FPT UNIVERSITY

BỘ GIÁO DỤC VÀ ĐÀO TẠO

Đại học FPT

Tài liệu Dự án Tốt nghiệp

Phát triển hệ thống tự động giám sát tuân thủ chính sách bảo mật hồ sơ bệnh án điện tử (EHR) tại các cơ sở y tế quy mô nhỏ và vừa.

Thành viên nhóm	**Tên học sinh**	**Thẻ sinh viên**
	Trần Gia Quý	DA170010
	Nguyễn Khánh Toàn	DE170585
	Nguyễn Xuân Hoàng	DE170316
	Nguyễn Khánh Linh	DE170403
	Nguyễn Hữu Khôi	DE170017
Người giám sát	**Tên người hướng dẫn**	
	Nguyễn Văn Điền	
	Phạm Hồ Trọng Nguyên	
Mã dự án tốt nghiệp	IAP491	

- Hà Nội, tháng 9/2025 -

TÓM TẮT

LỜI CẢM ƠN

Lời đầu tiên, nhóm thực hiện đề tài xin gửi lời tri ân sâu sắc nhất đến hai giảng viên hướng dẫn: **Thầy Nguyễn Văn Điền** và **Thầy Phạm Hồ Trọng Nguyên**.

Mặc dù đề tài đi sâu vào lĩnh vực y tế số với nhiều quy trình nghiệp vụ đặc thù và mới mẻ, nhưng chính sự định hướng sắc bén về tư duy nghiên cứu cùng những kinh nghiệm quý báu của các thầy trong lĩnh vực Công nghệ và An toàn thông tin đã chỉ ra hướng đi chính xác để giúp chúng em không hiểu sai vấn đề. Từ những ngày đầu loay hoay xác định bài toán cho đến khi hoàn thiện hệ thống, các thầy không chỉ là người truyền đạt kiến thức mà còn là người truyền lửa, kiên nhẫn động viên chúng em vượt qua những giai đoạn bế tắc nhất về giải pháp kỹ thuật.

Đặc biệt, chúng em xin cảm ơn những phản hồi khắt khe nhưng đầy tính xây dựng của các thầy về phương pháp triển khai và cách trình bày vấn đề. Những câu hỏi phản biện của các thầy đã thúc đẩy chúng em phải tự tìm tòi, đào sâu nghiên cứu để hiểu rõ hơn về tính tuân thủ trong y tế dưới góc nhìn của một kỹ sư công nghệ.

Cuối cùng, luận văn này chắc chắn sẽ không thể hoàn thiện nếu thiếu đi sự hỗ trợ từ gia đình và bạn bè – những người đã luôn bên cạnh chia sẻ và khích lệ tinh thần cho nhóm trong suốt hành trình vừa qua.

Dù đã rất nỗ lực, nhưng do giới hạn về thời gian và kinh nghiệm thực tiễn, luận văn khó tránh khỏi những thiếu sót. Chúng em rất mong nhận được sự đóng góp ý kiến của quý Thầy Cô để đề tài ngày càng hoàn thiện hơn.

Chúng em xin chân thành cảm ơn!

MỤC LỤC

VIẾT TẮT

Từ viết tắt	Nghĩa
API	Giao diện lập trình ứng dụng
Hồ sơ bệnh án điện tử	Hồ sơ sức khỏe điện tử
TÔI LÀ	Quản lý danh tính và quyền truy cập
JSON	Ký hiệu đối tượng JavaScript
JWT	Mã thông báo web JSON
KPI	Chỉ số hiệu suất chính
MTTD	Thời gian trung bình để phát hiện
MTTR	Thời gian phản hồi trung bình
OPA	Đại lý Chính sách Mở
PEP	Điểm thực thi chính sách
PDP	Điểm quyết định chính sách
PIPEDA	Đạo luật bảo vệ thông tin cá nhân và tài liệu điện tử
RBAC	Kiểm soát truy cập dựa trên vai trò
NGHỈ NGƠI	Chuyển đổi trạng thái đại diện
SIEM	Quản lý thông tin và sự kiện an ninh
SSO	Đăng nhập một lần
TLS	Bảo mật lớp vận chuyển

Bảng 1 – *Danh sách các từ viết tắt*

CHƯƠNG 1 - INTRODUCTION

(Cung cấp thông tin nền, giới thiệu vấn đề nghiên cứu và nêu rõ mục đích cũng như ý nghĩa của nghiên cứu.)

1.1. Bối cảnh

Trong xu thế chuyển đổi số đang diễn ra mạnh mẽ và nhanh chóng trên toàn cầu thì ngành y tế Việt Nam cũng đang từng bước thực hiện quá trình hiện đại hoá hệ thống quản lý và khám chữa bệnh. Trọng tâm của chiến lược này là việc chuyển đổi từ hồ sơ bệnh án giấy truyền thống sang hệ thống Hồ sơ sức khỏe điện tử toàn dân (Electronic Health Record – EHR), đây là một nền tảng dữ liệu y tế tập trung, cho phép tích hợp và quản lý thông tin sức khỏe trọn đời của mỗi cá nhân, từ lịch sử tiêm chủng, tiền sử bệnh lý đến các kết quả chẩn đoán hình ảnh. Cơ sở pháp lý vững chắc cho định hướng này đã được xác lập thông qua Quyết định số 5349/QĐ-BYT của Bộ Y tế về kế hoạch triển khai Hồ sơ sức khỏe điện tử, và đặc biệt là Luật khám bệnh, chữa bệnh số 15/2023/QH15. Những bộ luật này không chỉ công nhận giá trị pháp lý của dữ liệu điện tử mà còn quy định bắt buộc về việc liên thông dữ liệu giữa các cơ sở khám chữa bệnh với Cơ sở dữ liệu quốc gia về dân cư, từ đó đã đánh dấu một bước mới về sự chuyển đổi cơ bản từ quản lý phân tán sang quản lý tập trung dựa trên dữ liệu [1], [2]. Được thúc đẩy mạnh mẽ bởi kế hoạch phát triển của Chính phủ, việc triển khai hệ thống Hồ sơ bệnh án Điện tử trong thời gian vừa qua đã ghi nhận một kết quả rất đáng kể. Theo số liệu thống kê chính thức từ bộ Y tế và Bảo hiểm xã hội Việt Nam tính đến tháng 10 năm 2024, cả nước đã thiết lập thành công hơn 32,1 triệu hồ sơ sức khỏe điện tử cho người dân. Và điều đáng nói hơn là việc triển khai Hồ sơ bệnh án Điện tử đã kết nối dữ liệu từ hơn 12.000 cơ sở khám bệnh trên toàn quốc để tích hợp trực tiếp vào ứng dụng định danh điện tử VneID, từ đó tạo điều kiện thuận lợi cho người dân trong việc tiếp cận và quản lý thông tin y tế thuận tiện hơn [3], [4]. Từ việc triển khai hồ sơ sức khỏe điện tử trên quy mô toàn quốc đã

cho chúng ta nhận ra rằng sự chuyển đổi số hoá đã đi sâu vào các mạng lưới y tế cơ sở, bao phủ từ các bệnh viện trung ương đến các phòng khám tư nhân.

