Phần 2. YÊU CẦU VỀ KỸ THUẬT
Chương V. YÊU CẦU VỀ KỸ THUẬT

Yêu cầu về kỹ thuật bao gồm các nội dung cơ bản như sau:

1. Giới thiệu chung về dự án/dự toán mua sắm, gói thầu:

- Tên dự toán mua sắm: Thuê dịch vụ Công nghệ thông tin nâng cấp phần mềm HIS, thuê bệnh án điện tử (EMR) của Trung tâm Y tế Mường Nhé;
- Tên Thuê dịch vụ Công nghệ thông tin nâng cấp phần mềm HIS, thuê bệnh án điện tử (EMR) của Trung tâm Y tế Mường Nhé.
- Chủ đầu tư: Trung tâm Y tế Mường Nhé. Địa chỉ: Tổ dân cư số 3, xã Mường Nhé, Tỉnh Điện Biên
- Hình thức lựa chọn nhà thầu: Đấu thầu rộng rãi, trong nước, qua mạng.
- Phương thức lựa chọn nhà thầu: Một giai đoạn 01 túi hồ sơ
- Nguồn vốn: Nguồn ngân sách Nhà nước, nguồn thu từ dịch vụ khám chữa bệnh, và nguồn thu hợp pháp khác của đơn vị.
- Thời gian bắt đầu tổ chức lựa chọn nhà thầu: Tháng 10, 2025
- Loại hợp đồng: Trọn gói
- Thời gian thực hiện gói thầu: 60 tháng

2. Mục tiêu công việc:

2.1. Mục tiêu chung

Cung cấp một hệ thống bệnh án điện tử hiện đại bao gồm các quy trình từ tác nghiệp đến các báo cáo trong công tác khám bệnh lâm sàng, cận lâm sàng, điều trị, dược, … và hệ thống quản trị hệ thống dữ liệu trong toàn Trung tâm, phù hợp với yêu cầu của Trung tâm giúp nâng cao hiệu quả, chất lượng khám chữa bệnh, chăm sóc sức khỏe nhân dân được tốt hơn và giảm tải cho cán bộ, y bác sỹ và hướng đến xây dựng Trung tâm thông minh trong tương lai theo Thông tư 54/2017/TT-BYT.

2.2. Mục tiêu cụ thể

Nâng cấp phần mềm HIS, thuê bệnh án điện tử bao gồm các chức năng:

- Quản lý tạo bệnh án điện tử;
- Quản lý vỏ bệnh án;
- Quản lý biểu mẫu, phiếu, tờ;
- Quản lý kết quả cận lâm sàng;
- Quản lý ký số;
- Nâng cấp 6 phân hệ của phần mềm HIS bao gồm: phân hệ Khám bệnh, Dược, Xét Nghiệm, Chẩn đoán hình ảnh, Báo cáo, Viện phí.

3. Yêu cầu kỹ thuật

3.1. Yêu cầu về chất lượng dịch vụ CNTT

3.1.1. Yêu cầu về chất lượng của phần mềm

STT	Hạng mục dịch vụ	Yêu cầu dịch vụ

1	Yêu cầu về chất lượng dịch vụ	Giải pháp phải có tính ổn định cao (phần mềm, phần cứng, hạ tầng mạng), đáp ứng nhu cầu xử lý công việc cho các phòng, ban chức năng trong việc quản lý khám chữa bệnh. Khi có sự thay đổi các tính năng yêu cầu thì phải đáp ứng kịp thời và linh hoạt tùy biến cho người sử dụng.
2	Phương án, cách thức cung cấp dịch vụ	Chủ trì thuê dịch vụ ký kết với nhà cung cấp dịch vụ. Nhà cung cấp dịch vụ đáp ứng nhu cầu cho bên sử dụng mọi lúc, mọi nơi.
3	Điều kiện cung cấp dịch vụ	Bên Thuê: cử cán bộ, công chức, viên chức phối hợp với Bên cho Thuê trong việc tập huấn, khai thác sử dụng. Bên cho Thuê: Hệ thống đảm bảo các tính năng, yêu cầu kỹ thuật do Bộ Thông tin và Truyền thông, Bộ y tế, Bộ Công an quy định, hệ thống chạy liên tục, ổn định; đáp ứng nhu cầu cho người sử dụng mọi lúc, mọi nơi khi có yêu cầu. Cung cấp dịch vụ đảm bảo chất lượng tốt nhất. Cải tạo, nâng cấp hạ tầng CNTT của Trung tâm để đáp ứng với yêu cầu phần mềm và bảo mật an toàn an ninh thông tin

Yêu cầu kỹ thuật dựa trên chất lượng đầu ra của phần mềm

✓ (Thông tư số 23/2020/TT-BTTTT ngày 09/9/2020 của Bộ trưởng Bộ TT&TT).

Bảng yêu cầu kỹ thuật dựa trên chất lượng đầu ra của Hệ thống phần mềm bệnh án điện tử như sau:

STT	**Tiêu chí**		**Yêu cầu chất lượng**	**Yêu cầu đầu ra**	
				Giai đoạn chuẩn bị cung cấp dịch vụ	**Giai đoạn thuê dịch vụ**
				Chỉ số/hoạt động thành phần tham khảo cho phép kiểm tra đánh giá	*Chỉ số/hoạt động thành phần tham khảo cho phép đánh giá*
1	**Các tiêu chí về công nghệ**				
	Cơ sở dữ liệu		Oracle 11 trở lên hoặc tương đương		*Đáp ứng*

	Hệ điều hành máy chủ hệ thống		Windows Server 2012 R2 trở lên		*Đáp ứng*
	Ngôn ngữ lập trình		Backend: C# (.NET Core), sử dụng để xây dựng các API, xử lý nghiệp vụ (Services), và kết nối cơ sở dữ liệu. Frontend: Angular dùng để xây dựng giao diện người dùng và giao tiếp với API backend.		*Đáp ứng*
	Môi trường thực thi		Phần mềm vận hành trên nền Web application và nền tảng App mobile.		*Đáp ứng*
	Ngôn ngữ		Tiếng Việt, theo tiêu chuẩn Unicode TCVN 6909:2001		*Đáp ứng*
	Hệ điều hành máy trạm		Hệ điều hành Windows 10 trở lên		*Đáp ứng*
2	**Các tiêu chí về chức năng nghiệp vụ**				
2.1	Tính đầy đủ của chức năng nghiệp vụ		Hệ thống bao gồm các nhóm chức năng: - Quản trị danh mục - Quản trị hệ thống - Quản lý tiếp nhận - Quản lý khám bệnh ngoại trú - Quản lý khám bệnh nội trú - Quản lý kết quả chẩn đoán hình ảnh	Thực hiện vận hành kiểm thử để đánh giá mức độ đáp ứng yêu cầu chất lương	Thực hiện kiểm tra các báo cáo kết quả cung cấp dịch vụ của hệ thống để đánh giá mức độ đáp ứng yêu cầu chất lượng

			- Quản lý kết quả thăm dò chức năng - Quản lý cấp cứu - Quản lý khoa lâm sàng/người bệnh nội trú - Quản lý phòng mổ - Quản lý thủ thuật - Quản lý danh sách, hàng đợi - Quản lý thẻ, barcode - Quản lý thanh toán viện phí và BHYT - Quản lý dược, nhà thuốc Trung tâm - Khai thác thống kê, báo cáo - Quản lý nhân viên - Quản lý xét nghiệm - Kết nối máy xét nghiệm		
2.2	Tính chính xác của các chức năng nghiệp vụ		Phải ghi nhận toàn bộ nội dung, thông tin Hệ thống phần mềm bệnh án điện tử theo quy định của Bộ Y tế: - Thông tư số 53/2014/TT-BYT ngày 29/12/2014 của Bộ Y tế quy định điều kiện hoạt động y tế trên môi trường mạng; - Thông tư số 54/2017/TT-BYT ngày 29/12/2017 của Bộ Y tế về ban	Thực hiện vận hành kiểm thử để đánh giá mức độ đáp ứng yêu cầu chất lượng	Thực hiện kiểm tra các báo cáo kết quả cung cấp dịch vụ của hệ thống để đánh giá mức độ đáp ứng yêu cầu chất lượng

			hành Bộ Tiêu chí ứng dụng CNTT tại các cơ sở khám bệnh, chữa bệnh; - Quyết định số 2035/QĐ-BYT ngày 12/06/2013 của Bộ Y tế về việc công bố danh mục kỹ thuật về ứng dụng CNTT trong lĩnh vực y tế; - Quyết định số 5573/QĐ-BYT, ngày 29 tháng 12 năm 2006 của Bộ Y tế về việc ban hành "Tiêu chí phần mềm và nội dung một số phân hệ phần mềm tin học quản lý Trung tâm"; - Quyết định số 5004/QĐ-BYT, ngày 19 tháng 9 năm 2016 của Bộ trưởng Bộ Y tế về việc phê duyệt mô hình kiến trúc tổng thể hệ thống thông tin khám chữa bệnh bảo hiểm y tế.		
2.3	Tính phù hợp của chức năng với nghiệp vụ		- Chuẩn y khoa HL7, HL7CDA - Tiêu chuẩn hình ảnh số và truyền tải trong y tế: DICOM; - Tiêu chuẩn kết nối, liên thông và trao đổi dữ liệu giữa các	Thực hiện vận hành kiểm thử để đánh giá mức độ đáp ứng yêu cầu chất lượng	Thực hiện kiểm tra các báo cáo kết quả cung cấp dịch vụ của hệ thống để đánh giá mức độ đáp

			ứng dụng và thiết bị y tế. Đáp ứng các quy định của Bộ Y Tế: 5573, 4210, 13, 54… - Tiêu chuẩn kết nối, tích hợp dữ liệu, truy cập thông tin, an toàn thông tin và đặc tả dữ liệu; - Tiêu chuẩn kết nối, tiêu chuẩn về tích hợp dữ liệu, tiêu chuẩn về truy cập thông tin, tiêu chuẩn về an toàn thông tin, tiêu chuẩn về dữ liệu đặc tả sẽ căn cứ theo Danh mục tiêu chuẩn về ứng dụng CNTT trong cơ quan nhà nước đã được ban hành theo Thông tư số 39/2017/TT-BTTTT của Bộ Thông tin và Truyền thông công bố Danh mục tiêu chuẩn kỹ thuật về ứng dụng CNTT trong cơ quan nhà nước.		ứng yêu cầu chất lượng
3	**Các tiêu chí về hiệu năng vận hành**				
3.1	Hiệu năng đáp ứng của dịch vụ		Hệ thống phải đáp ứng yêu cầu về các chức năng, số lượng người dùng tham gia khai thác, sử dụng hệ thống; khả năng tích hợp dữ	Thực hiện vận hành kiểm thử để đánh giá mức độ đáp ứng yêu cầu chất lượng	Thực hiện kiểm tra các báo cáo kết quả cung cấp dịch vụ của hệ thống để đánh giá

			liệu với các bộ, ngành, địa phương như đã nêu trên và các yêu cầu sau đây: + Về thời gian: Thời gian cho phép để hệ thống phản hồi lại thông tin đã tiếp nhận yêu cầu xử lý từ phía người sử dụng là 3 giây (s); thời gian cho phép để hiện thị đầy đủ KPI là 10 (s); thời gian cho phép để gửi kết quả tìm kiếm thông tin là 10 (s). + Hiệu năng không bị ảnh hưởng từ các yếu tố như:		mức độ đáp ứng yêu cầu chất lượng
			Thời gian, sự tăng trưởng về dữ liệu chính; bảo đảm có khả năng hoạt động không bị ảnh hưởng về dữ liệu trong tối thiểu 10 năm (trong điều kiện sẵn sàng về hạ tầng lưu trữ).		
3.2	Khả năng mở rộng của dịch vụ		Giải pháp đưa ra phải dễ dàng kết nối cũng như tích hợp thêm các giải pháp khác khi cần thiết. Hệ thống cho phép dễ dàng mở rộng khi Trung tâm cần triển khai thêm hoặc ngưng các Trung tâm vệ tinh (Trung	Thực hiện kiểm tra các tài liệu liên quan đến giải pháp, phương án triển khai của nhà cung cấp dịch vụ	

			tâm dã chiến…) triển khai mô hình tập trung, trên cùng nền tảng, công nghệ, hạ tầng và server tập trung.		
			Hiệu suất lưu trữ, sao lưu dữ liệu phải đáp ứng 100%	Thực hiện kiểm tra các tài liệu liên quan đến giải pháp	
4	**Các tiêu chí về an toàn thông tin**				
4.1	Bảo mật thông tin		- Hệ thống phần mềm có một module bảo mật được thiết kế riêng cho mức ứng dụng. Một người sử dụng muốn chạy chương trình và thực hiện một số chức năng cụ thể thì phải được quản trị hệ thống cấp cho một tài khoản và gán cho các quyền tương ứng với các chức năng (xem thêm yêu cầu chức năng về quản trị hệ thống được trình bày tại mục trên). - Hệ thống ứng dụng phải có khả năng kiểm soát chặt chẽ việc thay đổi các dữ liệu quan trọng để đảm bảo các dữ liệu này không thể thay đổi nếu chưa được	Thực hiện vận hành kiểm thử để đánh giá mức độ đáp ứng yêu cầu chất lượng	Thực hiện kiểm tra các báo cáo kết quả cung cấp dịch vụ của hệ thống để đánh giá mức độ đáp ứng yêu cầu chất lượng

			xử lý một cách đúng đắn. - Hệ thống phải được thiết kế dựa trên một hệ thống bảo mật nhiều lớp và chặt chẽ. Các cấp bảo mật mà hệ thống đưa ra bao gồm: - Mức hệ điều hành: Các hệ điều hành có rất nhiều công cụ và công nghệ bảo mật cao. Mỗi sản phẩm chạy trên hệ điều hành đều có thể tận dụng các tính năng này. - Mức cơ sở dữ liệu: hệ cơ sở dữ liệu đa người dùng phải cung cấp các tính năng bảo mật, kiểm soát việc truy cập và sử dụng cơ sở dữ liệu như: ngăn chặn các truy cập dữ liệu bất hợp pháp, ngăn chặn việc truy cập bất hợp pháp vào các bảng dữ liệu, các thủ tục, tiến trình thiết lập trong CSDL. - Mức ứng dụng: Người sử dụng hệ thống phải được cấp		

			quyền và xác thực trước khi sử dụng. - Bảo mật mạng truyền thông: Bao gồm. + Bảo mật WebServer: Là cơ chế dựa chủ yếu vào các cơ chế bảo mật của phần mềm máy chủ Web (WebServer). +Tường lửa: Là mức bảo mật ở mức hệ thống, đóng vai trò quan trọng đối với hệ thống được xây dựng dựa trên các ứng dụng 3 lớp. Bức tường lửa được xây dựng như một máy chủ kiểm soát các luồng thông tin vào ra với hệ thống nhằm mục đích tránh bị tấn công từ Internet và các cơ hội bị kiểm soát hệ thống từ xa. - Hệ thống được xây dựng và thực hiện giải pháp sao lưu dự phòng, được thiết kế để bảo đảm khắc phục, phục hồi các sự cố về dữ liệu, ứng dụng, cũng như hệ điều hành. Khi cơ sở dữ liệu, máy chủ ứng dụng hoặc		

			hệ điều hành bị sụp đổ, hệ thống phải đảm bảo các dữ liệu backup cho việc phục hồi trạng thái làm việc ổn định. Việc thực hiện sao lưu (back-up) hệ thống được thực hiện theo quy định cụ thể và theo các chu kỳ khác nhau bao gồm ngày, tuần và tháng. - Hỗ trợ khả năng cấu hình ứng dụng đảm bảo khả năng bảo mật nhiều mức (trình diễn, nghiệp vụ, truy cập dữ liệu); giải pháp xác thực đạt mức độ bảo mật cao theo tiêu chuẩn quốc tế; sử dụng kênh kết nối an toàn trong việc truy cập máy chủ ứng dụng và công cụ quản lý. - Bảo đảm đáp ứng khả năng an toàn, bảo mật theo nhiều mức (hạ tầng, hệ thống, định danh đơn vị, cá nhân, xác thực đến thiết bị,…); tất cả các truy xuất vào kênh truyền dữ liệu đều phải được an toàn,		

			dữ liệu phải bảo đảm toàn vẹn, bảo mật trên đường truyền; hỗ trợ cơ chế bảo vệ dữ liệu; có hiệu năng cao, không bị trễ và chạy ổn định. Đồng bộ thời gian gửi, nhận báo cáo điện tử giữa các hệ thống thông tin báo cáo, hệ thống quản lý văn bản và điều hành của các bộ, ngành, địa phương bảo đảm thống nhất, đồng bộ theo múi giờ Việt Nam (Tiêu chuẩn ISO 8601). Áp dụng các công nghệ xác thực, cơ chế kiểm soát quyền truy cập và cơ chế ghi lịch sử hoạt động của Hệ thống để quản lý, sẵn sàng cho kiểm tra, kiểm soát khi cần thiết. - Hỗ trợ công cụ theo dõi, kiểm tra, giám sát, phát hiện, xử lý các nguy cơ, rủi ro mất an toàn, an ninh thông tin; áp dụng giải pháp phân tích, đánh giá, đưa ra phương án khắc phục sự cố mất an toàn an ninh thông		

			tin với thời gian nhanh nhất; triển khai các biện pháp, giải pháp phòng chống mã độc; áp dụng các biện pháp hành chính, kỹ thuật để tăng cường quản lý, giám sát, kiểm soát trong kết nối, chia sẻ, gửi, nhận báo cáo điện tử. - Dữ liệu của toàn bộ hệ thống được sao lưu dự phòng định kỳ; dữ liệu khi lưu chuyển và lưu trữ được mã hóa bằng mật mã theo quy định nhằm chống theo dõi, thu thập và sửa chữa trái phép. - Bảo đảm an toàn hệ thống thông tin theo cấp độ, các phương án bảo đảm an toàn thông tin, giám sát thông tin đáp ứng yêu cầu an toàn tối thiểu, cơ bản theo quy định; kết nối, chia sẻ thông tin với cơ quan giám định an toàn không gian mạng. - Hệ thống được kiểm tra, đánh giá và quản lý rủi ro		

			trước khi đưa vào sử dụng, định kỳ hoặc đột xuất kiểm tra, đánh giá; có kế hoạch ứng phó sự cố bảo đảm an toàn thông tin mạng cho - - Hệ thống đáp ứng các yêu cầu; trang thiết bị phải có nguồn gốc xuất xứ rõ ràng và phải được kiểm định về an ninh, an toàn thông tin theo quy định của pháp luật.		
4.2	Khả năng truy xuất nguồn gốc		- Có khả năng lưu Logs hệ thống theo thời gian định kỳ để phục vụ truy xuất. - Các hành động của người sử dụng trên hệ thống được lưu vết hoặc có thể tra cứu được khi cần	Thực hiện vận hành kiểm thử để đánh giá mức độ đáp ứng yêu cầu chất lượng	Thực hiện kiểm tra các báo cáo kết quả cung cấp dịch vụ của hệ thống để đánh giá mức độ đáp ứng yêu cầu chất lượng
4.3	Cam kết về bảo mật thông tin		Đơn vị cung cấp phần mềm ứng dụng phải cam kết không có các đoạn mã độc hại trong sản phẩm.	Nhà cung cấp phải cam kết về bảo mật thông tin trong suốt quá trình cung cấp dịch vụ	
4.4	Bảo đảm an toàn hệ thống thông tin theo cấp độ		Bảo đảm an toàn hệ thống thông tin theo cấp độ, các phương án bảo đảm an toàn thông tin, giám sát thông tin đáp ứng yêu cầu an toàn tối	Thực hiện kiểm tra các nội dung bảo đảm an toàn thông tin theo cấp độ để đánh giá mức độ đáp	Thực hiện kiểm tra các nội dung bảo đảm an toàn thông tin theo cấp độ để đánh

			thiểu, cơ bản theo quy định; kết nối, chia sẻ thông tin với cơ quan giám định an toàn không gian mạng.	ứng của yêu cầu chất lượng	giá mức độ đáp ứng của yêu cầu chất lượng
5	**Các tiêu chí phi chức năng khác**				
5.1	Tuân thủ các yêu cầu chung về kỹ thuật				
5.1.1	Tuân thủ các tiêu chuẩn kỹ thuật về ứng dụng CNTT trong cơ quan nhà nước		Áp dụng các tiêu chuẩn quốc gia, quốc tế trong quá trình xây dựng các ứng dụng CNTT y tế: - Tiêu chuẩn HL7 (bản tin HL7 phiên bản 2.x, bản tin HL7 phiên bản 3, kiến trúc tài liệu lâm sàng CDA); - Tiêu chuẩn hình ảnh số và truyền tải trong y tế: DICOM; - Tiêu chuẩn kết nối, liên thông và trao đổi dữ liệu giữa các ứng dụng và thiết bị y tế: ISO/IEEE 11073; - Tiêu chuẩn trao đổi và chia sẻ các chỉ số, siêu dữ liệu thống kê trong lĩnh vực y tế: SDMX-HD. - Tiêu chuẩn kết nối, tiêu chuẩn về tích hợp dữ liệu, tiêu	Thực hiện kiểm tra các tài liệu liên quan đến giải pháp	

			chuẩn về truy cập thông tin, tiêu chuẩn về an toàn thông tin, tiêu chuẩn về dữ liệu đặc tả sẽ căn cứ theo Danh mục tiêu chuẩn về ứng dụng CNTT trong cơ quan nhà nước đã được ban hành theo Thông tư số 39/2017/TT-BTTTT của Bộ Thông tin và Truyền thông công bố Danh mục tiêu chuẩn kỹ thuật về ứng dụng CNTT trong cơ quan nhà nước.		
5.1.2	Nền tảng công nghệ		Xây dựng phần mềm theo mô hình ứng dụng Web application, quản lý tập trung.	Thực hiện kiểm tra các tài liệu liên quan đến giải pháp	
5.2	Khả năng sử dụng				
5.2.1	Khả năng sử dụng		Giải pháp phải có tính ổn định cao (phần mềm, phần cứng, hạ tầng mạng), đáp ứng nhu cầu xử lý công việc cho các phòng, ban chức năng trong việc quản lý khám chữa bệnh. Khi có sự thay đổi các tính năng yêu cầu thì phải đáp ứng kịp	Thực hiện vận hành thử để đánh giá mức độ đáp ứng yêu cầu	Thực hiện tổ chức kiểm tra thực tế để đánh giá mức độ đáp ứng yêu cầu chất lượng

			thời và linh hoạt tùy biến cho người sử dụng.		
5.2.2	Khả năng ngăn chặn lỗi cơ bản từ người sử dụng		Phần mềm cung cấp cần phải ngăn chặn và cách báo các lỗi cơ bản người sử dụng gặp phải trong quá trình truy cập, nhập liệu, liên thông dữ liệu.	Thực hiện vận hành thử để đánh giá mức độ đáp ứng yêu cầu	Thực hiện tổ chức kiểm tra thực tế để đánh giá mức độ đáp ứng yêu cầu chất lượng
5.2.3	Khả năng truy cập, sử dụng hệ thống đa dạng		Hỗ trợ truy cập, khai thác dịch vụ trên nền tảng Web và thiết bị di động (IOS/ Adroid)	Thực hiện vận hành thử để đánh giá mức độ đáp ứng yêu cầu	Thực hiện khảo sát, thu thập thông tin của người sử dụng để đánh giá mức độ đáp ứng yêu cầu chất lượng
5.2.4	Tính dễ học, dễ sử dụng		Nhà cung cấp phải cung cấp đầy đủ các tài liệu hướng dẫn sử dụng và hướng dẫn quản trị hệ thống.	Thực hiện kiểm tra thực tế các tài liệu do Nhà cung cấp bàn giao để đánh giá mức độ đáp ứng yêu cầu	Thực hiện khảo sát, thu thập thông tin của người sử dụng để đánh giá mức độ đáp ứng yêu cầu chất lượng
5.3	Tính tin cậy				
5.3.1	Tính liên tục, sẵn sàng		- Hệ thống phần mềm bệnh án điện tử phải đảm bảo hoạt động liên tục 24/7; được thiết kế hỗ trợ khả năng sao		Thực hiện khảo sát, thu thập thông tin của người sử dụng để

			lưu dữ liệu thời gian thực, hỗ trợ khả năng tự động chuyển đổi khi xảy ra lỗi, không ảnh hưởng tới việc trao đổi thông tin, dữ liệu báo cáo. - Không hình thành một điểm lỗi tập trung hoặc điểm nghẽn hiệu năng tập trung. Tính sẵn sàng của hệ thống phải đạt mức 99,5% theo năm, trong đó không kể thời gian bảo trì theo kế hoạch định trước; thời gian không sẵn sàng của hệ thống phải nhỏ hơn 1 giờ/1 tháng không tính thời gian bảo trì hệ thống. - Hệ thống đảm bảo hoạt động bình thường trong trường hợp một trong các máy chủ vật lý/máy chủ ứng dụng bị lỗi.		đánh giá mức độ đáp ứng yêu cầu chất lượng
5.3.2	Khả năng phục hồi sau sự cố		Khả năng phục hồi: Trong mọi trường hợp xảy ra sự cố (dữ liệu, máy chủ vật lý, máy chủ ứng dụng), thời gian cho phép để hệ thống phục hồi trạng thái hoạt	Thực hiện vận hành thử để đánh giá mức độ đáp ứng yêu cầu	

			động bình thường là 3 giờ.		
5.4	Khả năng bảo trì				
5.4.1	Khả năng phân tích sự cố		- Theo dõi tải hoạt động các thiết bị, ứng dụng, có biện pháp tối ưu, nâng cấp khi cần thiết để đảm bảo hiệu năng hệ thống, luôn đáp ứng cho người dùng. - Xử lý các sự cố và yêu cầu phát sinh khác trong quá trình vận hành. - Nâng cấp phần mềm theo phản ánh, đề xuất của người dùng. - Nâng cấp điều chỉnh ngay trong quá trình triển khai (thực hiện các giải pháp gấp để khắc phục các tình huống, xử lý các sự cố). - Đơn vị cung cấp dịch vụ phải có trách nhiệm chỉnh sửa theo các yêu cầu của đơn vị sử dụng dịch vụ. Thời gian hoàn thành việc chỉnh sửa nâng cấp sẽ thống nhất giữa 2 bên với tình huống cụ thể và độ phức	Cam kết của nhà cung cấp dịch vụ	Thực hiện tổ chức kiểm tra thực tế để đánh giá mức độ đáp ứng yêu cầu chất lượng

			tạp của các yêu cầu thay đổi.		
5.4.2	Khả năng thay thế linh hoạt		Khi có sự thay đổi các tính năng yêu cầu thì phải đáp ứng kịp thời và linh hoạt tùy biến cho người sử dụng.	Cam kết của nhà cung cấp dịch vụ	Thực hiện tổ chức kiểm tra thực tế để đánh giá mức độ đáp ứng yêu cầu chất lượng
5.4.3	Khả năng dự báo sự cố		Yêu cầu hệ thống có khả năng dự báo, cảnh báo sự cố một cách kịp thời và đưa ra hướng dẫn khắc phục sự cố không quá 05h kể từ thời điểm xảy ra sự cố	Cam kết của nhà cung cấp dịch vụ	Thực hiện tổ chức kiểm tra thực tế để đánh giá mức độ đáp ứng yêu cầu chất lượng
5.5	Khả năng điều chỉnh		Nâng cấp điều chỉnh ngay trong quá trình triển khai (thực hiện các giải pháp gấp để khắc phục các tình huống, xử lý các sự cố).	Cam kết của nhà cung cấp dịch vụ	Thực hiện tổ chức kiểm tra thực tế để đánh giá mức độ đáp ứng yêu cầu chất lượng
5.5.1	Khả năng tùy biến toàn bộ hoặc một số thành phần dịch vụ		Có khả năng tùy biến hiển thị trên các màn hình máy tính, máy tính bảng, điện thoại di động thông minh, kios thông tin… với độ phân giải khác nhau mà không làm thay đổi về giao diện, hiển thị và các tính năng khác của hệ thống. Tuy nhiên, giao diện ứng dụng phải thân thiện với	Cam kết của nhà cung cấp dịch vụ	Thực hiện tổ chức kiểm tra thực tế để đánh giá mức độ đáp ứng yêu cầu chất lượng

			người sử dụng và dễ dùng. Hỗ trợ tối đa sử dụng các chức năng bằng bàn phím máy tính.		
5.6	Khả năng tích hợp, kết nối				
5.6.1	Phương án kết nối, chia sẻ dữ liệu		Tiêu chuẩn trao đổi và chia sẻ các chỉ số, siêu dữ liệu thống kê trong lĩnh vực y tế: SDMX-HD	Cam kết của nhà cung cấp dịch vụ; Thực hiện vận hành thử để đánh giá mức độ đáp ứng yêu cầu	Thực hiện tổ chức kiểm tra thực tế để đánh giá mức độ đáp ứng yêu cầu chất lượng
5.6.2	Khả năng tích hợp, kết nối với các hệ thống giám sát, các hệ thống của bên thứ ba để phục vụ nhu cầu quản lý, theo dõi, giám sát của chủ trì thuê dịch vụ		- Có khả năng kết nối với các hệ thống bảo đảm an toàn thông tin của Quốc gia. - Có khả năng kết nối với các hệ thống dữ liệu Quốc gia (Bộ Y tế, Bộ Công an, BHXH); - Tích hợp chữ ký điện tử; - Tích hợp với IoT với các thiết bị thông minh (Máy đo HA, máy tiểu đường, điện tim). - Tích hợp với mọi dạng dữ liệu số. - Có khả năng tích hợp với các hệ thống phần mềm ứng dụng khác: PACS	Cam kết của nhà cung cấp dịch vụ	

5.7	Mức độ sử dụng, khai thác của dịch vụ trong kỳ đánh giá		Đảm bảo việc triển khai tổng thể hệ các hoạt động của Trung tâm: thu chi, khám chữa bệnh, dược, căng tin, suất ăn…Trong đó Hệ thống phần mềm bệnh án điện tử là trọng điểm.	Cam kết của nhà cung cấp dịch vụ	Thực hiện tổ chức kiểm tra thực tế để đánh giá mức độ đáp ứng yêu cầu chất lượng
6	**Các tiêu chí về sự hài lòng của người sử dụng**				
6.1	Tính kịp thời		Yêu cầu về thời gian nhà cung cấp dịch vụ hoàn tất việc cung cấp dịch vụ tới người sử dụng so với thời hạn quy định của Chủ trì thuê dịch vụ yêu cầu.	Theo dõi giám sát thực tế việc chuẩn bị cung cấp dịch vụ; mức độ đáp ứng yêu cầu	Thực hiện kiểm tra các báo cáo kết quả cung cấp dịch vụ của hệ thống để đánh giá mức độ đáp ứng yêu cầu chất lượng
6.2	Phản hồi của người sử dụng		Hệ thống có chức năng khảo sát ghi nhận phản hồi từ phía người dùng mức độ đáp ứng tối thiểu 80% phản hồi là Đáp ứng		Tổ chức khảo sát, thu thập, phân tích phản hồi của đơn vị và người sử dụng (sử dụng tiêu chí đáp ứng, chưa đáp ứng) để đánh giá mức độ chất lượng
6.3	Khả năng hỗ trợ người sử dụng		- Hệ thống sẵn sàng hotline 24/24h và 07 ngày trong tuần hỗ trợ người dùng. Số		Tổ chức khảo sát, thu thập, phân tích phản

			điện thoại hotline được hiển thị ngay màn hình đăng nhập. - Công cụ theo dõi đánh giá mức hỗ trợ người dùng Mức độ đáp ứng tối thiểu 80% phản hồi là Đáp ứng		hồi của đơn vị và người sử dụng (sử dụng tiêu chí đáp ứng, chưa đáp ứng) để đánh giá mức độ chất lượng
6.4	Thái độ phục vụ		Phục vụ hỗ trợ người sử dụng kịp thời mức độ đáp ứng tối thiểu 80% phản hồi là Đáp ứng người sử dụng	Đáp ứng yêu cầu	Đáp ứng yêu cầu
7	**Các tiêu chí về quản lý dịch vụ**				
7.1	Tuân thủ quy trình		Nhà cung cấp dịch vụ phải xây dựng và thống nhất với Chủ trì thuê dịch vụ về quy trình thực hiện cung cấp dịch vụ CNTT theo 03 giai đoạn: Chuẩn bị cung cấp dịch vụ, Chính thức cung cấp dịch vụ, Kết thúc	Kiểm tra thực tế quy định do Nhà cung cấp thực hiện để đánh giá mức độ đáp ứng yêu cầu chất lượng	Thực hiện kiểm tra báo cáo kết quả cung cấp dịch vụ của hệ thống để đánh giá mức độ đáp ứng yêu cầu chất lượng
7.2	Môi trường làm việc		Có các công cụ hỗ trợ, giám sát, theo dõi, giám sát hệ thống cung cấp dịch vụ	Cam kết của nhà cung cấp dịch vụ	
			Có bộ phận chuyên trách của Nhà cung cấp dịch vụ cho việc quản lý và cung cấp phải hỗ trợ 24/24h,	Cam kết của nhà cung cấp dịch vụ; kiểm tra các công cụ hỗ trợ, phương án triển	Thực hiện kiểm tra báo cáo kết quả cung cấp dịch vụ của

			07 ngày trong tuần và trả lời các yêu cầu hỗ trợ Chủ trì thuê dịch vụ (điện thoại, hotline, thư điện tử…). Thời gian hỗ trợ ≥ 01 giờ	khai của đơn vị cung cấp dịch vụ	hệ thống để đánh giá mức độ đáp ứng yêu cầu chất lượng
7.3	Báo cáo dịch vụ		Nhà cung cấp dịch vụ phải có Báo cáo kết quả chuẩn bị cung cấp dịch vụ, báo cáo kết quả cung cấp dịch vụ (theo kỳ thanh toán và toàn bộ quá trình)	Nhà cung cấp có báo cáo kết quả chuẩn bị cung cấp dịch vụ được Chủ trì thuê dịch vụ chấp nhận	Nhà cung cấp có báo cáo kết quả chuẩn bị cung cấp dịch vụ được Chủ trì thuê dịch vụ chấp nhận
7.4	Thỏa thuận mức dịch vụ		Chủ trì thuê dịch vụ và Nhà cung cấp dịch vụ sẽ đàm phán, ký kết thỏa thuận mức dịch vụ, bảo đảm phù hợp với quy mô, tính chất và các quy định của pháp luật	Có thảo thuận mức dịch vụ được ký kết giữa Chủ trì thuê dịch vụ và Nhà cung cấp dịch vụ	Đánh giá của Chủ trì thuê dịch vụ về mức độ tuân thủ (sử dụng tiêu chí đáp ứng, chưa đáp ứng)
7.5	Quản lý tính sẵn sàng và tính liên tục của dịch vụ		Nhà cung cấp dịch vụ phải đáp ứng các yêu cầu về quản lý khai thác và vận hành hệ thống phục vụ cung cấp dịch vụ tại mục "Phương án duy trì, vận hành, sử dụng phần mềm" trong Kế hoạch	Nhà cung cấp phải có cam kết và phương án quản lý tính sẵn sàng và tính liên tục của dịch vụ	Thực hiện kiểm tra báo cáo kết quả cung cấp dịch vụ của hệ thống để đánh giá mức độ đáp ứng yêu cầu chất lượng
7.6	Quản lý thay đổi		Thông tin về việc thay đổi của hệ thống phải được ghi nhận trong suốt quá	Nhà cung cấp phải có cam kết và phương án quản lý tính sẵn	Thực hiện kiểm tra báo cáo kết quả cung cấp

			trình cung cấp dịch vụ	sang và tính liên tục của dịch vụ được Chủ trì thuê dịch vụ chấp nhận	dịch vụ của hệ thống để đánh giá mức độ đáp ứng yêu cầu chất lượng
7.7	Quản lý và triển khai phiên bản		Thông tin về các phiên bản của hệ thống phải được ghi nhận trong suốt quá trình cung cấp dịch vụ (nếu có thay đổi)	Nhà cung cấp phải có cam kết và phương án quản lý tính sẵn sang và tính liên tục của dịch vụ được Chủ trì thuê dịch vụ chấp nhận	Thực hiện kiểm tra báo cáo kết quả cung cấp dịch vụ của hệ thống để đánh giá mức độ đáp ứng yêu cầu chất lượng
8	Đào tạo chuyển giao công nghệ và các yêu cầu khác		Việc triển khai xây dựng phần mềm phải đảm bảo tuân thủ quy trình, nội dung các công việc thực hiện theo đúng quy định của Nhà nước về quản lý đầu tư ứng dụng CNTT sử dụng nguồn vốn ngân sách nước. Việc đào tạo, chuyển giao công nghệ được Nhà thầu cung cấp miễn phí bao gồm các nội dung sau: - Cung cấp các tài liệu về đào tạo, chuyển giao công nghệ: tài liệu hướng dẫn sử dụng; tài liệu quản trị, vận hành	Kiểm tra, theo dõi đánh giá mức độ đáp ứng yêu cầu	

			ứng dụng; tài liệu thiết kế hệ thống. Cung cấp giảng viên, trợ giảng hỗ trợ đào tạo chuyển giao công nghệ.		

