
Thời điểm bắt đầu và kết thúc	.....	.....
RTO được phê duyệt	.....	.....
RPO được phê duyệt	.....	.....
Bản sao và thời điểm dữ liệu	.....	.....
Ứng dụng, cấu hình, khóa và phụ thuộc	.....	.....
Kiểm tra toàn vẹn kỹ thuật	.....	.....
Kiểm tra hồ sơ mẫu và chức năng nghiệp vụ	.....	.....
Kiểm tra kết nối và phân quyền	.....	.....
Lỗi hoặc dữ liệu thiếu phát hiện	.....	.....

Xác nhận kết quả

Phạm vi đạt yêu cầu: .....
Phạm vi chưa đạt và tác động: .....
Việc cần khắc phục, người phụ trách và hạn: .....
Ngày thử lại hoặc kế hoạch tiếp theo: .....
Xác nhận kỹ thuật: ..... Xác nhận khoa sử dụng: .....
Người có thẩm quyền kết luận: .....
Đính kèm bằng chứng kiểm thử cần thiết trong hồ sơ nội bộ. Không đưa dữ liệu người bệnh thật vào bản báo cáo chia sẻ khi không có căn cứ và nhu cầu hợp pháp.

Mẫu 07 Kịch bản diễn tập gián đoạn hệ thống trong bốn giờ

Đây là diễn tập bàn hoặc diễn tập trong môi trường kiểm thử, dùng dữ liệu giả lập. Thời gian dưới đây là các mốc tình huống để luyện tập, không phải thời hạn pháp luật hay yêu cầu phải ngắt hệ thống bệnh viện thật.

Thiết lập tình huống

09 giờ sáng, HIS không đăng nhập được tại khoa khám bệnh. Một máy trạm có thông báo nghi mã độc tống tiền. LIS vẫn thực hiện được xét nghiệm nhưng không chuyển kết quả sang HIS; một số người bệnh đang cần kết quả để xử trí. Sau đó, bộ phận kỹ thuật báo chưa xác định được bản sao lưu sạch gần nhất. Sự cố kéo dài bốn giờ theo kịch bản.

Mốc tình huống	Thông tin bổ sung	Quyết định cần luyện tập
Từ 0 đến 15 phút	HIS ngừng truy cập; đầu mối kỹ thuật đang xác minh	Ai chỉ huy; khoa nào chuyển dự phòng; cách báo ca trực và bảo toàn chứng cứ
Từ 15 đến 30 phút	Có kết quả xét nghiệm nguy cấp không truyền được	Kênh bàn giao kết quả; xác nhận người nhận; theo dõi xử lý chuyên môn
Từ 30 đến 60 phút	Nhà thầu đề nghị mở quyền truy cập quản trị từ xa	Ai cho phép; phạm vi và thời hạn; người giám sát; ghi nhận thao tác
Giờ thứ hai	Hàng chờ tăng; chưa rõ dữ liệu có bị lấy cắp không	Phân luồng người bệnh; bổ sung nhân lực; thông tin chính thức; xem xét nghĩa vụ thông báo
Giờ thứ ba	Có một bản sao có thể khôi phục nhưng chưa kiểm tra	Phạm vi thử; môi trường cách ly; thứ tự phục hồi; tiêu chí chấp nhận
Giờ thứ tư	Ứng dụng hoạt động thử; còn hồ sơ ghi tay và dữ liệu BHYT chưa gửi	Ai cho phép vận hành; cách nhập bù, kiểm tra trùng, đối soát và đóng sự cố

Phân công nhóm diễn tập

Nhóm chỉ huy gồm lãnh đạo và đầu mối điều phối. Nhóm chuyên môn gồm cấp cứu, khoa lâm sàng, điều dưỡng, xét nghiệm, chẩn đoán hình ảnh và dược. Nhóm kỹ thuật gồm CNTT, an toàn thông tin và nhà cung cấp. Nhóm hỗ trợ gồm BHYT, tài chính, pháp chế, phụ trách dữ liệu và truyền thông. Người quan sát ghi thời điểm, quyết định và điểm chưa rõ trách nhiệm.

Tiêu chí quan sát

- Danh bạ liên lạc dùng được và có người thay thế khi đầu mối chính vắng mặt.
- Cấp cứu và hoạt động thiết yếu được tổ chức theo phương án đã phê duyệt; nhân viên biết biểu mẫu cần dùng.

- Nhận diện người bệnh, mẫu, chỉ định, kết quả và cấp phát thuốc được kiểm soát trong quy trình dự phòng.
- Biện pháp kỹ thuật có người quyết định; chứng cứ và nhật ký không bị mất do thao tác tùy tiện.
- Nghĩa vụ báo cáo và thông báo được xem xét đúng căn cứ, đúng đầu mối.
- Việc phục hồi được kiểm tra cả kỹ thuật lẫn chuyên môn; dữ liệu phát sinh thủ công có người đối soát.

Biên bản rút kinh nghiệm

Điểm làm được: .....

Điểm chưa đạt và nguyên nhân: .....

Nhiệm vụ cải tiến, người và hạn hoàn thành: .....

Người theo dõi kết quả và thời điểm đánh giá lại: .....

Mẫu 08 Theo dõi lỗi liên thông và đối soát dữ liệu BHYT

Tên bệnh viện: ..... Kỳ đối soát: .....

Đầu mối chịu trách nhiệm: ..... Người kiểm tra: .....

Nhóm lỗi	Bằng chứng cần có	Đơn vị phối hợp và điều kiện đóng
Định danh hoặc quyền lợi	Thông tin đã đối chiếu, nguồn kiểm tra, thời điểm	Tiếp đón và BHYT; xác nhận thông tin hợp lệ theo quy định
Nội dung chuyên môn	Hồ sơ nguồn, chỉ định và xác nhận chuyên môn	Khoa chuyên môn; chỉnh sửa hợp lệ và lưu dấu vết
Danh mục hoặc định dạng	Mã lỗi, phiên bản chuẩn, phản hồi nhận dữ liệu	BHYT và CNTT; gửi lại đúng chuẩn và có xác nhận tiếp nhận
Kết nối tại bệnh viện	Nhật ký truyền nhận và kiểm tra đường truyền	CNTT và nhà cung cấp; kiểm tra hoạt động gửi nhận thực tế
Hệ thống bên ngoài	Yêu cầu hỗ trợ chính thức và mã phản hồi	Đầu mối quản lý hệ thống hoặc BHXH liên quan; xác nhận kết quả đối soát
Gửi trùng hoặc còn tồn	Mã giao dịch, danh sách đã gửi và phản hồi	BHYT và tài chính; đối chiếu trước khi đóng để tránh cộng trùng

Phiếu theo dõi một vướng mắc

Mã theo dõi nội bộ: ..... Thời điểm phát hiện: .....