Tuy nhiên, bên cạnh những mặt tích cực về việc triển khai Hồ sơ sức khỏe điện tử thì các phòng khám tư nhân hay những cơ sở chăm sóc sức khoẻ vừa và nhỏ cũng tham gia triển khai nhưng từ đó cũng kéo theo những rủi ro rất lớn về an ninh mạng. Bởi vì thực tế cho thấy đang tồn tại một khoảng cách lớn về khả năng tự bảo vệ hệ thống của họ. Nếu như các bệnh viện lớn tuyến Trung ương có đội ngũ kỹ thuật xịn và hệ thống máy móc bảo mật hiện đại, thì ngược lại đã có hàng nghìn phòng khám tư nhân và các cơ sở y tế vừa và nhỏ, nơi cũng đang nắm giữ rất nhiều dữ liệu nhạy cảm của người bệnh nhưng những vấn đề bảo mật thì vẫn còn rất lỏng lẻo và bị hạn chế rất nhiều, và đôi khi họ ít quan tâm tới vấn đề sẽ có hacker xâm nhập vào hệ thống của họ, nếu có thì các biện pháp hết sức sơ sài và lỏng lẻo [5], [6]. Sự yếu kém này cũng xuất phát từ 2 lý do chính mà các cơ sở nhỏ đều gặp phải: đó là thiếu nhân sự và thiếu tài chính. Đầu tiên về nhân sự, thực trạng chung là các phòng khám này rất hiếm khi tuyển dụng được nhân viên chuyên trách về an toàn thông tin. Cán bộ IT ở các cơ sở vừa và nhỏ này họ phải đảm nhận hầu hết đủ việc tạp vụ về công nghệ, từ việc phải sửa máy in, cài Win cho đến kéo dây mạng, nên hầu như họ không còn thời gian và cũng thiếu các kiến thức chuyên sâu để lo cho mảng bảo mật [7]. Bên cạnh đó thì họ ít được đi học các chứng chỉ quốc tế về an ninh mạng, nên thường không biết cách xử lý khi có sự cố tấn công xảy ra. Tiếp theo là về mặt kinh phí, đây cũng là một vấn đề gây ra nhiều bất lợi cho các cơ sở y tế vừa và nhỏ. Bởi vì các cơ sở như tư nhân thường ưu tiên tiền bạc để mua sắm máy móc khám chữa bệnh để có thể dễ dàng kiếm lợi nhuận nhưng lại không chi nhiều tiền cho các phần mềm diệt virus bản quyền hay hệ thống tường lửa đắt đỏ. Thậm chí theo thống kê, mức chi an toàn thông tin tại nhiều nơi còn chưa đạt nổi con số tối thiểu là 10% tổng ngân sách công nghệ thông tin, một con số bắt buộc mà chính phủ đã quy định rõ trong Chỉ thị 14/CT-TTg [8]. Chính vì sự lỏng lẻo “từ con người đến công cụ” này mà các

phòng khám nhỏ đang trở thành mục tiêu dễ bị tấn công nhất, là con đường để tin tặc xâm nhập sâu hơn vào hệ thống dữ liệu y tế [9]

1.2 Phát biểu vấn đề

Sau khi đã hiểu rõ được bối cảnh mà các cơ sở y tế vừa và nhỏ gặp phải trong quá trình chuyển đổi sang Hồ sơ bệnh án điện tử (EHR) thì sau đây chúng ta sẽ đi sâu hơn vào vấn đề là "liệu việc hạn chế về nhân sự và cũng như hạ tầng hay không quá quan tâm về vấn đề bảo mật có thật sự đang diễn ra ở mỗi cơ sở y tế vừa và nhỏ thôi hay các cơ sở lớn cũng đang gặp phải vấn đề đó?". Để hiểu rõ hơn thì chúng ta sẽ có những bài báo, dẫn chứng nêu rõ ra câu hỏi này. Theo bài báo cáo của Ponemon Sullivan Privacy report thì tác giả của bài báo có nói rằng "Current legacy technologies have difficulty protecting the enormous amounts of PHI across our systems (66 percent of respondents)" có nghĩa là đã có tới 66% các giải pháp công nghệ hiện hành tại các cơ sở này bị đánh giá là đã cũ và không đủ khả năng bảo vệ hồ sơ bệnh nhân trước các cuộc tấn công hiện đại [10], và nguyên nhân sâu xa của tình trạng này cũng đã được nêu rõ trong bài khảo sát của Black Book Market Research (2024), những nhà nghiên cứu có nói rằng "Legacy systems and EHR/RCM software (77% strongly agree). Hospitals and physician practices still rely on legacy systems and outdated software that do not receive regular security updates making them vulnerable to attacks, the cost and compatibility issues of migrating to more secure cloud technologies is still implementing better solutions", dẫn chứng này có nghĩa là đã có 77% các bệnh viện và phòng khám bác sĩ sử dụng các hệ thống cũ, phần mềm EHR/RCM, bên cạnh đó thì các phần mềm lỗi thời không được cập nhật bảo mật thường xuyên, từ đó khiến chúng dễ bị tấn công hơn và tạo lỗ hổng gây hại cho hệ thống, ngoài ra thì vấn đề chi phí và sự tương thích khi chuyển sang các công nghệ tốt, an toàn hơn chẳng hạn như đám mây vẫn đang cản trở việc triển khai các giải pháp tốt hơn [11]. Từ những bài khảo sát đó, chúng ta có thể thấy rằng việc hạn chế về cơ

sở hạ tầng cũng như chi phí vận hành đã nảy sinh ra ba vấn đề kỹ thuật nghiêm trọng:

Thứ nhất, cơ chế kiểm soát truy cập phân quyền theo vai trò (RBAC) mặc dù cũng là mô hình tiêu chuẩn trong việc kiểm soát người dùng và hạn chế việc lạm dụng quyền khi truy cập vào Hồ sơ bệnh án điện tử nhưng bản chất tĩnh của nó đang trở thành một điểm yếu trong môi trường y tế hiện đại ngày nay. Đã có những báo cáo nói về vấn đề này, chẳng hạn theo báo cáo "Claroty's State of CPS Security Report: Healthcare Exposures 2025" về an ninh hệ thống thực-ảo (CPS), CISOs phải quản lý các hệ thống thiết bị kết nối, và một số thiết bị vẫn chạy trên các hệ điều hành cũ không cong được các nhà cung cấp hỗ trợ cập nhật bảo mật và tính năng, đây là một tình huống thật sự đáng lo ngại vì phân tích của họ đã phát hiện ra các thiết bị chứa các lỗ hổng bảo mật đã bị khai thác (KEV) trong 99% các tập dữ liệu của họ, điều đó cho thấy được rằng khi các cơ sở y tế chỉ sử dụng mô hình RBAC hiện tại sẽ hoàn toàn gặp vấn đề rủi ro vì nó chỉ cấp quyền dựa trên "vai trò" mà không kiểm tra trạng thái an ninh cũng như ngữ cảnh của người dùng và , thiết bị họ sử dụng khi truy cập vào Hồ sơ bệnh án điện tử [12]. Về mặt lý thuyết, Park và R.Sandhu (2004) đã chỉ ra trong báo cáo của họ rằng các mô hình truyền thống như Role Based Access Control vốn chỉ được thiết kế trong môi trường khép kín [14], việc đó gây ra một số bất lợi đối với các bác sĩ, khi họ muốn truy cập vào Hồ sơ bệnh án điện tử thì chỉ có thể sử dụng máy tính ở nơi làm việc cũng như chỉ sử dụng mạng nội bộ của cơ sở họ làm việc, họ bị hạn chế cũng như bất tiện khi muốn làm việc từ xa và mô hình RBAC còn hoàn toàn thiếu khả năng kiểm soát liên tục, một sự cần thiết cho các môi trường y tế ngày nay.

Vấn đề tiếp theo, một thách thức lớn khác là các file log hiện tại còn thiếu sót những thông tin cần thiết và quan trong cho việc kiểm toán sau này vấn đề là do nhật ký kiểm toán (Audit logs) bị thiếu đi thông tin ngữ cảnh và còn chưa nêu rõ đầy đủ thông tin của người truy cập vào hệ thống. Chẳng hạn như Bác sĩ A truy

cập vào hồ sơ bệnh án điện tử thì nhật ký chỉ ghi lại khoảng thời gian và địa chỉ IP và tên máy chủ mà bác sĩ sử dụng chứ không ghi lại rõ tài khoản của người truy cập và mục đích truy cập là gì?. Theo bài hướng dẫn quản lý nhật ký an toàn NIST SP 800-92 (một tiêu chuẩn nền tảng cho cả hệ thống HIPAA), đã nêu ở mục 3.3.1 (Syslog Format) rằng "Syslog is intended to be very simple, and each syslog message has only three parts. The first part specifies the facility and severity as numerical values. The second part of the message contains a timestamp and the hostname or IP address of the source of the log. The third part is the actual log message content. No standard fields are defined within the message content; it is intended to be humanreadable, and not easily machine-parseable", từ đó có thể thấy ở bài báo này cũng chỉ ra rằng hoàn toàn không có trường thông tin nào quy định về mục đích nghiệp vụ hay ý định người dùng, và không có dữ liệu raw để hệ thống có thể phân tích được hành vi người dùng[13].Tiếp theo ở bài báo Park và R.Sandhu (2004) cũng chỉ ra rõ rằng "Traditionally, access control has focused on the protection of computer and information resources in a closed system environment. The enforcement of control has been primarily based on identities and attributes of known users by using a reference monitor and specified authorization rules [Sandhu and Samarati 1994].", như vậy có thể thấy rằng việc kiểm soát hành vi của người dùng dựa trên ngữ cảnh còn rất hạn chế và phụ thuộc theo cách truyền thống là sử dụng RBAC hơn, tuy nhiên, họ đã giới thiệu mô hình UCON-ABC thông qua trích dẫn "we introduce the UCON-ABC (Authorizations, oBligations, and Conditions)model family as a core model for UCON that covers these aspects in a sin-gle framework systematically and comprehensively", từ đó chúng ta nhận ra được rằng: Hệ thống cần phải tích hợp thêm yếu tố ngữ cảnh và nghĩa vụ thì mới đạt được khả năng kiểm soát tối đa đối với hành vi người dùng và ngăn chặn được các hành vi lạm dụng quyền hạn hơn, điều mà các mô hình kiểm soát truyền thống khó thực hiện được [14].

Vấn đề cuối cùng cũng rất quan trọng và gây nhiều rủi ro trong việc kiểm soát truy cập người dùng đó chính là nhật ký kiểm toán nằm rải rác và dễ bị tác động vào, từ đó bằng chứng kiểm toán có thể bị sửa đổi hoặc khó có thể truy vết lại sau này. Đặc biệt những tổ chức chăm sóc sức khoẻ vừa và nhỏ, thiếu chuyên môn thì dữ liệu thường nằm rải rác trên nhiều phần mềm khác nhau mà không có sự liên kết. Dựa vào tài liệu hướng dẫn quản trị dữ liệu của AHIMA (2022), với trích dẫn "Many healthcare organizations have given some thought to data governance but perhaps are unsure where to start or how to achieve a robust data governance program. An obstacle to implementing organizational healthcare data governance may be a lack of understanding of data as an asset by key stakeholders which may lead to data silos and delays in the formation of an organizational wide program." đã nêu ra được vấn đề quan trọng rằng ở các tổ chức y tế thiếu hiểu biết về cách quản lý dữ liệu sẽ dẫn đến tình trạng hình thành các "kho dữ liệu bị cô lập" và ngăn cản sự thống nhất và gây ra sự chậm trễ cho hệ thống chăm sóc sức khỏe [15]. Bên cạnh đó thì vấn đề thiếu nhân lực có chuyên môn về bảo mật cũng gây ra trở ngại lớn cho các doanh nghiệp vừa và nhỏ này, theo báo cáo của ENISA (2021) về an ninh mạng cho doanh nghiệp SMEs đã nêu ra rằng "Cybersecurity is a specialized topic, requiring specialized knowledge, however it is quite common within an SME that individuals multitask and may have multiple roles assigned to them. As a result, an employee within a SME may be responsible for cybersecurity, as well as for other processes" ," Compounding the challenges in this area is that many cybersecurity solutions require specialized IT knowledge to implement and manage them properly. All of these issues combined make managing cybersecurity within a SME a big challenge.". Họ đã chỉ ra rằng ở các doanh nghiệp y tế vừa và nhỏ thì việc cá nhân đảm nhận nhiều nhiệm vụ và được giao nhiều vai trò thì khá là phổ biến, vì vậy nên một nhân viên có thể chịu trách nhiệm về an ninh mạng cũng như các quy trình khác, điều này sẽ gây thách thức lớn cho doanh nghiệp chăm sóc sức khỏe đó [16]