3.1.2. Yêu cầu về kỹ thuật, công nghệ để đáp ứng yêu cầu chất lượng

3.1.2.1. Danh mục các quy chuẩn, tiêu chuẩn kỹ thuật được áp dụng

3.1.2.1.1. Tiêu chuẩn về CNTT trong y tế

Hệ thống phần mềm bệnh án điện tử đảm bảo đáp ứng tiêu chí kỹ thuật quy định là bắt buộc được nêu tại các văn bản như sau:

- Thông tư số 53/2014/TT-BYT ngày 29/12/2014 của Bộ Y tế quy định điều kiện hoạt động y tế trên môi trường mạng;
- Thông tư số 54/2017/TT-BYT ngày 29/12/2017 của Bộ Y tế về ban hành Bộ Tiêu chí ứng dụng CNTT tại các cơ sở khám bệnh, chữa bệnh;
- Quyết định số 2035/QĐ-BYT ngày 12/06/2013 của Bộ Y tế về việc công bố danh mục kỹ thuật về ứng dụng CNTT trong lĩnh vực y tế;
- Quyết định số 5004/QĐ-BYT, ngày 19 tháng 9 năm 2016 của Bộ trưởng Bộ Y tế về việc phê duyệt mô hình kiến trúc tổng thể hệ thống thông tin khám chữa bệnh bảo hiểm y tế.

3.1.2.1.2. Các tiêu chuẩn kỹ thuật ứng dụng CNTT trong các hệ thống thông tin y tế

Áp dụng các tiêu chuẩn quốc gia, quốc tế trong quá trình xây dựng các ứng dụng CNTT y tế:

- Tiêu chuẩn HL7 (bản tin HL7 phiên bản 2.x, bản tin HL7 phiên bản 3, kiến trúc tài liệu lâm sàng CDA);
- Tiêu chuẩn hình ảnh số và truyền tải trong y tế: DICOM;
- Tiêu chuẩn kết nối, liên thông và trao đổi dữ liệu giữa các ứng dụng và thiết bị y tế: ISO/IEEE 11073;
- Tiêu chuẩn trao đổi và chia sẻ các chỉ số, siêu dữ liệu thống kê trong lĩnh vực y tế: SDMX-HD.

3.1.2.1.3. Các tiêu chuẩn kỹ thuật ứng dụng CNTT trong các hệ thống thông tin y tế

✓ Công văn số 3788/BTTTT-THH ngày 26/12/2014 của Bộ Thông tin và Truyền thông về việc Hướng dẫn liên thông, trao đổi dữ liệu có cấu trúc bằng ngôn ngữ XML giữa các hệ thống thông tin trong cơ quan nhà nước;

✓ Sản phẩm phát triển phải tuân thủ các tiêu chuẩn sau (Bảng tiêu chuẩn dưới đây được trích rút từ Thông tư số 39/2017/TT-BTTTT của Bộ Thông tin và Truyền thông, yêu cầu hoặc bắt buộc thực hiện đối với phần mềm của các cơ quan nhà nước)

TT	Loại tiêu chuẩn	Ký hiệu tiêu chuẩn	Tên đầy đủ của tiêu chuẩn	Quy định áp dụng
1	Tiêu chuẩn về kết nối			
1.1	Truyền siêu văn bản	HTTP v1.1	Hypertext Transfer Protocol version 1.1	Bắt buộc áp dụng
		HTTP v2.0	Hypertext Transfer Protocol version 2.0	Khuyến nghị áp dụng
1.2	Truyền tệp tin	FTP	File Transfer Protocol	Bắt buộc áp dụng một hoặc cả hai tiêu chuẩn
		HTTP v1.1	Hypertext Transfer Protocol version 1.1	
		HTTP v2.0	Hypertext Transfer Protocol version 2.0	Khuyến nghị áp dụng
		WebDAV	Web-based Distributed Authoring and Versioning	Khuyến nghị áp dụng
1.3	Truyền, phát luồng âm thanh/ hình ảnh	RTSP	Real-time Streaming Protocol	Khuyến nghị áp dụng
		RTP	Real-time Transport Protocol	Khuyến nghị áp dụng
		RTCP	Real-time Control Protocol	Khuyến nghị áp dụng
1.4	Truy cập và chia sẻ dữ liệu	OData v4	Open Data Protocol version 4.0	Khuyến nghị áp dụng
1.5	Truyền thư điện tử	SMTP/ MIME	Simple Mail Transfer Protocol/Multipurpose Internet Mail Extensions	Bắt buộc áp dụng
1.6	Cung cấp dịch vụ truy cập hộp thư điện tử	POP3	Post Office Protocol version 3	Bắt buộc áp dụng cả hai tiêu chuẩn đối với máy chủ
		IMAP 4rev1	Internet Message Access Protocol version 4 revision 1	
1.7	Truy cập thư mục	LDAP v3	Lightweight Directory Access Protocol version 3	Bắt buộc áp dụng
1.8	Dịch vụ tên miền	DNS	Domain Name System	Bắt buộc áp dụng
1.9	Giao vận mạng có kết nối	TCP	Transmission Control Protocol	Bắt buộc áp dụng

TT	Loại tiêu chuẩn	Ký hiệu tiêu chuẩn	Tên đầy đủ của tiêu chuẩn	Quy định áp dụng
1.10	Giao vận mạng không kết nối	UDP	User Datagram Protocol	Bắt buộc áp dụng
1.11	Liên mạng LAN/WAN	IPv4	Internet Protocol version 4	Bắt buộc áp dụng
		IPv6	Internet Protocol version 6	Bắt buộc áp dụng đối với các thiết bị có kết nối Internet
1.12	Mạng cục bộ không dây	IEEE 802.11g	Institute of Electrical and Electronics Engineers Standard (IEEE) 802.11g	Bắt buộc áp dụng
		IEEE 802.11n	Institute of Electrical and Electronics Engineers Standard (IEEE) 802.11n	Khuyến nghị áp dụng
1.13	Truy cập Internet với thiết bị không dây	WAP v2.0	Wireless Application Protocol version 2.0	Bắt buộc áp dụng
1.14	Dịch vụ Web dạng SOAP	SOAP v1.2	Simple Object Access Protocol version 1.2	Bắt buộc áp dụng một, hai hoặc cả ba tiêu chuẩn
		WSDL V2.0	Web Services Description Language version 2.0	
		UDDI v3	Universal Description, Discovery and Integration version 3	
1.15	Dịch vụ Web dạng RESTful	RESTful web service	Representational state transfer	Khuyến nghị áp dụng
1.16	Dịch vụ đặc tả Web	WS BPEL v2.0	Web Services Business Process Execution Language Version 2.0	Khuyến nghị áp dụng
		WS-I Simple SOAP Binding Profile Version 1.0	Simple SOAP Binding Profile Version 1.0	Khuyến nghị áp dụng
		WS-	Web Services Federation	Khuyến nghị áp

TT	Loại tiêu chuẩn	Ký hiệu tiêu chuẩn	Tên đầy đủ của tiêu chuẩn	Quy định áp dụng
		Federation v1.2	Language Version 1.2	dụng
		WS-Addressing v1.0	Web Services Addressing 1.0	Khuyến nghị áp dụng
		WS-Coordination Version 1.2	Web Services Coordination Version 1.2	Khuyến nghị áp dụng
		WS-Policy v1.2	Web Services Coordination Version 1.2	Khuyến nghị áp dụng
		OASIS Web Services Business Activity Version 1.2	Web Services Business Activity Version 1.2	Khuyến nghị áp dụng
		WS-Discovery Version 1.1	Web Services Dynamic Discovery Version 1.1	Khuyến nghị áp dụng
		WS-MetadataExchange	Web Services Metadata Exchange	Khuyến nghị áp dụng
1.17	Dịch vụ đồng bộ thời gian	NTPv3	Network Time Protocol version 3	Bắt buộc áp dụng một trong hai tiêu chuẩn
		NTPv4	Network Time Protocol version 4	
2	Tiêu chuẩn về tích hợp dữ liệu			
2.1	Ngôn ngữ định dạng văn bản	XML v1.0 (5th Edition)	Extensible Markup Language version 1.0 (5th Edition)	Bắt buộc áp dụng một trong hai tiêu chuẩn
		XML v1.1 (2nd Edition)	Extensible Markup Language version 1.1	
2.2	Ngôn ngữ định dạng văn bản cho giao dịch điện tử	ISO/TS 15000:2014	Electronic Business Extensible Markup Language (ebXML)	Bắt buộc áp dụng

TT	Loại tiêu chuẩn	Ký hiệu tiêu chuẩn	Tên đầy đủ của tiêu chuẩn	Quy định áp dụng
2.3	Định nghĩa các lược đồ trong tài liệu XML	XML Schema V1.1	XML Schema version 1.1	Bắt buộc áp dụng
2.4	Biến đổi dữ liệu	XSL	Extensible Stylesheet Language	Bắt buộc áp dụng phiên bản mới nhất.
2.5	Mô hình hóa đối tượng	UML v2.5	Unified Modelling Language version 2.5	Khuyến nghị áp dụng
2.6	Mô tả tài nguyên dữ liệu	RDF	Resource Description Framework	Khuyến nghị áp dụng
		OWL	Web Ontology Language	Khuyến nghị áp dụng
2.7	Trình diễn bộ kí tự	UTF-8	8-bit Universal Character Set (UES)/Unicode Transformation Format	Bắt buộc áp dụng
2.8	Khuôn thức trao đổi thông tin địa lý	GML v3.3	Geography Markup Language version 3.3	Bắt buộc áp dụng
2.9	Truy cập và cập nhật các thông tin địa lý	WMS v1.3.0	OpenGIS Web Map Service version 1.3.0	Bắt buộc áp dụng
		WFS v1.1.0	Web Feature Service version 1.1.0	Bắt buộc áp dụng
2.10	Trao đổi dữ liệu đặc tả tài liệu XML	XMI v2.4.2	XML Metadata Interchange version 2.4.2	Khuyến nghị áp dụng
2.11	Sổ đăng ký siêu dữ liệu (MDR)	ISO/IEC 11179:2015	Sổ đăng ký siêu dữ liệu (Metadata registries - MDR)	Khuyến nghị áp dụng
2.12	Bộ phần tử siêu dữ liệu Dublin Core	ISO 15836-1:2017	Bộ phần tử siêu dữ liệu Dublin Core	Khuyến nghị áp dụng (*)
2.13	Định dạng trao đổi dữ liệu mô tả đối	JSON RFC 7159	JavaScript Object Notation	Khuyến nghị áp dụng

TT	Loại tiêu chuẩn	Ký hiệu tiêu chuẩn	Tên đầy đủ của tiêu chuẩn	Quy định áp dụng
	tượng dạng kịch bản JavaScript			
2.14	Ngôn ngữ mô hình quy trình nghiệp vụ	BPMN 2.0	Business Process Model and Notation version 2.0	Khuyến nghị áp dụng
3	Tiêu chuẩn về truy cập thông tin			
3.1	Chuẩn nội dung Web	HTML v4.01	Hypertext Markup Language version 4.01	Bắt buộc, áp dụng
		WCAG 2.0	W3C Web Content Accessibility Guidelines (WCAG) 2.0	Khuyến nghị áp dụng
		HTML 5	Hypertext Markup Language version 5	Khuyến nghị áp dụng
3.2	Chuẩn nội dung Web mở rộng	XHTML v1.1	Extensible Hypertext Markup Language version 1.1	Bắt buộc áp dụng
3.3	Giao diện người dùng	CSS2	Cascading Style Sheets Language Level 2	Bắt buộc áp dụng một trong ba tiêu chuẩn
		CSS3	Cascading Style Sheets Language Level 3	
		XSL	Extensible Stylesheet Language version	
3.4	Văn bản	(.txt)	Định dạng Plain Text (.txt): Dành cho các tài liệu cơ bản không có cấu trúc	Bắt buộc áp dụng
		(.rtf) v1.8, v1.9.1	Định dạng Rich Text (.rtf) phiên bản 1.8, 1.9.1: Dành cho các tài liệu có thể trao đổi giữa các nền khác nhau	Bắt buộc áp dụng
		(.docx)	Định dạng văn bản Word mở rộng của Microsoft (.docx)	Khuyến nghị áp dụng
		(.pdf) v1.4, v1.5, v1.6,	Định dạng Portable Document (.pdf) phiên bản	Bắt buộc áp dụng một, hai hoặc cả

TT	Loại tiêu chuẩn	Ký hiệu tiêu chuẩn	Tên đầy đủ của tiêu chuẩn	Quy định áp dụng
		v1.7	1.4, 1.5, 1.6, 1.7: Dành cho các tài liệu chỉ đọc	ba tiêu chuẩn
		(.doc)	Định dạng văn bản Word của Microsoft (.doc)	
		(.odt) v1.2	Định dạng Open Document Text (.odt) phiên bản 1.2	
3.5	Bảng tính	(.csv)	Định dạng Comma eparated Variable/Delimited (.csv): Dành cho các bảng tính cần trao đổi giữa các ứng dụng khác nhau.	Bắt buộc áp dụng
		(.xlsx)	Định dạng bảng tính Excel mở rộng của Microsoft (.xlsx)	Khuyến nghị áp dụng
		(.xls)	Định dạng bảng tính Excel của Microsoft (.xls)	Bắt buộc áp dụng một hoặc cả hai tiêu chuẩn
		(.ods) v1.2	Định dạng Open Document Spreadsheets (.ods) phiên bản 1.2	
3.6	Trình diễn	(.htm)	Định dạng Hypertext Document (.htm): cho các trình bày được trao đổi thông qua các loại trình duyệt khác nhau	Bắt buộc áp dụng
		(.pptx)	Định dạng PowerPoint mở rộng của Microsoft (.pptx)	Khuyến nghị áp dụng
		(.pdf)	Định dạng Portable Document (.pdf): cho các trình bày lưu dưới dạng chỉ đọc	Bắt buộc áp dụng một, hai hoặc cả ba tiêu chuẩn
		(.ppt)	Định dạng PowerPoint (.ppt) của Microsoft	
		(.odp) v1.2	Định dạng Open Document Presentation (.odp) phiên bản 1.2	
3.7	Ảnh đồ họa	JPEG	Joint Photographic Expert	Bắt buộc áp dụng

TT	Loại tiêu chuẩn	Ký hiệu tiêu chuẩn	Tên đầy đủ của tiêu chuẩn	Quy định áp dụng
			Group (.jpg)	một, hai, ba hoặc cả bốn tiêu chuẩn
		GIF v89a	Graphic Interchange (.gif) version 89a	
		TIFF	Tag Image File (.tif)	
		PNG	Portable Network Graphics (.png)	
3.8	Ảnh gắn với tọa độ địa lý	GEO TIFF	Tagged Image File Format for GIS applications	Bắt buộc áp dụng
3.9	Phim ảnh, âm thanh	MPEG-1	Moving Picture Experts Group-1	Khuyến nghị áp dụng
		MPEG-2	Moving Picture Experts Group-2	Khuyến nghị áp dụng
		MPEG-4	Moving Picture Experts Group-4	Khuyến nghị áp dụng
		MP3	MPEG-1 Audio Layer 3	Khuyến nghị áp dụng
		AAC	Advanced Audio Coding	Khuyến nghị áp dụng
3.10	Luồng phim ảnh, âm thanh	(.asf), (.wma), (.wmv)	Các định dạng của Microsoft Windows Media Player (.asf), (.wma), (.wmv)	Khuyến nghị áp dụng
		(.ra), (.rm), (.ram), (.rmm)	Các định dạng Real Audio/Real Video (.ra), (.rm), (.ram), (.rmm)	Khuyến nghị áp dụng
		(.avi), (.mov), (qt)	Các định dạng Apple Quicktime (.avi), (.mov), (qt)	Khuyến nghị áp dụng
3.11	Hoạt họa	GIF v89a	Graphic Interchange (.gif) version 89a	Khuyến nghị áp dụng
		(.swf)	Định dạng Macromedia Flash (.swf)	Khuyến nghị áp dụng
		(.swf)	Định dạng Macromedia Shockwave (.swf)	Khuyến nghị áp dụng
		(.avi), (qt), (.mov)	Các định dạng Apple Quicktime (.avi),(.qt),(.mov)	Khuyến nghị áp dụng

TT	Loại tiêu chuẩn	Ký hiệu tiêu chuẩn	Tên đầy đủ của tiêu chuẩn	Quy định áp dụng
3.12	Chuẩn nội dung cho thiết bị di động	WML v2.0	Wireless Markup Language version 2.0	Bắt buộc áp dụng
3.13	Bộ ký tự và mã hóa	ASCII	American Standard Code for Information Interchange	Bắt buộc áp dụng
3.14	Bộ ký tự và mã hóa cho tiếng Việt	TCVN 6909:2001	TCVN 6909:2001 "CNTT - Bộ mã ký tự tiếng Việt 16-bit"	Bắt buộc áp dụng
3.15	Nén dữ liệu	Zip	Zip (.zip)	Bắt buộc áp dụng một hoặc cả hai tiêu chuẩn
		.gz v4.3	GNU Zip (.gz) version 4.3	
3.16	Ngôn ngữ kịch bản phía trình khách	ECMA 262	ECMAScript version 6 (6th Edition)	Bắt buộc áp dụng
3.17	Chia sẽ nội dung Web	RSS v1.0	RDF Site Summary version 1.0	Bắt buộc áp dụng một trong hai tiêu chuẩn
		RSS v2.0	Really Simple Syndication version 2.0	
		ATOM v1.0	ATOM version 1.0	Khuyến nghị áp dụng
3.18	Chuẩn kết nối ứng dụng cổng thông tin điện tử	JSR 168	Java Specification Requests 168 (Portlet Specification)	Bắt buộc áp dụng
		JSR286	Java Specification Requests 286 (Portlet Specification)	Khuyến nghị áp dụng
		WSRP v1.0	Web Services for Remote Portlets version 1.0	Bắt buộc áp dụng
		WSRP v2.0	Web Services for Remote Portlets version 2.0	Khuyến nghị áp dụng
4	Tiêu chuẩn về an toàn thông tin			
4.1	An toàn thư điện tử	S/MIME v3.2	Secure Multi-purpose Internet Mail Extensions version 3.2	Bắt buộc áp dụng
		OpenPGP	OpenPGP	Khuyến nghị áp dụng

TT	Loại tiêu chuẩn	Ký hiệu tiêu chuẩn	Tên đầy đủ của tiêu chuẩn	Quy định áp dụng
4.2	An toàn tầng giao vận	SSH v2.0	Secure Shell version 2.0	Bắt buộc áp dụng
		TLS v1.2	Transport Layer Security version 1.2	Bắt buộc áp dụng
4.3	An toàn truyền tệp tin	HTTPS	Hypertext Transfer Protocol Secure	Bắt buộc áp dụng
		FTPS	File Transfer Protocol Secure	Khuyến nghị áp dụng
		SFTP	SSH File Transfer Protocol	Khuyến nghị áp dụng
4.4	An toàn truyền thư điện tử	SMTPS	Simple Mail Transfer Protocol Secure	Bắt buộc áp dụng
4.5	An toàn dịch vụ truy cập hộp thư	POP3S	Post Office Protocol version 3 Secure	Bắt buộc áp dụng một hoặc cả hai tiêu chuẩn
		IMAPS	Internet Message Access Protocol Secure	
4.6	An toàn dịch vụ DNS	DNSSEC	Domain Name System Security Extenssions	Khuyến nghị áp dụng
4.7	An toàn tầng mạng	IPsec - IP ESP	Internet Protocol security với IP ESP	Bắt buộc áp dụng
4.8	An toàn thông tin cho mạng không dây	WPA2	Wi-fi Protected Access 2	Bắt buộc áp dụng
4.9	Giải thuật mã hóa	TCVN 7816:2007	CNTT. Kỹ thuật mật mã thuật toán mã dữ liệu AES	Khuyến nghị áp dụng
		3DES	Triple Data Encryption Standard	Khuyến nghị áp dụng
		PKCS #1 V2.2	RSA Cryptography Standard - version 2.2	Khuyến nghị áp dụng, sử dụng lược đồ RSAES-OAEP để mã hóa
		ECC	Elliptic Curve Cryptography	Khuyến nghị áp dụng
4.10	Giải thuật	PKCS #1	RSA Cryptography Standard	Bắt buộc áp dụng,

TT	Loại tiêu chuẩn	Ký hiệu tiêu chuẩn	Tên đầy đủ của tiêu chuẩn	Quy định áp dụng
	chữ ký số	V2.2	- version 2.2	sử dụng lược đồ RSASSA-PSS để ký
		ECDSA	Elliptic Curve Digital Signature Algorithm	Khuyến nghị áp dụng
4.11	Giải thuật băm cho chữ ký số	SHA-2	Secure Hash Algorithms-2	Khuyến nghị áp dụng
4.12	Giải thuật truyền khóa	RSA-KEM	Rivest-Shamir-Adleman - KEM (Key Encapsulation Mechanism) Key Transport Algorithm	Bắt buộc áp dụng
		ECDHE	Elliptic Curve Diffie Hellman Ephemeral	Khuyến nghị áp dụng
4.13	Giải pháp xác thực người sử dụng	SAML v2.0	Security Assertion Markup Language version 2.0	Khuyến nghị áp dụng
4.14	An toàn trao đổi bản tin XML	XML Encryption Syntax and Processing	XML Encryption Syntax and Processing	Bắt buộc áp dụng
		XML Signature Syntax and Processing	XML Signature Syntax and Processing	Bắt buộc áp dụng
4.15	Quản lý khóa công khai bản tin XML	XKMS v2.0	XML Key Management Specification version 2.0	Khuyến nghị áp dụng
4.16	Giao thức an toàn thông tin cá nhân	P3P v1.1	Platform for Privacy Preferences Project version 1.1	Khuyến nghị áp dụng
4.17	Hạ tầng khóa công khai			Khuyến nghị áp dụng
	Cú pháp thông điệp	PKCS#7 v1.5 (RFC 2315)	Cryptographic message syntax for file-based signing	

TT	Loại tiêu chuẩn	Ký hiệu tiêu chuẩn	Tên đầy đủ của tiêu chuẩn	Quy định áp dụng
	mật mã cho ký, mã hóa		and encrypting version 1.5	
	Cú pháp thông tin thẻ mật mã	PKCS#15 v1.1	Cryptographic token information syntax version 1.1	
	Cú pháp thông tin khóa riêng	PKCS#8 V1.2 (RFC 5958)	Private-Key Information Syntax Standard version 1.2	
	Giao diện thẻ mật mã	PKCS#11 v2.20	Cryptographic token interface standard version 2.20	
	Cú pháp trao đổi thông tin cá nhân	PKCS#12 v1.1	Personal Information Exchange Syntax version 1.1	
	Khuôn dạng danh sách chứng thư số thu hồi	RFC 5280	Certificate Revocation List Profile	
	Khuôn dạng chứng thư số	RFC 5280	Public Key Infrastructure Certificate	
	Cú pháp yêu cầu chứng thực	PKCS#10 v1.7 (RFC 2986)	Certification Request Syntax Specification version 1.7	
	Giao thức trạng thái chứng thư trực tuyến	RFC 6960	On-line Certificate status protocol	
	Giao thức gắn tem thời gian	RFC 3161	Time stamping protocol	
	Dịch vụ tem thời gian	ISO/EEC 18014-1:2008 ISO/EEC 18014-2:2009 ISO/EEC 18014-3:2009	Information technology Security techniques - Time stamping services Part 1: Framework Part 2: Mechanisms producing independent	

TT	Loại tiêu chuẩn	Ký hiệu tiêu chuẩn	Tên đầy đủ của tiêu chuẩn	Quy định áp dụng
		ISO/EEC 18014-4:2015	tokens Part 3: Mechanisms producing linked tokens Part 4: Traceability of time sources	
4.18	An toàn cho dịch vụ Web	WS-Security v1.1.1	Web Services Security: SOAP Message Security Version 1.1.1	Khuyến nghị áp dụng
4.19	Khuôn dạng dữ liệu trao đổi sự cố an toàn mạng	RFC 7970	The Incident Object Description Exchange Format version 2 (IODEF)	Khuyến nghị áp dụng

3.1.2.2. Yêu cầu đáp ứng về chức năng của phần mềm và Phương án thuê dịch vụ

3.1.2.2.1. Yêu cầu cần đáp ứng về chức năng của phần mềm

Hệ thống phần mềm bệnh án điện tử đảm bảo:

- Tính khả thi: Giải pháp đưa ra phải giải quyết được các yêu cầu đang đặt ra, phù hợp với điều kiện thực tế của Trung tâm. Giải pháp chọn lựa phải đảm bảo tính khả thi của chương trình sao cho hệ thống sau khi đầu tư lại phải dễ dàng trong việc triển khai cũng như vận hành sau này.

- Tính hiện đại: Các giải pháp đưa ra dựa trên các công nghệ mới hiện đại và đang được sử dụng phổ biến.

- Tính tương thích cao: Phải tương thích với các mô hình khác đang được sử dụng rộng rãi. Phải tương thích với hệ thống PACS sẵn có của Trung tâm.

- Tính bảo mật: Ngoài các thông tin được đăng tải rộng rãi thì các giải pháp phần mềm phải đảm bảo tính an toàn và nguyên vẹn cho thông tin. Các giải pháp về bảo mật đối với hệ thống phải đảm bảo hệ thống không bị đánh cắp dữ liệu hay bị phá hoại. Sử dụng các cơ chế phân quyền người sử dụng, cũng như các thiết bị như tường lửa và các thiết bị khác để đảm bảo an toàn cho trang thông tin và hệ thống.

- Tính mở: Giải pháp đưa ra phải dễ dàng kết nối cũng như tích hợp thêm các giải pháp khác khi cần thiết. Hệ thống cho phép dễ dàng mở rộng khi Trung tâm cần triển khai thêm hoặc ngưng các Trung tâm vệ tinh (Trung tâm dã chiến…) trên cùng nền tảng, công nghệ, hạ tầng và server tập trung.

- Tính linh động: Hệ thống cần phải linh động để đáp ứng được các thay đổi dựa trên yêu cầu từ phía người sử dụng cũng như các yêu cầu phát sinh từ hệ thống.

- Tính toàn vẹn: Giải pháp phải có các cơ chế sao lưu phục hồi khi hệ thống có lỗi để tránh việc mất mát dữ liệu.

- Hệ quản trị CSDL: Phần mềm phải hoạt động tốt và ổn định trên hệ quản trị CSDL PostgreSQL.

- CSDL lớn: Quản lý được cơ sở dữ liệu lớn với tốc độ tra cứu nhanh.

- Hệ điều hành: Chạy trên hệ điều hành Windows 2016 hoặc phiên bản cao hơn cho máy chủ nghiệp vụ.

- Hỗ trợ đa ngữ: Quản lý dữ liệu đa ngữ bằng mã UNICODE và cung cấp giao diện làm việc theo nhiều bảng mã tiếng Việt (Unicode, ABC,VNI,..).

- Tra cứu toàn văn: Tích hợp với mọi dạng dữ liệu số.

3.1.2.2.2. Yêu cầu chức năng, phân hệ của phần mềm

Phần mềm cho thuê khai thác sử dụng phải đáp ứng yêu cầu các chức năng, phân hệ như bảng sau:

Stt	Tính năng	Mô tả tính năng
A – DANH MỤC NÂNG CẤP PHẦN MỀM		
I – Nâng cấp (HIS)		
1	Quản lý suất ăn cho bệnh nhân	- Quản lý đăng ký suất ăn cho người bệnh, tổng hợp suất ăn theo ngày, theo khoa; - Quản lý chế độ ăn, dinh dưỡng thông qua y lệnh của bác sĩ cho từng người bệnh; - Báo cáo, thống kê suất ăn theo ngày, theo khoa.
2	Quản lý phác đồ điều trị	- Quản lý và cập nhật danh mục phác đồ do Bộ Y tế ban hành; - Quản lý danh mục và danh sách phác đồ điều trị đã được thông qua tại Trung tâm; - Quản lý danh mục nhân viên y tế tham gia xây dựng phác đồ; - Quản lý xây dựng và cập nhật phác đồ; - Quản lý kết nối đến với danh mục thuốc, danh mục kỹ thuật, danh mục vật tư tiêu hao phục vụ phác đồ; - Quản lý các báo cáo, thống kê theo quy định; Khuyến khích các ứng dụng thông minh hỗ trợ quản lý phác đồ.
3	Ký số bệnh nhân	
3.1	Tạo chứng thư số bệnh nhân	
3.1.1	Xác thực sinh trắc học bằng khuôn mặt, vân tay	Lấy vân tay, khuôn mặt bệnh nhân tại tiếp đón để xác thực, sử dụng các thuật toán sinh trắc học để hiển thị tỉ lệ trùng khớp
3.1.2	Xác thực NFC căn cước công dân	Dùng thiết bị hỗ trợ đọc NFC để đọc thông tin trong căn cước công dân gắn chip
3.1.3	Thực hiện Ekyc khuôn mặt	Thực hiện nhận diện khuôn mặt bằng eKyc, xác thực C06 bộ công an

Stt	Tính năng	Mô tả tính năng
3.1.4	Tạo chứng thư số bệnh nhân	Tạo chứng thư số thông qua các nhà cung cấp chữ ký số bệnh nhân, VNEID
3.2	Ký số bệnh nhân	- Ký số bằng chứng thư số của bệnh nhân
4	Gửi hồ sơ bệnh án điện tử	
4.1	Liên kết tài khoản với bệnh án điện tử	- Liên kết tài khoản của bác sĩ với tài khoản được cấp tại phần mềm Quản lý bệnh án điện tử (EMR)
4.2	Tạo bệnh án điện tử	- Gửi thông tin tạo bệnh án điện tử
4.2	Gửi giấy tờ lên bệnh án điện tử	- Chiết file định dạng PDF các biểu mẫu có trong bệnh án - Chiết file định dạng XML hồ sơ bệnh án điện tử - Upload các giấy tờ scan, file ảnh chụp giấy tờ lên bệnh án điện tử - Mã hóa dữ liệu trao đổi - Gửi hồ sơ bệnh án điện tử đi ký số và lưu trữ
4.3	Cảnh báo thay đổi nội dung giấy tờ	- Cảnh báo trên HIS khi có sự thay đổi nội dung so với giấy tờ đã gửi
4.4	Kiểm tra giấy tờ	- Kiểm tra và cảnh báo các giấy tờ chưa gửi - Kiểm tra và cảnh báo thiếu chữ ký đối với giấy tờ đã gửi
4.5	Xem hồ sơ bệnh án	- Tích hợp xem hồ sơ bệnh án tại HIS
4.6	Xem danh sách giấy tờ cần ký số	- Xem danh sách giấy tờ cần ký của mỗi bác sĩ, giám đốc, đóng dấu Trung tâm
4.7	Kết thúc hồ sơ bệnh án	- Nhập thông tin kết thúc hồ sơ bệnh án, khóa sửa thông tin bệnh án
4.8	Nộp hồ sơ bệnh án	- Chuyển thông tin bệnh án lên giám đốc ký, khóa gửi hồ sơ bệnh án
4.9	Mượn, thay thế, bổ sung bệnh án	- Phiếu mượn, thay thế, bổ sung hồ sơ bệnh án
5	Quản lý dinh dưỡng	- Quản lý khám và đánh giá dinh dưỡng cho người bệnh ngoại trú; - Quản lý chế độ ăn bệnh lý đối với người bệnh điều trị bằng chế độ ăn; - Quản lý đánh giá và nhận xét dinh dưỡng của người bệnh thông qua bệnh án; - Quản lý chỉ định chế độ ăn hàng ngày thông qua mã bệnh nhân; - Quản lý kế hoạch can thiệp dinh dưỡng với người bệnh cần hỗ trợ dinh dưỡng; - Quản lý thực đơn và chế độ ăn.
6	Xem hình ảnh Pacs tại phòng khám	- Xem hình ảnh Xquang, Siêu âm, Điện tim, Nội soi tại phòng khám.