Số hồ sơ ảnh hưởng và mức độ đã xác minh: .....

Mô tả lỗi và kết quả kiểm tra tại bệnh viện: .....

Đầu mối bên ngoài đã liên hệ, thời điểm và yêu cầu: .....

Biện pháp bảo đảm quyền lợi người bệnh trong khi chờ: .....

Kết quả tiếp nhận và đối soát dữ liệu: .....

Người xác nhận đóng lỗi và ngày xác nhận: .....

Phiếu phổ biến tại cuộc họp nên dùng mã theo dõi và dữ liệu tổng hợp. Chứng cứ có thông tin người bệnh được quản lý trong hồ sơ có phân quyền; không đính kèm toàn bộ bệnh án vào yêu cầu hỗ trợ khi không cần thiết.

Mẫu 09 Quản lý phiên hỗ trợ từ xa của nhà cung cấp

Mã yêu cầu: ..... Hệ thống: .....
Nhà cung cấp và nhân sự được phép: .....
Mục đích hỗ trợ và công việc được duyệt: .....
Người phê duyệt tại bệnh viện: .....

Điểm kiểm soát	Thông tin hoặc xác nhận
Thời gian bắt đầu và kết thúc được phép	.....
Tài khoản, phạm vi quyền và hệ thống được vào	.....
Kênh kết nối và biện pháp xác thực	.....
Người giám sát tại bệnh viện	.....
Dữ liệu được phép tiếp cận hoặc trích xuất	.....
Thay đổi dự kiến, sao lưu và phương án quay lại	.....
Nhật ký thực tế và tài liệu bàn giao	.....
Kết quả kiểm tra ứng dụng sau hỗ trợ	.....
Thu hồi hoặc điều chỉnh quyền sau phiên	.....

Bất thường hoặc thay đổi ngoài phạm vi: .....
Người quyết định xử lý phát sinh: .....
Người tiếp nhận kết quả và thời điểm: .....
Không ghi mật khẩu, mã xác thực hoặc khóa truy cập vào mẫu. Nơi lưu nhật ký phải có phân quyền và thời hạn lưu phù hợp. Một phiên hỗ trợ mới cần được đánh giá theo công việc thực tế, tránh duy trì quyền cao thường trực chỉ để thuận tiện.

Mẫu 10 Báo cáo kết quả triển khai sau tập huấn

Bệnh viện: ..... Thời điểm báo cáo: .....

Người chịu trách nhiệm tổng hợp: .....

Kết quả đã kiểm chứng

Nội dung	Kết quả và minh chứng	Phần còn tồn và người phụ trách
Danh mục hệ thống và trách nhiệm	.....	.....
Hồ sơ và biện pháp bảo vệ theo cấp độ	.....	.....
Quản lý tài khoản, dữ liệu và nhà thầu	.....	.....
Sao lưu và thử khôi phục	.....	.....
Quy trình khám chữa bệnh dự phòng	.....	.....
Diễn tập và cải tiến	.....	.....
Liên thông, báo cáo và đối soát BHYT	.....	.....

Các quyết định cần lãnh đạo xem xét

Nguy cơ cần xử lý ngay: .....

Nhu cầu nguồn lực hoặc hỗ trợ chuyên môn: .....

Nội dung cần báo cáo cơ quan có thẩm quyền: .....

Mốc kiểm tra kết quả tiếp theo: .....

Người xác nhận báo cáo: .....

Báo cáo nêu đúng trạng thái đã hoàn thành, đang thực hiện, chưa đáp ứng và không áp dụng có lý do. Không đưa số liệu hoàn thành hoặc mức độ an toàn khi chưa có căn cứ kiểm tra.

Phần thứ năm Văn bản và tài liệu tham khảo để triển khai

Danh mục văn bản gắn với trách nhiệm của bệnh viện

Danh mục sau giúp bệnh viện tra cứu đúng nguồn và xác định nội dung cần tổ chức thực hiện. Văn bản pháp luật có thể được sửa đổi, bổ sung; khi lập hồ sơ hoặc thực hiện thủ tục, đơn vị đối chiếu toàn văn hiện hành, đối tượng áp dụng và hướng dẫn của cơ quan có thẩm quyền. Các đường dẫn là nguồn tra cứu chính thức được kiểm tra trong quá trình biên soạn ngày 29/10/2026.

PL1 Luật An ninh mạng số 116/2025/QH15

Ban hành 10/12/2025; hiệu lực 01/7/2026. Trọng tâm: Điều 9, Điều 10 về hệ thống và biện pháp bảo vệ; Điều 44 về hiệu lực; Điều 45 về chuyển tiếp.

Việc bệnh viện cần tổ chức: Rà soát căn cứ pháp lý, cấp độ hiện có và điều kiện phải hoàn thiện.

Trang thông tin chính thức về văn bản

PL2 Nghị định số 331/2026/NĐ-CP về bảo vệ an ninh mạng đối với hệ thống thông tin

Ban hành và hiệu lực 19/8/2026. Trọng tâm: phạm vi hệ thống, tiêu chí cấp độ, thẩm quyền, hồ sơ, biện pháp, trách nhiệm và báo cáo.

Việc bệnh viện cần tổ chức: Xác định chủ quản, đơn vị vận hành; lập hoặc rà soát hồ sơ; triển khai phương án và quản lý minh chứng.

Trang thông tin chính thức về văn bản

PL3 Luật Khám bệnh chữa bệnh số 15/2023/QH15 và các sửa đổi bổ sung hiện hành

Trọng tâm: khoản 2 Điều 10 về bí mật riêng tư; Điều 60 về trách nhiệm cơ sở; Điều 69 về hồ sơ bệnh án.

Việc bệnh viện cần tổ chức: Bảo mật hồ sơ, kiểm soát khai thác và tổ chức khám chữa bệnh an toàn trong cả quy trình dự phòng.

Trang thông tin chính thức về văn bản

PL4 Luật Bảo vệ dữ liệu cá nhân số 91/2025/QH15

Ban hành 26/6/2025; hiệu lực 01/01/2026. Trọng tâm: nguyên tắc xử lý, quyền của chủ thể và Điều 23 về thông báo vi phạm.

Việc bệnh viện cần tổ chức: Xác định vai trò xử lý dữ liệu, căn cứ sử dụng, đầu mối và nghĩa vụ thông báo khi có vi phạm thuộc diện áp dụng.