1.3 Mục tiêu nghiên cứu

Sau khi đã đi sâu vào những rủi ro và điểm yếu mà trong các cơ sở y tế vừa và nhỏ đều gặp phải thì chúng ta đã nhận ra rằng việc quan trọng nhất cần phải thay đổi và khắc phục đó chính là vấn đề hạn chế nghiêm trọng về cơ chế kiểm soát và giám sát trong các hệ thống cũ, vì vậy mục tiêu nghiên cứu lần này của chúng ta hướng tới đó chính là xây dựng một hệ thống tự động giám sát tuân thủ chính sách dành cho Hồ sơ bệnh án điện tử (EHR) tại các cơ sở y tế vừa và nhỏ ở Việt Nam, và hệ thống này sẽ khắc phục được thêm điểm yếu đó là nguồn nhân sự hạn chế và tài chính hạn hẹp. Bên cạnh đó hệ thống sẽ triển khai theo mô hình đã có sẵn ở các bài báo nghiên cứu trước đây để khắc phục được nhược điểm của mô hình phân quyền tĩnh (RBAC) là yêu cầu truy cập bị hạn chế và các ràng buộc nghiêm ngặt, bằng cách kết hợp thêm mô hình Attribute Based Access Control (ABAC), mô hình này chứa nhiều thuộc tính liên quan đến môi trường, tài nguyên và người dùng được xem xét để thực thi chính sách hiệu quả, chi tiết và tối ưu hơn trong quá trình thu thập hành động truy cập của người dùng khi vào EHR bởi vì các thuộc tính này bao gồm vai trò người dùng, giới hạn thời gian, vị trí và ngữ cảnh khác nên rất thuận lợi trong việc kiểm toán sau này. Nhóm sẽ đưa ra các bài báo nghiên cứu, dẫn chứng cho thấy rằng việc sử dụng mô hình RBAC kết hợp ABAC đạt hiệu quả cao hơn rất nhiều, chẳng hạn như theo trích dẫn trong bài nghiên cứu: ‘An access control system for cloud-based healthcare systems driven by blockchain’ đã cho chúng ta thấy “sự kết hợp giữa blockchain với kiến trúc kiểm soát truy cập lại là sử dụng kết hợp ABAC và RBAC có thể cung cấp cơ chế kiểm soát truy cập mạnh mẽ cho các tài nguyên điện toán không đồng nhất, đặc biệt là trong môi trường điện toán đám mây, và việc tích hợp này được thực hiện qua các thành phần sau như: Lưu trữ vai trò/thuộc tính trên các kho lưu trữ chống giả mạo, Thực thi chính sách thông qua hợp đồng thông minh, Kiểm soát phi tập trung và Khả năng kiểm toán và tính minh bạch”. Qua nghiên cứu triển khai ABAC và RBAC trong hệ thống blockchain cho chúng ta thấy được nó mang lại nhiều lợi ích, chẳng hạn như tăng cường bảo mật, tính minh bạch, quyền sở hữu

và ghi nhật ký chặt chẽ, bảo hiểm chống lại quản lý rủi ro…[17]. Song song với đó, nhó cũng tìm thấy những bài nghiên cứu nói về việc tập trung phát triển kỹ thuật làm giàu nhật ký để bổ sung thông tin ngữ cảnh vào bằng chứng kiểm toán. Bài nghiên cứu "Context-Aware Electronic Health Record - Internet of Things and Blockchain Approach" của Tiago Guimaraes đã đề xuất rằng việc tích hợp nhận thức ngữ cảnh (Context-awareness) vào hệ thống EHR là yếu tố then chốt có thể giúp phân biệt chính xác hành vi truy cập hợp lệ và các hành vi lạm dụng quyền hạn tinh trong môi trường Y tế, cụ thể hơn trong bài nghiên cứu này ở mục "5.Pervasive and Context-Aware EHR" với 3 phases: (1) Phase A- Fine the location of the users, (2) Phase B - Development of a Mobile EHR app, (3) Phase C - Maintain an immutable log of the data generated, với các giai đoạn này thì bài nghiên cứu này đã cho chúng ta thấy rằng việc có ngữ cảnh cũng như quyền hạn được phân rõ ràng với mỗi vai trò truy cập vào EHR đã trở thành một lớp tường lửa chắc chắn. Nó giám sát và ngăn chặn các hành vi truy cập không đúng phận sự hoặc trái phép từ xa mà người quản trị không cần phải cài đặt thủ công hay quá nhiều thao tác phức tạp. Thông tin ngữ cảnh được ghi lại trong bằng chứng kiểm toán rất chi tiết, nếu có sự cố xảy ra trong y khoa thì người vi phạm không thể chối cãi [18]

1.4. Ý nghĩa của nghiên cứu

Mục tiêu nghiên cứu được đề ra ở 1.3 đã mang lại một ý nghĩa rất to lớn đối với các cơ sở y tế vừa và nhỏ trong lúc họ đang gặp khó khăn và thách thức khi phải đảm bảo những bộ luật và pháp lý khắt khe trong quy trình khám chữa bệnh, bên cạnh đó họ còn phải ghi nhật ký kiểm toán liên tục để đảm bảo mọi người dùng truy cập đều phải đúng quyền và đúng ngữ cảnh trong pháp lý nêu ra, và những khó khăn đó đã được Hệ thống tự động giám sát tuân thủ chính sách của chúng tôi giải quyết, nó bao gồm 2 vấn đề: Thứ nhất đó là giúp cho các cơ sở y tế vừa và nhỏ đều đảm bảo những điều khoản khắt khe trong các pháp lý về chăm sóc sức khỏe. Chẳng hạn như Nghị Định 13/2023/NĐ-CP có đặt ra các yêu cầu