Stt	Tính năng	Mô tả tính năng
II – Nâng cấp xét nghiệm (LIS)		
1	Quản lý mẫu xét nghiệm	- Quản lý thông tin mẫu xét nghiệm: mã định danh mẫu xét nghiệm theo bệnh nhân, loại mẫu (máu, dịch, nước tiểu,…), ngày giờ thực hiện lấy mẫu, tình trạng của mẫu, trạng thái của mẫu, người lấy mẫu, nơi lấy mẫu bệnh. - Quản lý lưu và hủy mẫu: nơi lưu mẫu, vị trí lưu nơi, trạng thái và người hủy.
2	Quản lý hóa chất xét nghiệm	
2.1	Quản lý định mức hóa chất	- Quản lý định mức hóa chất sử dụng cho các lần trả kết quả xét nghiệm cho bệnh nhân, lượng hóa chất dùng để vệ sinh máy xét nghiệm.
2.2	Báo cáo sử dụng hóa chất theo thời gian, máy xét nghiệm	- Báo cáo sử dụng số lượng hóa chất sử dụng theo thời gian, theo máy xét nghiệm.
3	Gửi phiếu kết quả và ký số	- Gửi phiếu kết quả xét nghiệm lên bệnh án điện tử và ký số phiếu kết quả
4	Xem kết quả xét nghiệm qua WebView	- Cho phép bệnh nhân xem kết quả xét nghiệm bằng đường link trên phiếu kết quả hoặc tra cứu trên webview.
III – Nâng cấp CDHA (RIS-PACS)		
1	Cấu hình quản lý máy chủ PACS	- Cấu hình máy chủ PACS để nhận ảnh, đường dẫn hình ảnh phục vụ cho việc lưu và chuẩn bị cho máy trạm xem ảnh.
2	Cấu hình quản lý máy trạm PACS	- Cấu hình máy trạm có thể xem ảnh sau khi lưu máy chủ.
3	Hỗ trợ xem ảnh DICOM qua WebView	- Cho phép người bệnh xem lại kết quả Chẩn đoán hình ảnh và cho phép các bác sĩ chuyên môn xem ảnh gốc, các chức năng hỗ trợ xem ảnh trực tiếp.
4	Chức năng biên tập và xử lý hình ảnh DICOM	- Xử lý ảnh cho y, bác sĩ xem trên phần mềm và chuẩn bị cho việc WebView cho người bệnh xem trên môi trường số.
5	Chức năng nén ảnh theo giải thuật JPEG2000	- Xử lý ảnh nhằm việc giảm dung lượng ảnh để đính kèm vào mẫu in kết quả cho bệnh nhân và không gian lưu trữ của đơn vị.
6	Gửi hồ sơ phiếu kết quả, ký số	- Gửi phiếu kết quả chẩn đoán hình ảnh lên bệnh án điện tử và ký số phiếu kết quả
IV – Nâng cấp Viện Phí		
1	Gửi giây tờ bệnh án điện tử và ký số	
1.1	Gửi giấy tờ lên bệnh án điện tử	- Gửi bảng kê lên bệnh án điện tử - Gửi các giấy tờ khác của bệnh án điện tử

Stt	Tính năng	Mô tả tính năng
1.2	Ký số	- Kế toán viện phí ký số vào bảng kê, giấy tờ
1.3	Ký số bệnh nhân	- Ký số bệnh nhân vào bảng kê và các giấy tờ khác
B – PHẦN MỀM BỆNH ÁN ĐIỆN TỬ		
1	**Quản lý tạo bệnh án điện tử**	
1.1	Tạo bệnh án điện tử từ HIS	Đồng bộ tự động từ hệ thống HIS:
		Thông tin định danh bệnh nhân: mã BN, họ tên, ngày sinh, giới tính ….
		Thông tin BHYT
		Thông tin đăng ký khám
		Thông tin chuyển tuyến
1.2	Cấp mã định danh cho bệnh án điện tử	Hệ thống cho phép:
		Cấp mã định danh cho bệnh án điện tử để phục vụ tìm kiếm
		Cấp mã định danh cho bệnh án điện tử theo mã của phần mềm HIS
1.3	Cấp số Bệnh án điện tử	Hệ thống cho phép:
		Cấp số bệnh án cho đối tượng BHYT, Viện phí
		Cấp số bệnh án theo diện điều trị: Ngoại trú, Nội trú
		Cấp số bệnh án theo khoa: Mã khoa/số tăng dần
		Cấp số bệnh án theo năm: Số bệnh án tự động tăng dần theo năm và tự động reset về 01 khi qua năm mới (ví dụ đến 01/01/2024 thì bệnh nhân đầu tiên cấp bệnh án sẽ có mã 2024/00001)
1.4	Cập nhật thông tin bệnh nhân từ HIS	Cho phép cập nhật lại thông tin của bệnh nhân khi HIS sửa thông tin. Các thông tin cập nhật:
		Thông tin hành chính, thông tin điều trị, thông tin BHYT
1.5	Quản lý file ký	Folder quản lý file ký lưu trữ theo mã bệnh nhân, mã điều trị, họ tên bệnh nhân và năm sinh
2	**Quản lý vỏ bệnh án**	
2.1	Phân loại vỏ bệnh án	Cho phép phân loại vỏ bệnh án nội trú, ngoại trú, chuyên khoa: Mắt, TMH, RHM, Da Liễu…
2.2	Sắp xết thứ tự hiển thị vỏ bệnh án	Sắp xếp số ưu tiên cao hơn thì hiển thị lên trên để dễ dàng lựa chọn
		Thay vì sắp xếp vỏ bệnh án theo tên có thể ưu tiên vỏ bệnh án sử dụng nhiều lên trên. Ví dụ: Bệnh án nội khoa sử dụng nhiều nhất
		Hoặc cùng là bệnh án mắt có 7 loại (có thể ưu tiên loại vỏ bệnh án nào lên trên trong danh sách)
2.3	Tự động chọn vỏ bệnh án theo khoa điều trị	Cho phép cấu hình khoa điều trị để khi bệnh nhân nhập khoa sẽ map tự động với bệnh án tương ứng của His

Stt	Tính năng	Mô tả tính năng
2.4	Danh sách vỏ bệnh án đã tạo của bệnh nhân	Hiển thị danh sách vỏ bệnh án đã tạo của bệnh nhân
2.5	Xem vỏ bệnh án đã tạo của bệnh nhân	Hiển thị chi tiết vỏ bệnh án đã tạo của bệnh nhân
2.6	Tạo vỏ bệnh án mới	Phục vụ cho việc scan lại bệnh án cũ để số hóa kho bệnh án đã lưu trữ trước khi làm bệnh án điện tử
2.7	Nhận dữ liệu từ His	Cho phép nhận thông tin của bệnh nhân vào vỏ bệnh án điện tử hệ thống HIS như:
		Thông tin chung:
		+ Thông tin hành chính: Nơi chuyển đến
		+ Thông tin chẩn đoán: nơi chuyển đến, khoa khám bệnh, khoa điều trị, trước phẫu thuật, sau phẫu thuật
		+ Bệnh chính, bệnh kèm theo
		+ Tình trạng ra viện: kết quả điều trị, tình hình tử vong, lý do tử vong, chẩn đoán giải phẫu tử thi
		- Thông tin hỏi bệnh
2.8	Kết xuất vỏ bệnh án	Cho phép kết xuất vỏ bệnh án ra file PDF
2.9	Ký số vào vỏ bệnh án	Ký số vào vỏ bệnh án để đảm bảo pháp lý như ký giấy
2.10	Danh sách vỏ bệnh án	Bệnh án Nội khoa
		Bệnh án Nhi khoa
		Bệnh án Truyền nhiễm
		Bệnh án Phụ khoa
		Bệnh án Sản khoa
		Bệnh án Sơ sinh
		Bệnh án Tâm thần
		Bệnh án Da liễu
		Bệnh án Huyết học-Truyền máu
		Bệnh án Ngoại khoa
		Bệnh án Bỏng
		Bệnh án Ung bướu
		Bệnh án Răng Hàm Mặt
		Bệnh án Tai Mũi Họng
		Bệnh án Ngoại trú chung
		Bệnh án Ngoại trú Răng Hàm Mặt
		Bệnh án Nội trú Y học cổ truyền
		Bệnh án Ngoại trú Y học cổ truyền
		Bệnh án Nội trú Nhi Y học cổ truyền
		Bệnh án Mắt
		Bệnh án Mắt (chấn thương)

Stt	Tính năng	Mô tả tính năng
		Bệnh án Mắt (Bán phần trước)
		Bệnh án Mắt (Đáy mắt)
		Bệnh án Mắt (Glocom)
		Bệnh án Mắt (Lác)
		Bệnh án Mắt trẻ em
		Bệnh án phục hồi chức năng
		Bệnh án phục hồi chức năng nhi
		Bệnh án ngoại trú phục hồi chức năng
		Bệnh án tăng huyết áp
		Bệnh án đái tháo đường
		Bệnh án ARV
		Bệnh án Nội tiết
		Bệnh án Lao phổi
2.11	Tra cứu vỏ bệnh án	Tìm kiếm vỏ bệnh án theo các tiêu tùy chọn
3	**Quản lý biểu mẫu, phiếu, tờ**	
3.1	Phân loại biểu mẫu, phiếu, tờ	Cho phép phân loại biểu mẫu, phiếu, tờ trong bệnh án theo danh mục (tờ điều trị, chăm sóc, truyền dịch, công khai…)
3.2	Sắp xết thứ tự hiển thị biểu mẫu, phiếu, tờ	Sắp xết thứ tự hiển thị biểu mẫu, phiếu, tờ
3.3	Danh sách biểu mẫu, phiếu, tờ đã tạo của bệnh nhân	Quản lý danh sách biểu mẫu, phiếu, tờ đã tạo của bệnh nhân
3.4	Tìm kiếm, sắp xếp biểu mẫu, phiếu, tờ trong danh sách	Hiển thị danh sách biểu mẫu, phiếu, tờ đã tạo của bệnh nhân theo điều kiện tìm kiếm:
		Tìm kiếm theo tên
		Tìm kiếm theo loại phiếu
		Tìm kiếm theo ngày tạo
		Tìm kiếm theo trạng thái phiếu: hoàn thành, chưa hoàn thành
3.5	Xem biểu mẫu, phiếu, tờ đã tạo của bệnh nhân	Hiển thị chi tiết phiếu, biểu mẫu, tờ đã tạo của bệnh nhân
3.6	Tạo biểu mẫu, phiếu, tờ mới	Tạo biểu mẫu, phiếu, tờ mới
		Phục vụ cho việc scan lại bệnh án cũ để số hóa kho bệnh án đã lưu trữ trước khi làm bệnh án điện tử
3.7	Nhận dữ liệu biểu mẫu, phiếu, tờ từ HIS	Nhận dữ liệu biểu mẫu, phiếu, tờ từ HIS
		Thông tin nhận dữ liệu các biểu mẫu, phiếu, tờ trong bệnh án như:
		Thông tin chẩn đoán

Stt	Tính năng	Mô tả tính năng
		Thông tin diễn biến
		Thông tin chăm sóc
		Thông tin truyền dịch
		Thông tin phản ứng thuốc
		Thông tin phẫu thuật thủ thuật
		…
3.8	Kết xuất biểu mẫu, phiếu, tờ	Kết xuất biểu mẫu, phiếu, tờ ra PDF
3.9	Ký số vào từng biểu mẫu, phiếu, tờ ký gộp nhiều ngày	Ký số vào biểu mẫu, phiếu, tờ để đảm bảo pháp lý như ký giấy
		Xây dựng quy trình ký.
4	**Quản lý kết quả cận lâm sàng**	
4.1	Ký số cận lâm sàng	- Ký số kết quả xn sinh hóa
		- Ký số kết quả xn huyết học
		- Ký số kết quả xn nước tiểu
		- Ký số kết quả xn chung
		- Ký số kết quả nội soi
		- Ký số kết quả x-quang
		- Ký số kết quả siêu âm
		- Ký số kết quả điện tim
		- Ký số kết quả CT scan
		- Ký số kết quả điện não
		- Ký số kết quả lưu huyết não
		- Ký số kết quả điện cơ
		- Ký số kết quả DSA
		- Ký số kết quả giải phẫu bệnh
		- Ký số kết quả đo độ loãng xương
		- Ký số kết quả thang đánh giá tâm lý
		- Module xem kết quả CĐHA file dạng: dicom, jpg, png, jpge.
4.2	Đính kèm ảnh, đường dẫn link xem ảnh từ các hệ thống PACS	Đính kèm ảnh, đường dẫn link xem ảnh từ các hệ thống PACS
5	**Quản lý ký số**	
5.1	Tích hợp chữ ký số HSM	Tích hợp với chữ ký HSM để ký trên tất cả văn bản
5.2	Thêm ảnh ký tươi vào chữ ký số	Cho phép chèn thêm ảnh chữ ký tay để làm sinh động thêm văn bản

Stt	Tính năng	Mô tả tính năng
5.3	Tạo văn bản cần ký	Người dùng khi muốn ký 1 văn bản nào đó trong bệnh án điện tử thì có thể tạo văn bản, văn bản được tạo sẽ tự động lưu vào EMR
5.4	Thiết lập người ký	Cho phép người tạo có thể thêm người vào văn bản được ký. Người được thêm có thể là nhân viên y tế hoặc bệnh nhân
5.5	Thiết lập luồng ký	Với những văn bản nhiều người ký, tùy vào hình thức có thể thiết lập ký nối tiếp (từng người ký lần lượt) hoặc ký song song (nhiều người cùng ký một lúc) hoặc vừa nối tiếp vừa song song (lãnh đạo ký cuối cùng còn lại có thể ký cùng một lúc)
5.6	Thực hiện ký số	- Cho phép người dùng ký số vào văn bản: vỏ bệnh án, các phiếu, biểu mẫu, phiếu chỉ định, phiếu kết quả cận lâm sàng - Ký số con dấu Trung tâm trên file tổng hợp giấy tờ trong hồ sơ bệnh án của bệnh nhân
5.7	Lựa chọn vị trí ký	Tùy chọn vị trí trên văn bản để ký: - Ký theo từ khóa - Ký theo vị trí - Ký nháy - Đóng dấu Trung tâm - Chọn vị trí ký trên tài liệu
5.8	Kiểm tra chữ ký số hợp lệ	- Kiểm tra các chữ ký số có trong văn bản, hiển thị trạng thái hợp lệ của chữ ký số
5.9	Ký điện tử	- Cho phép ký điện tử các giấy tờ của bệnh án
6	Lưu trữ file ký số	
6.1	Mã hóa file lưu trữ	- File văn bản sẽ được mã hóa TripleDes trước khi lưu trữ.
6.2	Lưu trữ file ký số	- Lưu trữ 1 bản tại ổ cứng của máy chủ Trung tâm - Lưu trữ 1 bản tại Nat, SAN thông qua giao thức FTP - Lưu trữ 1 bản tại Cloud S3
6.3	Đồng bộ bệnh án	- Tự động đồng bộ bệnh án lên cloud trong trường hợp mất internet.
6.4	Báo cáo lưu trữ	- Báo cáo số lượng file hồ sơ, dung lượng còn trống, cảnh báo khi sắp hết dung lượng
7	Quản lý danh mục	Có phần quản lý danh mục cho phép thêm, sửa, không dùng
7.1	Danh mục bệnh án	Quản lý danh sách bệnh án sử dụng trong Trung tâm
7.2	Danh mục giấy tờ trong bệnh án	Quản lý Danh sách loại giấy tờ của bệnh án
7.3	Danh mục nhân viên	Quản lý danh sách nhân viên
7.4	Danh mục khoa phòng	Quản lý danh sách khoa phòng trong Trung tâm

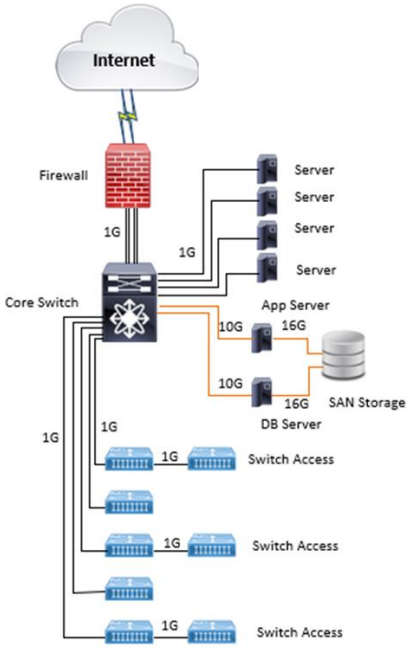
Stt	Tính năng	Mô tả tính năng
7.5	Các danh mục khác	Quản lý các danh mục khác liên quan trong quá trình triển khai bệnh án
8	Quản lý mượn, bổ sung, thay thế	
8.1	Quản lý mượn trả	- Cho phép tạo phiếu mượn trả, duyệt mượn in ấn, phục vụ chuyên môn của các cơ quan chức năng.
8.2	Quản lý bổ sung, thay thế	- Thay thế bổ sung các giấy tờ trong bệnh án khi chưa chốt lưu trữ, khi thay đổi phải lập phiếu được duyệt và lưu lịch sử thay đổi
9	Lưu lịch sử thao tác người dùng	- Lưu trữ, tra cứu lịch sử thao tác người dùng
10	Phân quyền người dùng	- Thực hiện phân quyền truy cập, thao tác theo từng người dùng
11	Báo cáo	
11.1	Báo cáo hồ sơ theo khoa phòng	- Tổng hợp báo cáo bệnh án theo khoa phòng
11.2	Thống kê hồ sơ theo nhóm bệnh, độ tuổi, Phái	- Tổng hợp báo cáo bệnh án tách theo nhóm bệnh, độ tuổi, phái
11.3	Chiết xuất dữ liệu hồ sơ bệnh án dạng XML, HL7, LIS, RIS/PACS	- Chiết xuất dữ liệu phục vụ trao đổi dữ liệu với các phần mềm khác
12	Ứng dụng di động	
12.1	Quản lý hồ sơ bệnh án	- Tra cứu, xem hồ sơ bệnh án - Chụp, tải file nội dung bệnh án - Nhập thông tin hồ sơ bệnh án - Kết thúc hồ sơ bệnh án
12.2	Ký số	- Cho phép người dùng ký số
12.3	Ký số bệnh nhân	- Tạo chứng thư số bệnh nhân - Ký số bệnh nhân
C – Danh mục nâng cấp khác		
1	Cài đặt tưởng lửa	- Chặn các truy cập không được phép - Chống tấn công mạng
2	Mã hóa dữ liệu lưu trữ	- Mã hóa các dữ liệu khi lưu trữ nhằm mục đích dù bị lộ vẫn không thể sử dụng được thông tin. Phải cần khóa của đơn vị phần mềm giải mã để xem tài liệu.
3	Cài đặt chống sao chép dữ liệu trên máy chủ	- Chống việc sao chép dữ liệu từ máy chủ ra thiết bị ngoại vi để tránh việc lộ thông tin.
4	Sao lưu dữ liệu	- Sao lưu định kỳ kết hợp sao lưu dữ liệu thời gian thực - Máy chủ dự phòng cho phép thay thế máy chủ chính khi xảy ra sự cố đảm bảo hoạt động thông suốt

3.1.2.2.4. Yêu cầu đối với hạ tầng kỹ thuật vận hành phần mềm

a. Yêu cầu về mô hình triển khai

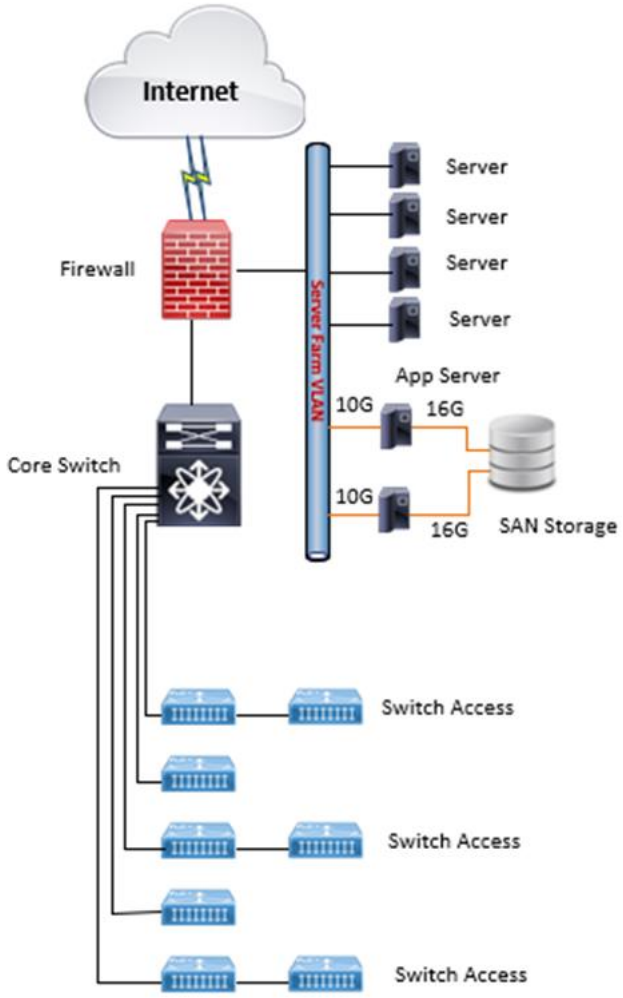
Mô hình triển khai hệ thống được mô tả như các sơ đồ kết nối vật lý và mô hình kết nối logic dưới đây:

✓ Mô hình kết nối vật lý:



SƠ ĐỒ KẾT NỐI VẬT LÝ HỆ THỐNG CNTT BỆNH VIỆN

✓ Mô hình kết nối logic:



SƠ ĐỒ KẾT NỐI LOGIC HỆ THỐNG CNTT BỆNH VIỆN

Trong đó:

- Hệ thống được trang bị 01 thiết bị chuyển mạch lõi (Core Switch), có các kết nối 10G, và các kết nối 1G. Switch này sẽ cung cấp kết nối cho các Máy chủ (Server) với kết nối 10G, và kết nối quang 1G đến các thiết bị chuyển mạch truy cập (Access Switch). Thiết bị
- Trang bị 01 Firewall làm chức năng kiểm soát truy cập và bảo vệ hệ thống trước các nguy cơ an ninh từ internet và mạng nội bộ xâm nhập vào hệ thống máy chủ. Theo đó các truy cập ra Internet được kiểm soát, các truy cập vào hệ thống máy chủ cũng được giám sát chặt chẽ.
- Trang bị các thiết bị chuyển mạch truy cập (Access Switch) đảm bảo kết nối cho các máy trạm đến máy chủ là 1G.
- Trang bị 01 máy chủ ứng dụng (App Server) và 01 máy chủ cơ sở dữ liệu (DB Server) tin cậy, ổn định phục vụ cho ứng dụng.
- Hệ thống trang bị 01 thiết bị lưu trữ SAN Storage. Hệ thống này có cơ chế dự phòng: 02 controller, 02 nguồn, cơ chế dự phòng dữ liệu qua RAID. Tất cả các dữ liệu của hệ thống sẽ được lưu trữ trên thiết bị này.

3.1.3. Yêu cầu, điều kiện về khả năng kết nối, liên thông ứng dụng, hệ thống khác

Yêu cầu về khả năng kết nối, liên thông các hệ thống, phần mềm phục vụ khám chữa bệnh tuân thủ và yêu cầu tại mục 2.2.3. Danh mục các quy chuẩn, tiêu chuẩn kết nối, tích hợp dữ liệu, truy cập thông tin, an toàn thông tin và đặc tả dữ liệu

Ngoài ra yêu cầu kết nối với các thiết bị IOT sử dụng trong Trung tâm được miêu tả tại mục "Các quy trình nghiệp vụ cần được tin học hóa (tổ chức, vận hành của quy trình, sản phẩm của quá trình nghiệp vụ, các giao tác xử lý của quy trình nghiệp vụ)"

3.1.3.1. Yêu cầu kết nối với hệ thống lưu trữ và truyền tải hình ảnh (RIS-PACS)

Tin học hóa việc quản lý yêu cầu và trả lời kết quả chẩn đoán hình ảnh. Yêu cầu được mô tả chức năng như sau:

Mã	Mô tả chức năng
CDHA.01	Chỉ định dịch vụ: Dùng để bác sĩ khám và điều trị chỉ định dịch vụ cận lâm sàng cho bệnh nhân.
CDHA.02	Trả lời kết quả Chẩn đoán hình ảnh: Dùng để bác sĩ trả lời kết quả, kỹ thuật viên ghi nhận thông tin sau khi thực hiện dịch vụ.
CDHA.03	Trả lời kết quả X-Quang: Bác sĩ trả lời kết quả, kỹ thuật viên ghi nhận thông tin sau khi thực hiện dịch vụ X Quang
CDHA.04	Trả lời kết quả CT-Scanner: Bác sĩ trả lời kết quả, kỹ thuật viên ghi nhận thông tin sau khi thực hiện dịch vụ CT-Scanner
CDHA.05	Trả lời kết quả MRI: Bác sĩ trả lời kết quả, kỹ thuật viên ghi nhận thông tin sau khi thực hiện dịch vụ MRI
CDHA.06	Trả lời kết quả Siêu Âm: Bác sĩ trả lời kết quả, kỹ thuật viên ghi nhận thông tin sau khi thực hiện dịch vụ Siêu âm
CDHA.07	Trả lời kết quả Siêu Âm tim: Bác sĩ trả lời kết quả, kỹ thuật viên ghi nhận thông tin sau khi thực hiện dịch vụ Siêu âm tim
CDHA.08	Trả lời kết quả nội soi/nội soi phế quản/nội soi tiêu hóa: Bác sĩ trả lời kết quả, kỹ thuật viên ghi nhận thông tin sau khi thực hiện các dịch vụ nội soi
CDHA.09	Trả lời kết quả đo loãng xương: Bác sĩ trả lời kết quả, kỹ thuật viên ghi nhận thông tin sau khi thực hiện dịch vụ đo loãng xương
CDHA.10	Xem kết quả: Bác sĩ khám, điều trị xem kết qua thực hiện CĐHA-TDCN để hỗ trợ công tác chẩn đoán và điều trị
CDHA.11	In kết quả: Bác sĩ khám, điều trị xem và kết quả thực hiện chẩn đoán hình ảnh để lưu trữ hồ sơ hoặc trả kết quả cho bệnh nhân
CDHA.12	Định nghĩa từ điển kết quả: Bác sĩ kết luận mô tả kết quả một cách nhanh chóng dựa trên các mẫu đã được định nghĩa
CDHA.13	Báo cáo chẩn đoán hình ảnh

CDHA.14	Kết nối hệ thống PACS

3.1.3.2. Yêu cầu kết nối với hệ thống thông tin xét nghiệm (LIS)

Kết nối với hệ thống phần mềm quản lý máy xét nghiệm để gửi yêu cầu xét nghiệm và nhận lại kết quả xét nghiệm tự động để lưu trữ, in kết quả trả cho bệnh nhân. Tin học hóa việc quản lý yêu cầu và trả lời kết quả xét nghiệm.

Mã	Mô tả chức năng
XN.01	Chỉ định dịch vụ: Bác sĩ khám và điều trị chỉ định dịch vụ cận lâm sàng cho bệnh nhân.
XN.02	Trả lời kết quả xét nghiệm: Bác sĩ thực hiện, kỹ thuật viên ghi nhận thông tin sau khi thực hiện dịch vụ
XN.03	Trả lời kết quả Huyết học: Bác sĩ thực hiện, kỹ thuật viên ghi nhận thông tin sau khi thực hiện dịch vụ huyết học
XN.04	Trả lời kết quả Sinh hóa: Bác sĩ thực hiện, kỹ thuật viên ghi nhận thông tin sau khi thực hiện dịch vụ Sinh hóa
XN.05	Trả lời kết quả Miễn dịch: Bác sĩ thực hiện, kỹ thuật viên ghi nhận thông tin sau khi thực hiện dịch vụ Miễn dịch
XN.06	Trả lời kết quả Vi sinh: Bác sĩ thực hiện, kỹ thuật viên ghi nhận thông tin sau khi thực hiện dịch vụ Vi sinh
XN.07	Trả lời kết quả giải phẫu bệnh: Bác sĩ thực hiện, kỹ thuật viên ghi nhận thông tin sau khi thực hiện dịch vụ giải phẫu bệnh
XN.08	Xem kết quả: Bác sĩ khám, điều trị xem kết quả thực hiện xét nghiệm để hỗ trợ công tác chẩn đoán và điều trị
XN.09	In kết quả: Cho phép bác sĩ khám, điều trị xem và kết quả thực hiện xét nghiệm để lưu trữ hồ sơ hoặc trả kết quả cho bệnh nhân
XN.10	Báo cáo xét nghiệm

3.1.4. Yêu cầu cần đáp ứng của phần mềm

3.1.4.1. Tên phần mềm cho thuê khai thác sử dụng

Hệ thống phần mềm bệnh án điện tử

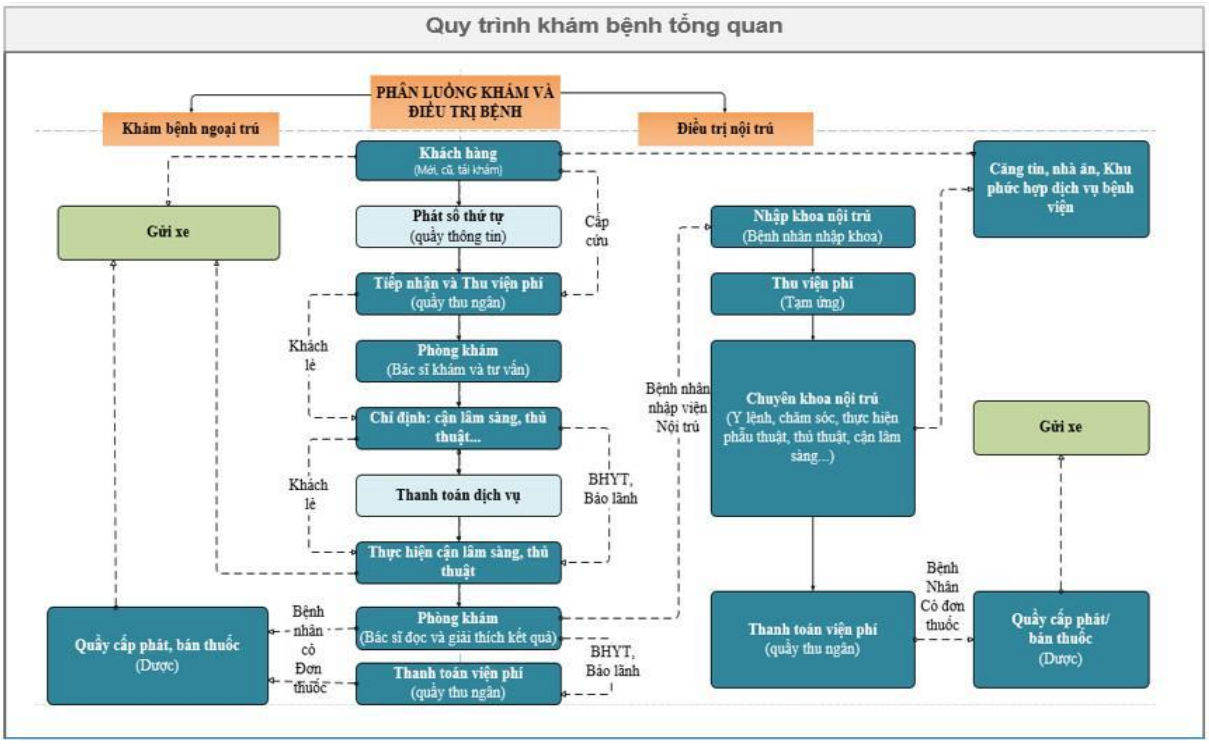
3.1.4.2. Các thông số chủ yếu

3.1.4.2.1. Các quy trình nghiệp vụ cần được tin học hóa (tổ chức, vận hành của quy trình, sản phẩm của quá trình nghiệp vụ, các giao tác xử lý của quy trình nghiệp vụ)

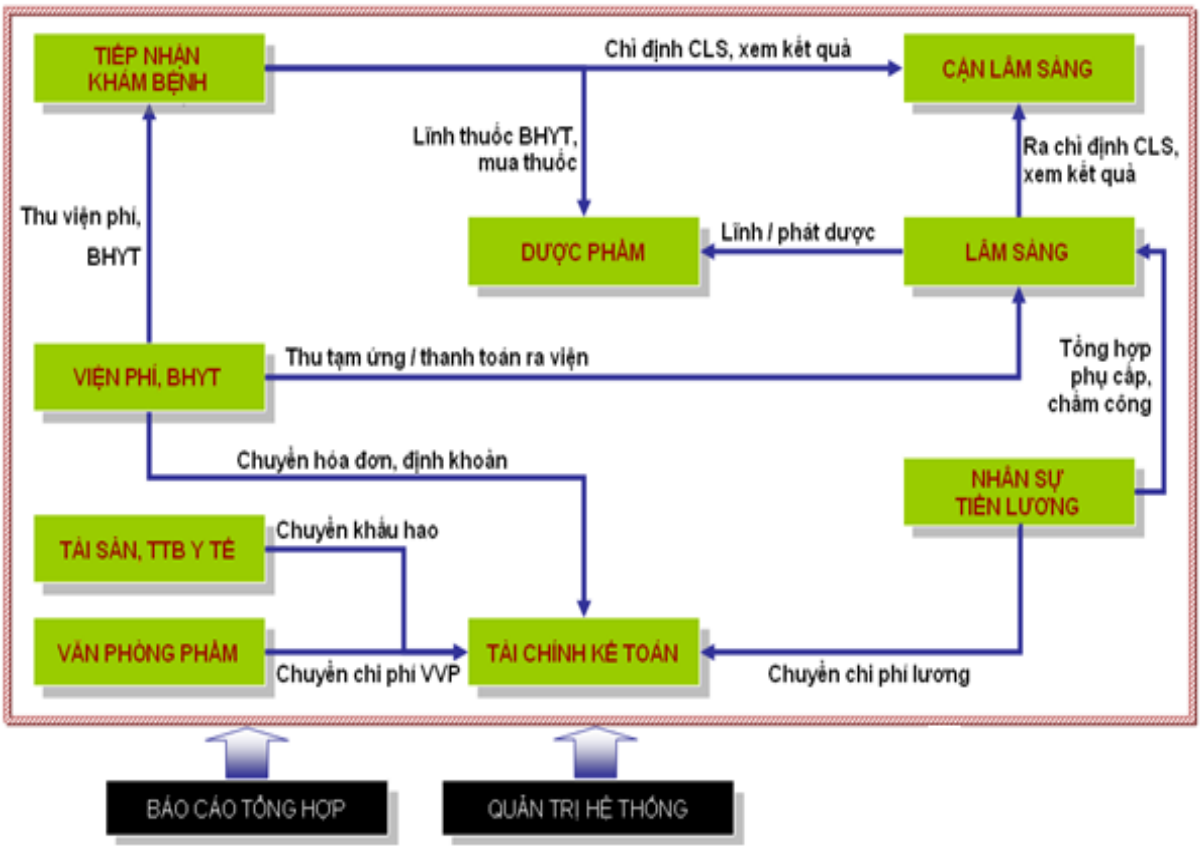
3.1.4.2.1.1. Quy trình khám chữa bệnh tổng quan

Chương trình gồm nhiều chương trình phần mềm chuyên môn (module) quản lý từng phần việc chuyên biệt khác nhau. Mỗi chương trình phần mềm chuyên môn quản lý kết nối thành một thể thống nhất, số liệu tập trung duy nhất toàn Trung tâm. Các

chương trình quản lý nghiệp vụ bao gồm nhiều chương trình con và được phân bổ thành các phân hệ quản lý (module) chính như sau:

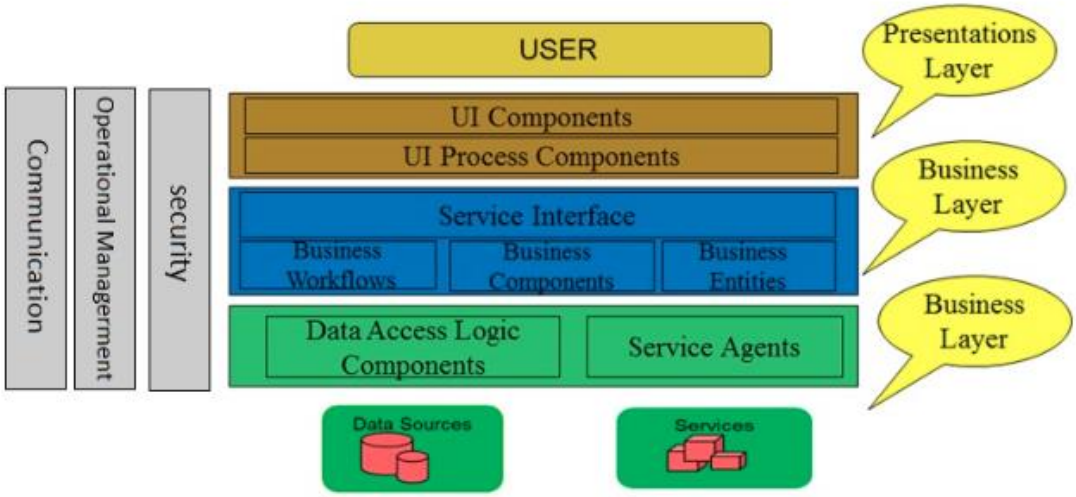


3.1.4.2.1.2. Mô hình kiến trúc tổng thể



Kiến trúc tổng thể Hệ thống phần mềm bệnh án điện tử (HIS)

3.1.4.2.1.3. Mô hình ứng dụng tổng thể



Mô hình ứng dụng tổng thể hệ thống phần mềm

- Hệ thống phần mềm được thiết kế theo mô hình ứng dụng 3 lớp (3 Layers):

+ Lớp trình bày (Presentation Layer): Lớp này làm nhiệm vụ giao tiếp với người dùng cuối để thu thập dữ liệu và hiển thị kết quả/dữ liệu thông qua các thành phần trong giao diện người sử dụng. Lớp này sẽ sử dụng các dịch vụ do lớp Business Logic cung cấp.