Trang thông tin chính thức về văn bản

PL5 Nghị định số 356/2025/NĐ-CP hướng dẫn Luật Bảo vệ dữ liệu cá nhân

Ban hành 31/12/2025; hiệu lực 01/01/2026. Trọng tâm: điều kiện và biện pháp thực hiện; Điều 28 và Mẫu số 08 về thông báo vi phạm.

Việc bệnh viện cần tổ chức: Rà soát hồ sơ, quy trình và biểu mẫu theo vai trò, trường hợp áp dụng; dùng đúng mẫu pháp luật quy định.

Trang thông tin chính thức về văn bản

PL6 Thông tư số 13/2025/TT-BYT hướng dẫn triển khai hồ sơ bệnh án điện tử

Ban hành 06/6/2025; hiệu lực 21/7/2025. Trọng tâm: hạ tầng và phục hồi, ký hoặc xác nhận điện tử, trách nhiệm và lộ trình.

Việc bệnh viện cần tổ chức: Kiểm tra tính đầy đủ, truy xuất, dự phòng và khả năng phục hồi của hồ sơ bệnh án điện tử.

Trang thông tin chính thức về văn bản

PL7 Thông tư số 33/2025/TT-BYT về thời hạn lưu trữ hồ sơ tài liệu ngành y tế

Ban hành và hiệu lực 01/7/2025. Tra cứu cả thông tư và phụ lục phân loại hồ sơ.

Việc bệnh viện cần tổ chức: Quản lý thời hạn lưu trữ theo đúng loại hồ sơ; không tự xóa bệnh án theo yêu cầu kỹ thuật của phần mềm.

Trang thông tin chính thức về văn bản

PL8 Nghị định số 188/2025/NĐ-CP hướng dẫn Luật Bảo hiểm y tế

Ban hành 01/7/2025; hiệu lực 15/8/2025. Cần đối chiếu cùng chuẩn dữ liệu và hướng dẫn hiện hành.

Việc bệnh viện cần tổ chức: Quản lý chứng từ, dữ liệu, việc xác thực và phối hợp xử lý vướng mắc phục vụ quyền lợi, giám định và thanh toán BHYT.

Trang thông tin chính thức về văn bản

PL9 Quyết định số 5066/QĐ-UBND ngày 09/10/2025 của UBND thành phố Hà Nội

Quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Sở Y tế thành phố Hà Nội.

Việc bệnh viện cần tổ chức: Xác định đầu mối tham mưu, hướng dẫn và phối hợp thuộc chức năng quản lý ngành; tôn trọng thẩm quyền cơ quan chuyên trách.

Trang thông tin chính thức về văn bản

PL10 Luật Giao dịch điện tử số 20/2023/QH15

Ban hành 22/6/2023; hiệu lực 01/7/2024. Tra cứu các quy định liên quan thông điệp dữ liệu và chữ ký điện tử.

Việc bệnh viện cần tổ chức: Kiểm soát việc ký, xác nhận, tính toàn vẹn và khả năng sử dụng của hồ sơ điện tử theo trường hợp áp dụng.

Trang thông tin chính thức về văn bản

PL11 Nghị định số 333/2026/NĐ-CP hướng dẫn Luật An ninh mạng

Ban hành và hiệu lực 19/8/2026. Quy định chi tiết một số điều và biện pháp thi hành Luật.

Việc bệnh viện cần tổ chức: Tra cứu bổ sung đối với các hoạt động, dịch vụ và trách nhiệm thuộc phạm vi điều chỉnh; đọc cùng Nghị định 331.

Trang thông tin chính thức về văn bản

PL12 Thông tư số 12/2026/TT-BTC về giám định chi phí khám chữa bệnh BHYT

Ban hành và hiệu lực 10/02/2026. Quy định trình tự, thủ tục, biểu mẫu tổng hợp thanh toán, quyết toán và biện pháp thi hành Nghị định 188.

Việc bệnh viện cần tổ chức: Đối chiếu quy trình nghiệp vụ, hồ sơ và phối hợp với cơ quan BHXH khi xử lý dữ liệu và thanh toán.

Trang thông tin chính thức về văn bản

Những điểm pháp lý cần kiểm tra khi lập kế hoạch

Quy định chuyển tiếp của khung an ninh mạng

Điều 45 Luật An ninh mạng 2025 quy định hệ thống đã được xác định cấp độ theo luật cũ tiếp tục giữ cấp độ đã được xác định; trong thời hạn 12 tháng kể từ khi Luật có hiệu lực phải bảo đảm điều kiện, tiêu chuẩn và biện pháp tương ứng theo Luật mới [PL1].

Khoản 1 Điều 39 Nghị định 331/2026/NĐ-CP quy định: đối với hệ thống đang đầu tư, xây dựng trước ngày 01/7/2026, trong thời hạn 06 tháng kể từ khi Luật An ninh mạng 2025 có hiệu lực, các bên liên quan hoàn thành thẩm định, phê duyệt cấp độ theo Nghị định 85/2016/NĐ-CP; trong thời hạn 12 tháng kể từ mốc Luật có hiệu lực, phải bảo đảm điều kiện, tiêu chuẩn và biện pháp tương ứng theo Nghị định mới [PL2].

Cách thực hiện tại bệnh viện là lập danh sách các hệ thống thuộc từng trường hợp, ghi quyết định đã có, thay đổi thực tế, công việc cần hoàn thiện và đầu mối phối hợp. Tài liệu từ giai đoạn Nghị định 85/2016/NĐ-CP và Thông tư 12/2022/TT-BTTTT cần được đối chiếu trong hồ sơ lịch sử và trường hợp chuyển tiếp cụ thể; không dùng danh mục căn cứ cũ như một hướng dẫn đầy đủ cho mọi hồ sơ mới.

Thẩm quyền đối với cấp độ thường gặp

Trường hợp đề xuất	Tóm tắt theo Điều 18 Nghị định 331	Điểm bệnh viện cần xác minh
Cấp độ 1 hoặc cấp độ 2	Đơn vị chuyên trách về an ninh mạng của chủ quản thẩm định, phê duyệt hồ sơ và báo cáo chủ quản	Ai là chủ quản; đơn vị chuyên trách nào được xác định hợp lệ
Cấp độ 3	Đơn vị chuyên trách của chủ quản thẩm định; chủ quản phê duyệt hồ sơ	Bệnh viện là chủ quản hay đơn vị vận hành; hồ sơ phải trình đúng chủ thể
Cấp độ 4 hoặc cấp độ 5	Áp dụng khoản 3 Điều 18 theo chủ thể và loại hệ thống; không suy rộng quy trình cấp độ 3	Phối hợp chủ quản và cơ quan có thẩm quyền; tra cứu toàn văn trước khi trình
Đơn vị chuyên trách đồng thời vận hành	Áp dụng cơ chế tổ chức thẩm định tại khoản 4 Điều 18	Tránh tự đồng nhất việc vận hành và xác nhận thẩm định

Khi đối chiếu tiêu chí dữ liệu, cần đọc đúng phạm vi từng loại hệ thống tại Điều 12 và Điều 13. Tiêu chí quy mô chủ thể dữ liệu của nhóm cung cấp dịch vụ trực tuyến khác không được hiểu thành việc chỉ cần đếm số lượt khám để tự kết luận cấp độ. Thông tin sức khỏe, quy mô dữ liệu và loại dịch vụ phải được kiểm tra cùng các tiêu chí khác; nếu cùng đáp ứng nhiều cấp độ thì áp dụng nguyên tắc tại Điều 8 [PL2].