khắt khe về bảo vệ dữ liệu cá nhân và các quy định về khả năng truy xuất nguồn gốc hành vi của người dùng và tính toàn vẹn của hồ sơ dữ liệu bệnh án [19]. Tuy cơ sở hạ tầng kỹ thuật còn hạn chế nhưng hệ thống tự động của chúng tôi vẫn hoạt động như một cơ chế có thể xác định mọi hành vi truy cập vào EHR đều có thể cung cấp bằng chứng tuân thủ chính xác và thức thời theo các điều luật, khung pháp lý của cơ quan chính phủ đưa ra mà không cần phải can thiệp thủ công, từ đó có thể giải quyết triệt để rủi ro sai sót trong quy trình báo cáo giải trình và điều này còn giúp cho các đơn vị y tế đó đảm bảo tuân thủ đầy đủ các điều khoản mà pháp lý đã đưa ra, từ đó tránh được những mức phát pháp lý mà các cơ sở y tế vừa và nhỏ khó có thể chấp nhận được. Vấn đề thứ hai là củng cố niềm tin với người bệnh để nâng cao hiệu quả khám chữa bệnh, việc đảm bảo an toàn dữ liệu không còn là vấn đề kỹ thuật mà là yếu tố ảnh hưởng đến quá trình chăm sóc sức khoẻ cho bệnh nhân. Theo bài nghiên cứu có tiêu đều là "Trust and digital privacy in healthcare: a cross-sectional descriptive study of trust…." đã chứng minh được sự liên hệ rõ rệt giữa niềm tin vào hệ thống bảo mật và mức độ sẵn lòng chia sẽ dữ liệu sức khoẻ của bệnh nhân [20]. Cụ thể hơn trong bài khảo sát đã chỉ ra rằng có khoảng 81,9% người tham gia có mức độ tin tưởng cao sẽ sẵn sàng chia sẻ dữ liệu riêng tư của họ trong quá trình khám chữa bệnh, ngược lại những người có niềm tin thấp thường có xu hướng yêu cầu kiểm soát khắt khe hơn và đôi khi họ có thể chủ động giấu đi thông tin bệnh lý nhạy cảm của họ. Hệ quả của việc thiếu niềm tin này là rất nghiêm trọng vì nếu bệnh nhân thấy không an toàn, họ sẽ không cung cấp đầy đủ thông tin bệnh lý, dẫn đến bác sĩ thiếu thông tin sức khoẻ của họ và không thể đưa ra hướng điều trị chính xác. Vì vậy, hệ thống của chúng tôi phải đảm bảo bảo vệ được quyền riêng tư chặt chẽ và từ đó mới có thể giúp bệnh nhân yên tâm chia sẽ và hợp tác tối đa đối với các bác sĩ.

1.5. Phạm vi và giới hạn

1.5.1. Phạm vi nghiên cứu:

Về đối tượng và không gian triển khai: Nghiên cứu của chúng tôi được xây dựng và triển khai theo mô hình ABAC + RBAC để khắc phục nhiều vấn đề mà các cơ sở y tế vừa và nhỏ gặp phải. Chúng tôi chọn nhóm đối tượng bao gồm các phòng khám đa khoa, trung tâm y tế nhỏ hoặc các bệnh viện tư nhân tầm trung vì chúng tôi nhận thấy rằng đặc điểm chung của nhóm này là hạ tầng công nghệ thông tin thường bị phân tán, nguồn lực tài chính còn hạn chế và nhân sự IT thì chưa có chuyên môn cao về an ninh mạng, họ còn dễ gặp rủi ro về vấn đề tuân thủ pháp lý. Còn các bệnh viện lớn thì nằm ngoài đối tượng nghiên cứu của chúng tôi vì nhân sự cũng như hạ tầng ở đó rất mạnh mẽ, họ có thể đảm bảo được tuân thủ các pháp lý nhờ có các công cụ giám sát mạnh mẽ. Về quy trình của hệ thống này sẽ tập trung vào việc kiểm soát và giám sát chặt chẽ các luồng truy cập vào Hồ sơ bệnh án điện tử (EHR). Phạm vi giám sát của hệ thống chúng tôi bao gồm 3 quy trình chính: 1. Quy trình truy cập xem chi tiết Hồ sơ bệnh án điện tử và lịch sử khám chữa bệnh, 2. Quy trình chỉnh sửa và cập nhật kết quả thăm khám lâm sàng đối với các bác sĩ chuyên khoa (bao gồm kết quả xét nghiệm và hình ảnh chẩn đoán). 3. Quy trình tra cứu thông tin bệnh nhân và các thủ tục hành chính. Còn các quy trình như quản lý vật liệu y tế hay chấm công cho các nhân sự sẽ không thuộc quyền giám sát của hệ thống chúng tôi. Tiếp đến là giới hạn về mặt kỹ thuật: Hệ thống này sẽ giám sát tại tầng Ứng dụng (Application) và tầng Dữ liệu (Data Layer) bởi vì hệ thống sẽ thu thập lại các hành vi người dùng và đưa ra các bằng chứng kiểm toán bao gồm tên người dùng đó, hành động của họ trong EHR là gì và họ có truy cập đúng ngữ cảnh không, sau đó sẽ tiến hành so sánh với các điều khoản pháp lý và cho người quản trị hệ thống biết được liệu hành vi này có tuân thủ hay vi phạm. Các biện pháp ngăn chặn hacker tấn công vào hệ thống cũng triển khai và ngăn chặn, sau đó được đưa lên bảng giám sát chung (Dashboard) để người quản trị cũng có thể nắm rõ tình trạng của hệ thống.

1.5.2. Giới hạn của nghiên cứu:

Mặc dù hệ thống này đã giúp cho các cơ sở y tế vừa và nhỏ khắc phục những điểm yếu thì bên cạnh đó nó cũng có 2 giới hạn cụ thể mà hệ thống này gặp phải. Đầu tiên là về khả năng mở rộng: vì ưu tiên tính khả thi và chi phí thấp để phù hợp với cơ sở nhỏ, thì kiến trúc hệ thống chưa được triển khai để chịu được một lượng truy cập đồng thời cực lớn thường thấy ở các hệ thống SIEM nước ngoài. Tiếp theo là mô hình đe doạ: những thuật toán mà chúng tôi sử dụng chủ yếu để phát hiện các hành vi vi phạm chính sách nội bộ, ví dụ: nhân viên xem hồ sơ không thuộc phạm vi của mình. Còn khả năng ngăn chặn các cuộc tấn công mạnh như sử dụng mã độc hay những lỗ hổng chưa được công bố thì đều nằm ngoài khả năng của hệ thống chúng tôi.

1.6. Cấu trúc luận văn

Luận văn này được tổ chức thành sáu chương, cung cấp một phân tích toàn diện về những thách thức trong giám sát an ninh mạng y tế trong quá trình chuyển đổi số y tế tại Việt Nam và giải pháp kỹ thuật được đề xuất sử dụng kiến trúc ba luồng (IAM/Gateway, EHR, SIEM).

CHƯƠNG 2: LITERATURE REVIEW

Mục tiêu của chương này là khảo sát các nghiên cứu, tiêu chuẩn và giải pháp hiện có liên quan đến bảo mật EHR, tập trung vào các câu hỏi: những gì đã được thực hiện và những hạn chế khi áp dụng trong bối cảnh các cơ sở y tế vừa và nhỏ. Từ đó, chương này tổng hợp khoảng trống nghiên cứu và làm cơ sở cho sự đóng góp của dự án.