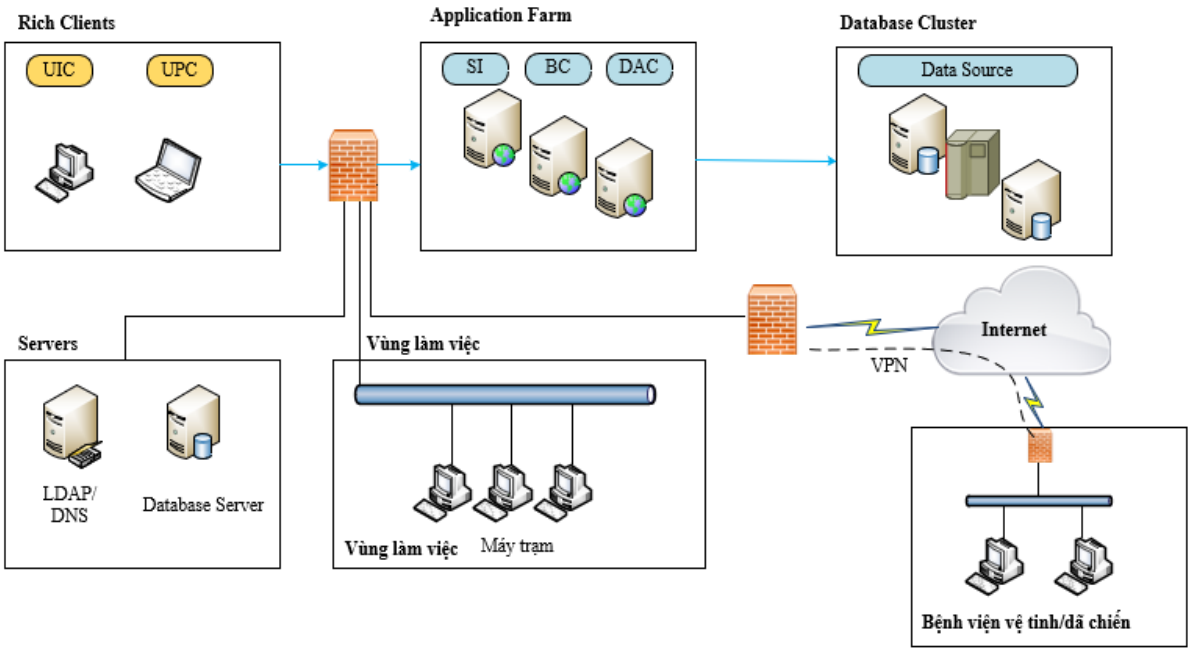
+ Lớp nghiệp vụ (Business Layer): Lớp này thực hiện các nghiệp vụ chính của hệ thống, sử dụng các dịch vụ do lớp Data Access cung cấp, và cung cấp các dịch vụ cho lớp Presentation.

+ Lớp truy xuất dữ liệu (Data Access Layer): Lớp này thực hiện các nghiệp vụ liên quan đến lưu trữ và truy xuất dữ liệu của ứng dụng. Thường lớp này sẽ sử dụng các dịch vụ của các hệ quản trị cơ sở dữ liệu như SQL Serve,MySQL, Oracle DB, PostgreSQL… để thực hiện nhiệm vụ của mình.

- Thành phần hỗ trợ (Cross-Cutting): Cung cấp các thư viện, các thành phần hỗ trợ xử lý cho các lớp Presentation, Business, Data.

3.1.4.2.1.4. Mô hình triển khai

- Mô hình triển khai hệ thống như sau:



- Hệ thống được phân chia thành các phân vùng riêng biệt để quản lý luồng dữ liệu. Giữa các phân vùng được kiểm soát bởi thiết bị Firewall nhằm đảm bảo an ninh.
- Cơ sở dữ liệu Phần mềm được tập trung tại máy chủ đóng vai trò Database Server.
- Phân vùng mạng LAN: cung cấp các điểm kết nối mạng cho người dùng đầu cuối tại các khoa, phòng ban chức năng; đồng thời kết nối thông suốt đến tất cả các thành phần trong hệ thống.
- Các máy trạm cài đặt chương trình ứng dụng để truy cập và xử lý dữ liệu.
- Mỗi người dùng được phân quyền sẽ sử dụng tại máy tính tại các khoa, toàn bộ số liệu sẽ tổng hợp lại thông qua hệ thống mạng máy tính về máy chủ trung tâm (Server) xử lý và kết xuất báo cáo theo từng khoa phòng phòng hay tổng thể Trung tâm.
- Người dùng tại các Trung tâm vệ tinh, Trung tâm dã chiến khi có yêu cầu sẽ kết nối về trung tâm thông qua mạng riêng ảo (VPN) để khai thác và sử dụng phần mềm cũng như cơ sở dữ liệu tại trung tâm. Các kết nối này sẽ được định danh và quản lý thông qua Firewall.

3.1.4.2.1.5. Kiến trúc, mô hình hệ thống hồ sơ bệnh án điện tử

Kiến trúc tổng thể hệ thống hồ sơ bệnh án điện tử bao gồm 3 phần chính:

* Phục vụ chuyên môn: Đây là phần chính của hệ thống phục vụ các công tác quản lý, điều hành, hoạt động chuyên môn của Trung tâm; bao gồm:

Nhóm chức năng về Quản lý bệnh nhân

Nhóm chức năng Dịch vụ hỗ trợ lâm sàng như: hệ thống Cận lâm sàng (LIS, RIS/PACs), hệ thống Quản lý Dược, hệ thống Quản lý phòng mổ (Operative Theatre Management System), ….

Nhóm chức năng liên quan đến Bệnh án điện tử:

1. CPOE – Computerized Physican Order Entry: ra Y lệnh điện tử
2. CDSS – Clinical Decision Suport Service: dịch vụ hỗ trợ ra quyết định lâm sàng
3. Quản lý tài liệu lâm sàng
4. Quản lý quy trình tác nghiệp (công việc, quy trình kỹ thuật, …)

Nhóm chức năng liên quan đến quản lý thông tin điều hành (Báo cáo, thống kê điều hành, …)

Nhóm chức năng quản lý Kế toán, tài chính (Doanh thu, chi phí, BHYT, …)

Nhóm chức năng Quản lý chung: bao gồm Quản lý cơ cấu tổ chức, quản lý cán bộ y tế, ...

Nhóm chức năng Quản lý kho: bao gồm quản lý Kho dược, trang thiết bị, vật tư y tế, ngân hàng máu, ...

Nhóm chức năng liên quan đến Dịch vụ tích hợp: kết nối các hệ máy xét nghiệm, chẩn đoán hình ảnh, các hệ thống máy tại ICU, ...

Nhóm chức năng liên quan đến trích xuất, trao đổi dữ liệu, thông tin y tế: trích xuất, trao đổi thông tin tóm tắt bệnh nhân theo CCD – Continue of Care Documents, ...

Nhóm chức năng Quản trị hệ thống

Bệnh nhân, người nhà bệnh nhân tra cứu, sử dụng dịch vụ và tương tác với Trung tâm qua các kênh: KIOS, ứng dụng web, thiết bị di động, IoT, ứng dụng desktop, mạng xã hội …

Lãnh đạo, quản lý khoa phòng, bác sỹ, điều dưỡng, nhân viên y tế tác nghiệp với hệ thống thông qua các kênh: ứng dụng desktop, ứng dụng web, thiết bị di động, IoT, …

* Hệ thống các ứng dụng nội bộ bao gồm:

Hệ thống chuyên ngành: HIS, LIS, RIS/PACS, …

* Hệ thống các ứng dụng tương tác với các hệ thống bên ngoài:

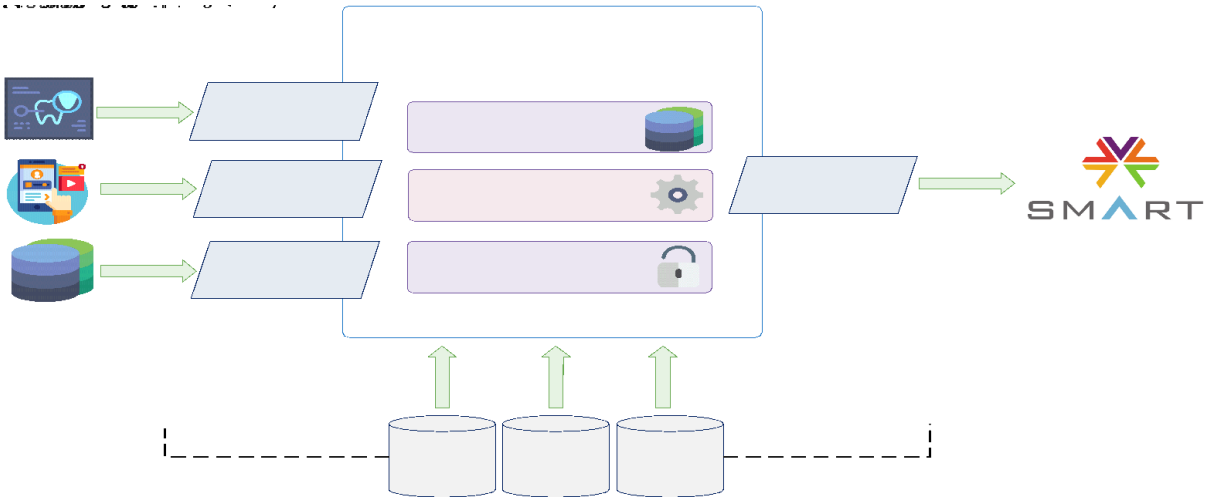
Hệ thống thông tin quản lý ngành của Bộ Y tế như: hệ thống quản lý Danh mục dùng chung, hệ thống quản lý Hồ sơ sức khỏe điện tử, hệ thống thống kê y tế điện tử ….

Hệ thống giám định, thanh toán BHYT

Hệ thống Chữ ký số

Hệ thống thanh toán online

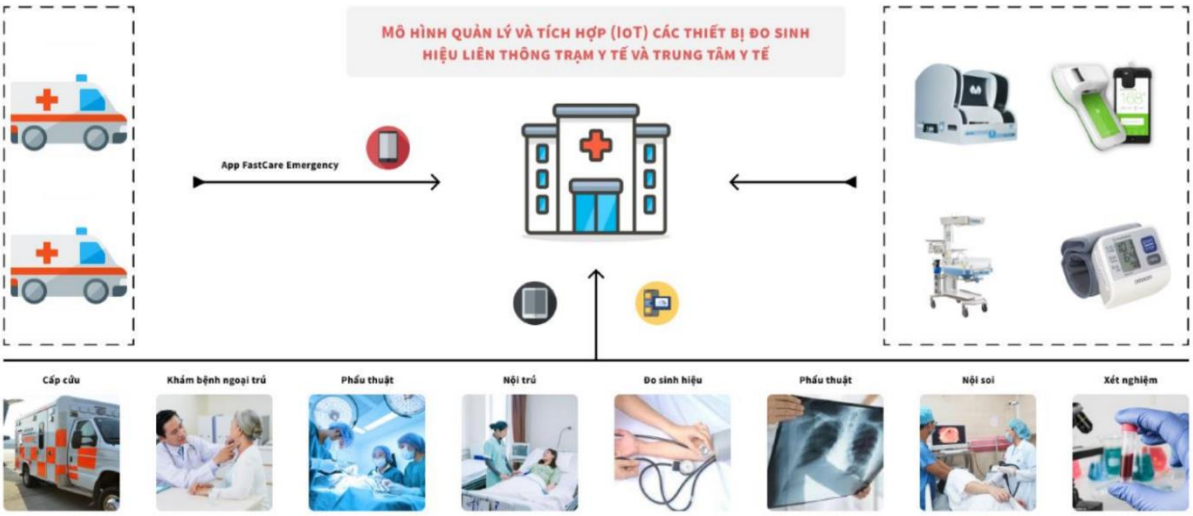
3.1.4.2.1.6. Kiến trúc kho dữ liệu lâm sàng (CDR) dựa trên bộ tiêu chuẩn HL7 FHIR



Kiến trúc kho dữ liệu lâm sàng dựa trên bộ tiêu chuẩn HL7 FHIR bao gồm các thành phần sau:

- CSDL lưu trữ thông tin.
- HL7 FHIR Endpoints: các kênh giao tiếp (API) được mô tả và định nghĩa theo bộ tiêu chuẩn HL7 FHIR.
- HL7 v2.x message Adapters: đối với các hệ thống như hệ thống LIS, RIS/PACs sử dụng cơ chế trao đổi gói tin dựa trên bộ tiêu chuẩn HL7 v2.x message thì hệ thống cần hỗ trợ tích hợp và trao đổi với các kênh giao tiếp này.
- Các kênh giao tiếp khác: thông qua các ETL tools đối với các CSDL sẵn có, đặc thù của từng cơ sở khám, chữa bệnh.

3.1.4.2.1.7. Mô hình tích hợp thiết bị IOT vào HIS



3.1.4.2.1.8.Các tác nhân tham gia vào hệ thống

Stt	Tên tác nhân	Ghi chú
1	Nhân viên y tế	Là các bác sĩ, điều dưỡng, các cán bộ ngành khác phục vụ khám chữa bệnh, lập bệnh án, cấp phát thuốc, thanh toán chi phí và thanh quyết toán BHYT. Lập bệnh án, nhập các giấy tờ liên quan
2	Quản trị viên	Người được giao trách nhiệm quản trị hệ thống phần mềm và các vấn đề liên quan CNTT. Khai báo và quản trị các danh mục bệnh án, phân quyền sử dụng bệnh án cho các khoa phòng và các danh mục liên quan, kết xuất báo cáo
3	Máy chủ hệ thống	Máy chủ dựng trang web HIS và module quản lý bệnh án điện tử EMR, thực hiện việc xác thực user, điều khiển quá trình kí số, lưu trữ, truy vấn file kí số
4	Máy chủ kí số	Máy chủ chuyên dụng để kí số, cung cấp giải pháp kí số trên các dạng dữ liệu XML,PDF, Text… và xác thực có tính pháp lý.
5	Người quản lý hồ sơ	Người chịu trách nhiệm tiếp nhận hồ sơ bệnh án từ khoa phòng, được giao nhiệm vụ quản lý, lập phiếu mượn trả, quản lý lưu trữ kho bệnh án giấy.
6	Các tác nhân khác	Usb kí số, Api của hệ thống BHYT…

3.1.4.2.2. Danh sách các yêu cầu của người sử dụng

Các chức năng Hệ thống phần mềm Bệnh án điện tử (EMR)

Stt	Tính năng
A – DANH MỤC NÂNG CẤP PHẦN MỀM	

I – Nâng cấp (HIS)	
1	Quản lý suất ăn cho bệnh nhân
2	Quản lý phác đồ điều trị
3	Ký số bệnh nhân
3.1	Tạo chứng thư số bệnh nhân
3.1.1	Xác thực sinh trắc học bằng khuôn mặt, vân tay
3.1.2	Xác thực NFC căn cước công dân
3.1.3	Thực hiện Ekyc khuôn mặt
3.1.4	Tạo chứng thư số bệnh nhân
3.2	Ký số bệnh nhân
4	Gửi hồ sơ bệnh án điện tử
4.1	Liên kết tài khoản với bệnh án điện tử
4.2	Tạo bệnh án điện tử
4.2	Gửi giấy tờ lên bệnh án điện tử
4.3	Cảnh báo thay đổi nội dung giấy tờ
4.4	Kiểm tra giấy tờ
4.5	Xem hồ sơ bệnh án
4.6	Xem danh sách giấy tờ cần ký số
4.7	Kết thúc hồ sơ bệnh án
4.8	Nộp hồ sơ bệnh án
4.9	Mượn, thay thế, bổ sung bệnh án
5	Quản lý dinh dưỡng
6	Xem hình ảnh Pacs tại phòng khám
II – Nâng cấp xét nghiệm (LIS)	
1	Quản lý mẫu xét nghiệm
2	Quản lý hóa chất xét nghiệm
2.1	Quản lý định mức hóa chất
2.2	Báo cáo sử dụng hóa chất theo thời gian, máy xét nghiệm
3	Gửi phiếu kết quả và ký số
4	Xem kết quả xét nghiệm qua WebView
III – Nâng cấp CDHA (RIS-PACS)	
1	Cấu hình quản lý máy chủ PACS
2	Cấu hình quản lý máy trạm PACS
3	Hỗ trợ xem ảnh DICOM qua WebView
4	Chức năng biên tập và xử lý hình ảnh DICOM
5	Chức năng nén ảnh theo giải thuật JPEG2000
6	Gửi hồ sơ phiếu kết quả, ký số
IV – Nâng cấp Viện Phí	
1	Gửi giấy tờ bệnh án điện tử và ký số
1.1	Gửi giấy tờ lên bệnh án điện tử
1.2	Ký số
1.3	Ký số bệnh nhân

B – PHẦN MỀM BỆNH ÁN ĐIỆN TỬ	
1	Quản lý tạo bệnh án điện tử
1.1	Tạo bệnh án điện tử từ HIS
1.2	Cấp mã định danh cho bệnh án điện tử
1.3	Cấp số Bệnh án điện tử
1.4	Cập nhật thông tin bệnh nhân từ HIS
1.5	Quản lý file ký
2	Quản lý vỏ bệnh án
2.1	Phân loại vỏ bệnh án
2.2	Sắp xết thứ tự hiển thị vỏ bệnh án
2.3	Tự động chọn vỏ bệnh án theo khoa điều trị
2.4	Danh sách vỏ bệnh án đã tạo của bệnh nhân
2.5	Xem vỏ bệnh án đã tạo của bệnh nhân
2.6	Tạo vỏ bệnh án mới
2.7	Nhận dữ liệu từ His
2.8	Kết xuất vỏ bệnh án
2.9	Ký số vào vỏ bệnh án
2.10	Danh sách vỏ bệnh án
2.11	Tra cứu vỏ bệnh án
3	Quản lý biểu mẫu, phiếu, tờ
3.1	Phân loại biểu mẫu, phiếu, tờ
3.2	Sắp xết thứ tự hiển thị biểu mẫu, phiếu, tờ
3.3	Danh sách biểu mẫu, phiếu, tờ đã tạo của bệnh nhân
3.4	Tìm kiếm, sắp xếp biểu mẫu, phiếu, tờ trong danh sách
3.5	Xem biểu mẫu, phiếu, tờ đã tạo của bệnh nhân
3.6	Tạo biểu mẫu, phiếu, tờ mới
3.7	Nhận dữ liệu biểu mẫu, phiếu, tờ từ HIS
3.8	Kết xuất biểu mẫu, phiếu, tờ
3.9	Ký số vào từng biểu mẫu, phiếu, tờ ký gộp nhiều ngày
4	Quản lý kết quả cận lâm sàng
4.1	Ký số cận lâm sàng
4.2	Đính kèm ảnh, đường dẫn link xem ảnh từ các hệ thống PACS
5	Quản lý ký số
5.1	Tích hợp chữ ký số HSM
5.2	Thêm ảnh ký tươi vào chữ ký số
5.3	Tạo văn bản cần ký
5.4	Thiết lập người ký
5.5	Thiết lập luồng ký
5.6	Thực hiện ký số
5.7	Lựa chọn vị trí ký
5.8	Kiểm tra chữ ký số hợp lệ
5.9	Ký điện tử

6	Lưu trữ file ký số
6.1	Mã hóa file lưu trữ
6.2	Lưu trữ file ký số
6.3	Đồng bộ bệnh án
6.4	Báo cáo lưu trữ
7	Quản lý danh mục
7.1	Danh mục bệnh án
7.2	Danh mục giấy tờ trong bệnh án
7.3	Danh mục nhân viên
7.4	Danh mục khoa phòng
7.5	Các danh mục khác
8	Quản lý mượn, bổ sung, thay thế
8.1	Quản lý mượn trả
8.2	Quản lý bổ sung, thay thế
9	Lưu lịch sử thao tác người dùng
10	Phân quyền người dùng
11	Báo cáo
11.1	Báo cáo hồ sơ theo khoa phòng
11.2	Thống kê hồ sơ theo nhóm bệnh, độ tuổi, Phái
11.3	Chiết xuất dữ liệu hồ sơ bệnh án dạng XML, HL7, LIS, RIS/PACS
12	Ứng dụng di động
12.1	Quản lý hồ sơ bệnh án
12.2	Ký số
12.3	Ký số bệnh nhân
C – Danh mục nâng cấp khác	
1	Cài đặt tưởng lửa
2	Mã hóa dữ liệu lưu trữ
3	Cài đặt chống sao chép dữ liệu trên máy chủ
4	Sao lưu dữ liệu

3.1.4.2.3. Yêu cầu phi chức năng

3.1.4.2.3.1.Yêu cầu cần đáp ứng đối với hệ thống quản trị CSDL

- CSDL phải có chế độ thiết lập chế độ sao lưu dữ liệu định kỳ, đột xuất (người quản trị có thể thiết lập chế độ sao lưu dữ liệu theo ngày, giờ) và tùy chọn các thành phần cần sao lưu:
  + Dữ liệu cấu hình hệ thống.
  + Cơ sở dữ liệu lưu trữ nội dung.
  + Các dữ liệu khác có liên quan.
- Cho phép phục hồi dữ liệu theo phiên bản đã được lưu trữ khi cần thiết hoặc khi có sự cố xảy ra.
- CSDL phải cung cấp khả năng xử lý và lưu trữ dữ liệu lớn

- Hệ quản trị CSDL cho phép giám sát hoạt động lâu dài, sử dụng giao diện đồ họa để dễ dàng thao tác. Có cơ chế tự động gửi các thông tin giám sát về cho người quản trị.
- Hệ quản trị CSDL có hỗ trợ khả năng chẩn đoán về cả các hoạt động của cơ sở dữ liệu và khả năng phần cứng để cung cấp mối tương quan giữa việc sử dụng cơ sở dữ liệu và hiệu suất phần cứng.
- Hệ quản trị CSDL có cung cấp các tính năng để hạn chế các cán bộ quản trị cơ sở dữ liệu, cán bộ phát triển ứng dụng, hỗ trợ ứng dụng hoặc những người sử dụng có đặc quyền khác truy cập vào dữ liệu ứng dụng nghiệp vụ hoặc thực hiện những thay đổi không được phép.
- Hệ quản trị CSDL hỗ trợ cho khả năng truy vấn song song tự động.
- Hệ quản trị CSDL có cung cấp tính năng audit dữ liệu thay đổi.
- Hệ quản trị CSDL phải hỗ trợ khả năng phân vùng dữ liệu theo một hoặc một số chiều dữ liệu.
- Hệ quản trị CSDL phải hỗ trợ khả năng truy vấn và quản lý giao dịch phân tán giữa các CSDL khác nhau.

3.1.4.2.3.2.Yêu cầu về mỹ thuật, kỹ thuật cần đạt được của các giao diện chương trình

- Hệ thống cho phép lưu trữ tất cả dữ liệu theo định dạng Unicode, chấp nhận tất cả các kỹ tự tiếng việt có dấu.
- Giao diện màn hình, các thông báo lỗi và trợ giúp là ngôn ngữ tiếng việt theo chuẩn TCVN 6909:2001 dựa trên bảng mã Unicode (ISO 10646), với trợ giúp các bộ gõ Unikey, Vietkey.
- Các biểu tượng, hình ảnh được thống nhất trong toàn bộ chương trình.
- Các màn hình cập nhật dữ liệu về cơ bản phải thống nhất về các nút lệnh cũng như về màu sắc, phông chữ.
- Hiển thị ngày theo dạng DD/MM/YYYY và căn giữa.
- Các trường thông tin dạng text thì căn lề trái.
- Hệ thống phải cung cấp giao diện trực quan, thân thiện với người sử dụng và phù hợp đối với các nhóm người sử dụng khác nhau.
- Các giao diện thiết kế một cách đơn giản nhưng hiệu quả cao về thao tác, giảm thiểu việc mở quá nhiều cửa sổ, hiển thị và xử lý hình ảnh nhanh, màu sắc không gây cảm giác nhàm chán cho người sử dụng và theo một chuẩn giao diện thống nhất.
- Tất cả các ngày tháng sẽ được lưu với 4 chữ số cho phần Năm.
- Các thành phần trong giao diện màn hình nhập liệu phải được focus tuần tự liên tiếp nhau khi thực hiện phím Enter.
- Trong các màn hình nhập số liệu, các trường bắt buộc phải nhập cần phải đánh dấu (*) bên cạnh để phân biệt.
- Trong mỗi màn hình cập nhật thông tin, các trường được phép cập nhật phải có màu khác để phân biệt.

3.1.4.2.3.3.Các yêu cầu cần đáp ứng về thời gian xử lý, độ phức tạp xử lý của các chức năng phần mềm

- Hệ thống đảm bảo có thể vận hành ổn định trên hạ tầng mạng của Trung tâm.
- Thời gian đáp ứng trung bình đối với các chức năng nghiệp vụ, trong điều kiện bình thường đạt dưới 05 giây.
- Thời gian đáp ứng trung bình đối với các chức năng nghiệp vụ, khi có người sử dụng chạy chức năng báo cáo tổng hợp dữ liệu toàn quốc đạt mức dưới 30 giây.
- Thời gian chạy các báo cáo tổng hợp trên phạm vi toàn Trung tâm với tham số cả năm (không bao gồm thời gian tổng hợp dữ liệu) phải không quá nửa (1/2) giờ đồng hồ và không có lỗi timeout.
- Hệ thống phải đảm bảo khả năng xử lý cho khoảng 800 người sử dụng hệ thống đồng thời.

3.1.4.2.3.4.Các yêu cầu về ràng buộc xử lý lôgic đối với việc nhập dữ liệu thông qua sử dụng các ô nhập liệu do giao diện chương trình cung cấp

- Trong quá trình thiết kế, xây dựng phần mềm phải có các quy tắc quy định việc đưa các thông tin dữ liệu đầu vào và các thủ tục kiểm tra dữ liệu đầu ra như:
  + Kiểm tra giá trị nằm trong khoảng cho phép
  + Dữ liệu nhập đúng định dạng.
  + Kiểm tra tính toàn vẹn và hợp lệ của các trường dữ liệu, chỉ mục và các trường khóa.
  + Kiểm tra tính hợp lý, logic, chính xác của dữ liệu đầu ra.
  + Phải có thủ tục để thông báo và thoát khỏi lỗi nhập liệu.
- Trong quá trình phát triển, nâng cấp phần mềm phải có biện pháp kiểm soát, phòng tránh việc các đoạn mã lệnh trong chương trình được kích hoạt trái phép và thực hiện những thao tác không mong muốn trong hệ thống.

3.1.4.2.3.5.Các yêu cầu về cài đặt, hạ tầng, đường truyền, an toàn vận hành, khai thác, sử dụng

- Bộ cài đặt và mã nguồn hệ thống phải được đóng gói và mã hóa để có thể chuyển giao qua các thiết bị lưu trữ tháo rời.
- Hệ thống phải đảm bảo khả năng vận hành hạ tầng mạng của Trung tâm
- Công cụ xây dựng và kết xuất báo cáo có khả năng kết xuất báo cáo theo nhiều định dạng file như: Excel, pdf, word.
- Hệ thống phải hỗ trợ nhiều hệ điều hành của các máy trạm: Window 7, 8 ,10 hoặc cao hơn.
- Hệ thống phải được cài đặt và ổn định tại Trung tâm trên cơ sở đảm bảo phù hợp, tương thích với hạ tầng kỹ thuật CNTT được kế thừa hoặc đầu tư trong dự án để đảm bảo hệ thống luôn hoạt động ở trạng thái tốt nhất, việc xử lý các nghiệp vụ của Trung tâm luôn được thống nhất và thông suốt.

- Quy trình triển khai, vận hành, bảo trì, bảo dưỡng và khai thác, sử dụng hệ thống phải đảm bảo phù hợp với quy định của Trung tâm.
- Với Các lỗi do phần mềm/hệ thống gây ra, phải thông báo cho người dùng biết; đối với lỗi nghiệp vụ thì có thông báo nếu vi phạm nguyên tắc nghiệp vụ; và có cơ chế cảnh báo các lỗi gửi đến cho người quản trị.
- Hệ thống phải đảm bảo khi triển khai sẽ không làm ảnh hưởng tới hoạt động, sự mất mát thông tin của các hệ thống ứng dụng nghiệp vụ đóng vai trò là nguồn dữ liệu khác khi triển khai hệ thống.
- Hệ thống phải được thiết kế đảm bảo hoạt động ổn định 24 giờ/7 ngày làm việc.
- Hệ thống cần cung cấp chức năng sao lưu và phục hồi để đảm bảo trong trường hợp có sự cố do bất kỳ nguyên nhân nào, sau khi hệ thống trở lại hoạt động ổn định với lượng dữ liệu bị mất mát tối đa bằng lượng dữ liệu không quá 01 ngày làm việc kể từ trước khi thời điểm xảy ra sự cố.

3.1.4.2.3.6. Yêu cầu về mức độ chịu đựng sai hỏng đối với các lỗi cú pháp lập trình, lỗi logic trong xử lý dữ liệu, lỗi kiểm soát tính đúng đắn của dữ liệu đầu vào

- Các dữ liệu trước khi nhập vào hệ thống cần phải được kiểm tra tính đúng đắn về cấu trúc, định dạng và logic và phải thông báo ngay cho người sử dụng khi có lỗi xảy ra.
- Đảm bảo lỗi ở một phiên làm việc của người dùng (tác nhân) này không làm ảnh hưởng đến phiên làm việc của người dùng khác của hệ thống.
- Có quy trình hoặc phương pháp giúp giảm thiểu các lỗi cú pháp lập trình, lỗi logic xử lý dữ liệu.
- Hệ thống cần cung cấp chức năng làm sạch, loại bỏ các dữ liệu không nhất quán trong quá trình xử lý dữ liệu.
- Hệ thống cần có các chức năng thông báo lỗi hệ thống một cách hợp lý giúp người quản trị và người sử dụng xác định được các vấn đề trong quá trình vận hành.
- Hệ thống phải đảm bảo: Khi có lỗi ở một phiên làm việc của người dùng (tác nhân) này không làm ảnh hưởng đến phiên làm việc của người dùng khác (tác nhân khác) của hệ thống.

3.1.4.2.3.7. Phân tích và mô tả chức năng của phần mềm

3.1.4.2.3.7.1. Phân tích lựa chọn giải pháp kỹ thuật, công nghệ

Bảng tổng hợp các yêu cầu về giải pháp kỹ thuật, công nghệ cần đáp ứng

Tiêu chí kỹ thuật	**Kỹ thuật xây dựng**
Cơ sở dữ liệu	Oracle 11 trở lên hoặc tương đương
Hệ điều hành máy chủ hệ thống	Windows Server 2012 R2 trở lên
Ngôn ngữ lập trình	Backend: C# (.NET Core), sử dụng để xây dựng các API, xử lý nghiệp vụ (Services), và kết nối cơ sở dữ liệu.