Hồ sơ cấp độ cần đi cùng khả năng vận hành

Bệnh viện nên quản lý một danh mục đối chiếu giữa yêu cầu trong hồ sơ được phê duyệt, biện pháp đã triển khai, người vận hành và bằng chứng kiểm tra. Khi hệ thống thay đổi phạm vi, kết nối hoặc mô hình khai thác, đầu mối phụ trách cần đánh giá yêu cầu cập nhật thay vì chỉ giữ quyết định cũ trong hồ sơ hành chính.

Thời hạn báo cáo sự cố theo trách nhiệm của chủ quản

Điểm d khoản 2 Điều 31 Nghị định 331/2026/NĐ-CP quy định trách nhiệm báo cáo sự cố của chủ quản tới cơ quan chuyên trách tương ứng. Các mốc dưới đây cần được xem xét cùng tính chất sự cố; đơn vị vận hành chủ động chuyển thông tin tới chủ quản và đầu mối ứng cứu, không chờ hết thời hạn mới báo [PL2].

Trường hợp	Mốc pháp lý cần đối chiếu
Có dấu hiệu xâm phạm an ninh quốc gia, trật tự, an toàn xã hội hoặc gây gián đoạn nghiêm trọng hệ thống	Báo cáo ngay khi phát hiện
Sự cố an ninh mạng nghiêm trọng	Thông báo ban đầu trong 24 giờ kể từ khi phát hiện
Báo cáo nguyên nhân, phạm vi ảnh hưởng và biện pháp khắc phục	Trong 72 giờ kể từ khi phát hiện; sự cố phức tạp báo cáo sơ bộ, tiếp tục cập nhật và báo cáo kết thúc theo quy định

Đây là trách nhiệm báo cáo sự cố mạng của chủ quản theo Nghị định 331. Nghĩa vụ thông báo vi phạm dữ liệu cá nhân tại Điều 23 Luật Bảo vệ dữ liệu cá nhân có căn cứ riêng và có thể đồng thời phát sinh. Bệnh viện phải xác định đúng vai trò, đầu mối và hồ sơ cho từng nghĩa vụ.

Bảo vệ dữ liệu không tách khỏi nghĩa vụ lưu trữ bệnh án

Cơ sở cần xem xét từng yêu cầu cung cấp, sửa, hạn chế hoặc xóa dữ liệu trong quan hệ với nghĩa vụ lưu trữ và khai thác hồ sơ bệnh án. Không xóa dữ liệu chỉ theo một thao tác trên phần mềm khi còn nghĩa vụ pháp lý phải lưu. Cũng không dùng nghĩa vụ lưu trữ để cho phép mọi người trong đơn vị truy cập không giới hạn. Bộ phận pháp chế, lưu trữ, chuyên môn và CNTT cần có quy trình phối hợp [PL3 –PL7].

Bệnh án điện tử cần được kiểm tra thực chất

Thông tư 13/2025/TT-BYT xác định lộ trình khác nhau giữa bệnh viện và các cơ sở khám chữa bệnh khác thuộc diện áp dụng. Bệnh viện cần đối chiếu đầy đủ việc đã triển khai, khả năng truy xuất và phục hồi, thay vì xem ngày tổ chức công bố là điểm kết thúc của công việc [PL6]. Trong mỗi lần thử phục hồi, khoa sử dụng cần kiểm tra được nội dung và chức năng trong phạm vi thử.

Nguồn kỹ thuật và thuật ngữ sử dụng

KT1 Cơ quan An ninh mạng Singapore

Critical Vulnerabilities in PHP PHP2Shell, công bố 21/10/2026, cập nhật 23/10/2026. Dùng làm ví dụ về tiếp nhận cảnh báo và quản lý thành phần phần mềm.

Mở tài liệu gốc

KT2 Bộ Y tế và Dịch vụ Nhân sinh Hoa Kỳ

Thư ngày 13/3/2024 về vụ tấn công Change Healthcare. Dùng làm bài học về phụ thuộc nhà cung cấp và liên tục hoạt động; các quy định HIPAA được nêu tại nguồn không phải pháp luật áp dụng thay thế ở Việt Nam.

Mở tài liệu gốc

KT3 NIST

SP 800-61 Rev.3, tháng 4/2025. Tài liệu về tích hợp ứng phó sự cố vào quản trị rủi ro an ninh mạng.

Mở tài liệu gốc

KT4 CISA và các cơ quan phối hợp

StopRansomware Guide. Hướng dẫn tham khảo về phòng ngừa, sao lưu, ứng phó và phục hồi.

Mở tài liệu gốc

Thuật ngữ thường gặp

Thuật ngữ	Ý nghĩa sử dụng trong tài liệu
HIS	Hệ thống thông tin quản lý bệnh viện
EMR	Hồ sơ hoặc hệ thống bệnh án điện tử tùy ngữ cảnh
LIS	Hệ thống thông tin xét nghiệm
RIS và PACS	Hệ thống thông tin và hệ thống lưu trữ, truyền tải ảnh trong chẩn đoán hình ảnh
SOC	Năng lực hoặc trung tâm tổ chức giám sát, phân tích và phối hợp ứng phó an toàn thông tin
SIEM và log	Nền tảng quản lý, tương quan sự kiện và các nhật ký làm căn cứ phân tích
MFA	Xác thực đa yếu tố đối với truy cập hệ thống
RTO và RPO	Mục tiêu thời gian phục hồi và mục tiêu điểm dữ liệu có thể phục hồi
SLA	Thỏa thuận về mức dịch vụ và trách nhiệm thực hiện
AI Agent	Tác tử AI sử dụng tri thức và công cụ được cấp quyền để hỗ trợ một nhiệm vụ
Chủ quản và đơn vị vận hành	Hai vai trò cần được xác định theo quy định và mô hình quản lý từng hệ thống

Tài liệu nội bộ được sử dụng để biên soạn

Phát biểu khai mạc của lãnh đạo Sở Y tế; bài đề dẫn của Giám đốc Trung tâm; các bài chuẩn bị của bộ phận văn phòng, nghiệp vụ y, quản lý BHYT và CNTT; đề cương chuyên đề dành cho chuyên gia Hà Văn Triệu; tài liệu nền về kiến trúc SOC; chương trình lớp tập huấn đã điều chỉnh; các thuyết minh OHKE, Medcap, MedCore và AI Agent; báo cáo tầm nhìn và báo cáo sản phẩm của Trung tâm; kế hoạch đào tạo và dùng thử công cụ. Những nội dung này được tổ chức lại thành tài liệu học tập, kết hợp cập nhật pháp lý và bổ sung công cụ thực hành.