2.1. Review of Previous Studies

2.1.1. An ninh mạng trong y tế kỹ thuật số

2.1.1.1. Các mối đe dọa và xu hướng tấn công

Nghiên cứu về an ninh mạng trong y tế kỹ thuật số thường mô tả chuỗi phòng thủ chuyên sâu: từ quản lý rủi ro, quy trình vận hành, kiểm soát truy cập, chính sách, phân đoạn mạng, mã hóa và giám sát liên tục. Tuy nhiên, thực tế cho thấy điểm yếu thường xuất hiện ở khâu vận hành: quyền truy cập tăng theo thời gian, cấu hình thay đổi mà thiếu truy vết kiểm toán, và khi có nghi vấn thì không đủ dữ liệu/ngữ cảnh để xác minh đúng hay sai. Ngoài ra, với ransomware, một nghiên cứu định tính về ransomware tại các bệnh viện Hoa Kỳ giai đoạn 2016–2022 cho biết riêng dữ liệu OCR đã ghi nhận 562 sự cố; tuy nhiên chỉ 65 trường hợp có đủ thông tin để phân tích chuyên sâu về động cơ tấn công và phản hồi/ứng phó sự cố [47]. Điều này cho thấy rào cản lớn không chỉ nằm ở tần suất tấn công, mà còn ở chất lượng và mức đầy đủ của dữ liệu phục vụ điều tra. Bên cạnh đó, DBIR 2024 lưu ý rằng trong lĩnh vực chăm sóc sức khỏe, ba nhóm kiểu sự cố (miscellaneous errors, privilege misuse và system intrusion) chiếm tỷ lệ lớn (tổng cộng 83%), đồng thời tác nhân nội bộ xuất hiện trong phần đáng kể các vụ việc (70% so với 30% tác nhân bên ngoài), nhấn mạnh nhu cầu giám sát hành vi truy cập và phát hiện bất thường dựa trên bằng chứng log [45].

2.1.1.2. Khuôn khổ pháp lý của Việt Nam và các yêu cầu tuân thủ

Tại Việt Nam, các quy định về bảo vệ dữ liệu cá nhân và an ninh mạng như Nghị định 13/2023/NĐ-CP, Luật An ninh mạng 2018 cùng các văn bản hướng dẫn đã đặt ra những yêu cầu cơ bản về kiểm soát truy cập, xử lý dữ liệu đúng mục đích và khả năng truy vết khi có sự cố xảy ra [25], [26], [27]. Trong phạm vi hồ sơ bệnh án điện tử (EHR), Thông tư 46/2018/TT-BYT cũng nhấn mạnh khá rõ việc hệ thống cần ghi nhận đầy đủ dấu vết thao tác của người dùng. Cụ thể, nhật ký cần thể hiện thời điểm thực hiện (ngày, giờ) và loại thao tác (chẳng hạn như

xem, nhập mới, chỉnh sửa, hủy hay khôi phục dữ liệu). Việc ghi vết này không chỉ áp dụng với nhân viên y tế (bác sĩ, điều dưỡng) mà cả đội ngũ quản trị hệ thống (IT) cũng cần được đưa vào phạm vi giám sát, nhằm phục vụ kiểm tra, kiểm toán hoặc điều tra khi cần thiết, đồng thời góp phần bảo đảm quyền riêng tư cho người bệnh [28]. Dù vậy, phần lớn các văn bản hiện hành vẫn dừng ở mức nêu yêu cầu mang tính nguyên tắc. Khi đi vào thực tế vận hành, câu hỏi "làm sao tự động hóa việc giám sát tuân thủ hằng ngày" lại phụ thuộc khá nhiều vào năng lực triển khai của từng cơ sở, mức độ chuẩn hóa nhật ký, và đặc biệt là khả năng gắn log với ngữ cảnh nghiệp vụ (ai truy cập – truy cập hồ sơ nào – vì lý do gì – trong bối cảnh nào). Khoảng trống này thường bộc lộ rõ ở các cơ sở vừa và nhỏ: hệ thống có thể có log, nhưng log chưa đủ ngữ cảnh để kiểm chứng tuân thủ một cách nhất quán [25], [26], [27], [28].

Ở cấp quản lý, Quyết định 326/QĐ-BYT (2024) tiếp tục nhấn mạnh yêu cầu giám sát an toàn thông tin và quản lý nhật ký trong quá trình vận hành hệ thống. Điều này cho thấy tuân thủ không chỉ nằm ở việc đáp ứng "quy định trên giấy", mà còn nằm ở năng lực ghi nhận, theo dõi và truy vết trong thực tế [28], [50].

2.1.1.3. Tiêu chuẩn quốc tế (HIPAA/NIST/ISO) và bài học thực hiện

Ở nhiều quốc gia, các khung chuẩn và hướng dẫn đều xem nhật ký log và cơ chế giám sát là nền tảng để đảm bảo tuân thủ trong môi trường y tế, đặc biệt với dữ liệu nhạy cảm như ePHI. Chẳng hạn, HIPAA Security Rule (nhóm biện pháp kỹ thuật) yêu cầu hệ thống phải ghi nhận và cho phép rà soát các hoạt động liên quan đến ePHI. Nói cách khác, không chỉ dừng ở việc ai được quyền truy cập, mà còn phải để lại dấu vết để khi cần có thể kiểm tra và đối chiếu [21]. Ở góc độ quản trị, ISO 27799 nhìn vấn đề rộng hơn: thay vì coi log như một tính năng kỹ thuật rời rạc, tiêu chuẩn này đặt nó trong khung tổng thể về quản trị an toàn thông tin y tế, gắn với kiểm soát truy cập, phân quyền, quản lý rủi ro và các cơ chế đảm bảo vận hành an toàn [22]. Bổ sung cho hai khung trên, NIST SP 800-92 đi sâu vào cách quản lý log một cách bài bản (từ thu thập, chuẩn hóa, lưu giữ đến bảo vệ tính