	Frontend: Angular dùng để xây dựng giao diện người dùng và giao tiếp với API backend.
Môi trường thực thi	Phần mềm vận hành trên nền Web application và nền tảng App mobile.
Ngôn ngữ	Tiếng Việt, theo tiêu chuẩn Unicode TCVN 6909:2001
Hệ điều hành máy trạm	Hệ điều hành Windows 10 trở lên

3.1.4.2.3.7.2. Chức năng của phần mềm

Stt	Tính năng	Mô tả tính năng
A – DANH MỤC NÂNG CẤP PHẦN MỀM		
I – Nâng cấp (HIS)		
1	Quản lý suất ăn cho bệnh nhân	- Quản lý đăng ký suất ăn cho người bệnh, tổng hợp suất ăn theo ngày, theo khoa; - Quản lý chế độ ăn, dinh dưỡng thông qua y lệnh của bác sĩ cho từng người bệnh; - Báo cáo, thống kê suất ăn theo ngày, theo khoa.
2	Quản lý phác đồ điều trị	- Quản lý và cập nhật danh mục phác đồ do Bộ Y tế ban hành; - Quản lý danh mục và danh sách phác đồ điều trị đã được thông qua tại Trung tâm; - Quản lý danh mục nhân viên y tế tham gia xây dựng phác đồ; - Quản lý xây dựng và cập nhật phác đồ; - Quản lý kết nối đến với danh mục thuốc, danh mục kỹ thuật, danh mục vật tư tiêu hao phục vụ phác đồ; - Quản lý các báo cáo, thống kê theo quy định; Khuyến khích các ứng dụng thông minh hỗ trợ quản lý phác đồ.
3	Ký số bệnh nhân	
3.1	Tạo chứng thư số bệnh nhân	
3.1.1	Xác thực sinh trắc học bằng khuôn mặt, vân tay	Lấy vân tay, khuôn mặt bệnh nhân tại tiếp đón để xác thực, sử dụng các thuật toán sinh trắc học để hiển thị tỉ lệ trùng khớp
3.1.2	Xác thực NFC căn cước công dân	Dùng thiết bị hỗ trợ đọc NFC để đọc thông tin trong căn cước công dân gắn chip

3.1.3	Thực hiện Ekyc khuôn mặt	Thực hiện nhận diện khuôn mặt bằng eKyc, xác thực C06 bộ công an
3.1.4	Tạo chứng thư số bệnh nhân	Tạo chứng thư số thông qua các nhà cung cấp chữ ký số bệnh nhân, VNEID
3.2	Ký số bệnh nhân	- Ký số bằng chứng thư số của bệnh nhân
4	Gửi hồ sơ bệnh án điện tử	
4.1	Liên kết tài khoản với bệnh án điện tử	- Liên kết tài khoản của bác sĩ với tài khoản được cấp tại phần mềm Quản lý bệnh án điện tử (EMR)
4.2	Tạo bệnh án điện tử	- Gửi thông tin tạo bệnh án điện tử
4.2	Gửi giấy tờ lên bệnh án điện tử	- Chiết file định dạng PDF các biểu mẫu có trong bệnh án - Chiết file định dạng XML hồ sơ bệnh án điện tử - Upload các giấy tờ scan, file ảnh chụp giấy tờ lên bệnh án điện tử - Mã hóa dữ liệu trao đổi - Gửi hồ sơ bệnh án điện tử đi ký số và lưu trữ
4.3	Cảnh báo thay đổi nội dung giấy tờ	- Cảnh báo trên HIS khi có sự thay đổi nội dung so với giấy tờ đã gửi
4.4	Kiểm tra giấy tờ	- Kiểm tra và cảnh báo các giấy tờ chưa gửi - Kiểm tra và cảnh báo thiếu chữ ký đối với giấy tờ đã gửi
4.5	Xem hồ sơ bệnh án	- Tích hợp xem hồ sơ bệnh án tại HIS
4.6	Xem danh sách giấy tờ cần ký số	- Xem danh sách giấy tờ cần ký của mỗi bác sĩ, giám đốc, đóng dấu Trung tâm
4.7	Kết thúc hồ sơ bệnh án	- Nhập thông tin kết thúc hồ sơ bệnh án, khóa sửa thông tin bệnh án
4.8	Nộp hồ sơ bệnh án	- Chuyển thông tin bệnh án lên giám đốc ký, khóa gửi hồ sơ bệnh án
4.9	Mượn, thay thế, bổ sung bệnh án	- Phiếu mượn, thay thế, bổ sung hồ sơ bệnh án
5	Quản lý dinh dưỡng	- Quản lý khám và đánh giá dinh dưỡng cho người bệnh ngoại trú; - Quản lý chế độ ăn bệnh lý đối với người bệnh điều trị bằng chế độ ăn;

		- Quản lý đánh giá và nhận xét dinh dưỡng của người bệnh thông qua bệnh án; - Quản lý chỉ định chế độ ăn hàng ngày thông qua mã bệnh nhân; - Quản lý kế hoạch can thiệp dinh dưỡng với người bệnh cần hỗ trợ dinh dưỡng; - Quản lý thực đơn và chế độ ăn.
6	Xem hình ảnh Pacs tại phòng khám	- Xem hình ảnh Xquang, Siêu âm, Điện tim, Nội soi tại phòng khám.
II – Nâng cấp xét nghiệm (LIS)		
1	Quản lý mẫu xét nghiệm	- Quản lý thông tin mẫu xét nghiệm: mã định danh mẫu xét nghiệm theo bệnh nhân, loại mẫu (máu, dịch, nước tiểu,…), ngày giờ thực hiện lấy mẫu, tình trạng của mẫu, trạng thái của mẫu, người lấy mẫu, nơi lấy mẫu bệnh. - Quản lý lưu và hủy mẫu: nơi lưu mẫu, vị trí lưu nơi, trạng thái và người hủy.
2	Quản lý hóa chất xét nghiệm	
2.1	Quản lý định mức hóa chất	- Quản lý định mức hóa chất sử dụng cho các lần trả kết quả xét nghiệm cho bệnh nhân, lượng hóa chất dùng để vệ sinh máy xét nghiệm.
2.2	Báo cáo sử dụng hóa chất theo thời gian, máy xét nghiệm	- Báo cáo sử dụng số lượng hóa chất sử dụng theo thời gian, theo máy xét nghiệm.
3	Gửi phiếu kết quả và ký số	- Gửi phiếu kết quả xét nghiệm lên bệnh án điện tử và ký số phiếu kết quả
4	Xem kết quả xét nghiệm qua WebView	- Cho phép bệnh nhân xem kết quả xét nghiệm bằng đường link trên phiếu kết quả hoặc tra cứu trên webview.
III – Nâng cấp CDHA (RIS-PACS)		
1	Cấu hình quản lý máy chủ PACS	- Cấu hình máy chủ PACS để nhận ảnh, đường dẫn hình ảnh phục vụ cho việc lưu và chuẩn bị cho máy trạm xem ảnh.
2	Cấu hình quản lý máy trạm PACS	- Cấu hình máy trạm có thể xem ảnh sau khi lưu máy chủ.

3	Hỗ trợ xem ảnh DICOM qua WebView	- Cho phép người bệnh xem lại kết quả Chẩn đoán hình ảnh và cho phép các bác sĩ chuyên môn xem ảnh gốc, các chức năng hỗ trợ xem ảnh trực tiếp.
4	Chức năng biên tập và xử lý hình ảnh DICOM	- Xử lý ảnh cho y, bác sĩ xem trên phần mềm và chuẩn bị cho việc WebView cho người bệnh xem trên môi trường số.
5	Chức năng nén ảnh theo giải thuật JPEG2000	- Xử lý ảnh nhằm việc giảm dung lượng ảnh để đính kèm vào mẫu in kết quả cho bệnh nhân và không gian lưu trữ của đơn vị.
6	Gửi hồ sơ phiếu kết quả, ký số	- Gửi phiếu kết quả chẩn đoán hình ảnh lên bệnh án điện tử và ký số phiếu kết quả
IV – Nâng cấp Viện Phí		
1	Gửi giây tờ bệnh án điện tử và ký số	
1.1	Gửi giấy tờ lên bệnh án điện tử	- Gửi bảng kê lên bệnh án điện tử - Gửi các giấy tờ khác của bệnh án điện tử
1.2	Ký số	- Kế toán viện phí ký số vào bảng kê, giấy tờ
1.3	Ký số bệnh nhân	- Ký số bệnh nhân vào bảng kê và các giấy tờ khác
B – PHẦN MỀM BỆNH ÁN ĐIỆN TỬ		
1	**Quản lý tạo bệnh án điện tử**	
1.1	Tạo bệnh án điện tử từ HIS	Đồng bộ tự động từ hệ thống HIS:
		Thông tin định danh bệnh nhân: mã BN, họ tên, ngày sinh, giới tính ….
		Thông tin BHYT
		Thông tin đăng ký khám
		Thông tin chuyển tuyến
1.2	Cấp mã định danh cho bệnh án điện tử	Hệ thống cho phép:
		Cấp mã định danh cho bệnh án điện tử để phục vụ tìm kiếm
		Cấp mã định danh cho bệnh án điện tử theo mã của phần mềm HIS
1.3	Cấp số Bệnh án điện tử	Hệ thống cho phép:
		Cấp số bệnh án cho đối tượng BHYT, Viện phí
		Cấp số bệnh án theo diện điều trị: Ngoại trú, Nội trú
		Cấp số bệnh án theo khoa: Mã khoa/số tăng dần
		Cấp số bệnh án theo năm: Số bệnh án tự động tăng dần theo năm và tự động reset về 01 khi qua năm mới (ví dụ

		đến 01/01/2024 thì bệnh nhân đầu tiên cấp bệnh án sẽ có mã 2024/00001)
1.4	Cập nhật thông tin bệnh nhân từ HIS	Cho phép cập nhật lại thông tin của bệnh nhân khi HIS sửa thông tin. Các thông tin cập nhật:
		Thông tin hành chính, thông tin điều trị, thông tin BHYT
1.5	Quản lý file ký	Folder quản lý file ký lưu trữ theo mã bệnh nhân, mã điều trị, họ tên bệnh nhân và năm sinh
2	**Quản lý vỏ bệnh án**	
2.1	Phân loại vỏ bệnh án	Cho phép phân loại vỏ bệnh án nội trú, ngoại trú, chuyên khoa: Mắt, TMH, RHM, Da Liễu…
2.2	Sắp xết thứ tự hiển thị vỏ bệnh án	Sắp xếp số ưu tiên cao hơn thì hiển thị lên trên để dễ dàng lựa chọn
		Thay vì sắp xếp vỏ bệnh án theo tên có thể ưu tiên vỏ bệnh án sử dụng nhiều lên trên. Ví dụ: Bệnh án nội khoa sử dụng nhiều nhất
		Hoặc cùng là bệnh án mắt có 7 loại (có thể ưu tiên loại vỏ bệnh án nào lên trên trong danh sách)
2.3	Tự động chọn vỏ bệnh án theo khoa điều trị	Cho phép cấu hình khoa điều trị để khi bệnh nhân nhập khoa sẽ map tự động với bệnh án tương ứng của His
2.4	Danh sách vỏ bệnh án đã tạo của bệnh nhân	Hiển thị danh sách vỏ bệnh án đã tạo của bệnh nhân
2.5	Xem vỏ bệnh án đã tạo của bệnh nhân	Hiển thị chi tiết vỏ bệnh án đã tạo của bệnh nhân
2.6	Tạo vỏ bệnh án mới	Phục vụ cho việc scan lại bệnh án cũ để số hóa kho bệnh án đã lưu trữ trước khi làm bệnh án điện tử
2.7	Nhận dữ liệu từ His	Cho phép nhận thông tin của bệnh nhân vào vỏ bệnh án điện tử hệ thống HIS như:
		Thông tin chung:
		+ Thông tin hành chính: Nơi chuyển đến
		+ Thông tin chẩn đoán: nơi chuyển đến, khoa khám bệnh, khoa điều trị, trước phẫu thuật, sau phẫu thuật
		+ Bệnh chính, bệnh kèm theo
		+ Tình trạng ra viện: kết quả điều trị, tình hình tử vong, lý do tử vong, chẩn đoán giải phẫu tử thi
		- Thông tin hỏi bệnh

2.8	Kết xuất vỏ bệnh án	Cho phép kết xuất vỏ bệnh án ra file PDF
2.9	Ký số vào vỏ bệnh án	Ký số vào vỏ bệnh án để đảm bảo pháp lý như ký giấy
2.10	Danh sách vỏ bệnh án	Bệnh án Nội khoa
		Bệnh án Nhi khoa
		Bệnh án Truyền nhiễm
		Bệnh án Phụ khoa
		Bệnh án Sản khoa
		Bệnh án Sơ sinh
		Bệnh án Tâm thần
		Bệnh án Da liễu
		Bệnh án Huyết học-Truyền máu
		Bệnh án Ngoại khoa
		Bệnh án Bỏng
		Bệnh án Ung bướu
		Bệnh án Răng Hàm Mặt
		Bệnh án Tai Mũi Họng
		Bệnh án Ngoại trú chung
		Bệnh án Ngoại trú Răng Hàm Mặt
		Bệnh án Nội trú Y học cổ truyền
		Bệnh án Ngoại trú Y học cổ truyền
		Bệnh án Nội trú Nhi Y học cổ truyền
		Bệnh án Mắt
		Bệnh án Mắt (chấn thương)
		Bệnh án Mắt (Bán phần trước)
		Bệnh án Mắt (Đáy mắt)
		Bệnh án Mắt (Glocom)
		Bệnh án Mắt (Lác)
		Bệnh án Mắt trẻ em
		Bệnh án phục hồi chức năng
		Bệnh án phục hồi chức năng nhi
		Bệnh án ngoại trú phục hồi chức năng
		Bệnh án tăng huyết áp
		Bệnh án đái tháo đường
		Bệnh án ARV
		Bệnh án Nội tiết
		Bệnh án Lao phổi

2.11	Tra cứu vỏ bệnh án	Tìm kiếm vỏ bệnh án theo các tiêu tùy chọn
3	**Quản lý biểu mẫu, phiếu, tờ**	
3.1	Phân loại biểu mẫu, phiếu, tờ	Cho phép phân loại biểu mẫu, phiếu, tờ trong bệnh án theo danh mục (tờ điều trị, chăm sóc, truyền dịch, công khai…)
3.2	Sắp xết thứ tự hiển thị biểu mẫu, phiếu, tờ	Sắp xết thứ tự hiển thị biểu mẫu, phiếu, tờ
3.3	Danh sách biểu mẫu, phiếu, tờ đã tạo của bệnh nhân	Quản lý danh sách biểu mẫu, phiếu, tờ đã tạo của bệnh nhân
3.4	Tìm kiếm, sắp xếp biểu mẫu, phiếu, tờ trong danh sách	Hiển thị danh sách biểu mẫu, phiếu, tờ đã tạo của bệnh nhân theo điều kiện tìm kiếm:
		Tìm kiếm theo tên
		Tìm kiếm theo loại phiếu
		Tìm kiếm theo ngày tạo
		Tìm kiếm theo trạng thái phiếu: hoàn thành, chưa hoàn thành
3.5	Xem biểu mẫu, phiếu, tờ đã tạo của bệnh nhân	Hiển thị chi tiết phiếu, biểu mẫu, tờ đã tạo của bệnh nhân
3.6	Tạo biểu mẫu, phiếu, tờ mới	Tạo biểu mẫu, phiếu, tờ mới
		Phục vụ cho việc scan lại bệnh án cũ để số hóa kho bệnh án đã lưu trữ trước khi làm bệnh án điện tử
3.7	Nhận dữ liệu biểu mẫu, phiếu, tờ từ HIS	Nhận dữ liệu biểu mẫu, phiếu, tờ từ HIS
		Thông tin nhận dữ liệu các biểu mẫu, phiếu, tờ trong bệnh án như:
		Thông tin chẩn đoán
		Thông tin diễn biến
		Thông tin chăm sóc
		Thông tin truyền dịch
		Thông tin phản ứng thuốc
		Thông tin phẫu thuật thủ thuật
		…
3.8	Kết xuất biểu mẫu, phiếu, tờ	Kết xuất biểu mẫu, phiếu, tờ ra PDF

3.9	Ký số vào từng biểu mẫu, phiếu, tờ ký gộp nhiều ngày	Ký số vào biểu mẫu, phiếu, tờ để đảm bảo pháp lý như ký giấy
		Xây dựng quy trình ký.
4	**Quản lý kết quả cận lâm sàng**	
4.1	Ký số cận lâm sàng	- Ký số kết quả xn sinh hóa
		- Ký số kết quả xn huyết học
		- Ký số kết quả xn nước tiểu
		- Ký số kết quả xn chung
		- Ký số kết quả nội soi
		- Ký số kết quả x-quang
		- Ký số kết quả siêu âm
		- Ký số kết quả điện tim
		- Ký số kết quả CT scan
		- Ký số kết quả điện não
		- Ký số kết quả lưu huyết não
		- Ký số kết quả điện cơ
		- Ký số kết quả DSA
		- Ký số kết quả giải phẫu bệnh
		- Ký số kết quả đo độ loãng xương
		- Ký số kết quả thang đánh giá tâm lý
		- Module xem kết quả CĐHA file dạng: dicom, jpg, png, jpge.
4.2	Đính kèm ảnh, đường dẫn link xem ảnh từ các hệ thống PACS	Đính kèm ảnh, đường dẫn link xem ảnh từ các hệ thống PACS
5	**Quản lý ký số**	
5.1	Tích hợp chữ ký số HSM	Tích hợp với chữ ký HSM để ký trên tất cả văn bản
5.2	Thêm ảnh ký tươi vào chữ ký số	Cho phép chèn thêm ảnh chữ ký tay để làm sinh động thêm văn bản
5.3	Tạo văn bản cần ký	Người dùng khi muốn ký 1 văn bản nào đó trong bệnh án điện tử thì có thể tạo văn bản, văn bản được tạo sẽ tự động lưu vào EMR
5.4	Thiết lập người ký	Cho phép người tạo có thể thêm người vào văn bản được ký. Người được thêm có thể là nhân viên y tế hoặc bệnh nhân

5.5	Thiết lập luồng ký	Với những văn bản nhiều người ký, tùy vào hình thức có thể thiết lập ký nối tiếp (từng người ký lần lượt) hoặc ký song song (nhiều người cùng ký một lúc) hoặc vừa nối tiếp vừa song song (lãnh đạo ký cuối cùng còn lại có thể ký cùng một lúc)
5.6	Thực hiện ký số	- Cho phép người dùng ký số vào văn bản: vỏ bệnh án, các phiếu, biểu mẫu, phiếu chỉ định, phiếu kết quả cận lâm sàng - Ký số con dấu Trung tâm trên file tổng hợp giấy tờ trong hồ sơ bệnh án của bệnh nhân
5.7	Lựa chọn vị trí ký	Tùy chọn vị trí trên văn bản để ký: - Ký theo từ khóa - Ký theo vị trí - Ký nháy - Đóng dấu Trung tâm - Chọn vị trí ký trên tài liệu
5.8	Kiểm tra chữ ký số hợp lệ	- Kiểm tra các chữ ký số có trong văn bản, hiển thị trạng thái hợp lệ của chữ ký số
5.9	Ký điện tử	- Cho phép ký điện tử các giấy tờ của bệnh án
6	Lưu trữ file ký số	
6.1	Mã hóa file lưu trữ	- File văn bản sẽ được mã hóa TripleDes trước khi lưu trữ.
6.2	Lưu trữ file ký số	- Lưu trữ 1 bản tại ổ cứng của máy chủ Trung tâm - Lưu trữ 1 bản tại Nat, SAN thông qua giao thức FTP - Lưu trữ 1 bản tại Cloud S3
6.3	Đồng bộ bệnh án	- Tự động đồng bộ bệnh án lên cloud trong trường hợp mất internet.
6.4	Báo cáo lưu trữ	- Báo cáo số lượng file hồ sơ, dung lượng còn trống, cảnh báo khi sắp hết dung lượng
7	Quản lý danh mục	Có phần quản lý danh mục cho phép thêm, sửa, không dùng
7.1	Danh mục bệnh án	Quản lý danh sách bệnh án sử dụng trong Trung tâm
7.2	Danh mục giấy tờ trong bệnh án	Quản lý Danh sách loại giấy tờ của bệnh án
7.3	Danh mục nhân viên	Quản lý danh sách nhân viên
7.4	Danh mục khoa phòng	Quản lý danh sách khoa phòng trong Trung tâm

7.5	Các danh mục khác	Quản lý các danh mục khác liên quan trong quá trình triển khai bệnh án
8	Quản lý mượn, bổ sung, thay thế	
8.1	Quản lý mượn trả	- Cho phép tạo phiếu mượn trả, duyệt mượn in ấn, phục vụ chuyên môn của các cơ quan chức năng.
8.2	Quản lý bổ sung, thay thế	- Thay thế bổ sung các giấy tờ trong bệnh án khi chưa chốt lưu trữ, khi thay đổi phải lập phiếu được duyệt và lưu lịch sử thay đổi
9	Lưu lịch sử thao tác người dùng	- Lưu trữ, tra cứu lịch sử thao tác người dùng
10	Phân quyền người dùng	- Thực hiện phân quyền truy cập, thao tác theo từng người dùng
11	Báo cáo	
11.1	Báo cáo hồ sơ theo khoa phòng	- Tổng hợp báo cáo bệnh án theo khoa phòng
11.2	Thống kê hồ sơ theo nhóm bệnh, độ tuổi, Phái	- Tổng hợp báo cáo bệnh án tách theo nhóm bệnh, độ tuổi, phái
11.3	Chiết xuất dữ liệu hồ sơ bệnh án dạng XML, HL7, LIS, RIS/PACS	- Chiết xuất dữ liệu phục vụ trao đổi dữ liệu với các phần mềm khác
12	Ứng dụng di động	
12.1	Quản lý hồ sơ bệnh án	- Tra cứu, xem hồ sơ bệnh án - Chụp, tải file nội dung bệnh án - Nhập thông tin hồ sơ bệnh án - Kết thúc hồ sơ bệnh án
12.2	Ký số	- Cho phép người dùng ký số
12.3	Ký số bệnh nhân	- Tạo chứng thư số bệnh nhân - Ký số bệnh nhân
C – Danh mục nâng cấp khác		
1	Cài đặt tưởng lửa	- Chặn các truy cập không được phép - Chống tấn công mạng
2	Mã hóa dữ liệu lưu trữ	- Mã hóa các dữ liệu khi lưu trữ nhằm mục đích dù bị lộ vẫn không thể sử dụng được thông tin. Phải cần khóa của đơn vị phần mềm giải mã để xem tài liệu.
3	Cài đặt chống sao chép dữ liệu trên máy chủ	- Chống việc sao chép dữ liệu từ máy chủ ra thiết bị ngoại vi để tránh việc lộ thông tin.

4	Sao lưu dữ liệu	- Sao lưu định kỳ kết hợp sao lưu dữ liệu thời gian thực - Máy chủ dự phòng cho phép thay thế máy chủ chính khi xảy ra sự cố đảm bảo hoạt động thông suốt
Stt	Tính năng	Mô tả tính năng

3.1.4.2.8. Các yêu cầu phi chức năng khác

- Cần có giải pháp kiểm tra sự tương thích giữa phiên bản ứng dụng và CSDL.
- Người sử dụng hệ thống không phải thực hiện bất kỳ 01 thao tác đăng ký bản quyền nào khi sử dụng.

3.1.4.2.9.Yêu cầu về kiểm thử

- Trước khi triển khai vận hành chính thức hệ thống, đơn vị phát triển phần mềm phải phối hợp với Chủ trì thuê để lập kế hoạch và thực hiện kiểm thử chất lượng, vận hành thử nghiệm hệ thống, đảm bảo hệ thống sau khi xây dựng sẽ hoạt động an toàn, ổn định và hiệu quả theo đúng nhu cầu người dùng.

3.1.4.2.10.Yêu cầu về giao diện, trải nghiệm người dùng

Stt	Yêu cầu
1	Giao diện thân thiện với người dùng, thiết kế đồ họa khoa học, có tính mỹ thuật cao. Hệ thống có khả năng hiển thị, hoạt động chính xác, đầy đủ trên hầu hết các trình duyệt phổ biến với phiên bản mới nhất như: Firefox, Chrome, Internet Explorer. Hệ thống của Nhà cung cấp dịch vụ phải cho phép hỗ trợ ứng dụng khai thác hệ thống thông tin báo cáo trên nền tảng thiết bị di động như điện thoại di động thông minh, máy tỉnh bảng (App mobile).
2	Người sử dụng có thể tuỳ chỉnh giao diện phù hợp với nhu cầu sử dụng ở mức cao. Có khả năng tùy biến hiển thị trên các màn hình máy tính, máy tính bảng, điện thoại di động thông minh, kios thông tin… với độ phân giải khác nhau mà không làm thay đổi về giao diện, hiển thị và các tính năng khác của hệ thống. Tuy nhiên, giao diện ứng dụng phải thân thiện với người sử dụng và dễ dùng. Hỗ trợ tối đa sử dụng các chức năng bằng bàn phím máy tính. Các màn hình nhập và cập nhật dữ liệu về cơ bản phải thống nhất về các thao tác trên bàn phím cũng như về màu sắc, fonts chữ. Các màn hình tra cứu điều kiện lọc báo cáo cũng phải thống nhất với nhau. Các biểu tượng và phím nóng phải được thống nhất trong toàn bộ chương trình.
3	Các giao diện thiết kế một cách đơn giản nhưng hiệu quả cao về thao tác, giảm thiểu việc mở quá nhiều tab, hiển thị và xử lý hình ảnh nhanh, màu sắc không gây cảm giác nhàm chán cho người sử dụng và theo một chuẩn giao diện thống nhất.
4	Hệ thống sẽ cho phép lưu trữ tất cả dữ liệu theo định dạng Unicode, chấp nhận tất cả các ký tự tiếng Việt có dấu.

	Giao diện màn hình, các thông báo lỗi và trợ giúp là ngôn ngữ tiếng Việt theo chuẩn TCVN6909:2001 dựa trên bảng mã Unicode dựng sẵn (ISO 10646), với trợ giúp của các bộ gõ Unikey, Vietkey. Giao diện chương trình dùng các Font chuẩn của hệ thống như Arial hay Times New Roman. Người dùng không phải cài thêm bất cứ font chữ nào.
5	Các chức năng phần mềm được xây dựng với một cơ chế thông báo lỗi thân thiện và rõ ràng. Thông báo lỗi phải được Việt hóa tối đa, giúp cho người sử dụng biết được lý do gây ra lỗi để tránh lặp lại các trường hợp tương tự. Hệ thống báo lỗi xác định rõ ràng đâu là lỗi do người sử dụng gây ra và đâu là lỗi do hệ thống phần mềm gây ra và chỉ ra hướng khắc phục.
6	Với các lỗi do phần mềm/hệ thống gây ra, phải thông báo cho người dùng biết nguyên nhân và phương pháp xử lý. Có các biện pháp tự động phục hồi trong các trường hợp xác định. Tất cả các lỗi loại này phải được ghi lại thành log phục vụ cho mục đích bảo trì phần mềm, hệ thống.
7	Cung cấp cơ chế cá nhân hóa cho nhiều đối tượng sử dụng khác nhau: lãnh đạo, cán bộ nghiệp vụ, cán bộ chuyên trách, người sử dụng dịch vụ…

3.1.4.2.11.Yêu cầu về khả năng xử lý dữ liệu

Stt	Yêu cầu
1	Hệ thống sẽ cung cấp công suất xử lý và dung lượng lưu trữ để hỗ trợ các khối lượng dự kiến, có thể tăng theo thời gian.
2	Hệ thống sẽ đáp ứng tối thiểu thời gian phản hồi như sau: -Từ 1 đến 6 giây đối với các giao dịch không đòi hỏi truy vấn CSDL. -Từ 1 đến 8 giây đối với các giao dịch đòi hỏi ghi vào CSDL hoặc truy vấn CSDL với một liên kết. -Từ 1 đến 10 giây đối với các giao dịch đòi hỏi truy vấn CSDL đến 5 liên kết.
3	Có giải pháp đảm bảo được việc nhập dữ liệu đầu vào ngay cả khi đường truyền hoạt động không ổn định.
4	Có giải pháp xử lý được dữ liệu quản lý tập trung với Trung tâm và các Trung tâm dã chiến do 30-4 quản lý, các Trung tâm vệ tinh về đội ngũ y bác sỹ, cấp phát dược, dịch vụ liên kết… Đồng thời phải bóc tách độc lập các dịch vụ, báo cáo của Trung tâm, các Trung tâm dã chiến do Trung tâm quản lý, các Trung tâm vệ tinh có liên kết với Trung tâm

3.1.4.2.12.Yêu cầu về ràng buộc logic nhập liệu

Stt	Yêu cầu
1	Tất cả các ngày tháng sẽ được lưu với 4 chữ số cho phần Năm, và có thể được hiển thị theo tất cả các định dạng ngày chung như trong MSOffice.
2	Hệ thống sẽ hỗ trợ kiểm tra tức thời tính hợp lệ của các giá trị nhập vào qua phương thức nhập trực tiếp hoặc qua tệp dữ liệu.

3	Hệ thống sẽ cung cấp chức năng kiểm tra tính nhất quán và toàn vẹn của các trường dữ liệu có quan hệ ràng buộc với nhau trong cơ sở dữ liệu thông qua các quy tắc đã được định nghĩa như ràng buộc khóa khi xây dựng CSDL.

3.1.4.2.13.Yêu cầu về hiệu năng

Hạ tầng phần cứng của hệ thống phải đáp ứng yêu cầu về các chức năng, số lượng người dùng tham gia khai thác, sử dụng hệ thống; khả năng tích hợp dữ liệu với các bộ, ngành, địa phương như đã nêu trên và các yêu cầu sau đây:

Stt	Yêu cầu
1	Về thời gian: Thời gian cho phép để hệ thống phản hồi lại thông tin đã tiếp nhận yêu cầu xử lý từ phía người sử dụng là 3 giây (s); thời gian cho phép để hiện thị đầy đủ KPI là 10 (s); thời gian cho phép để gửi kết quả tìm kiếm thông tin là 10 (s).
2	Về tài nguyên sử dụng: Tài nguyên lưu trữ chiếm dụng của hệ thống trong trạng thái hoạt động bình thường không được phép lớn hơn 80% tài nguyên lưu trữ được phép sử dụng hoặc 20% tài nguyên lưu trữ dùng chung tại mọi thời điểm; tài nguyên vi xử lý mà các phần mềm ứng dụng thuộc hệ thống chiếm dụng của các máy chủ không được phép lớn hơn 40% tài nguyên vi xử lý dùng chung tại mọi thời điểm; bộ nhớ truy cập ngẫu nhiên mà các phần mềm ứng dụng thuộc hệ thống chiếm dụng của các máy chủ không được phép lớn hơn 50% bộ nhớ truy cập ngẫu nhiên của máy chủ.
3	Hiệu năng không bị ảnh hưởng từ các yếu tố như: Thời gian, sự tăng trưởng về dữ liệu chính; bảo đảm có khả năng hoạt động không bị ảnh hưởng về dữ liệu trong suất quá trình thuê sử dụng dịch vụ (trong điều kiện sẵn sàng về hạ tầng lưu trữ).

3.1.4.2.14.Yêu cầu về tính sẵn sàng

Stt	Yêu cầu
1	Hệ thống phần mềm bệnh án điện tử phải đảm bảo hoạt động liên tục 24/7; được thiết kế hỗ trợ khả năng sao lưu dữ liệu thời gian thực, hỗ trợ khả năng tự động chuyển đổi khi xảy ra lỗi, không ảnh hưởng tới việc trao đổi thông tin, dữ liệu báo cáo.
2	Không hình thành một điểm lỗi tập trung hoặc điểm nghẽn hiệu năng tập trung. Tính sẵn sàng của hệ thống phải đạt mức 99,5% theo năm, trong đó không kể thời gian bảo trì theo kế hoạch định trước; thời gian không sẵn sàng của hệ thống phải nhỏ hơn 1 giờ/1 tháng không tính thời gian bảo trì hệ thống.
3	Hệ thống đảm bảo hoạt động bình thường trong trường hợp một trong các máy chủ vật lý/máy chủ ứng dụng bị lỗi.

4	Khả năng phục hồi: Trong mọi trường hợp xảy ra sự cố (dữ liệu, máy chủ vật lý, máy chủ ứng dụng), thời gian cho phép để hệ thống phục hồi trạng thái hoạt động bình thường là 3 giờ.
5	Thời gian giữa các lần xảy ra sự cố gián đoạn hoạt động của hệ thống: Thời gian cho phép giữa hai lần liên tiếp xảy ra sự cố là 01 năm.

3.1.4.2..Yêu cầu về toàn vẹn dữ liệu

Stt	Yêu cầu
1	Đảm bảo tính toàn vẹn và tính xác thực của thông điệp dữ liệu báo cáo điện tử và cung cấp thông tin cho phép theo dõi sự trạng thái của thông điệp dữ liệu báo cáo điện tử.

3.1.4.2.16.Yêu cầu về vận hành, hỗ trợ

Stt	Yêu cầu
1	Trong thời gian thuê dịch vụ, mọi lỗi phát sinh trong Hệ thống phải được sửa hoặc loại bỏ mà không phát sinh bất kỳ chi phí nào.
2	Nhà cung cấp dịch vụ xây dựng Hệ thống (Nhà cung cấp dịch vụ) phải bảo đảm an toàn bảo mật dữ liệu, Hệ thống phần mềm bệnh án điện tử không được cung cấp cho bất kỳ cá nhân, tổ chức nào trừ khi được sự đồng ý của Lãnh đạo Trung tâm bảo đảm tuân thủ các quy định về bảo vệ dữ liệu cá nhân, chia sẻ thông tin, dữ liệu.

3.1.4.2.17.Yêu cầu về môi trường cho phát triển, nâng cấp, chỉnh sửa phần mềm

- Môi trường: Hệ thống phải được phát triển trên môi trường phát triển tích hợp (IDE) cung cấp cho người lập trình công cụ viết code (code editor), công cụ đóng gói (build) và công cụ tìm lỗi (debugger).
- Ngôn ngữ lập trình: Để tăng khả năng bảo trì và tính dễ hiểu của mã nguồn (source code), hệ thống phải được phát triển bằng ngôn ngữ lập trình hướng đối tượng phổ biến. Đối với cơ sở dữ liệu cần sử dụng cơ sở dữ liệu quan hệ cho phép quản lý dữ liệu lớn, ổn định và tránh dư thừa dữ liệu.

3.1.4.2.18.Yêu cầu về độ phức tạp kỹ thuật-công nghệ của phần mềm

- Độ phức tạp kỹ thuật - công nghệ của phần mềm phải được tính toán dựa trên các tiêu chí sau:

Stt	Các hệ số tác động môi trường
1	Có áp dụng qui trình phát triển phần mềm theo mẫu RUP và có hiểu biết về RUP hoặc quy trình phát triển phần mềm tương đương
2	Có kinh nghiệm về ứng dụng tương tự (application experiences)
3	Có kinh nghiệm về hướng đối tượng (Object Oriented)

4	Có khả năng lãnh đạo Nhóm
5	Tính năng động
	Đánh giá chung
6	Độ ổn định của các yêu cầu
7	Có sử dụng các nhân viên làm bán thời gian (Part-time)
8	Dùng ngôn ngữ lập trình loại khó

3.1.4.2.19.Yêu cầu về hạ tầng kỹ thuật

Hệ thống cần đáp ứng các yêu cầu sau:

- Yêu cầu về bảo mật: hệ thống có thiết bị Firewall chuyên dụng kiểm soát mọi truy cập từ mạng Internet cũng như các luồng dữ liệu trao đổi nội bộ của hệ thống.
- Yêu cầu về khả năng chịu lỗi: tất cả các thiết bị của hệ thống cần được dự phòng. Đối với máy chủ và thiết bị lưu trữ cần thực hiện theo mô hình dự phòng đảm bảo không có gián đoạn dịch vụ khi có lỗi máy chủ hoặc thiết bị lưu trữ.
- Yêu cầu về khả năng chịu tải: để khai thác tối đa tài nguyên và đáp ứng các yêu cầu dự phòng, các máy chủ ứng dụng hoạt động qua cơ chế cache của Reddit và quản lý hàng đợi RabbitMQ.

3.1.4.2.20.Yêu cầu đối với hạ tầng mạng và bảo mật

- Các đơn vị trong Trung tâm kết nối đến hệ thống thông qua Internet để khai thác và sử dụng dịch vụ.
- Có sử dụng firewall và các biện pháp đảm bảo an toàn an ninh bảo mật thông tin đối với hệ thống khi bị tấn công trên môi trường mạng.
- Hệ thống sử dụng cân bằng tải để thực hiện việc cân bằng tải đối với ứng dụng cũng như chuyển lưu lượng dịch vụ.

3.1.4.2.5. Yêu cầu tuân thủ kiến trúc Chính phủ điện tử của Bộ Y tế phiên bản 2.1

Trong thời gian qua, Bộ Y tế đã thực hiện đồng bộ các giải pháp, nhiệm vụ nhằm đẩy mạnh ứng dụng CNTT, tăng cường đảm bảo an toàn, an ninh thông tin trong hoạt động của các đơn vị trong ngành y tế, hướng tới xây dựng Chính phủ điện tử, góp phần nâng cao chất lượng, hiệu quả hoạt động của các đơn vị; phục vụ người dân và doanh nghiệp ngày càng tốt hơn. Ngày 21/4/2023, Bộ trưởng Bộ Y tế ban hành kèm theo Quyết định 1928/QĐ-BYT "Kiến trúc Chính phủ điện tử Bộ Y tế phiên bản 2.1", đồng thời tổ chức thực hiện các nhiệm vụ từng bước mang lại những kết quả khả quan. Dự án đầu tư, nâng cấp hệ thống CNTT tại Trung tâm Hữu Nghị Việt Nam Cu Ba tuân thủ theo Khung kiến trúc chính phủ điện tử của Bộ Y tế, cụ thể:

- Kết nối, liên thông một số hệ thống thông tin, cơ sở dữ liệu của Trung tâm với Bộ Y tế, trao đổi bệnh án điện tử, trích chuyển giám định Bảo hiểm xã hội.