Phần thứ sáu Các nền tảng và chương trình hỗ trợ của Trung tâm

Từ một lớp tập huấn đến năng lực chung của ngành

PGS.TS. Doãn Ngọc Hải Giám đốc Trung tâm

Ngành y tế có nhiều chuyên gia, đơn vị chuyên môn và công nghệ, nhưng một bài toán chung vẫn có thể phải giải quyết lặp lại ở nhiều nơi. Một bệnh viện đã làm được quy trình tốt nhưng đơn vị khác khó tiếp cận; một cán bộ đã tham dự lớp học nhưng chưa có dữ liệu cho thấy có áp dụng được vào công việc; một yêu cầu quản lý mới cần minh chứng mà mỗi cơ sở lại tự xây biểu mẫu từ đầu. Đây là những khoảng trống về tổ chức và năng lực thực hiện mà Trung tâm hướng tới giải quyết.

Trung tâm Đào tạo và Chuyển giao công nghệ Y tế Hà Nội được thành lập theo Quyết định số 2644/QĐ-UBND ngày 25/5/2026; chức năng, nhiệm vụ được quy định tại Quyết định số 2645/QĐ-UBND cùng ngày. Giá trị Trung tâm cần tạo ra là kết nối đào tạo, nghiên cứu ứng dụng, chuyển giao công nghệ, chuyển đổi số và hợp tác quốc tế thành kết quả sử dụng được tại các cơ sở y tế.

Với an toàn thông tin, chuỗi công việc bắt đầu từ khảo sát nhu cầu và rủi ro, xác định yêu cầu quản lý, xây dựng học liệu, tổ chức trao đổi và diễn tập, hỗ trợ đơn vị lập kế hoạch, sau đó theo dõi việc áp dụng. Một lớp tập huấn tạo ra giá trị khi bệnh viện biết cách tổ chức thực hiện và kiểm chứng được năng lực dự phòng, phục hồi.

Sở Y tế thực hiện quản lý nhà nước và quyết định theo thẩm quyền. Bệnh viện làm chủ nghiệp vụ, dữ liệu và hoạt động của mình. Doanh nghiệp cung cấp năng lực kỹ thuật theo phạm vi được giao. Trung tâm kết nối các bên, làm rõ bài toán, chuẩn hóa học liệu và công cụ, tổ chức thử nghiệm, đánh giá và chuyển giao để năng lực của một nơi có thể phục vụ nhiều đơn vị.

Các nền tảng dưới đây được thiết kế để hỗ trợ chuỗi công việc đó. Khi triển khai tại đơn vị, cần xác nhận phạm vi, trạng thái sản phẩm, căn cứ xử lý dữ liệu, điều kiện kỹ thuật và tiêu chí đánh giá. Phiên bản trình diễn và thử nghiệm là cơ sở để xem xét sử dụng; việc mở rộng phải gắn với trách nhiệm quản lý, kết quả kiểm tra và quyết định theo thẩm quyền.

Các bài toán và công cụ tương ứng

Nhu cầu của đơn vị	Nền tảng hoặc công cụ	Giá trị có thể kiểm tra
Điều phối nhân lực và lịch khám sức khỏe	OHKE	Kế hoạch, tiến độ, điểm nghẽn và kết quả theo từng khâu khám
Biết năng lực hiện có và phần cần bồi dưỡng	Medcap	Hồ sơ đã xác minh, khoảng trống năng lực và kế hoạch phát triển
Xây dựng vị trí việc làm bằng minh chứng	Cẩm nang điện tử và công cụ VTVL	Mô tả công việc, khối lượng, nguồn dữ liệu và tiến độ hồ sơ

Nhu cầu của đơn vị	Nền tảng hoặc công cụ	Giá trị có thể kiểm tra
Tổ chức học có phản hồi và theo dõi	MEDU và các cấu phần quản lý đào tạo	Lượt học, kết quả trả lời, nội dung cần hướng dẫn lại
Khảo sát đúng nhu cầu	MedSurvey	Dữ liệu nhu cầu theo nhóm đơn vị và ưu tiên đào tạo
Tổng hợp, tra cứu và hỗ trợ điều hành	MedCore và AI Agent dành cho lãnh đạo	Dự thảo có nguồn, số liệu đối chiếu được và bước phê duyệt

OHKE Nền tảng quản lý và điều phối nguồn lực khám sức khỏe

OHKE phát triển từ sáng kiến cải cách công vụ của Trung tâm, nhằm hỗ trợ tổ chức khám sức khỏe theo một quy trình có thể điều phối và theo dõi. Thay vì tổng hợp rời rạc bằng nhiều bảng, công cụ kết nối nhu cầu tại địa bàn với năng lực chuyên môn, nhân lực, thiết bị, xét nghiệm và lịch có thể huy động của cơ sở tham gia.

Các khâu điều phối

Quy trình hướng tới quản lý đối tượng và nhu cầu khám; lập kế hoạch, phân công nguồn lực và lịch; mời, tiếp đón, phân luồng; theo dõi hoàn thành các nội dung khám; trả kết quả và theo dõi tiếp sau khám. Việc liên thông hoặc cập nhật sang hệ thống sức khỏe điện tử, VNeID và các hệ thống khác được thực hiện khi có quyền, chuẩn và kết nối được xác nhận.

Lãnh đạo cần nhìn thấy địa bàn chậm, khâu còn thiếu và nguồn lực có thể bổ sung. Ví dụ, một điểm khám còn tồn do thiếu năng lực siêu âm hoặc xét nghiệm; công cụ hỗ trợ xác định phần thiếu, đối chiếu cơ sở có thể hỗ trợ và đề xuất lịch điều phối. Quyết định chuyên môn và huy động nguồn lực vẫn do chủ thể có thẩm quyền thực hiện.