toàn vẹn và khai thác log cho kiểm toán/điều tra), còn NIST SP 800-137 nhấn mạnh tinh thần giám sát liên tục: theo dõi thường xuyên, có ngưỡng cảnh báo và cơ chế phản hồi, thay vì chỉ đợi đến kỳ mới rà soát [39], [24]. Điểm giống nhau của các tài liệu này là: tuân thủ cần đi kèm bằng chứng vận hành. Khi kiểm toán hoặc điều tra, hệ thống cần trả lời được những câu hỏi rất cụ thể như ai đã truy cập dữ liệu, truy cập vào thời điểm nào, thao tác gì và trên đối tượng nào. Tuy nhiên, khi đưa vào môi trường EHR, khoảng cách thường nằm ở bước chuyển từ nguyên tắc sang triển khai. Trong các hệ thống vận hành kiểu phân tán, log có thể nằm rải rác ở ứng dụng, cơ sở dữ liệu, API gateway… nhưng lại thiếu đồng bộ thời gian, thiếu chính sách lưu giữ phù hợp, không được chuẩn hóa định dạng, hoặc chưa có cơ chế bảo vệ khỏi sửa/xóa. Khi đó, log vẫn tồn tại, nhưng giá trị làm bằng chứng để đối chiếu lại bị giảm đi đáng kể [39]. Thậm chí, ngay cả khi log đầy đủ, bài toán vẫn chưa hẳn đã xong vì để kết luận tuân thủ, thường cần đi ngữ cảnh nghiệp vụ. Ví dụ cùng là hành vi "xem hồ sơ", nhưng còn phải biết người truy cập có thuộc nhóm điều trị hay không, truy cập trong ca trực hay ngoài giờ, truy cập một hồ sơ hay truy cập hàng loạt, và truy cập đó phục vụ nghiệp vụ hay có dấu hiệu bất thường. Các khung như HIPAA/ISO/NIST nhấn mạnh yêu cầu kiểm soát và giám sát, nhưng thường không đi sâu đến mức "làm thế nào gắn log kỹ thuật với ngữ cảnh EHR" để giảm mơ hồ khi đánh giá vi phạm [21], [22], [24], [39].

Với các cơ sở y tế vừa và nhỏ, khó khăn thực sự còn đến từ nguồn lực. Vận hành SIEM không đơn giản là gom log về một chỗ, mà còn cần dung lượng lưu trữ, chính sách lưu giữ đủ dài, có quy trình vận hành rõ ràng, và đội ngũ theo dõi để xử lý cảnh báo, tinh chỉnh luật cũng như hạn chế cảnh báo giả. Trong khi đó, các hướng dẫn về quản lý log nhấn mạnh việc cần xác định mục tiêu và ưu tiên những yêu cầu quan trọng do nguồn lực có hạn [39]; còn các nghiên cứu tổng quan về SIEM cũng cho thấy xu hướng hướng tới việc cải thiện hiệu quả phát hiện và giảm tải cho người vận hành [41]. Vì vậy, trong triển khai thực tế, cách

tiếp cận "tối giản nhưng tập trung" thường khả thi hơn: ưu tiên một số kịch bản tuân thủ rủi ro cao (ví dụ truy cập ngoài quan hệ điều trị, truy cập ngoài giờ, truy cập khối lượng lớn…), thiết kế các quy tắc phát hiện phù hợp, và khi điều kiện cho phép thì bổ sung thêm ngữ cảnh từ EHR/IAM (vai trò, khoa/phòng, ca trực, quan hệ điều trị…) để cảnh báo trở nên sát thực tế hơn và giảm gánh nặng vận hành. So với việc cố gắng bao quát mọi loại sự kiện ngay từ đầu, cách làm này thường dễ triển khai và dễ duy trì hơn [39], [41].

2.1.2. Hồ sơ sức khỏe điện tử (EHR)

2.1.2.1. HL7 FHIR và SMART theo tiêu chuẩn FHIR

Hồ sơ sức khỏe điện tử hiện đại thường phải kết nối và trao đổi dữ liệu với nhiều hệ thống khác nhau như xét nghiệm, chẩn đoán hình ảnh, dược hay quản lý, thậm chí còn cần chia sẻ dữ liệu giữa các cơ sở. Trên thực tế, mỗi hệ thống có thể dùng một cách biểu diễn dữ liệu và cách tích hợp riêng, nên nếu thiếu một chuẩn chung thì việc liên thông sẽ khó đồng bộ và khó mở rộng. Và HL7 chính là bộ chuẩn trao đổi dữ liệu y tế; trong đó FHIR (Fast Healthcare Interoperability Resources) mô hình hóa dữ liệu dưới dạng các "tài nguyên", cung cấp cơ chế truy cập theo kiểu web/API giúp cho việc trình bày và trao đổi dữ liệu trở nên nhất quán hơn. Trên nền FHIR, mô hình SMART on FHIR bổ sung cơ chế tích hợp ứng dụng bên thứ ba dựa trên OAuth 2.0 và OIDC. OAuth 2.0 cho phép cấp quyền truy cập bằng token thay vì chia sẻ mật khẩu, còn OIDC bổ sung lớp xác thực danh tính trên nền OAuth 2.0, từ đó cho phép người dùng/ứng dụng truy cập tài nguyên FHIR theo phạm vi quyền được cấp. Nhờ vậy, nhiều hệ thống EHR có thể phát triển theo hướng mô-đun, đồng thời tái sử dụng các dịch vụ xác thực và ủy quyền dùng chung [29], [30], [35], [36].

2.1.2.2. Kiểm toán Sự kiện và theo dõi hoạt động trong EHR

Trong chuẩn HL7 FHIR, AuditEvent là một đối tượng dữ liệu dùng để ghi nhận dấu vết kiểm toán cho các hoạt động truy cập hoặc xử lý dữ liệu. Theo đặc tả, AuditEvent có thể mô tả tương đối đầy đủ "ai làm gì, tác động lên đối tượng

nào, tại thời điểm nào và từ nguồn/kênh nào" [31]. So với các log thuần kỹ thuật như trạng thái HTTP, endpoint, thông tin kết nối…, AuditEvent có ưu điểm ở chỗ thông tin được tổ chức theo cấu trúc chuẩn và hướng tới ý nghĩa nghiệp vụ, nhờ đó thuận lợi hơn cho việc truy xuất, điều tra và đánh giá tuân thủ.

Dù vậy khi triển khai thực tế, mức độ hữu dụng của AuditEvent lại phụ thuộc nhiều vào cách từng hệ thống ghi nhận sự kiện. Lý do là trong đặc tả, một số phần liên quan đến phân loại/diễn giải sự kiện cho phép linh hoạt theo cách của từng đơn vị triển khai, nên nếu mỗi hệ thống ghi theo một kiểu thì dữ liệu audit dễ thiếu nhất quán [31]. Vì vậy, nếu không có quy ước chuẩn hóa nội bộ (chẳng hạn thống nhất mức độ chi tiết cần ghi, cách đặt loại sự kiện, cách gắn đối tượng liên quan…), audit log có thể rơi vào tình trạng khó tổng hợp, khó đối chiếu giữa các hệ thống, và khi cần kiểm toán hay truy vết thì thiếu căn cứ để kết luận rõ ràng [31].