- Đảm bảo trích xuất được file XML chuẩn dữ liệu theo 4210 và 130 phục vụ đồng bộ dữ liệu lên hệ thống hồ sơ sức khỏe toàn dân theo quy định của Bộ Y tế.

- Đảm bảo quản lý hoạt động khám, chữa bệnh tại Trung tâm:

+ Công tác khám sức khỏe tại các cơ sở khám bệnh, chữa bệnh;

+ Hoạt động khoa Dược Trung tâm;

+ Sử dụng thuốc trong Trung tâm;

+ Hoạt động xét nghiệm trong Trung tâm;

+ Hoạt động dược lâm sàng trong Trung tâm;

+ Hoạt động pháp y, pháp y tâm tâm thần;

+ Hệ thống các báo cáo khám bệnh, chữa bệnh;

+ Báo cáo công tác điều dưỡng Trung tâm;

+ Báo cáo quản lý chất lượng xét nghiệm tại cơ sở khám bệnh, chữa bệnh;

+ Báo cáo về việc thực hiện chế độ luân phiên có thời hạn đối với người hành nghề tại cơ sở khám bệnh, chữa bệnh;

+ Báo cáo hoạt động Trung tâm 3-6-9-12 tháng;

+ Báo cáo Đánh giá chất lượng xét nghiệm tất cả các labo;

+ Báo cáo Danh mục xét nghiệm được phép liên thông của các Trung tâm;

+ Báo cáo sự cố y khoa để phòng ngừa tại các cơ sở khám chữa bệnh;

+ Báo cáo kiểm tra kết quả hoạt động Trung tâm;

+ Báo cáo Danh mục kỹ thuật đã phê duyệt và thực hiện tại Trung tâm;

+ Báo cáo Danh sách người hành nghề có chứng chỉ tại Trung tâm;

+ Danh sách khoa phòng của Trung tâm;

+ Danh mục trang thiết bị tại Trung tâm.

- Các hệ thống thông tin của Trung tâm được áp dụng phương án bảo đảm an toàn thông tin phù hợp với tiêu chuẩn, quy chuẩn kỹ thuật về bảo đảm an toàn hệ thống thông tin theo cấp độ và có giám sát an toàn an ninh mạng.

Với các nội dung trình bày ở trên, có thể thấy các hạng mục đầu tư tại dự án đáp ứng các yêu cầu tại Quyết định số 1928/QĐ-BYT ngày 21/4/2023 Bộ Y tế ban hành kiến trúc Chính phủ điện tử phiên bản 2.1.

3.1.4.2.6. Đảm bảo an toàn hệ thống thông tin theo cấp độ

Luật Công nghệ thông tin số 67/2006/QH11 ngày 29/6/2006;

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

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

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

Quyết định số 742/QĐ-BTTTT ngày 22/4/2022 của Bộ Thông tin và Truyền thông về việc yêu cầu an toàn cơ bản đối với phần mềm nội bộ.

Văn bản số 166/CATTT-ATHTTT ngày 10/02/2022 của Bộ Thông tin và Truyền thông về việc ban hành hướng dẫn khung phát triển phần mềm an toàn.

Việc xác định và thuyết minh cấp độ an toàn hệ thống thông tin với hệ thống trong hoạt động ƯDCNTT này gồm các thông tin như dưới đây:

3.1.4.2.6.1.Phân loại hệ thống thông tin

- Hệ thống thông tin được triển khai trong hoạt động này theo mô hình triển khai đầu tư mới;
- Hệ thống thông tin phục vụ nghiệp vụ, hệ thống trực tiếp hoặc hỗ trợ cung cấp dịch vụ trong lĩnh vực y tế.

3.1.4.2.6.2.Xác định loại thông tin được xử lý

Căn cứ Khoản 2 Điều 6 của Nghị định số 85/2016/NĐ-CP, thông tin được xử lý trên hệ thống này là: Hệ thống thông tin phục vụ hoạt động nội bộ là hệ thống chỉ phục vụ hoạt động quản trị, vận hành nội bộ của cơ quan, tổ chức.

3.1.4.2.6.3.Xác định cấp độ an toàn thông tin

Theo Điều 8. Tiêu chí xác định Cấp độ 2

Hệ thống thông tin Cấp độ 2 là hệ thống thông tin có một trong các tiêu chí cụ thể như sau:

1. Hệ thống thông tin phục vụ hoạt động nội bộ của cơ quan, tổ chức và có xử lý thông tin riêng, thông tin cá nhân của người sử dụng nhưng không xử lý thông tin bí mật nhà nước.

2. Hệ thống thông tin phục vụ người dân, doanh nghiệp thuộc một trong các loại hình như sau:

a) Cung cấp thông tin và dịch vụ công trực tuyến từ mức độ 2 trở xuống theo quy định của pháp luật;

b) Cung cấp dịch vụ trực tuyến không thuộc danh Mục dịch vụ kinh doanh có Điều kiện;

c) Cung cấp dịch vụ trực tuyến khác có xử lý thông tin riêng, thông tin cá nhân của dưới 10.000 người sử dụng.

3. Hệ thống cơ sở hạ tầng thông tin phục vụ hoạt động của một cơ quan, tổ chức.

Dựa trên việc xác định cấp độ an toàn của hệ thống thông tin đã nêu, các Hệ thống được triển khai trong hoạt động này cần tuân thủ Yêu cầu cơ bản đảm bảo an toàn thông tin đối với hệ thống thông tin Cấp độ 2, được quy định tại Thông tư số 12/2022/TT-BTTTT ngày 12/8/2022.

3.1.4.2.6.4. Thuyết minh phương án bảo đảm an toàn thông tin

Phương án đảm bảo an toàn thông tin đối với hệ thống thông tin cần đáp ứng được các yêu cầu theo quy định về bảo đảm an toàn hệ thống thông tin cấp độ 2 theo Nghị định 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ và Thông tư số 12/2022/TT-BTTTT ngày 12/8/2022 của Bộ Thông tin và Truyền thông như trình bày dưới đây.

3.1.4.2.6.1. Đáp ứng yêu cầu quản lý

3.1.4.2.6.1.1. Chính sách chung

a) Quy chế bảo đảm an toàn thông tin

Yêu cầu	Xác định các mục tiêu, nguyên tắc bảo đảm an toàn thông tin
Phương án	Mục tiêu: Bảo vệ thông tin, hệ thống thông tin trên mạng tránh bị truy nhập, sử dụng, tiết lộ, gián đoạn, sửa đổi hoặc phá hoại trái phép nhằm bảo

	đảm tính nguyên vẹn, tính bảo mật và tính khả dụng của thông tin. Nguyên tắc bảo đảm an toàn thông tin: 1. Việc bảo đảm an toàn thông tin (ATTT) là yêu cầu bắt buộc trong quá trình tạo lập, xử lý, sử dụng thông tin và quá trình thiết kế, xây dựng, vận hành, nâng cấp, hệ thống thông tin. 2. Các cơ quan, đơn vị và cá nhân có trách nhiệm đảm bảo ATTT theo quy định của Nhà nước và hướng dẫn của các cơ quan, đơn vị có thẩm quyền trong lĩnh vực ATTT. 3. Người dùng phải được tập huấn, phổ biến kiến thức cơ bản về ATTT trên môi trường máy tính, mạng máy tính và kiến thức nâng cao đối với cán bộ chuyên môn. 4. Thông tin thuộc danh mục bí mật nhà nước trên môi trường máy tính và mạng máy tính phải được bảo vệ theo các quy định của Nhà nước và các nội dung tương ứng trong quy định này. 5. Giảm thiểu các nguy cơ gây mất ATTT trong sử dụng hệ thống thông tin. 6. Đảm bảo tính bảo mật a) Đảm bảo thông tin chỉ có thể được truy cập bởi những đối tượng (người, chương trình máy tính,...) được cấp quyền truy cập. b) Mật khẩu truy cập, khóa mã hóa và các mã khóa khác được mã hóa trong quá trình truy cập, trên đường truyền và lưu trữ tại đơn vị quản lý thông tin. 7. Đảm bảo tính nguyên vẹn a) Đảm bảo tính nguyên vẹn thông tin là việc thông tin chỉ được phép xóa hoặc sửa bởi những đối tượng được phép và phải đảm bảo rằng nội dung cung cấp trên Hệ thống được kiểm duyệt chặt chẽ. b) Việc quản lý, sử dụng, lưu trữ, truyền đưa các thông tin phải đảm bảo tính nguyên vẹn, không được thay đổi khi chưa được phép của đơn vị quản lý thông tin. c) Việc đảm bảo tính nguyên vẹn phải được thực hiện trong toàn bộ các quá trình truy cập, các quá trình nhập, lưu trữ, sử dụng, xử lý, truyền tải, trích rút và khôi phục dữ liệu. 8. Đảm bảo tính khả dụng a) Đảm bảo khả năng hoạt động liên tục của hệ thống thông tin. b) Đảm bảo thông tin phải được truy cập nhanh chóng khi có sự yêu cầu từ phía cá nhân, tổ chức được cho phép truy cập thông tin. c) Đảm bảo nguồn nhân lực trong việc vận hành hệ thống thông tin.
Yêu cầu	Xác định trách nhiệm của đơn vị chuyên trách về an toàn thông tin, các cán bộ làm về an toàn thông tin và các đối tượng thuộc phạm vi điều chỉnh của chính sách an toàn thông tin

Phương án	a) Trách nhiệm của bộ phận chuyên trách về an toàn thông tin trong Trung tâm dữ liệu: i) Chịu trách nhiệm bảo đảm an toàn thông tin mạng của các hệ thống phần mềm và máy chủ; ii) Tham mưu lãnh đạo huyện ban hành các quy chế, quy trình nội bộ, triển khai các giải pháp kỹ thuật bảo đảm an toàn thông tin mạng; iii) Thực hiện việc giám sát, đánh giá, báo cáo lãnh đạo các rủi ro mất an toàn thông tin mạng và mức độ nghiêm trọng của các rủi ro đó; iv) Phối hợp với các cá nhân, đơn vị có liên quan trong việc kiểm soát, phát hiện và khắc phục các sự cố an toàn thông tin mạng; v) Thường xuyên cập nhật nâng cao kiến thức, trình độ chuyên môn đáp ứng yêu cầu bảo đảm an toàn thông tin mạng của đơn vị. b) Trách nhiệm của người sử dụng - các cán bộ phụ trách: i) Nghiêm túc chấp hành các quy chế, quy trình nội bộ và các quy định khác của pháp luật về an toàn thông tin mạng. Chịu trách nhiệm bảo đảm an toàn thông tin mạng trong phạm vi trách nhiệm và quyền hạn được giao; ii) Có trách nhiệm tự quản lý, bảo quản thiết bị, tài khoản, ứng dụng mà mình được giao sử dụng; iii) Khi phát hiện nguy cơ hoặc sự cố mất an toàn thông tin mạng phải báo cáo ngay với cấp trên và bộ phận phụ trách CNTT của cơ quan, đơn vị để kịp thời ngăn chặn và xử lý; iv) Tham gia các chương trình đào tạo, hội nghị về an toàn thông tin mạng được huyện, thành phố hoặc đơn vị chuyên môn tổ chức.

b) Xây dựng và công bố

Yêu cầu	Quy định về xây dựng và công bố Quy chế bảo đảm an toàn thông tin
Phương án	Xây dựng và công bố Quy chế bảo đảm an toàn thông tin trong quá trình sử dụng, vận hành Hệ thống

c) Rà soát, sửa đổi

Yêu cầu	Có quy định về việc rà soát, sửa đổi Quy chế bảo đảm an toàn thông tin
Phương án	Rà soát, sửa đổi Quy chế bảo đảm an toàn thông tin: Định kỳ 02 năm hoặc khi có thay đổi Quy chế bảo đảm an toàn thông tin kiểm tra lại tính phù hợp và thực hiện rà soát, cập nhật, bổ sung.

d) Tổ chức, nhân sự

Phối hợp với những cơ quan/tổ chức có thẩm quyền

Yêu cầu	Có quy định về việc phối hợp với những cơ quan/tổ chức có thẩm quyền
Phương án	Phối hợp với những cơ quan/tổ chức có thẩm quyền: 1. Đầu mối liên hệ, phối hợp với các cơ quan, tổ chức có thẩm quyền quản

	lý về an toàn thông tin: Cục An Toàn Thông tin làm đầu mối, tổ chức thực hiện việc tiếp nhận và xử lý các sự cố về an toàn thông tin mạng. 2. Có đầu mối liên hệ, phối hợp với các cơ quan, tổ chức trong công tác hỗ trợ điều phối xử lý sự cố an toàn thông tin: Tùy theo mức độ sự cố, phối hợp Cục An toàn thông tin hoặc Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam và các đơn vị có liên quan hướng dẫn xử lý, ứng cứu các sự cố an toàn thông tin mạng

3.1.4.2.6.12. Quản lý thiết kế, xây dựng

Thiết kế an toàn hệ thống thông tin

Yêu cầu	Có quy định về thiết kế an toàn hệ thống thông tin
Phương án	Quy định đối với tài liệu thiết kế hệ thống: 1. Có tài liệu mô tả quy mô, phạm vi và đối tượng sử dụng, khai thác, quản lý vận hành hệ thống thông tin. 2. Có tài liệu mô tả thiết kế và các thành phần của hệ thống thông tin. 3. Có tài liệu mô tả phương án lựa chọn giải pháp công nghệ bảo đảm an toàn thông tin. 4. Có tài liệu mô tả phương án lựa chọn giải pháp công nghệ bảo đảm an toàn thông tin. 5. Khi có thay đổi thiết kế, đánh giá lại tính phù hợp của phương án thiết kế đối với các yêu cầu an toàn đặt ra đối với hệ thống.

a) Thử nghiệm và nghiệm thu hệ thống

Yêu cầu	Có quy định về việc thử nghiệm và nghiệm thu hệ thống
Phương án	Quy định đối với việc thử nghiệm và nghiệm thu hệ thống: 1. Bên triển khai xây dựng kế hoạch, nội dung thử nghiệm hệ thống, trình cấp có thẩm quyền phê duyệt, trước khi thực hiện thử nghiệm và nghiệm thu hệ thống. 2. Hệ thống phải được thực hiện kiểm thử hệ thống trước khi đưa vào vận hành, khai thác sử dụng theo nội dung, kế hoạch được phê duyệt. 3. Có bộ phận có trách nhiệm thực hiện thử nghiệm và nghiệm thu hệ thống. 4. Có báo cáo nghiệm thu được xác nhận của bộ phận chuyên trách và phê duyệt của chủ quản hệ thống thông tin trước khi đưa vào sử dụng.

3.1.4.2.6.1.3. Quản lý vận hành

a) Quản lý an toàn mạng

Yêu cầu	Có quy định về quản lý an toàn mạng
Phương án	Quy định về quản lý an toàn mạng: 1. Hệ thống mạng phải được thiết lập cấu hình để: Kiểm soát truy cập từ bên ngoài mạng; Kiểm soát truy cập từ bên trong mạng; Kết nối về

	hệ thống giám sát tập trung; Phòng chống xâm nhập giữa các vùng mạng; Phòng chống phần mềm độc hại trên môi trường mạng. 2. Các thiết bị mạng phải được cấu hình chức năng xác thực; Chỉ cho phép sử dụng các kết nối mạng an toàn (nếu hỗ trợ) khi truy cập, quản trị thiết bị từ xa; Giới hạn các địa chỉ mạng có thể kết nối, quản trị thiết bị từ xa; Hạn chế được số lần đăng nhập sai; Phân quyền truy cập, quản trị; Nâng cấp, xử lý điểm yếu an toàn thông tin của thiết bị hệ thống trước khi đưa vào sử dụng. 3. Hệ thống mạng phải được trang bị hệ thống kỹ thuật, công nghệ hiện đại để thường xuyên, liên tục quản lý, giám sát, kiểm soát mạng nhằm phát hiện, ngăn chặn các truy cập trái phép của người sử dụng, tin tặc tấn công. 4. Việc thanh lý, tiêu hủy thiết bị, vật mang thông tin trong mạng phải đảm bảo yêu cầu không để lộ, lọt thông tin. Phải có quy trình cụ thể và phải lưu giữ hồ sơ, biên bản việc thanh lý, tiêu hủy. 5. Có biện pháp bảo vệ, dự phòng, phòng chống các nguy cơ do mất cắp, cháy nổ, ngập lụt, động đất và các thảm họa khác do thiên nhiên hoặc con người gây ra và các phương án khôi phục hệ thống sau thảm họa.

b) Quản lý an toàn máy chủ và ứng dụng

Yêu cầu	Có quy định về quản lý an toàn máy chủ và ứng dụng
Phương án	Quy định về quản lý an toàn máy chủ và ứng dụng: 1. Quy định với máy chủ a) Hệ thống máy chủ phải có tính năng sẵn sàng cao, cơ chế dự phòng linh hoạt để đảm bảo hoạt động liên tục. b) Có biện pháp bảo vệ, dự phòng, phòng chống các nguy cơ do mất cắp, cháy nổ, ngập lụt, động đất và các thảm họa khác do thiên nhiên hoặc con người gây ra và các phương án khôi phục sau thảm họa cho hệ thống máy chủ. c) Máy chủ phải được thiết lập chính sách xác thực; Kiểm soát truy cập; Kết nối về hệ thống giám sát tập trung; Thực hiện biện pháp phòng chống xâm nhập; Phòng chống phần mềm độc hại và xử lý dữ liệu trên máy chủ khi chuyển giao. d) Máy chủ phải được nâng cấp, xử lý điểm yếu an toàn thông tin trên máy chủ trước khi đưa vào sử dụng. đ) Việc kết nối, gỡ bỏ máy chủ khỏi hệ thống phải được sự cho phép của lãnh đạo nhà trường và thực hiện theo quy trình đã được phê duyệt. e) Phần mềm hệ điều hành cài lên máy chủ ưu tiên là phần mềm hệ điều hành có bản quyền hoặc là phần mềm mã nguồn mở được sử dụng rộng rãi trong nước và quốc tế.

	g) Có tài liệu liệt kê, cài đặt với những phần mềm hệ thống cài trong máy chủ. 2. Quy định với ứng dụng: a) Các yêu cầu, thiết kế về an toàn bảo mật của phần mềm ứng dụng cần được xác định rõ trong tài liệu phân tích, thiết kế. Trong quá trình triển khai, vận hành các phần mềm ứng dụng cần đảm bảo nghiêm ngặt theo các yêu cầu, thiết kế về an toàn bảo mật. b) Ứng dụng phải được thiết lập chính sách xác thực; Kiểm soát truy cập; Kết nối về hệ thống giám sát tập trung; Có phương án bảo mật thông tin liên lạc, chống chối bỏ và biện pháp bảo đảm an toàn ứng dụng và mã nguồn. c) Có phương án xác định và khắc phục rủi ro trước, trong quá trình triển khai và khi vận hành các phần mềm ứng dụng. d) Ứng dụng phải kiểm tra, thử nghiệm và có biên bản đánh giá tính an toàn, bảo mật đối với phần mềm ứng dụng theo yêu cầu khi nghiệm thu các phần mềm này. Việc tiến hành thử nghiệm phải đảm bảo trên môi trường riêng biệt, không ảnh hưởng tới hoạt động và dữ liệu của đơn vị.

c) Quản lý an toàn dữ liệu

Yêu cầu	Có quy định về quản lý an toàn dữ liệu
Phương án	Quy định về quản lý an toàn dữ liệu: 1. Thực hiện quản lý, lưu trữ dữ liệu quan trọng trong hệ thống cùng với mã kiểm tra tính nguyên vẹn. 2. Định kỳ hoặc khi có thay đổi cấu hình trên hệ thống thực hiện quy trình sao lưu dự phòng: tập tin cấu hình hệ thống, bản dự phòng hệ điều hành máy chủ, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ. 3. Lưu trữ có mã hóa các thông tin, dữ liệu (không phải là thông tin, dữ liệu công khai) trên hệ thống lưu trữ/phương tiện lưu trữ.

d) Quản lý an toàn thiết bị đầu cuối

Yêu cầu	Có quy định về quản lý thiết bị đầu cuối
Phương án	Quy định về quản lý an toàn thiết bị đầu cuối: a) Thông tin về thiết bị đầu cuối (tên, chủng loại, địa chỉ MAC, địa chỉ IP) phải được quản lý và cập nhật. b) Các thiết bị đầu cuối phải được quản lý khi kết nối vào hệ thống mạng theo địa chỉ MAC, IP. c) Khi truy cập và sử dụng thiết bị đầu cuối từ xa phải có cơ chế xác thực và sử dụng giao thức mạng an toàn. c) Việc cài đặt, kết nối và gỡ bỏ thiết bị đầu cuối trong hệ thống phải được cho phép bởi người có thẩm quyền và thực hiện theo quy trình được phê duyệt.

e) Quản lý sự cố an toàn thông tin

Yêu cầu	Có quy định về quản lý sự cố an toàn thông tin
Phương án	Quy định về quản lý sự cố an toàn thông tin: 1. Đơn vị/bộ phận chuyên trách về an toàn thông tin có trách nhiệm: a) Phân nhóm sự cố an toàn thông tin mạng theo quy định tại Quyết định số 05/2017/NĐ-CP của Thủ tướng Chính phủ ngày 16/3/2017 quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia (Quyết định 05); Xây dựng phương án tiếp nhận, phát hiện, phân loại và xử lý ban đầu sự cố an toàn thông tin mạng, ứng phó sự cố an toàn thông tin mạng. b) Xây dựng quy trình ứng cứu sự cố an toàn thông tin mạng thông thường và nghiêm trọng theo quy định tại Điều 13,14 Quyết định số 05. c) Xây dựng và triển khai kế hoạch ứng phó sự cố an toàn thông tin theo quy định tại Điều 16 Quyết định số 05. d) Quyết định toàn diện về mặt kỹ thuật đối với các cơ quan trong quá trình khắc phục sự cố về ATTT; Hỗ trợ, phối hợp và hướng dẫn các cơ quan khắc phục sự cố mất ATTT; Yêu cầu ngưng hoạt động một phần hoặc toàn bộ các hệ thống thông tin của các cơ quan nhằm phục vụ công tác khắc phục sự cố về ATTT; Phối hợp với đơn vị chức năng trong điều tra các nguyên nhân gây ra sự cố mất an toàn thông tin theo chỉ đạo của Lãnh đạo. e) Phối hợp với cơ quan chức năng, các nhóm chuyên gia, bên cung cấp dịch vụ hỗ trợ trong việc xử lý, khắc phục sự cố an toàn thông tin; Yêu cầu bên cung cấp, hỗ trợ cung cấp quy trình xử lý sự cố cho các dịch vụ do bên cung cấp, hỗ trợ cung cấp liên quan đến hệ thống. g) Tổ chức diễn tập phương án xử lý sự cố an toàn thông tin theo chỉ đạo của Lãnh đạo. 2. Trách nhiệm của người dùng: Thông tin, báo cáo kịp thời cho cán bộ chuyên trách về ATTT của cơ quan khi phát hiện các sự cố gây mất ATTT trong quá trình tham gia vào hệ thống thông tin của đơn vị; Phối hợp tích cực trong suốt quá trình giải quyết và khắc phục sự cố.

3.1.4.2.6.1.4. Đáp ứng yêu cầu kỹ thuật

a) Bảo đảm an toàn mạng

Thiết kế hệ thống

- Các vùng mạng trong hệ thống:

STT	Yêu cầu	P/A	Ghi chú/Mô tả
1	Vùng mạng nội bộ	Có	Cung cấp kết nối mạng cho các máy trạm và các thiết bị đầu cuối, các thiết bị khác của người sử dụng vào hệ thống

STT	Yêu cầu	P/A	Ghi chú/Mô tả
2	Vùng mạng biên	Có	Kết nối hệ thống với mạng Internet và mạng diện rộng
3	Vùng DMZ	Có	Đặt máy chủ WEBAPP, cho phép truy cập trực tiếp từ các mạng bên ngoài và mạng Internet.
4	Vùng máy chủ nội bộ	Có	Là vùng đặt máy chủ cơ sở dữ liệu.

- Phương án bảo đảm an toàn thông tin:

STT	Yêu cầu	P/A	Ghi chú/Mô tả
1	Phương án quản lý truy cập, quản trị hệ thống từ xa an toàn	Có	Sử dụng tường lửa có tích hợp chức năng VPN để quản lý truy cập, quản trị hệ thống từ xa an toàn. Tính năng VPN này được cấu hình trực tiếp trên thiết bị, quản lý truy cập từ bên ngoài vào vùng mạng nội bộ, từ bên ngoài vào vùng máy chủ nội bộ.
2	Phương án quản lý truy cập giữa các vùng mạng và phòng chống xâm nhập sử dụng tường lửa có tích hợp chức năng phòng, chống xâm nhập hoặc sản phẩm chống tấn công, xâm nhập	Có	Sử dụng tường lửa có tích hợp chức năng IPS để quản lý truy cập giữa các vùng mạng và phòng chống xâm nhập. Tính năng IPS được cấu hình trên Firewall kiểm soát truy cập và phòng chống xâm nhập giữa các phân vùng mạng nội bộ, máy chủ nội bộ và phân vùng mạng DMZ.
3	Phương án phòng chống mã độc cho máy chủ và máy trạm	Có	Sử dụng sản phẩm Phòng chống mã độc hoặc phương án tương đương (Giải pháp Antivirus): Sử dụng phần mềm diệt virus cho các máy chủ, đồng thời UBND xã Quảng Long có sẵn phần mềm rà quét mã độc cho các máy trạm.
4	Phương án phòng chống tấn công mạng cho ứng dụng web		Không cài ứng dụng web lên hệ thống mới
5	Phương án bảo đảm an toàn thông tin cho hệ thống thư điện tử (đối với hệ thống thư điện tử)	Có	Hệ thống thư điện của UBND xã Quảng Long đang thuê dịch vụ của nhà cung cấp, đáp ứng tiêu chí quy định về ATTT tại khoản 2 Điều 9 Nghị định 85/2016/NĐ-CP
6	Phương án dự phòng cho các thiết bị mạng chính	Có	Các thiết bị mạng chính: Router, Firewall, Switch đều có thiết bị dự

STT	Yêu cầu	P/A	Ghi chú/Mô tả
			phòng

b) Kiểm soát truy cập từ bên ngoài mạng

STT	Yêu cầu	P/A	Ghi chú/Mô tả
1	Thiết lập hệ thống chỉ cho phép sử dụng các kết nối mạng an toàn khi truy cập thông tin nội bộ hoặc quản trị hệ thống từ các mạng bên ngoài và mạng Internet	Có	Hệ thống sử dụng Tường lửa có tích hợp chức năng VPN được thiết lập chỉ cho phép kết nối mạng có hỗ trợ mã hóa, xác thực khi truy cập thông tin nội bộ hoặc quản trị hệ thống từ các mạng bên ngoài và mạng Internet.
2	Kiểm soát truy cập từ bên ngoài vào hệ thống theo từng dịch vụ, ứng dụng cụ thể; chặn tất cả truy cập tới các dịch vụ, ứng dụng mà hệ thống không cung cấp hoặc không cho phép truy cập từ bên ngoài	Có	Tường lửa được thiết lập chỉ cho phép kiểm soát truy cập từ bên ngoài vào hệ thống theo từng dịch vụ, ứng dụng cụ thể; chặn tất cả truy cập tới các dịch vụ, ứng dụng mà hệ thống không cung cấp hoặc không cho phép truy cập từ bên ngoài
3	Thiết lập giới hạn thời gian chờ (timeout) để đóng phiên kết nối khi hệ thống không nhận được yêu cầu từ người dùng.	Có	Thiết lập giới hạn thời gian chờ (timeout) để đóng phiên kết nối khi hệ thống không nhận được yêu cầu từ người dùng trên Tường lửa và ngắt phiên kết nối VPN khi người dùng không thao tác sử dụng trong 1 khoảng thời gian

c) Kiểm soát truy cập từ bên trong mạng

STT	Yêu cầu	P/A	Ghi chú/Mô tả
1	Chỉ cho phép truy cập các ứng dụng, dịch vụ bên ngoài theo yêu cầu nghiệp vụ, chặn các dịch vụ khác không phục vụ hoạt động nghiệp vụ theo chính sách của tổ chức	Có	Chính sách kiểm soát truy cập từ các vùng mạng trong hệ thống đi ra các mạng bên ngoài và mạng Internet được thiết lập trên Tường lửa

d) Phòng chống xâm nhập

STT	Yêu cầu	P/A	Ghi chú/Mô tả
1	Có phương án phòng chống xâm nhập để bảo vệ các vùng mạng trong hệ thống	Đáp ứng	Sử dụng Tường lửa có tích hợp chức năng IPS để bảo vệ các vùng mạng trong hệ thống. Tính năng IPS được cấu hình trên kiểm soát truy cập và phòng chống xâm nhập giữa các phân vùng

STT	Yêu cầu	P/A	Ghi chú/Mô tả
			mạng nội bộ, máy chủ nội bộ và phân vùng mạng DMZ.
2	Định kỳ cập nhật cơ sở dữ liệu dấu hiệu phát hiện tấn công mạng	Đáp ứng	Thực hiện định kỳ cập nhật cơ sở dữ liệu dấu hiệu phát hiện tấn công mạng trên Tường lửa .

3.1.4.2.6.1.5. Bảo đảm an toàn máy chủ

a) Xác thực

Yêu cầu / Máy chủ	Thiết lập chính sách xác thực trên máy chủ	Thay đổi các tài khoản mặc định trên hệ thống hoặc vô hiệu hóa	Thiết lập chính sách mật khẩu an toàn: Yêu cầu thay đổi mật khẩu mặc định; Thiết lập quy tắc đặt mật khẩu về số ký tự, loại ký tự; Thiết lập thời gian yêu cầu thay đổi mật khẩu; Thiết lập thời gian mật khẩu hợp lệ
Web Server (máy ảo)/Cài đặt Web-App/Vùng DMZ/Window Server	+	+	+
Database Server (máy ảo)/Cài đặt SQL server/Vùng máy chủ nội bộ/Window Server	+	+	+

b) Kiểm soát truy cập

Yêu cầu / Máy chủ	Chỉ cho phép sử dụng các kết nối mạng an toàn khi truy cập, quản trị máy chủ từ xa	Thiết lập giới hạn thời gian chờ (timeout)
Web Server (máy ảo)/Cài đặt Web-App/Vùng DMZ/Window Server	+	+
Database Server (máy ảo)/Cài đặt SQL server/Vùng máy chủ nội bộ/Window Server	+	+

c) Nhật ký hệ thống

Yêu cầu	Thiết lập lập	Đồng bộ thời gian	Lưu nhật ký hệ thống

Máy chủ	chức năng ghi nhật ký hệ thống trên các máy chủ	giữa máy chủ với máy chủ thời gian	trong khoảng thời gian tối thiểu là 01 tháng
Web Server (máy ảo)/Cài đặt Web-App/Vùng DMZ/Window Server	+	+	+
Database Server (máy ảo)/Cài đặt SQL server/Vùng máy chủ nội bộ/Window Server	+	+	+

d) Phòng chống xâm nhập

Yêu cầu Máy chủ	Loại bỏ các tài khoản không sử dụng, các tài khoản không còn hợp lệ trên máy chủ	Sử dụng tường lửa của hệ điều hành và hệ thống để cấm các truy cập trái phép tới máy chủ	Vô hiệu hóa các giao thức mạng không an toàn, các dịch vụ hệ thống không sử dụng	Thực hiện nâng cấp, xử lý điểm yếu an toàn thông tin trên máy chủ trước khi đưa vào sử dụng
Web Server (máy ảo)/Cài đặt Web-App/Vùng DMZ/Window Server	+	+	+	+
Database Server (máy ảo)/Cài đặt SQL server/Vùng máy chủ nội bộ/Window Server	+	+	+	+

e) Phòng chống phần mềm độc hại

Yêu cầu **Máy chủ**	Cài đặt phần mềm phòng chống mã độc và thiết lập chế độ tự động cập nhật	Kiểm tra, dò quét, xử lý phần mềm độc hại cho các phần mềm trước khi cài đặt
Web Server (máy ảo)/Cài đặt Web-App/Vùng DMZ/Window Server	+	+

Database Server (máy ảo)/Cài đặt SQL server/Vùng máy chủ nội bộ/Window Server	+	+

f) Xử lý máy chủ khi chuyển giao

STT	Yêu cầu	P/A	Ghi chú/Mô tả
1	Có phương án xóa sạch thông tin, dữ liệu trên máy chủ khi chuyển giao hoặc thay đổi mục đích sử dụng	Đáp ứng	Hiện tại chưa có phương án chuyển giao cho đơn vị sử dụng. Sẽ có phương án xóa sạch thông tin, dữ liệu trên máy chủ khi chuyển giao hoặc thay đổi mục đích sử dụng

3.1.4.2.6.1.6. Bảo đảm an toàn ứng dụng

a) Xác thực

Yêu cầu	Thiết lập cấu hình ứng dụng để xác thực người sử dụng khi truy cập, quản trị, cấu hình ứng dụng	Lưu trữ có mã hóa thông tin xác thực hệ thống	Thiết lập cấu hình ứng dụng để đảm bảo an toàn mật khẩu người sử dụng	Hạn chế số lần đăng nhập sai trong khoảng thời gian nhất định với tài khoản nhất định
Ứng dụng				
Hệ thống trang thiết bị	+	+	+	+

b) Kiểm soát truy cập

Yêu cầu	Chỉ cho phép sử dụng các kết nối mạng an toàn khi truy cập, quản trị ứng dụng từ xa	Thiết lập giới hạn thời gian chờ (timeout) để đóng phiên kết nối khi ứng dụng không nhận được yêu cầu từ người dùng	Giới hạn địa chỉ mạng quản trị được phép truy cập, quản trị ứng dụng từ xa
Ứng dụng			
Hệ thống trang thiết bị	+	+	+

c) Nhật ký hệ thống

Yêu cầu	Ghi nhật ký hệ thống bao gồm những thông tin cơ bản sau:	Nhật ký hệ thống phải được lưu trữ trong khoảng thời
Ứng dụng		

	(1) Thông tin truy cập ứng dụng; (2) Thông tin đăng nhập khi quản trị ứng dụng; (3) Thông tin các lỗi phát sinh trong quá trình hoạt động; (4) Thông tin thay đổi cấu hình ứng dụng.	gian tối thiểu là 01 tháng
Hệ thống trang thiết bị	+	+

d) An toàn ứng dụng và mã nguồn

Yêu cầu	Có chức năng kiểm tra tính hợp lệ của thông tin, dữ liệu đầu vào trước khi xử lý
Ứng dụng	
Hệ thống trang thiết bị	+

3.1.4.2.6.1.7. Bảo đảm an toàn dữ liệu

a) Bảo mật dữ liệu

STT	Yêu cầu	P/A	Ghi chú/Mô tả
1	Lưu trữ có mã hóa các thông tin, dữ liệu (không phải là thông tin, dữ liệu công khai) trên hệ thống lưu trữ/phương tiện lưu trữ	Có	Dữ liệu được nén và được lưu trữ mã hóa sử dụng EAS 256

a) Sao lưu dự phòng

STT	Yêu cầu	P/A	Ghi chú/Mô tả
1	Thực hiện sao lưu dự phòng các thông tin, dữ liệu cơ bản sau: tập tin cấu hình hệ thống, bản dự phòng hệ điều hành máy chủ, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ	Có	Có thực hiện sao lưu dự phòng các thông tin, dữ liệu cơ bản sau: tập tin cấu hình hệ thống, bản dự phòng hệ điều hành máy chủ, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ trên ổ cứng di động

3.1.4.2.7. Yêu cầu về tính sẵn sàng với IPv6

TT	Yêu cầu
1	Đảm bảo phần mềm hỗ trợ IPv6;
2	Đảm bảo đường truyền kết nối Internet cho Webserver hỗ trợ IPv6
3	Khai báo Webserver lắng nghe được các kết nối qua mạng IPv6
4	Khai báo bản ghi AAAA cho tên miền trên hệ thống DNS Hosting

TT	Yêu cầu
5	Đảm bảo máy chủ DNS Hosting hỗ trợ IPv6
6	Sẵn sàng hỗ trợ địa chỉ Internet thế hệ mới IPv6, DNSSEC. Triển khai HTTPS sử dụng giao thức TLS v1.2 trở lên với các bộ mã hóa an toàn trong xác thực người dùng và truyền nhận các thông tin nhạy cảm (thông tin cá nhân, thông tin thanh toán).
7	Các thiết bị được đầu tư trong hoạt động này (gồm: Máy chủ, San storage, San switch, Firewall, Thiết bị phát wifi, Máy tính bảng) hỗ trợ IPv6.