Giá trị đối với từng nhóm

Nhóm sử dụng	Giá trị hướng tới	Dữ liệu hoặc kết quả cần xác nhận
Sở Y tế và đầu mối điều phối	Theo dõi tiến độ toàn mạng lưới, giao nhiệm vụ và xử lý điểm nghẽn	Tình trạng cập nhật, năng lực cung ứng, trách nhiệm và lịch đã xác nhận
Bệnh viện và đơn vị khám	Chuẩn bị đoàn khám, bố trí nhân lực và theo dõi kết quả	Lịch, nhân sự đủ điều kiện, dịch vụ đã thực hiện và hồ sơ kết quả
Trạm y tế và địa bàn	Tổ chức mời, tiếp nhận, hướng dẫn và theo dõi sau khám	Danh sách được phép sử dụng, trạng thái khám và nhu cầu theo dõi
Người dân	Được hướng dẫn rõ, giảm bỏ sót khâu và tiếp cận kết quả	Lịch và kênh thông tin hợp lệ; kết quả được bảo vệ

Phạm vi và trạng thái giới thiệu

Theo báo cáo sản phẩm của Trung tâm phục vụ cuộc họp ngày 29/10/2026, nền tảng điều phối đã có phiên bản hoàn thành, chạy thực tế và đang được đánh giá để trình Sở Y tế; Trung tâm xác định khả năng áp dụng từ ngày 01/11/2026. Phạm vi triển khai tại từng đơn vị cần được thống nhất và kiểm tra trước khi sử dụng chính thức; thông tin này không thay thế quyết định tổ chức triển khai trên toàn ngành.

Khám sức khỏe toàn dân theo vòng đời và khám sức khỏe định kỳ cho người lao động có mục tiêu, đối tượng và căn cứ áp dụng cần được phân biệt. Khi xây dựng luồng khám doanh nghiệp, công cụ phải phản ánh điều kiện lao động và nguy cơ nghề nghiệp trong phạm vi yêu cầu áp dụng; không mặc định một lần khám thay thế mọi nghĩa vụ khám khác.

Đơn vị quan tâm có thể đăng ký xem quy trình và đề nghị thử một đợt điều phối với mục tiêu cụ thể, ưu tiên dùng dữ liệu giả lập hoặc dữ liệu đã được phép. Kết quả thử cần đo được việc phân công, theo dõi hoàn tất, xử lý tồn đọng và khả năng bảo vệ dữ liệu.

Medcap Hộ chiếu năng lực số ngành y tế

Medcap tổ chức hồ sơ năng lực của mỗi người gắn với minh chứng, yêu cầu vị trí việc làm và kế hoạch phát triển. Cá nhân có thể nhìn thấy điểm mạnh và năng lực cần bổ sung; đơn vị có dữ liệu đã xác minh để bố trí đào tạo và chuẩn bị nguồn nhân lực. Báo cáo tổng hợp cần được xây dựng đúng phân quyền và từ dữ liệu đủ căn cứ.

Quy trình hình thành hồ sơ

Cá nhân cập nhật tài liệu như văn bằng, chứng chỉ và minh chứng công việc. AI có thể hỗ trợ nhận diện tài liệu, trích xuất thông tin và gợi ý liên kết với nhóm năng lực. Người dùng kiểm tra dữ liệu đề xuất; đơn vị thực hiện xác minh theo thẩm quyền. Dữ liệu đã được xác minh mới được sử dụng như thông tin chính thức trong phạm vi quy trình của nền tảng.

Từ hồ sơ đó, người dùng đối chiếu với năng lực yêu cầu của vị trí và lập kế hoạch bổ sung gồm mục tiêu, hoạt động, thời hạn, người hỗ trợ, minh chứng và tiêu chí hoàn thành. Việc dự học là một thông tin; khả năng áp dụng vào công việc cần có bằng chứng tiếp theo.

Ví dụ sử dụng sau lớp an toàn thông tin

Một đầu mối CNTT có thể bổ sung minh chứng đã tham gia lớp, bài tập đã hoàn thành và biên bản thử phục hồi do đơn vị xác nhận. Một trưởng khoa có thể bổ sung minh chứng đã hoàn thiện quy trình dự phòng và tham gia diễn tập. Cách ghi nhận này gắn đào tạo với năng lực làm việc thay vì chỉ lưu giấy chứng nhận.

Trạng thái và điều kiện thử nghiệm

Medcap đã có thuyết minh nền tảng và nguyên mẫu; việc dùng thử được tổ chức theo phạm vi Trung tâm xác nhận. Khi phối hợp, đơn vị cần thống nhất khung năng lực, quy trình xác minh, quyền của cá

nhân, mục đích sử dụng và chế độ bảo vệ hồ sơ nhân sự. Medcap hỗ trợ cung cấp dữ liệu; các quyết định nhân sự và công nhận điều kiện chuyên môn thuộc người có thẩm quyền theo quy định.

VTVL Cẩm nang điện tử và công cụ xây dựng đề án vị trí việc làm

Bộ công cụ VTVL hỗ trợ đơn vị đi từ chức năng, nhiệm vụ tới sản phẩm công việc, khối lượng, minh chứng, mô tả vị trí và yêu cầu năng lực. Đối với bệnh viện, điểm khó là chứng minh bằng hoạt động thực tế của nhiều khoa, phòng và tổ chức dữ liệu thống nhất, có nguồn kiểm tra.

Những việc công cụ hỗ trợ

- Tập hợp căn cứ, chức năng, nhiệm vụ và cơ cấu của đơn vị theo phiên bản được sử dụng.
- Phân tích công việc, đầu ra, quy trình và mối liên hệ giữa khoa chuyên môn với phòng chức năng.
- Tổ chức dữ liệu khối lượng công việc và minh chứng trong kỳ thống kê, có người kiểm tra và xác nhận.
- Hỗ trợ mô tả vị trí, yêu cầu năng lực, phân tích nhu cầu và hoàn thiện các phụ lục.
- Theo dõi tiến độ, phần còn thiếu và các vướng mắc cần người có thẩm quyền hướng dẫn.

Trạng thái và phương thức phối hợp

Theo báo cáo sản phẩm ngày 29/10/2026, Trung tâm đã hoàn thành cẩm nang điện tử và công cụ hỗ trợ thực hành, đã chạy thực tế và đang đánh giá tại Trung tâm cùng một bệnh viện hạng II. Định hướng tiếp theo là trình Sở Y tế thử nghiệm rộng hơn và phổ biến sau đánh giá. Việc thẩm định, phê duyệt đề án và quyết định nhân lực vẫn phải thực hiện theo đúng thẩm quyền.

Đơn vị đăng ký có thể lựa chọn lớp hướng dẫn phương pháp, lớp thực hành dữ liệu hoặc nhu cầu hỗ trợ rà soát hồ sơ. Sản phẩm cần thống nhất ngay từ đầu: dữ liệu nào phải thu thập, ai xác nhận, bộ phụ lục nào phải hoàn thành và cách kiểm tra tính nhất quán.

Liên hệ với an toàn thông tin: vị trí phụ trách CNTT, dữ liệu, quản lý chất lượng và ứng cứu cần được mô tả bằng nhiệm vụ và sản phẩm cụ thể. Khi nhân sự thay đổi, phải có cơ chế bàn giao quyền, tài liệu và trách nhiệm vận hành; hồ sơ vị trí việc làm cần giúp đơn vị duy trì được năng lực này.

MedCore và AI Agent dành cho lãnh đạo

AI Agent dành cho lãnh đạo là công cụ hỗ trợ tiếp nhận yêu cầu, tra cứu nguồn được cấp quyền, gọi các công cụ phù hợp và tạo dự thảo có căn cứ. Trên định hướng MedCore, Trung tâm đề xuất tổ chức năng lực hạ tầng, tri thức và AI dùng chung; các đơn vị quản lý dữ liệu và phát triển ứng dụng theo nghiệp vụ của mình.

Các tình huống sử dụng để thử nghiệm

Yêu cầu của lãnh đạo	Dữ liệu cần được phép sử dụng	Kết quả mong đợi và người quyết định
Tổng hợp nhiệm vụ chậm và nội dung cần xử lý	Văn bản giao việc, hạn, trạng thái và minh chứng	Báo cáo có nguồn, danh sách cần kiểm tra; lãnh đạo quyết định điều hành
Chuẩn bị báo cáo giao ban	Mẫu báo cáo và số liệu đã xác nhận	Bản dự thảo kèm nguồn và điểm mâu thuẫn; bộ phận phụ trách kiểm tra
Tra cứu quy trình và văn bản	Kho tri thức có phiên bản, hiệu lực và phân quyền	Câu trả lời có dẫn nguồn; người sử dụng đối chiếu văn bản gốc
Tổng hợp tiến độ khắc phục ATTT	Sổ rủi ro, người phụ trách, hạn và biên bản kiểm tra	Danh mục chưa đạt và câu hỏi cần làm rõ; không tự công nhận an toàn
Gợi ý phương án phân công hoặc lịch	Năng lực, số lượng người, điều kiện và ràng buộc đã xác nhận	Các phương án có giải thích; người có thẩm quyền phê duyệt

Thiết kế để lãnh đạo kiểm tra được

Số liệu và phép tính phải dựa trên nguồn dữ liệu hoặc công cụ xác định được, có thể đối chiếu. AI hỗ trợ diễn giải, tổng hợp và soạn thảo; kết quả cần hiển thị nguồn, thời điểm dữ liệu và giới hạn thông tin. Quyền xem, soạn nháp và thực hiện hành động có tác động cần được tách riêng trong thiết kế.

Những thao tác như sửa bệnh án, quyết định điều trị, phê duyệt nhân sự, chi trả, gửi văn bản hoặc chuyển dữ liệu ra bên ngoài phải tuân thủ thẩm quyền và quy trình được phê duyệt. Khi AI không hoạt động, các quy trình khám chữa bệnh cốt lõi và công việc thiết yếu phải có phương án tiếp tục.

Trạng thái và đề nghị tham gia

MedCore và AI Agent đã có tài liệu kiến trúc, thuyết minh và các kịch bản đề xuất; hạ tầng dùng chung và năng lực thực tế cần được kiểm chứng qua thử nghiệm. Bệnh viện quan tâm có thể đề nghị chọn một nhiệm vụ quản trị ít rủi ro, xác định dữ liệu được phép, tiêu chí đầu ra, thời gian tiết kiệm và cách kiểm tra sai số trước khi mở rộng.

MEDU và MedSurvey trong phát triển năng lực

MEDU hỗ trợ tổ chức học liệu chủ động theo nhiều lớp, kết hợp nội dung ngắn, ví dụ, câu hỏi và phần tra cứu sâu. Mỗi người có tài khoản để học; câu hỏi ngắn, trong đó có hình thức trả lời khoảng 10 giây, được sử dụng để tạo tương tác và nhận diện điểm chưa hiểu đúng. Dữ liệu học giúp người phụ trách biết ai đã bắt đầu, ai đã hoàn thành và nội dung nào cần hướng dẫn lại.

Hình thức câu hỏi nhanh cần phù hợp độ khó của nội dung. Đối với trách nhiệm pháp lý và quy trình có nguy cơ cao, cần kết hợp đọc tài liệu, giải thích, thảo luận và thực hành; số lượt trả lời nhanh không được dùng riêng để kết luận năng lực thực hiện. Kết quả áp dụng tại đơn vị có thể tiếp tục được ghi nhận trong hồ sơ năng lực.

MEDU đang được triển khai, thử nghiệm tại Trung tâm theo báo cáo nội bộ. MedSurvey hỗ trợ khảo sát nhu cầu theo nhóm bệnh viện, trạm y tế và các đơn vị khác, làm cơ sở lựa chọn lớp và ưu tiên hỗ trợ. Mỗi đợt sử dụng cần xác định mục đích, người xem báo cáo, dữ liệu được thu và tiêu chí đánh giá.

Với chuyên đề an toàn thông tin, Trung tâm có thể hỗ trợ xây dựng học liệu theo vị trí: lãnh đạo học cách chỉ đạo và kiểm tra; nhân viên chuyên môn học quy trình dự phòng; CNTT học cách tổ chức minh chứng kỹ thuật. Câu trả lời dễ sai trở thành đầu vào để điều chỉnh tập huấn và giảm nguy cơ hiểu khác nhau trong cùng bệnh viện.

Danh mục các lớp tập huấn và chương trình hỗ trợ

Danh mục dưới đây phục vụ đăng ký nhu cầu và tổ chức kế hoạch tiếp theo. Thời lượng là gợi ý; lịch, giảng viên, quy mô, kinh phí và hình thức tổ chức được Trung tâm thông báo khi có kế hoạch cụ thể. Việc cấp chứng nhận hoặc công nhận giờ cập nhật kiến thức y khoa liên tục thực hiện theo điều kiện và quy định áp dụng của từng chương trình.