3.1.4.3. Yêu cầu về an toàn bảo mật thông tin, dữ liệu

3.1.4.3. 1.Yêu cầu chung về an toàn bảo mật thông tin, dữ liệu

Hệ thống phần mềm bệnh án điện tử cần đảm bảo các yêu cầu chung về an toàn bảo mật thông tin, dữ liệu như sau:

TT	Nội dung yêu cầu	Yêu cầu
1	Bảo mật ứng dụng web	Kiểm soát truy vấn cơ sở dữ liệu để tránh lỗ hổng SQL Injection.
		Xử lý dữ liệu đầu vào để tránh lỗ hổng XSS.
		Sử dụng token trong các phương thức GET và POST tránh lỗ hổng CSRF: Phát sinh token theo từng request để đảm bảo an toàn cho các thao tác trên dữ liệu.
		Kiểm soát các thao tác với file: Có cơ chế kiểm tra tính hợp lệ và xử lý tập tin trong các thao tác người upload tập tin lên hệ thống.
		Mã hóa dữ liệu nhạy cảm Mã hóa một chiều các thông tin liên quan đến CSDL. Mật khẩu người dùng lưu trữ trong CSDL được mã hóa một chiều và kết hợp thêm salt khác nhau theo từng người dùng.
		Kiểm tra quyền truy cập của người dùng: Sử dụng hệ thống riêng để chứng thực người dùng đăng nhập và phân quyền.
		Phòng chống lỗi user enumeration.
		Phòng chống lỗi sesion fixation.
		Sử dụng cookie an toàn: Mã hóa thông tin sessionid trong cookies, sessionid được phát sinh là duy nhất, hủy các thông tin session khi người dùng thoát khỏi hệ thống.
		Chuyển hướng và chuyển tiếp thiếu thẩm tra (Unvalidated Redirects and Forwards).

TT	Nội dung yêu cầu	Yêu cầu
		Không để lộ dữ liệu của hệ thống: Mã hóa các thông tin nhạy cảm người dùng trong các kết quả trả về từ máy chủ.
		Chống thất thoát thông tin do kiểm soát lỗi và ngoại lệ không tốt: Không cho hiển thị các thông tin về ứng dụng khi ứng dụng bị lỗi.
		Sử dụng Captcha: Hạn chế các request liên tục và giống nhau lên server.
		Phòng chống lỗi file inclusion.
		Phòng chống lỗi Command injection.
		Phòng chống lỗi Xml/Xpath injection.
		Phòng chống các lỗi liên quan đến xử lý luồng nghiệp vụ, logic: Kiểm tra quyền hạn của người dùng trên từng thao tác.
		Bảo vệ cách tấn công Brute force: Thiết lập thời gian hết hiệu lực cho session để giới hạn thời gian kết nối.
2	Bảo mật trên hệ thống máy chủ	Các máy chủ được bảo vệ bởi hệ thống tường lửa cứng, đây là hệ thống để điều khiển các giao dịch ra vào các máy chủ bằng cách phân tích các gói dữ liệu và quyết định thành phần nào được truy cập vào các máy chủ, đảm bảo các máy chủ luôn bảo mật và tin cậy.
		Hệ thống máy chủ ứng dụng được đặt trong vùng an toàn được quy hoạch tại Trung tâm dữ liệu
3	Yêu cầu cơ bản đảm bảo an toàn hệ thống thông tin theo cấp độ	Hệ thống phần mềm bệnh án điện tử đạt cấp độ 3 của Nghị định số 85/2016/NĐ-CP ngày 11/7/2016 của Chính phủ về đảm bảo an toàn hệ thống thông tin theo cấp độ

3.1.4.3.2.Yêu cầu chi tiết về an toàn bảo mật thông tin, dữ liệu

3.1.4.3.2.1.Yêu cầu về bảo mật thông tin

STT	Yêu cầu
1	Hệ thống phần mềm có một module bảo mật được thiết kế riêng cho mức ứng dụng. Một người sử dụng muốn chạy chương trình và thực hiện một số chức năng cụ thể thì phải được quản trị hệ thống cấp cho một tài khoản và gán cho các quyền tương ứng với các chức năng (xem thêm yêu cầu chức năng về quản trị hệ thống được trình bày tại mục trên).

2	Hệ thống ứng dụng phải có khả năng kiểm soát chặt chẽ việc thay đổi các dữ liệu quan trọng để đảm bảo các dữ liệu này không thể thay đổi nếu chưa được xử lý một cách đúng đắn.
3	Hệ thống phải được thiết kế dựa trên một hệ thống bảo mật nhiều lớp và chặt chẽ. Các cấp bảo mật mà hệ thống đưa ra bao gồm: Mức hệ điều hành: Các hệ điều hành có rất nhiều công cụ và công nghệ bảo mật cao. Mỗi sản phẩm chạy trên hệ điều hành đều có thể tận dụng các tính năng này. Mức cơ sở dữ liệu: hệ cơ sở dữ liệu đa người dùng phải cung cấp các tính năng bảo mật, kiểm soát việc truy cập và sử dụng cơ sở dữ liệu như: ngăn chặn các truy cập dữ liệu bất hợp pháp, ngăn chặn việc truy cập bất hợp pháp vào các bảng dữ liệu, các thủ tục, tiến trình thiết lập trong CSDL. Mức ứng dụng: Người sử dụng hệ thống phải được cấp quyền và xác thực trước khi sử dụng. Bảo mật mạng truyền thông: Bao gồm. Bảo mật WebServer: Là cơ chế dựa chủ yếu vào các cơ chế bảo mật của phần mềm máy chủ Web (WebServer). Tường lửa: Là mức bảo mật ở mức hệ thống, đóng vai trò quan trọng đối với hệ thống được xây dựng dựa trên các ứng dụng 3 lớp. Bức tường lửa được xây dựng như một máy chủ kiểm soát các luồng thông tin vào ra với hệ thống nhằm mục đích tránh bị tấn công từ Internet và các cơ hội bị kiểm soát hệ thống từ xa.
4	Hệ thống được xây dựng và thực hiện giải pháp sao lưu dự phòng, được thiết kế để bảo đảm khắc phục, phục hồi các sự cố về dữ liệu, ứng dụng, cũng như hệ điều hành. Khi cơ sở dữ liệu, máy chủ ứng dụng hoặc hệ điều hành bị sụp đổ, hệ thống phải đảm bảo các dữ liệu backup cho việc phục hồi trạng thái làm việc ổn định. Việc thực hiện sao lưu (back-up) hệ thống được thực hiện theo quy định cụ thể và theo các chu kỳ khác nhau bao gồm ngày, tuần và tháng.
5	Hỗ trợ khả năng cấu hình ứng dụng đảm bảo khả năng bảo mật nhiều mức (trình diễn, nghiệp vụ, truy cập dữ liệu); giải pháp xác thực đạt mức độ bảo mật cao theo tiêu chuẩn quốc tế; sử dụng kênh kết nối an toàn trong việc truy cập máy chủ ứng dụng và công cụ quản lý.
6	Bảo đảm đáp ứng khả năng an toàn, bảo mật theo nhiều mức (hạ tầng, hệ thống, định danh đơn vị, cá nhân, xác thực đến thiết bị,…); tất cả các truy xuất vào kênh truyền dữ liệu đều phải được an toàn, dữ liệu phải bảo đảm toàn vẹn, bảo mật trên đường truyền; hỗ trợ cơ chế bảo vệ dữ liệu; có hiệu năng cao, không bị trễ và chạy ổn định.

7	Đồng bộ thời gian gửi, nhận báo cáo điện tử giữa các hệ thống thông tin báo cáo, hệ thống quản lý văn bản và điều hành của các bộ, ngành, địa phương bảo đảm thống nhất, đồng bộ theo múi giờ Việt Nam (Tiêu chuẩn ISO 8601).
8	Áp dụng các công nghệ xác thực, cơ chế kiểm soát quyền truy cập và cơ chế ghi lịch sử hoạt động của Hệ thống để quản lý, sẵn sàng cho kiểm tra, kiểm soát khi cần thiết.
9	Hỗ trợ công cụ theo dõi, kiểm tra, giám sát, phát hiện, xử lý các nguy cơ, rủi ro mất an toàn, an ninh thông tin; áp dụng giải pháp phân tích, đánh giá, đưa ra phương án khắc phục sự cố mất an toàn an ninh thông tin với thời gian nhanh nhất; triển khai các biện pháp, giải pháp phòng chống mã độc; áp dụng các biện pháp hành chính, kỹ thuật để tăng cường quản lý, giám sát, kiểm soát trong kết nối, chia sẻ, gửi, nhận báo cáo điện tử.
10	Dữ liệu của toàn bộ hệ thống được sao lưu dự phòng định kỳ; dữ liệu khi lưu chuyển và lưu trữ được mã hóa bằng mật mã theo quy định nhằm chống theo dõi, thu thập và sửa chữa trái phép.
11	Bảo đảm an toàn hệ thống thông tin theo cấp độ, các phương án bảo đảm an toàn thông tin, giám sát thông tin đáp ứng yêu cầu an toàn tối thiểu, cơ bản theo quy định; kết nối, chia sẻ thông tin với cơ quan giám định an toàn không gian mạng.
12	Hệ thống được kiểm tra, đánh giá và quản lý rủi ro trước khi đưa vào sử dụng, định kỳ hoặc đột xuất kiểm tra, đánh giá; có kế hoạch ứng phó sự cố bảo đảm an toàn thông tin mạng cho Hệ thống đáp ứng các yêu cầu; trang thiết bị phải có nguồn gốc xuất xứ rõ ràng và phải được kiểm định về an ninh, an toàn thông tin theo quy định của pháp luật.

3.1.4.3.2.2.An toàn, bảo mật thông tin đối với phần mềm ứng dụng:

- Có quy định ghi lại các lỗi và quá trình xử lý lỗi, đặc biệt là các lỗi về an toàn, bảo mật trong kiểm tra và thử nghiệm các phần mềm ứng dụng;
- Các phiên bản phần mềm bao gồm cả chương trình nguồn cần được quản lý tập trung, lưu trữ, bảo mật và có cơ chế phân quyền cho từng thành viên trong việc thao tác với các tập tin;
- Có kế hoạch định kỳ kiểm tra mã nguồn, nhằm loại trừ các đoạn mã độc hại, các lỗ hổng bảo mật;
- Đơn vị cung cấp phần mềm ứng dụng phải cam kết không có các đoạn mã độc hại trong sản phẩm.

3.1.4.3.2.3.Kiểm soát truy cập

- Hệ thống phải có khả năng kiểm soát truy cập của người sử dụng (tài khoản ứng dụng, tài khoản CSDL) theo vị trí, thời gian, mã số người sử dụng và chỉ cho phép mỗi mã số của người sử dụng được đăng nhập một lần tại một thời điểm từ một máy trạm bất kì.

- Hệ thống phải cung cấp chức năng logout tự động khi người dùng không sử dụng trong một khoảng thời gian nào đó. Tính năng này được thiết lập tùy từng thời kỳ và người quản trị có khả năng thiết lập mà không phải yêu cầu chỉnh sửa mã nguồn chương trình.

- Hệ thống phải có khả năng kiểm soát và ngăn ngừa các tài khoản ứng dụng CSDL, tài khoản người dùng sử dụng các công cụ để truy cập vào CSDL ứng dụng.

- Hệ thống phải có khả năng kiểm soát và ngăn ngừa các tài khoản ứng dụng CSDL, tài khoản người dùng thực thi các câu lệnh làm biến đổi cấu trúc CSDL, các modul của chương trình ứng dụng.

3.1.4.3.2.4.Giám sát truy cập

- Tất cả các hành động đăng nhập, truy cập vào CSDL (kể cả qua chương trình ứng dụng và qua các công cụ được phép) với mục đích khai thác, thay đổi dữ liệu đều phải được ghi nhận đầy đủ các thông tin về: Tài khoản truy cập, máy trạm truy cập, địa chỉ truy cập, thời gian truy cập, dữ liệu bị truy cập. Đối với việc làm thay đổi dữ liệu thì cần ghi nhận thêm các thông tin: giá trị mới, giá trị cũ của dữ liệu bị thay đổi.

- Tất cả các hành động làm biến đổi cấu trúc CSDL, các modul của chương trình ứng dụng phải được thực hiện ghi nhận đầy đủ các thông tin về: Tài khoản truy cập, máy trạm truy cập, địa chỉ truy cập, thời gian truy cập, câu lệnh thực hiện và gửi email cảnh bảo về cho các cán bộ có trách nhiệm xử lý.

3.1.4.3.2.5.Lưu trữ và khai thác thông tin giám sát

- Việc tổ chức quản lý, lưu trữ thông tin giám sát trên chương trình ứng dụng được thực hiện một cách tự động với chu kỳ lưu trữ, khai thác do người sử dụng tự định nghĩa (theo dung lượng, thời gian...).

- Chương trình phải có khả năng cung cấp các công cụ khai thác thông tin giám sát theo nhiều chiều: thời gian, người sử dụng, đối tượng bị thay đổi.

- Hệ thống phải được xây dựng với mô hình Web Application hoặc Web-base, được thiết kế dựa trên một hệ thống bảo mật nhiều lớp và chặt chẽ. Các cấp bảo mật mà hệ thống đưa ra bao gồm:

- Mức hệ điều hành: Sử dụng công nghệ bảo mật sẵn có của hệ điều hành và hạ tầng mạng.

- Mức cơ sở dữ liệu: Dựa vào cơ chế, công nghệ bảo mật cơ sở dữ liệu sẵn có của hệ quản trị cơ sở dữ liệu được sử dụng.

- Mức ứng dụng: Người sử dụng hệ thống phải được cấp quyền và xác thực trước khi sử dụng.

- Source code ứng dụng phải đảm bảo không có những lỗ hổng nghiêm trọng như: SQL Injection, Blind SQL Injection, Cross-site scripting...

3.1.4.3.2.6.An toàn dữ liệu

- Bảo đảm có cơ chế bảo vệ và phân quyền truy cập đối với các tài nguyên cơ sở dữ liệu;

- Ghi nhật ký đối với các truy cập cơ sở dữ liệu, các thao tác đối với cấu hình cơ sở dữ liệu;
- Có phương án sao lưu dữ liệu, bảo đảm khôi phục dữ liệu trong trường hợp cần thiết;
- Bảo đảm có thuật toán mã hóa phù hợp yêu cầu bảo đảm tính bí mật và khả năng xử lý của hệ thống;
- Rà soát, cập nhật các bản vá, các bản sửa lỗi hệ quản trị cơ sở dữ liệu theo định kỳ và theo khuyến cáo của nhà cung cấp;
- Có các giải pháp ngăn chặn các hình thức tấn công cơ sở dữ liệu.

3.1.4.3.2.7 Yêu cầu về khung phát triển phần mềm an toàn

Quy định	Nhiệm vụ	Ví dụ triển khai
1.Chuẩn bị của tổ chức (PO)		
1.1. Xác định yêu cầu bảo mật cho phát triển phần mềm (PO.1): Đảm bảo tính bảo mật luôn gắn liền với SDLC. Bao gồm các yêu cầu từ các nguồn nội bộ (ví dụ: chính sách, mục tiêu kinh doanh và chiến lược quản lý rủi ro của tổ chức) và các nguồn bên ngoài (ví dụ: luật và quy định hiện hành).	**PO.1.1:** Xác định và ghi lại các yêu cầu bảo mật cho cơ sở hạ tầng trong quá trình phát triển phần mềm, đồng thời thực hiện các yêu cầu này liên tục trong suốt SDLC.	• Xác định chính sách bảo mật cho cơ sở hạ tầng phát triển phần mềm, bao gồm cả việc bảo mật điểm cuối xuyên suốt SDLC và duy trì tính bảo mật liên tục.
		• Xác định chính sách để đảm bảo các quy trình phát triển phần mềm xuyên suốt SDLC và duy trì tính bảo mật liên tục, bao gồm các phần mềm nguồn mở, phần mềm bên thứ ba đang được sử dụng phục vụ phần mềm được phát triển.
		• Định kỳ thực hiện kiểm tra, đánh giá về bảo mật an toàn thông tin. Việc kiểm tra đánh giá ngoài thực hiện định kỳ, còn cần phải thực hiện khi có các yêu cầu mới từ các nguồn nội bộ và các nguồn bên ngoài, hoặc ngay khi có một sự cố lỗ hổng bảo mật lớn xảy ra.
		• Đào tạo, nâng cao kiến thức về an toàn thông tin cho nhân viên để đáp ứng được với các yêu cầu thực tế.
	PO.1.2: Xác định và áp dụng các yêu cầu bảo mật đối với các phần mềm để đáp ứng tiến độ đề ra.	• Xác định các chính sách, các yêu cầu từ khâu thiết kế và bảo đảm kiến trúc phần mềm dựa trên quản trị rủi ro.
		• Xác định các chính sách bảo mật cho phần mềm và kiểm tra tính tuân thủ quy định trong SDLC.
		• Phân tích rủi ro khi tích hợp nhiều công cụ, công nghệ trong cùng sản phẩm. Sau khi phân tích rủi ro, cần đề xuất các công cụ, công nghệ khác có khả năng giảm thiểu các rủi ro.
		• Quy định các yêu cầu về sao lưu và thời gian lưu trữ phần mềm dựa trên mô hình SDLC.

Quy định	Nhiệm vụ	Ví dụ triển khai
		• Tuân thủ các chính sách như: Vòng đời phần mềm, thông báo cho bên sử dụng về thời hạn và hỗ trợ đối với phần mềm.
		Kiểm tra, đánh giá tính bảo mật của phần mềm.
	PO.1.3: Các yêu cầu cho nhà cung cấp sản phẩm, dịch vụ.	• Xác định yêu cầu bảo mật trong các hợp đồng và tại các cam kết của bên cung cấp phần mềm.
		• Xác định các tiêu chí liên quan đến bảo mật trong quá trình lựa chọn, phát triển phần mềm.
		• Yêu cầu nhà cung cấp sản phẩm, dịch vụ chứng minh nguồn gốc và tính bảo mật của sản phẩm, cần bảo đảm tính bảo mật của sản phẩm phải tuân thủ các yêu cầu bảo mật của tổ chức.
		• Thiết lập và tuân thủ các quy trình đánh giá rủi ro.
		• Thiết lập và tuân theo các quy trình để giải quyết rủi ro.
1.2. Thực hiện các vai trò và trách nhiệm (PO.2): Đảm bảo mọi yếu tố liên quan đến SDLC được chuẩn bị để thực hiện các vai trò và trách nhiệm liên quan đến SSDF trong suốt quá trình phát triển phần mềm.	**PO.2.1:** Xác định vai trò và trách nhiệm cho các vị trí của SSDF. Thường xuyên đánh giá, xác định lại vai trò và trách nhiệm của các thành viên trong nhóm.	• Xác định vai trò và trách nhiệm liên quan đến SSDF cho tất cả các thành viên của nhóm phát triển phần mềm.
		• Tích hợp các vai trò bảo mật vào quy trình phát triển phần mềm.
		• Xác định vai trò về bảo đảm an toàn thông tin của từng vị trí (từ quản lý cấp cao đến nhân viên và bên sử dụng vận hành sản phẩm) có liên quan đến SDLC.
		• Định kỳ kiểm tra, đánh giá vai trò, trách nhiệm của từng vị trí nhân viên.
		• Đào tạo, nâng cao kiến thức về những xu hướng mới cho từng cá nhân liên quan.
	PO.2.2: Đào tạo, nâng cao kiến thức về an toàn thông tin cho tất cả nhân viên. Định kỳ kiểm tra, đánh giá trình độ của nhân sự để cập nhật, bổ sung kiến thức cần	• Xác định yêu cầu kiến thức đào tạo đối với từng đối tượng.
		• Xác định loại hình đào tạo hoặc chương trình đào tạo cần thiết cho từng vị trí nhân sự.
		• Tổ chức các khóa học phù hợp với từng vị trí nhân viên.
		• Kiểm tra, đánh giá năng lực định kỳ của từng nhân viên từ đó có định hướng và thay đổi chương trình đào tạo cho phù hợp.

Quy định	Nhiệm vụ	Ví dụ triển khai
	thiết về an toàn thông tin.	
	PO.2.3: Xây dựng và áp dụng các quy định về SDLC cùng các vai trò và trách nhiệm liên quan đến SSDF.	• Chỉ định một lãnh đạo hoặc nhóm lãnh đạo chịu trách nhiệm về toàn bộ quy trình phát triển phần mềm an toàn.
		• Nâng cao nhận thức về các rủi ro sẽ gặp khi phát triển phần mềm không tích hợp tính bảo mật trong suốt vòng đời phát triển và giảm thiểu rủi ro do thực tiễn SSDF cung cấp.
		• Phổ biến kiến thức cho nhân viên có vai trò, trách nhiệm liên quan đến SSDF về các quy định và tầm quan trọng của SSDF đối với tổ chức.
1.3. Triển khai các công cụ hỗ trợ (PO.3): Sử dụng tự động hóa để giảm bớt nhân lực, cải thiện độ chính xác, tính nhất quán, khả năng sử dụng và tính toàn diện của các phương thức bảo mật trong suốt SDLC, cung cấp cách lập hồ sơ và trình bày việc sử dụng phương pháp.	**PO.3.1:** Chỉ định công cụ hoặc nhóm công cụ cần thiết để giảm thiểu rủi ro và bảo đảm tính bảo mật khi tích hợp các công cụ.	• Xây dựng danh mục công cụ và xác định công cụ phù hợp đối với từng danh mục.
		• Xác định công cụ bảo mật để tích hợp vào chuỗi các công cụ dành cho nhà phát triển.
		• Đánh giá khả năng/năng lực của từng công cụ.
		• Sử dụng công nghệ tự động để quản lý và điều phối chuỗi công cụ.
		• Thường xuyên tối ưu công cụ để phù hợp với hoạt động, đặc thù ngôn ngữ, framework tại tổ chức.
	PO.3.2: Thực hiện theo các phương pháp bảo mật được khuyến nghị để triển khai và duy trì các công cụ và chuỗi các công cụ.	• Kiểm tra, đánh giá tính bảo mật của từng công cụ.
		• Tích hợp các công cụ và tuân theo các quy trình phát triển phần mềm hiện có.
		• Áp dụng công nghệ mới và các quy trình cần thiết cho các bản dựng mẫu.
		• Cập nhật, nâng cấp hoặc thay thế các công cụ có tính năng vá lỗ hổng bảo mật và thêm các tính năng mới cho công cụ.
		• Định kỳ kiểm tra, đánh giá các công cụ để phát hiện lỗ hổng bảo mật.
		• Định kỳ kiểm tra, đánh giá tính toàn vẹn của sản phẩm để xác định các rủi ro tiềm ẩn.
	PO.3.3: Cài đặt, cấu hình các công cụ để đáp ứng về tính năng	• Sử dụng công cụ sẵn có để tạo sự kiện kiểm tra về các hành động liên quan đến phát triển an toàn.
		• Xây dựng và áp dụng các chính sách bảo mật và sao lưu dữ liệu.

Quy định	Nhiệm vụ	Ví dụ triển khai
	bảo mật theo quy định	
1.4. Xác định và sử dụng các tiêu chí cho bảo mật phần mềm kiểm tra, đánh giá (PO.4): Bảo đảm phần mềm theo SDLC đáp ứng các tiêu chí khi được kiểm tra, đánh giá bảo mật trong quá trình phát triển.	**PO.4.1:** Xác định tiêu chí kiểm tra, đánh giá tính bảo mật của phần mềm và theo dõi trong suốt SDLC.	• Đảm bảo các tiêu chí về quản lý rủi ro an toàn thông tin.
		• Xác định các chỉ số hiệu suất chính (KPI) và các chỉ số rủi ro chính (KRI) để bảo mật phần mềm.
		• Bổ sung các tiêu chí bảo mật phần mềm vào các nội dung kiểm tra, đánh giá.
		• Theo dõi, phát hiện các bước bỏ qua không tuân thủ quy định vè kiểm ưa đánh giá yêu cầu bảo mật.
		• Báo cáo kết quả kiểm ưa, đánh giá an toàn thông tin.
	PO.4.2: Thực hiện các quy trình để thu thập và bảo vệ thông tin cần thiết để bảo đảm các tiêu chí về an toàn thông tin.	• Sử dụng các công cụ để thu thập thông tin cho việc đưa ra các yêu cầu bảo mật.
		• Bổ sung các công cụ cần thiết để hỗ trợ việc thu thập thông tin hỗ ượ các tiêu chí.
		• Tự động hóa các quy trình áp dụng các tiêu chí.
		• Chỉ cho phép nhân viên được ủy quyền để truy cập thông tin thu thập và ngăn chặn bất kỳ thay đổi hoặc xóa thông tin.
1.5. Thực hiện và duy trì bảo mật môi trường phát triển phần mềm (PO.5): Bảo đảm các yếu tố tác động từ môi trường để quy trình phát triển phần mềm được bảo vệ khỏi các mối đe dọa từ bên	**PO.5.1:** Tách biệt và bảo vệ từng môi trường liên quan đến phát triển phần mềm.	• Áp dụng phương pháp xác thực, nhận dạng riêng biệt với xác thực dựa trên rủi ro và quyền truy cập có điều kiện cho từng môi trường khác nhau.
		• Sử dụng phân đoạn mạng và kiểm soát truy cập để tách môi trường phát triển thành từng phần, từng khâu riêng biệt để giảm thiểu ảnh hưởng khi bị tấn công.
		• Triển khai xác thực và hạn chế các liên kết để tránh bị ảnh hưởng lẫn nhau giữa các môi trường khi xuất hiện các rủi ro. Chỉ sử dụng Internet khi thật sự cần thiết.
		• Thường xuyên ghi nhật ký giám sát và kiểm tra các môi trường liên kết giữa các thành phần.
		• Thực hiện ghi log thường xuyên và giám sát các hoạt động để kịp thời đưa ra các cảnh báo và có biện pháp ứng phó khi xuất hiện các sự cố mất an toàn thông tin mạng.

Quy định	Nhiệm vụ	Ví dụ triển khai
trong và bên ngoài.		• Cấu hình các biện pháp kiểm soát bảo mật và công cụ thực thi bảo mật để bảo vệ an toàn cho môi trường phát triển phần mềm.
		• Thường xuyên kiểm tra dữ liệu các phần mềm và kiểm tra, đánh giá lỗ hổng bảo mật trên các phần mềm đó.
	PO.5.2: Thực hiện quản lý, đánh giá rủi ro an toàn thông tin cho các sản phẩm, phần mềm trước khi đưa vào sử dụng.	• Cấu hình phần mềm trước khi đưa vào sử dụng dựa trên các quy định đã được phê duyệt.
		• Cấu hình phần mềm trước khi đưa vào sử dụng để cung cấp chức năng, dịch vụ cần thiết cho người dùng.
		• Liên tục theo dõi tình trạng bảo mật của các sản phẩm, phần mềm trước khi đưa vào sử dụng.
		• Áp dụng các biện pháp bảo mật và công cụ đánh giá, bảo đảm tính bảo mật cho các sản phẩm, phần mềm trước khi đưa vào sử dụng.
		• Yêu cầu xác thực đa yếu tố cho quyền truy cập vào các sản phẩm, phần mềm trước khi đưa vào sử dụng.
2.Bảo vệ phần mềm		
2.1. Bảo vệ tất cả các dạng mã nguồn không bị xâm nhập và giả mạo trái phép (PS.1): Ngăn chặn những thay đổi trái phép đối với mã nguồn.	**PS.1.1:** Lưu trữ các dạng mã, bao gồm cả mã nguồn và mã thực thi, chỉ những người được ủy quyền, các công cụ, các công cụ mới có thể truy cập khi cần thiết.	• Lưu trữ tất cả mã nguồn và hạn chế quyền truy cập. Ví dụ, các mã nguồn mở được sử dụng dùng cho mục đích truy cập công cộng, trường hợp này tính toàn vẹn và tính khả dụng phải được bảo vệ.
		• Sử dụng các tính năng kiểm soát để theo dõi các thay đổi được thực hiện đối với mã.
		• Xem xét và phê duyệt tất cả các thay đổi được thực hiện đối với mã sau khi mã đã được tự động quét các lỗ hổng bảo mật.
		• Sử dụng chữ ký số trên mã nguồn/mã thực thi để bảo vệ tính toàn vẹn của chúng.
		• Sử dụng mật mã (ví dụ: hàm băm mật mã) để giúp bảo vệ tính toàn vẹn của tệp.
2.2. Cung cấp cơ chế xác minh tính toàn vẹn của phần mềm (PS.2):	**PS.2.1:** Cam kết bảo đảm tính toàn vẹn cho người mua và người sử dụng phần mềm.	• Với các tệp được công bố, cung cấp mã băm trên các trang web an toàn.
		• Cung cấp các chứng chỉ đã được thẩm định bởi cơ quan có thẩm quyền, thiết lập ký mã khóa để hệ điều hành, công cụ và dịch vụ khác có thể xác nhận tính hợp lệ của chữ ký trước khi sử dụng.

Quy định	Nhiệm vụ	Ví dụ triển khai
Bảo đảm người mua và người sử dụng phần mềm là hợp pháp, không giả mạo.		• Định kỳ đánh giá quy trình ký mã khóa, bao gồm: Gia hạn chứng chỉ, luân phiên, thu hồi và bảo vệ.
2.3. Sao lưu bảo đảm tính bảo mật cho các phần mềm (PS.3): Sao lưu các phần mềm để giúp xác định, phân tích và loại bỏ các lỗ hổng được phát hiện trong phần mềm sau khi được đưa vào sử dụng.	**PS.3.1:** Lưu trữ an toàn các tệp cần thiết, các thông tin bổ sung (ví dụ: thông tin xác minh tính toàn vẹn, thông tin xuất xứ) của mỗi phần mềm đã được đưa vào sử dụng.	• Thiết lập quyền truy cập cho các đối tượng có thể sử dụng dữ liệu với mục đích kiểm tra, đánh giá.
		• Sao lưu và bảo đảm tính toàn vẹn của phần mềm đã được đưa vào sử dụng.
		• Mã hóa các tệp dữ liệu nhạy cảm bằng thuật toán mã hóa mạnh.
	PS.3.2: Thu thập, bảo vệ, duy trì và chia sẻ thông tin xuất xứ cho tất cả các thành phần của mỗi bản phát hành phần mềm (ví dụ: thông tin về ngày phát hành, năm phát hành, số phiên bản,... trong bản phát hành của mỗi phần mềm)	• Cung cấp thông tin xuất xứ cho cá nhân, tổ chức mua phần mềm để phù hợp với chính sách của tổ chức.
		• Cung cấp thông tin xuất xứ cho các nhóm ứng cứu sự cố để hỗ trợ trong việc giảm thiểu lỗ hổng phần mềm.
		• Cập nhật thường xuyên và liên tục thông tin xuất xứ để theo dõi sự thay đổi của phần mềm khi cập nhật.
3.Sản xuất phần mềm đáp ứng yêu cầu bảo mật tốt (PW)		
3.1. Thiết kế phần mềm để đáp ứng các yêu cầu	**PW.1.1:** Áp dụng phương pháp mô hình hóa rủi ro để	• Đào tạo, nâng cao nhận thức về bảo mật, an toàn thông tin cho nhóm phát triển hoặc cộng tác với cá nhân, tổ chức chuyên về mô hình rủi ro để có biện pháp xử lý, giảm thiểu.

Quy định	Nhiệm vụ	Ví dụ triển khai
bảo mật và giảm thiểu rủi ro bảo mật (PW.1): Xác định và đánh giá các yêu cầu bảo mật cho phần mềm; xác định những rủi ro bảo mật mà phần mềm có thể gặp phải trong quá trình hoạt động và cách thiết kế của phần mềm nhằm giảm thiểu những rủi ro.	đánh giá tính bảo mật phần mềm (VD: mô hình hóa mối đe dọa, mô hình hóa cuộc tấn công; mô hình hóa lược đồ tấn công).	• Thực hiện các đánh giá chuyên sâu hơn với các khu vực có nguy cơ rủi ro về bảo mật cao.
		• Rà soát các báo cáo và số liệu thống kê về lỗ hổng bảo mật phần mềm.
		• Phân loại dữ liệu để xác định từng loại dữ liệu mà phần mềm sẽ tương tác.
	PW.1.2: Sao lưu các yêu cầu về bảo mật phần mềm và các rủi ro để đưa ra các phương án thiết kế phù hợp.	• Ghi lại tác động đối với từng rủi ro, bao gồm các phương án giảm thiểu và lý do của bất kỳ trường hợp ngoại lệ nào đã được phê duyệt đối với các yêu cầu bảo mật.
	PW.1.3: Xây dựng các yêu cầu về tính năng và dịch vụ bảo mật. (ví dụ: tích hợp với hệ thống quản lý nhật ký, quản lý danh tính, kiểm soát truy cập và quản lý lỗ hổng bảo mật hiện có).	• Xây dựng thư viện phần mềm gồm các mô-đun để hỗ trợ các tính năng và dịch vụ bảo mật được tiêu chuẩn hóa.
		• Đưa ra các yêu cầu về tính năng và dịch vụ bảo mật trong quá trình phát triển phần mềm.
3.2. Rà soát, đánh giá thiết kế phần mềm để xác minh sự tuân thủ với các yêu cầu bảo mật và các yếu tố rủi ro (PW.2): Đảm	**PW.2.1:** Yêu cầu cá nhân, đơn vị độc lập với đơn vị thiết kế kiểm tra đánh giá rủi ro và các yêu cầu bảo mật.	• Rà soát từ khâu thiết kế phần mềm bảo đảm các yêu cầu, tính năng bảo mật.
		• Rà soát, đánh giá các yếu tố rủi ro trong quá trình thiết kế phần mềm.
		• Rà soát, đánh giá các phương án xử lý rủi ro.
		• Yêu cầu nhà thiết kế phần mềm sửa lỗi để đáp ứng các yêu cầu.
		• Thay đổi thiết kế hoặc chiến lược xử lý rủi ro nếu không thể đáp ứng các yêu cầu bảo mật.