Mã	Lớp và nhóm tham gia	Sản phẩm sau lớp
DT01	Trách nhiệm pháp lý và bảo vệ hệ thống theo cấp độ Lãnh đạo, pháp chế, CNTT Thời lượng gợi ý 0,5–1 ngày	Phiếu khoảng trống tuân thủ và kế hoạch hoàn thiện hồ sơ
DT02	SOC, sao lưu, ứng cứu và diễn tập ATTT CNTT, KHTH, quản lý chất lượng, khoa trọng yếu Thời lượng gợi ý 1–2 ngày	Kịch bản ứng cứu, biên bản thử khôi phục và danh mục cải tiến
DT03	Bệnh án điện tử và duy trì hoạt động an toàn Lãnh đạo, KHTH, CNTT, điều dưỡng Thời lượng gợi ý 1 ngày	Bảng rà soát quy trình, dữ liệu, xác nhận điện tử và dự phòng
DT04	Ứng dụng AI trong quản lý dành cho lãnh đạo Lãnh đạo đơn vị và trưởng khoa phòng Thời lượng gợi ý 0,5–1 ngày	Một quy trình sử dụng AI có nguồn, kiểm tra và phê duyệt
DT05	AI hỗ trợ xây dựng đề án vị trí việc làm TCCB, KHTH, trưởng khoa phòng Thời lượng gợi ý 1–2 ngày	Bộ dữ liệu và phụ lục mẫu có kiểm tra minh chứng
DT06	Thực hành xây dựng và rà soát hồ sơ VTVL Nhóm lập đề án tại đơn vị Thời lượng gợi ý Theo nhu cầu	Hồ sơ công việc, khối lượng, vị trí và danh mục cần hoàn thiện
DT07	Điều phối khám sức khỏe toàn dân với OHKE Đầu mối điều phối, BV, trạm y tế Thời lượng gợi ý 1 ngày	Kế hoạch một đợt khám, phân công, tiến độ và xử lý tồn đọng
DT08	Ứng dụng AI và dữ liệu trong quản lý khám sức khỏe Đơn vị khám, y tế lao động, CNTT Thời lượng gợi ý 1 ngày	Quy trình dữ liệu, báo cáo và kiểm soát chất lượng theo loại hình khám

Mã	Lớp và nhóm tham gia	Sản phẩm sau lớp
DT09	Hội thảo và lộ trình bệnh viện thông minh Ban giám đốc, chuyên môn, CNTT Thời lượng gợi ý 0,5–1 ngày	Danh mục bài toán ưu tiên và tiêu chí lựa chọn, thử nghiệm
DT10	Xây dựng kế hoạch chuyển giao công nghệ cho bệnh viện KHTH, đào tạo, chuyên môn, thiết bị Thời lượng gợi ý 1 ngày	Kế hoạch tiếp nhận, đào tạo, làm chủ và đánh giá công nghệ
DT11	Lập kế hoạch hợp tác quốc tế và phát triển dự án Lãnh đạo, HTQT, nghiên cứu, đào tạo Thời lượng gợi ý 1 ngày	Đầu bài hợp tác, vai trò đối tác, nguồn lực và sản phẩm
DT12	Quản trị bệnh viện bằng dữ liệu tài chính và BHYT Lãnh đạo, tài chính, BHYT, KHTH Thời lượng gợi ý 1 ngày	Bộ chỉ số và báo cáo điều hành có đối soát nguồn số liệu
DT13	MEDU và Medcap trong quản lý đào tạo và năng lực Đào tạo, tổ chức cán bộ, trưởng khoa Thời lượng gợi ý 0,5–1 ngày	Học liệu mẫu, hồ sơ năng lực và kế hoạch phát triển
DT14	Khảo sát nhu cầu và xây dựng kế hoạch đào tạo BV, trạm y tế và các đơn vị khác Thời lượng gợi ý 0,5–1 ngày	Phiếu khảo sát, phân nhóm nhu cầu và kế hoạch theo ưu tiên

Hỗ trợ theo bài toán của từng đơn vị

Ngoài lớp tập huấn, đơn vị có thể đề nghị khảo sát nhu cầu, hướng dẫn phương pháp, rà soát hồ sơ, tổ chức thử nghiệm công cụ hoặc xây dựng đề xuất chuyển giao. Phạm vi hỗ trợ, sản phẩm, trách nhiệm, dữ liệu sử dụng và điều kiện tài chính phải được thống nhất bằng hồ sơ phù hợp trước khi thực hiện.

Đăng ký nhu cầu và đầu mối phối hợp với Trung tâm

Một đề nghị rõ bài toán giúp Trung tâm lựa chọn chương trình, chuyên gia và hình thức hỗ trợ phù hợp. Đơn vị nên cử một đầu mối quản lý và một đầu mối chuyên môn hoặc kỹ thuật để trao đổi, xác nhận phạm vi và theo dõi kết quả.

Phiếu đăng ký nhu cầu

Tên đơn vị: .....

Đầu mối quản lý và liên hệ công vụ: .....

Đầu mối chuyên môn hoặc kỹ thuật: .....

Mã lớp hoặc nền tảng quan tâm: .....

Bài toán đang cần giải quyết: .....

Sản phẩm mong muốn sau phối hợp: .....

Số người và nhóm vị trí tham gia dự kiến: .....

Điều kiện hiện có và khó khăn chính: .....

Thời gian phù hợp đề nghị: .....

Người xác nhận của đơn vị: .....

Phiếu đăng ký chỉ ghi thông tin công vụ và mô tả nhu cầu. Hồ sơ bệnh án, dữ liệu định danh, tài khoản truy cập, mật khẩu và sơ đồ mạng chi tiết chỉ được trao đổi sau khi có phạm vi và biện pháp bảo vệ phù hợp.

Quy trình phối hợp

Trung tâm tiếp nhận nhu cầu, trao đổi để xác định bài toán, thống nhất điều kiện và phương thức thực hiện, tổ chức đào tạo hoặc thử nghiệm theo phạm vi được phê duyệt, sau đó đánh giá sản phẩm và đề xuất bước tiếp theo. Đơn vị tham gia kiểm tra dữ liệu, cử đúng người, xác nhận kết quả và tổ chức áp dụng trong phạm vi trách nhiệm của mình.

Thông tin liên hệ

Trung tâm Đào tạo và Chuyển giao công nghệ Y tế Hà Nội
Số 4 phố Sơn Tây, phường Ba Đình, Hà Nội
Điện thoại 0356 255 468
Đào tạo training@hanoimedtech.vn | Chuyển giao transfer@hanoimedtech.vn
Văn phòng office@hanoimedtech.vn

Lịch đào tạo và đăng ký nhu cầu hanoimedtech.vn/dao-tao-cme