Quy định	Nhiệm vụ	Ví dụ triển khai
bảo phần mềm đáp ứng các yêu cầu bảo mật và xử lý rủi ro.		
3.3. Kế thừa, phát triển tính năng bảo mật hiện có trên phần mềm thay vì đầu tư, mua sắm phần mềm mới bảo mật mới (PW.3): Giảm chi phí phát triển phàn mềm, đẩy nhanh quá trình phát triển phần mềm và giảm khả năng gia tăng lỗ hổng bảo mật vào phần mềm bằng cách sử dụng lại các mô-đun và dịch vụ phần mềm đã được kiểm tra tình trạng bảo mật.	**PW.3.1:** Mua sắm, đầu tư các thành phần phần mềm được bảo mật tốt (ví dụ: thư viện phần mềm, mô-đun, phần mềm trung gian...) từ các nhà phát triển và bên thứ ba.	• Rà soát, đánh giá các thành phần phần mềm trước khi đưa vào sử dụng.
		• Kiểm thử mã nguồn cho cho từng thành phần của phần mềm và đánh giá rủi ro có thể gây ra.
		• Xây dựng thư viện phần mềm để lưu trữ các thành phần mã nguồn mở đã được kiểm định và kiểm duyệt.
		• Xác định những thành phần phải có trong phát triển phần mềm.
	PW.3.2: Xây dựng các thành phần phần mềm được bảo mật tuân theo SDLC để đáp ứng các nhu cầu phát triển mà phần mềm của bên thứ ba không thể đáp ứng.	• Tuân thủ các yêu cầu bảo mật để phát triển phần mềm an toàn.
		• Xác định những thành phần phải có trong phát triển phần mềm.
	PW.3.3: Đã chuyển lên mục PW.1.3	
	PW.3.4: Kiểm tra, đánh giá tính tuân thủ các yêu cầu bảo mật ở các thành phần phần mềm, mã nguồn mở.	• Rà soát, đánh giá lỗ hổng bảo mật chưa được sửa chữa, khắc phục.

Quy định	Nhiệm vụ	Ví dụ triển khai
	PW.3.5: Rà soát, kiểm tra tính toàn vẹn của các thành phần phần mềm.	• Đảm bảo việc rà soát các thành phần của phần mềm được diễn ra định kỳ, thường xuyên; Phát hiện kịp thời, hạn chế xuất hiện lỗ hổng.
		• Lên phương án xử lý phần mềm không còn khả dụng.
		• Xác nhận tính toàn vẹn của các thành phần phần mềm thông qua chữ ký số hoặc các cơ chế khác.
3.4. Phát triển phần mềm bằng dựa trên các quy tắc bảo mật (PW.4): Giảm số lượng lỗ hổng bảo mật, giảm chi phí trong phần mềm với việc loại bỏ các lỗ hổng trong quá trình tạo mã nguồn, bằng cách tuân theo các tiêu chí về mức độ nghiêm trọng của lỗ hổng bảo mật do tổ chức xác định.	**PW.4.1:** Tuân thủ tất cả các phương pháp mã hóa an toàn phù hợp với ngôn ngữ và môi trường phát triển để đáp ứng các yêu cầu của tổ chức.	• Xác thực đầu vào, xác thực và mã hóa đầu ra.
		• Tránh sử dụng các chức năng và cuộc gọi không an toàn.
		• Cung cấp khả năng ghi nhật ký và truy vết.
		• Sử dụng các IDE có khả năng bảo mật tốt.
		• Kiểm tra các lỗ hổng bảo mật khác, thường gặp đối với môi trường và ngôn ngữ phát triển.
		• Yêu cầu nhà phát triển xem xét mã nguồn phần mềm để bổ sung (không thay thế), việc đánh giá mã do người hoặc công cụ khác thực hiện.
3.5. Cấu hình môi trường phát triển tích hợp, biên dịch, trình thông	**PW.5.1:** Sử dụng trình biên dịch, trình thông dịch và xây dựng các công cụ cung cấp các tính năng	• Sử dụng các bản cập nhật của công cụ biên dịch, công cụ thông dịch và công cụ thiết lập.
		• Tuân thủ các quy trình quản lý thay đổi khi triển khai hoặc cập nhật các công cụ biên dịch, công cụ thông dịch và công cụ thiết lập, đồng thời kiểm tra tất cả các thay đổi không hợp lệ đối với các công cụ.

Quy định	Nhiệm vụ	Ví dụ triển khai
dịch và xây dựng các quy trình để cải thiện khả năng bảo mật (PW.5): Giảm số lượng lỗ hổng bảo mật trong phần mềm, loại bỏ các lỗ hổng trước khi kiểm thử để giảm chi phí.	cải thiện tính bảo mật.	• Xác nhận thường xuyên tính xác thực và tính toàn vẹn của các công cụ biên dịch, công cụ thông dịch và công cụ thiết lập.
	PW.5.2: Xác định các tính năng của trình biên dịch, trình thông dịch, công cụ thiết lập và cách cấu hình từng tính năng, sau đó triển khai và sử dụng các cấu hình đã được phê duyệt.	• Bật các tính năng của trình biên dịch, tạo ra các cảnh báo cho mã bảo mật kém an toàn trong quá trình biên dịch.
		• Tiến hành kiểm thử để đảm bảo các tính năng hoạt động tốt, tránh gây ra sự cố vận hành hoặc các sự cố khác.
		• Xác minh liên tục các cấu hình đã phê duyệt và đang sử dụng.
		• Cung cấp thông tin về trình biên dịch, trình thông dịch và cấu hình công cụ thiết lập trong cơ sở kiến thức của các nhà phát triển có thể truy cập, tìm kiếm và tái tạo trong môi trường phát triển cục bộ.
3.6. Đánh giá và phân tích mã Human-Readable để xác định các lỗ hổng và xác minh sự tuân thủ với các yêu cầu bảo mật (PW.6): Xác định, khắc phục các lỗ hổng trước khi phần mềm được đưa vào sử dụng nhằm ngăn chặn việc khai thác lỗ hổng bảo mật. Sử dụng các công cụ, tính năng phát hiện lỗ hổng	**PW.6.1:** Xác định hai phương án: Thứ nhất, đánh giá mã nguồn được thực hiện trực tiếp bởi một nhân sự chuyên trách, thứ hai, sử dụng các công cụ tự động. Sẽ tùy vào tình hình thực tế của cơ quan tổ chức.	• Tuân thủ các chính sách và hướng dẫn của tổ chức về thời điểm nên thực hiện kiểm tra mã nguồn và cách thức tiến hành.
		• Lựa chọn phương pháp đánh giá hoặc phân tích mã nguồn dựa trên giai đoạn của phần mềm.
	PW.6.2: Kiểm tra, đánh giá, phân tích mã dựa trên các tiêu chuẩn an toàn thông tin. Phân loại và đưa ra phương án khắc phục lỗ hổng bảo mật.	• Thực hiện kiểm tra, đánh giá ngang hàng về mã nguồn
		• Yêu cầu chuyên gia thực hiện đánh giá để kiểm tra mã cho backdoor và mã độc khác.
		• Áp dụng công cụ phân tích tĩnh để tự động kiểm tra lỗ hổng bảo mật và đánh giá sự tuân thủ các tiêu chuẩn mã hóa an toàn.
		• Xác minh tính tuân thủ của mã thông qua các tiêu chí kiểm tra đánh giá.
		• Sử dụng các công cụ tự động để xác định và khắc phục các hoạt động phần mềm không an toàn.

Quy định	Nhiệm vụ	Ví dụ triển khai
có sẵn để giảm tải nguồn lực, chi phí, thời gian.		• Xác định và ghi lại nguyên nhân của mỗi vấn đề đã phát hiện.
3.7. Kiểm tra thực thi luật để xác định lỗ hổng và xác minh sự tuân thủ với yêu cầu bảo mật (PW.7): Xác định các lỗ hổng có thể xử lý trước khi phần mềm được đưa vào sử dụng nhằm tái khai thác. Sử dụng các phương pháp tự động làm giảm nguồn lực trong việc phát hiện các lỗ hổng.	**PW.7.1:** Xác định việc thực hiện kiểm tra mã thực thi để xác định và loại bỏ các lớp lỗ hổng không được đề cập trong các bài đánh giá, phân tích hoặc thử nghiệm trước đó.	• Tuân thủ các chính sách hoặc nguyên tắc của tổ chức về thời điểm nên thực hiện kiểm tra mã và cách thức tiến hành.
	PW.7.2: Triển khai thực hiện phạm vi, thiết kế, thực hiện kiểm tra đánh giá và ghi lại kết quả, bao gồm ghi lại và xử lý tất cả các vấn đề đã phát hiện và các biện pháp khắc phục được đề xuất trong quy trình làm việc của nhóm phát triển hoặc qua hệ thống theo dõi sự cố.	• Thực hiện kiểm tra chức năng của các tính năng bảo mật
		• Tích hợp kiểm tra lỗ hổng động vào bộ kiểm thử tự động của dự án.
		• Kết hợp các bài đánh giá lỗ hổng bảo mật trước đây vào bài đánh giá của dự án để đảm bảo các lỗi không xuất hiện lại.
		• Xem xét cơ sở hạ tầng và công nghệ phần mềm sẽ sử dụng trong khi phát triển các kế hoạch thử nghiệm.
		• Sử dụng các công cụ kiểm tra fuzz testing để tìm các vấn đề với việc xử lý đầu vào.
		• Sử dụng phương pháp kiểm thử xâm nhập trong trường hợp có sẵn mã nguồn nhằm nâng cao khả năng đánh giá.
		• Xác định và ghi lại nguyên nhân của từng vấn đề được phát hiện.
		• Ghi lại kinh nghiệm qua việc phân tích nguyên nhân lỗ hổng bảo mật để đưa ra hướng dẫn, khuyến nghị cho lập trình viên phát triển phần mềm có thể truy cập và tìm kiếm.
3.8. Cấu hình phần mềm	**PW.8.1:** Xác lập chính sách bảo	• Lên kế hoạch kiểm tra để đảm bảo các cài đặt cấu hình mặc định hoạt động một cách tốt nhất, không

Quy định	Nhiệm vụ	Ví dụ triển khai
cài đặt bảo mật theo mặc định (PW.8): cải thiện tình bảo mật của phần mềm tại thời điểm cài đặt giảm khả năng phần mềm được triển khai với cài đặt bảo mật yếu.	mật chuẩn để cài đặt, cấu hình bảo mật. Giúp các cài đặt mặc định được an toàn, không làm tác động tới các chức năng bảo mật được cung cấp bởi các nền tảng, cơ sở hạ tầng mạng.	gây ra điểm yếu và ảnh hưởng đến những hoạt động khác của hệ thống.
	PW.8.2: Triển khai cài đặt mặc định (hoặc nhóm cài đặt mặc định, nếu có), ghi lại từng cài đặt cho quản trị viên phần mềm.	• Xác minh cấu hình đã được phê duyệt có sẵn cho phần mềm.
		• Sao lưu mục đích của từng cài đặt, các tùy chọn, giá trị mặc định, mức độ liên quan đến bảo mật, tác động hoạt động tiềm năng và mối quan hệ với các cơ sở khác.
		• Sử dụng các cơ chế kỹ thuật để ghi lại cách mỗi cài đặt có thể được thực hiện và đánh giá bởi quản trị viên phần mềm.
		• Lưu trữ cấu hình mặc định ở định dạng có thể sử dụng được và tuân theo kiểm soát thay đổi thực hành để sửa đổi nó (ví dụ: cấu hình dưới dạng mã).
4. ứng phó với các lỗ hổng bảo mật (RV)		
4.1. Xác định và xác nhận các lỗ hổng trên một nền tảng đang triển khai (RV.1): Đảm bảo các lỗ hổng được xác định sớm để có phương án điều chỉnh kịp thời, giảm	**RV.1.1:** Thu thập thông tin từ người sử dụng, các nguồn công khai về các lỗ hổng tiềm năng trong phần mềm và các mô- đun phần mềm bên thứ ba sử dụng.	• Thiết lập chương trình báo cáo về các lỗ hổng bảo mật, giúp các chuyên gia bảo mật dễ dàng trong việc tiếp cận, tìm hiểu mã nguồn và báo cáo các lỗ hổng có thể gặp.
		• Giám sát cơ sở dữ liệu về lỗ hổng bảo mật, danh sách gửi thư bảo mật và các nguồn khác về báo cáo lỗ hổng thông qua các phương tiện thủ công hoặc tự động.
		• Sử dụng các nguồn thông tin tình báo về mối đe dọa để hiểu rõ hơn về cách các lỗ hổng đang bị khai thác.
		• Thường xuyên kiểm tra nguồn gốc và phần mềm dữ liệu cho mỗi bản phát hành phần mềm đang được

Quy định	Nhiệm vụ	Ví dụ triển khai
khả năng bị tấn công.		sử dụng để xác định các lỗ hổng mới tiềm ẩn trong các ứng dụng.
		• Quản lý danh sách các thư viện, các thành phần, framework có liên quan bao gồm tên và phiên bản đang sử dụng
	RV.1.2: Đánh giá, phân tích và kiểm tra mã nguồn phần mềm để xác định việc phần mềm không tồn tại những lỗ hổng bảo mật.	• Cấu hình chuỗi công cụ để thực hiện phân tích và kiểm tra mã tự động một cách thường xuyên hoặc liên tục.
		• Chủ động truy xuất nguồn gốc và dữ liệu của phần mềm nhằm xác định kịp thời các lỗ hổng mới của phần mềm.
	RV.1.3: Có chính sách giải quyết việc khắc phục lỗ hổng bảo mật, đồng thời thực hiện các vai trò, trách nhiệm và quy trình cần thiết để hỗ trợ chính sách.	• Có Nhóm ứng phó sự cố về bảo mật sản phẩm (PSIRT) và các quy trình để xử lý các phản hồi đối với các báo cáo và sự cố về lỗ hổng bảo mật.
		• Có nhật ký ghi lại những đánh giá, phản hồi về xử lý lỗ hổng, zero-days, lỗ hổng đang bị khai thác và những sự cố nghiêm trọng liên quan đến cộng đồng và ứng dụng.
4.2. Đánh giá và loại bỏ các lỗ hổng (RV.2): Để đảm bảo các lỗ hổng bảo mật được khắc phục kịp thời, tránh được những rủi ro bị tấn công	**RV.2.1:** Phân tích từng lỗ hổng để thu thập đầy đủ thông tin, đưa ra kế hoạch khắc phục.	• Sử dụng phần mềm theo dõi sự cố để ghi lại sự kiện rủi ro.
		• Dự trù kế hoạch để khắc phục các lỗ hổng
		• Tính toán ảnh hưởng của việc khai thác lỗ hổng.
		• Tính toán mọi phương án cần thiết để lập kế hoạch khắc phục lỗ hổng bảo mật.
	RV.2.2: Phát triển và thực hiện kế hoạch khắc phục cho từng lỗ hổng.	• Lập kế hoạch phản ứng nhanh với các lỗ hổng trước mắt, trước khi có những biện pháp khắc phục lâu dài.
		• Cung cấp biện pháp khắc phục cho người sử dụng sản phẩm thông qua thiết bị tự động và cơ chế phân phối đáng tin cậy.
		• Phát triển và ban hành các khuyến cáo bảo mật cho người sử dụng, bao gồm những mô tả về thay đổi trong phần mềm, cấu hình, cài đặt.

Quy định	Nhiệm vụ	Ví dụ triển khai
4.3. Phân tích chuyên sâu các lỗ hổng (RV.3): Giảm thiểu các lỗ hổng trong tương lai.	**RV.3.1:** Phân tích tất cả các lỗ hổng đã xác định để tìm ra nguyên nhân ban đầu.	• Ghi lại nguyên nhân của mỗi vấn đề khi được phát hiện.
		• Ghi lại kinh nghiệm qua việc phân tích nguyên nhân lỗ hổng để đưa ra hướng dẫn, khuyến nghị cho lập trình viên phát triển phần mềm có thể truy cập và tìm kiếm.
	RV.3.2: Phân tích nguyên nhân lỗ hổng theo từng thời điểm và từng giai đoạn để đưa ra những hướng dẫn chính xác.	• Ghi lại kinh nghiệm qua việc phân tích nguyên nhân lỗ hổng để đưa ra hướng dẫn, khuyến nghị cho lập trình viên phát triển phần mềm có thể truy cập và tìm kiếm.
		• Tích hợp thêm cơ chế tự động phát hiện vào các chuỗi công cụ để tự động phát hiện các nguyên nhân lỗ hổng trong tương lai.
	RV.3.3: Chủ động lên kế hoạch rà quét lỗ hổng trong các phần mềm, và đưa ra cách khắc phục.	Xem PW.6 và PW.7.
	RV.3.4: Rà soát lại SDLC để chủ động đưa ra những cập nhật thích hợp nhằm ngăn chặn, giảm khả năng của lỗ hổng trong các bản cập nhật phần mềm hoặc trong phần mềm mới được tạo.	• Ghi lại kinh nghiệm qua việc phân tích nguyên nhân lỗ hổng để đưa ra hướng dẫn, khuyến nghị cho lập trình viên phát triển phần mềm có thể truy cập và tìm kiếm. • Lập kế hoạch và chủ động lên phương án thực hiện chỉnh sửa thay đổi đối với các hướng dẫn của SSDF.

3.1.4.4. Yêu cầu khác

3.1.4.4.1. Ưu tiên sản phẩm vận hành thử, sử dụng thử trong lựa chọn sản phẩm thuê

Vận hành thử, sử dụng thử phần mềm là phương pháp kiểm tra, đánh giá tính phù hợp của phần mềm có phù hợp với các yêu cầu đặt ra ban đầu hay không? Đây là bước

quan trọng để tìm kiếm những sản phẩm phù hợp với những yêu cầu đặt ra của chủ sử dụng, đơn vị khai thác sử dụng phần mềm sau này.

Trong quá trình vận hành thử, chạy thử sản phẩm sẽ tìm ra những ưu điểm và nhược điểm có phù hợp với nhu cầu sử dụng hay không? Giúp đơn vị khắc phục được những phần tử, những chức năng hoặc bất kỳ lỗi nào để đơn vị cho thuê phần mềm khắc phục, sửa chữa.

Trên thực tế, Trung tâm đã cho chạy thử sản phẩm Hệ thống phần mềm bệnh án điện tử, đã đánh giá đạt yêu cầu với mục đích ban đầu của Trung tâm. Giúp người sử dụng (Cán bộ y tế của Trung tâm) được trải nghiệm phần mềm từ đó làm quen với phần mềm giúp giảm thời gian đào tạo, chuyển giao công nghệ và hướng dẫn sử dụng sau này.

Chính vì những yếu tố đó, đơn vị tư vấn đề xuất ưu tiên lựa chọn sản phẩm đã được vận hành thử, chạy thử tại Trung tâm. Tuy nhiên, để đảm bảo tính khách quan trong việc lựa chọn sản phẩm, sản phẩm đã chạy thử, vận hành thử chỉ mang tính định hướng sản phẩm thuê sau này và chỉ là 1 tiêu chí ưu tiên trong quá trình lựa chọn khi các sản phẩm tương tự nhau (được đánh giá kỹ thuật là tương đương).

3.1.4.4.2. Yêu cầu về tiêu chí ưu tiên đối với phần mềm sản xuất trong nước

Căn cứ vào mục 2, điều 4 thông tư 40/2020/TT-BTTTT ngày 30/11/2020 của Bộ Thông tin và Truyền thông Hệ thống phần mềm bệnh án điện tử của đơn vị cung cấp phải là sản phẩm, dịch vụ do cá nhân là người Việt Nam sản xuất hoặc cung cấp dịch vụ đáp ứng các tiêu chí quy định cụ thể

3.1.4.4.3. Tiêu chí chung đối với sản phẩm, dịch vụ được ưu tiên

✓ Có chi phí sản xuất trong nước đáp ứng quy định ưu đãi theo quy định pháp luật về đấu thầu.

✓ Có tài liệu kỹ thuật và tài liệu hướng dẫn sử dụng bằng tiếng Việt.

✓ Có cam kết hỗ trợ kỹ thuật, bảo hành, bảo trì, nâng cấp và dịch vụ hậu mãi của nhà cung cấp.

3.1.4.4.4. Tiêu chí cụ thể đối với sản phẩm phần mềm được ưu tiên

✓ Các chức năng, yêu cầu kỹ thuật của sản phẩm phù hợp với các yêu cầu nghiệp vụ hoặc quy định, hướng dẫn của cơ quan nhà nước (nếu có).

✓ Do tổ chức, doanh nghiệp, cá nhân Việt Nam thực hiện ít nhất một trong hai công đoạn sau: Xác định yêu cầu, Phân tích và thiết kế quy định tương ứng tại khoản 1 và khoản 2 Điều 3 Thông tư số 13/2020/TT-BTTTT ngày 03 tháng 7 năm 2020 của Bộ Thông tin và Truyền thông.

✓ Sản phẩm được cấp Giấy chứng nhận đăng ký quyền tác giả là người Việt Nam và được bảo hộ theo quy định của pháp luật Việt Nam.

✓ Tiêu chí về tiêu chuẩn chất lượng, an toàn bảo mật của sản phẩm:

✓ Sản phẩm do tổ chức, doanh nghiệp Việt Nam sản xuất có Giấy chứng nhận phù hợp tiêu chuẩn về hệ thống quản lý ISO 9001 được cấp bởi tổ chức chứng

nhận đã đăng ký hoặc có Chứng chỉ cho hoạt động sản xuất phần mềm theo chuẩn CMMI mức 3 trở lên hoặc tương đương;

✓ Sản phẩm phải bảo đảm an toàn thông tin theo quy định của pháp luật về an toàn thông tin hoặc sản phẩm được sản xuất, vận hành bởi nhà cung cấp đã được tổ chức chứng nhận đã đăng ký cấp giấy chứng nhận phù hợp tiêu chuẩn ISO/IEC 27001 hoặc tương đương.

✓ Hệ thống máy chủ cung cấp dịch vụ (nếu có) đặt tại Việt Nam. Đối với dịch vụ điện toán đám mây phải đáp ứng bộ tiêu chí, chỉ tiêu kỹ thuật theo hướng dẫn của Bộ Thông tin và Truyền thông.

✓ Có các biện pháp bảo đảm an toàn, bí mật thông tin, dữ liệu của khách hàng đối với các dịch vụ có liên quan đến lưu trữ, xử lý dữ liệu của khách hàng. Đối với các dịch vụ an toàn thông tin mạng thì thực hiện theo quy định của Luật An toàn thông tin mạng.

✓ Tỷ lệ chi phí cho nghiên cứu, phát triển sản phẩm trên tổng doanh thu sản phẩm đó của doanh nghiệp trong 03 năm gần nhất đạt từ 3% trở lên.

✓ Đối với dịch vụ CNTT sẵn có trên thị trường: dịch vụ đã được triển khai cung cấp tối thiểu cho 03 cơ quan, tổ chức.

3.1.4.4.5. Yêu cầu về quyền sở hữu trí tuệ và bản quyền phần mềm

✓ Nhà cung cấp dịch vụ thuê phải cam kết và chịu hoàn toàn trách nhiệm pháp lý về sở hữu trí tuệ bản quyền phần mềm.

3.1.4.4.6. Yêu cầu về chất lượng

✓ Phần mềm đáp ứng yêu cầu đảm bảo về an toàn, bảo mật thông tin theo quy định của Luật an toàn thông tin mạng 2015.

3.1.4.4.7. Yêu cầu về độ tin cậy

✓ Khả năng chịu lỗi: Phần mềm phải có khả năng hoạt động ổn định tại một mức độ ≤ 70% trong trường hợp có lỗi xảy ra ở phần mềm hoặc có những vi phạm trong giao diện.

✓ Khả năng phục hồi: Phần mềm có khả năng có thể tái thiết lại hoạt động tại một mức xác định và khôi phục lại 100% những dữ liệu có liên quan trực tiếp đến lỗi.

✓ Tính liên tục, sẵn sàng: Hệ thống bảo đảm hoạt động liên tục, luôn sẵn sàng cho người dùng có thể truy cập và khai thác 24/24h tất cả các ngày.

✓ Tính tin cậy chung: Phần mềm thỏa mãn các chuẩn, quy ước, quy định của đơn vị chủ trì dịch vụ yêu cầu và các tiêu chuẩn do cơ quan chuyên môn ban hành.

3.1.4.4.8. Yêu cầu về phương án lựa chọn thuê phần mềm

✓ Hệ thống phần mềm bệnh án điện tử được thuê theo phương án sản phẩm có sẵn trên thị trường, đồng thời phù hợp với các yêu cầu theo Quyết định số 5573/QĐ-BYT, ngày 29 tháng 12 năm 2006 của Bộ Y tế về việc ban hành "Tiêu chí phần mềm và

nội dung một số phân hệ phần mềm tin học quản lý Trung tâm" và các quy định của Luật đấu thầu.

3.1.4.4.9. Yêu cầu về đào tạo, chuyển giao và hướng dẫn sử dụng

3.1.4.4.1. Yêu cầu về mục tiêu đào tạo

Đơn vị cung cấp dịch vụ đào tạo, chuyển giao và hướng dẫn sử dụng Hệ thống phần mềm bệnh án điện tử cho Trung tâm và các Phòng/ ban thụ hưởng phải thực hiện:

- Xây dựng các tài liệu hướng dẫn sử dụng phù hợp với từng đối tượng tham gia quản trị, vận hành và sử dụng hệ thống phần mềm.
- Xây dựng quy trình vận hành và chuyển giao các giải pháp, sơ đồ kỹ thuật, phần mềm, thông tin dữ liệu nếu có.
- Cử cán bộ chuyên gia tư vấn kỹ thuật cho cán bộ tiếp nhận hệ thống phần mềm tại Sở Y tế.

3.1.4.4.2. Yêu cầu về phương án đào tạo

Đơn vị cho thuê phần mềm phải có phương án đào tạo, chuyển giao và hướng dẫn sử dụng phần mềm đảm bảo nhân viên y tế của Trung tâm khai thác và sử dụng phần mềm hiệu quả. Phương án phù hợp nhất là cầm tay chỉ việc theo phương thức trực tiếp.

3.1.4.4.3.Yêu cầu về nội dung đào tạo

Hướng dẫn quy trình khám chữa bệnh, nhập liệu và sử dụng khai thác phần mềm.

Hướng dẫn sử dụng việc quản lý, vận hành Hệ thống phần mềm bệnh án điện tử sau update chức năng phần mềm định kỳ hàng năm

3.1.4.4.10. Yêu cầu cầu đối với nhà cung cấp dịch vụ

3.1.4.4.10.1. Yêu cầu về năng lực, chuyên môn

Yêu cầu đơn vị cho thuê phần mềm đáp ứng các điều kiện sau:

Đội ngũ cán bộ quản trị dự án tối thiểu 01 cán bộ trình độ từ đại học trở lên với 5 năm kinh nghiệm làm việc trong lĩnh vực CNTT.

Nhóm giải pháp, phân tích, thiết kế: tối thiểu 1 cán bộ trình độ từ đại học trở lên, trong đó phải có kinh nghiệm tối thiểu 5 năm làm việc trong lĩnh vực CNTT; Đã tham gia xây dựng giải pháp, thiết kế cho các hệ thống CNTT lớn. Tối thiểu 2 cán bộ trình độ từ cao đẳng trở lên, trong đó phải có kinh nghiệm tối thiểu 2 năm làm việc trong lĩnh vực CNTT

Nhóm lập trình và triển khai hệ thống: tối thiểu 3 nhân sự trình độ từ cao đẳng trở lên, yêu cầu có kinh nghiệm triển khai các hệ thống phần mềm nghiệp vụ cho các đơn vị sự nghiệp, cơ quan nhà nước.

3.1.4.4.10.2.Yêu cầu về năng lực tài chính.

Nhà thầu phải chứng minh việc đáp ứng yêu cầu về nguồn lực tài chính cho gói thầu được xác định theo công thức sau bằng các tài sản có khả năng thanh khoản cao theo quy định của Bộ Kế hoạch và Đầu tư:

✓ Có doanh số hàng năm đạt và có giá trị ròng luôn lớn ≥ 0

✓ Có doanh thu bình quân trong ba năm gần nhất từ năm 2022, 2023 và 2024 đạt giá trị > ... đồng (> khoảng 1,5 lần giá thuê phần mềm 1 năm (12 tháng)).

✓ Có tài liệu chứng minh không nợ đọng thuế, được cơ quan thuế xác nhận.

✓ Có cam kết tình hình tài chính lành mạnh.

3.1.4.4.10.3. Điều kiện kỹ thuật, công nghệ, kinh nghiệm

✓ Nhà thầu phải cam kết thực hiện chuyển đổi dữ liệu của phần mềm do chính đơn vị mình cung cấp trong trường hợp có sự sát nhập, chia tách các đơn vị (theo yêu cầu về tổ chức của Nhà nước hiện hành). Thực hiện việc chuyển đổi dữ liệu theo nguyên tắc: Không phát sinh chi phí chuyển đổi và chi phí thuê dịch vụ trong trường hợp sát nhập hoặc chuyển đổi cơ quan quản lý cấp trên của đơn vị; chỉ phát sinh chi phí chuyển đổi và chi phí thuê dịch vụ trong trường hợp bổ sung, thành lập mới đơn vị.

✓ Nhà cung cấp dịch vụ có số năm hoạt động trong lĩnh vực sản xuất, kinh doanh về CNTT tối thiểu 03 năm.

✓ Nhà cung cấp dịch vụ có hợp đồng tương tự về cung cấp các sản phẩm, dịch vụ trong lĩnh vực CNTT. Ưu tiên với sản phẩm phần mềm Trung tâm cho thuê

3.1.4.4.10.4. Yêu cầu an toàn, bảo mật thông tin đối với nhà cung cấp dịch vụ

✓ Có cam kết bảo đảm an toàn, bảo mật và tính riêng tư về thông tin, dữ liệu của cơ quan nhà nước; tuân thủ quy định của pháp luật về an toàn, an ninh thông tin, Luật cơ yếu, Luật bảo vệ bí mật nhà nước, Luật khám chữa bệnh và các quy định khác có liên quan.

✓ Có kinh nghiệm trong quản lý, đảm bảo an toàn thông tin cho các hệ thống lớn.

✓ Có các giải pháp, hệ thống nhằm quản lý, giám sát, áp dụng chính sách đối với mỗi ứng dụng đang hoạt động 24/7. Giúp phân tích và đưa ra báo cáo tổng thể về hệ thống.

✓ Có cam kết về bảo mật thông tin: Các dữ liệu được người dùng cung cấp và đưa vào trong hệ thống và các dữ liệu sinh ra từ quá trình sử dụng dịch vụ phải được giữ nguyên vẹn không bị mất hay sai lệch về ý nghĩa trong quá trình hệ thống xử lý dữ liệu; Nhà cung cấp dịch vụ không được tự ý truy xuất hoặc khai thác nếu không có yêu cầu của cấp có thẩm quyền, đồng thời phải có cam kết chính thức về trách nhiệm bảo mật thông tin (ngay cả khi đã hết thời gian cung cấp dịch vụ).

Ngoài ra, nhà cung cấp dịch vụ phải đảm bảo an toàn thông tin đối với hệ thống dịch vụ cung cấp ở cấp độ 3 theo đúng quy định tại Phụ lục 3, Thông tư số 03/2017/TT-BTTTT ngày 24/4/2017 của Bộ trưởng Bộ Thông tin và Truyền thông.

3.1.4.5. Yêu cầu về các phát sinh trong quá trình khai thác, sử dụng dịch vụ

3.1.4.5.1.Yêu cầu về bảo trì, hỗ trợ kỹ thuật

Trong quá trình khai thác, sử dụng dịch vụ, đơn vị cung cấp dịch vụ phải luôn bảo trì hệ thống, nhằm hệ thống luôn hoạt động thường xuyên 24/7 và có phương án hỗ trợ kỹ thuật khi xảy ra sự cố, và yêu cầu chi tiết như sau:

✓ Phương thức hỗ trợ kĩ thuật: Trực tiếp ngay khi tiếp nhận thông tin về lỗi hoặc khó khăn trong quá trình sử dụng thông qua điện thoại, email, hoặc các phần mềm hỗ trợ trực tuyến từ xa. Trường hợp không khắc phục được sẽ bảo hành tận nơi trong vòng 48 tiếng.

✓ Hỗ trợ kĩ thuật: Tất cả các lỗi kỹ thuật phát sinh trong quá trình sử dụng.

✓ Hướng dẫn và tư vấn miễn phí qua điện thoại và internet trong suốt quá trình sử dụng và khai thác phần mềm.

✓ Đảm bảo hệ thống (hạ tầng kỹ thuật và phần mềm) hoạt động ổn định trong thời gian cung cấp; Thông báo đến chủ đầu tư khi có kế hoạch nâng cấp, cập nhật tính năng hệ thống.

3.1.4.5.2.Yêu cầu về nâng cấp và hỗ trợ khác

Trong quá trình khai thác, sử dụng dịch vụ, đơn vị cho thuê dịch vụ cần đảm bảo nâng cấp và hỗ trợ khác như sau:

✓ Phần mềm có thể linh hoạt nâng cấp, bổ sung những yêu cầu phát sinh thực tế trong quá trình sử dụng tại các đơn vị thông qua việc nâng cấp tính năng, bản vá lỗi, vận hành và kiểm thử trong thực tế liên tục.

✓ Đơn vị cung cấp phần mềm (nhà thầu) có kế hoạch đào tạo, hướng dẫn sử dụng. Các nội dung công việc như sau:

✓ Hỗ trợ vận hành và khắc phục các lỗi phát sinh tại các bộ phận liên quan.

✓ Hiệu chỉnh phù hợp thực tế (nếu có). Hỗ trợ vận hành chính thức cho các bộ phận có liên quan.

✓ Giới thiệu tổng quát các chức năng của Hệ thống phần mềm.

✓ Hướng dẫn cài đặt, cấu hình.

✓ Hướng dẫn vận hành các nghiệp vụ liên quan.

✓ Hướng dẫn xử lý các lỗi thường gặp.

4. Giải pháp và phương pháp luận:

Nhà thầu chuẩn bị đề xuất giải pháp, phương pháp luận tổng quát thực hiện dịch vụ theo các nội dung quy định tại Chương này, gồm các phần như sau:

1. Giải pháp và phương pháp luận;
2. Kế hoạch công tác.