2.1.2.3. Hạn chế và lỗ hổng trong đánh giá tuân thủ dựa trên EHR

FHIR/SMART giúp chuẩn hóa việc liên thông dữ liệu và tạo điều kiện tích hợp ứng dụng, trong đó trọng tâm chủ yếu nằm ở cách biểu diễn dữ liệu và cơ chế ủy quyền truy cập ở mức API [29]. Nhờ vậy, hệ thống có thể xác định một yêu cầu truy cập có đúng phạm vi quyền được cấp về mặt kỹ thuật hay không. Tuy nhiên, khi nói đến tuân thủ trong vận hành EHR, mục tiêu thường rộng hơn: để khẳng định một lần truy cập là phù hợp, cần đối chiếu thêm các yếu tố mang tính nghiệp vụ như mối quan hệ điều trị, khoa/phòng phụ trách, mục đích sử dụng, ca trực, hay các trường hợp ngoại lệ (chẳng hạn tình huống khẩn cấp). Ở phía ghi nhận hoạt động, FHIR có AuditEvent để mô tả sự kiện truy cập/xử lý dữ liệu theo một cấu trúc tương đối rõ ràng (ai làm gì, trên đối tượng nào, khi nào, qua kênh nào) [31]. Dẫu vậy, audit log về bản chất mới chỉ là "dữ liệu đầu vào". Nói đơn giản, log thô thường phải được xử lý và tổng hợp trước khi dùng cho giám sát. Một scoping review trên JAMIA cho thấy raw event log trong EHR có thể rất lớn (tới mức hàng trăm GB mỗi năm ở một cơ sở), và để tạo được các thước đo sử

dụng được thì thường phải xử lý dữ liệu đáng kể, chẳng hạn gom chuỗi thao tác thành hoạt động và xử lý khoảng trống giữa các thao tác [53]. Bài tổng quan này cũng chỉ ra rằng cách định nghĩa thước đo giữa các nghiên cứu còn khác nhau, khiến việc xây dựng chỉ số theo một cách nhất quán (và từ đó áp dụng vào giám sát thực tế) gặp nhiều khó khăn [53].

2.1.2.4. Quan điểm thực hiện ở Việt Nam và khoảng trống tại các cơ sở y tế vừa và nhỏ

Ở Việt Nam, khi triển khai EHR, nhiều đơn vị thường chọn cách làm là trước mắt tập trung số hóa quy trình khám chữa bệnh để hệ thống vận hành ổn, rồi sau đó mới tính đến việc chuẩn hóa và liên thông dữ liệu giữa các hệ thống. Vì ưu tiên triển khai nhanh, phần ghi vết/audit ở giai đoạn đầu thường chỉ dừng ở những thao tác cơ bản trong từng phần mềm. Điều này khiến việc trả lời các câu hỏi kiểm toán quan trọng vẫn còn khó, chẳng hạn ai đã truy cập hồ sơ nào, truy cập trong bối cảnh nào, và truy cập đó có gắn với quan hệ xử lý/điều trị hợp lệ hay không.

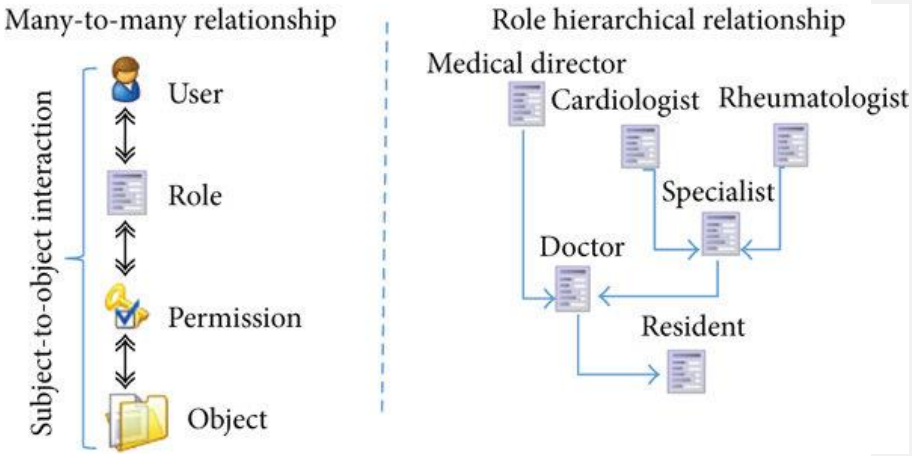
Trong khi đó, yêu cầu ghi dấu vết theo Thông tư 46/2018/TT-BYT không chỉ là "có log", mà còn cần đủ thông tin để tra cứu và đối chiếu khi cần [28]. Vì vậy, để đáp ứng tốt hơn, các cơ sở thường phải có thêm một lớp tổng hợp: chuẩn hóa và liên kết nhật ký từ các hệ thống liên quan, thay vì chỉ dựa vào log cục bộ của một hệ thống duy nhất [28], [31].

2.1.3. Kiểm soát truy cập

2.1.3.1. RBAC: đơn giản và dễ vận hành

RBAC là mô hình kiểm soát truy cập khá phổ biến vì cách làm tương đối trực quan: phân quyền theo vai trò. Trong môi trường bệnh viện, nơi các nhóm công việc như bác sĩ, điều dưỡng hay dược sĩ đã được phân định rõ, RBAC thường dễ triển khai và dễ giải thích cho người dùng. Chuẩn INCITS RBAC cũng cung cấp nền tảng để thiết kế vai trò và quyền theo nhóm một cách có cấu trúc [32]. Nhưng khi đưa vào EHR, câu chuyện thường phức tạp hơn vì một lượt truy cập

hợp lệ nhiều khi còn phụ thuộc vào ngữ cảnh: người đó có đang trong ca trực không, có liên quan điều trị với bệnh nhân không, hay có rơi vào tình huống khẩn cấp cần truy cập ngoại lệ hay không. Những yếu tố này RBAC không thể hiện tốt nếu chỉ dựa vào vai trò. NIST SP 800-162 cũng nhận xét rằng chỉ dùng các "định danh" như identity, groups và roles của người yêu cầu truy cập thường chưa đủ để diễn đạt các chính sách truy cập trong thực tế, và vì vậy cần xem xét thêm các thuộc tính của chủ thể/đối tượng/hành động, thậm chí cả điều kiện môi trường tại thời điểm ra quyết định [33].



2.1.3.2. ABAC và xu hướng Chính sách dưới dạng mã (OPA, PEP/PDP)

ABAC (Attribute-Based Access Control) mở rộng cách phân quyền bằng việc dựa trên nhiều loại thuộc tính hơn: thuộc tính của chủ thể (người dùng/ứng dụng), của đối tượng (tài nguyên), của hành động và cả điều kiện môi trường tại thời điểm truy cập. Theo NIST SP 800-162, ABAC là một cách tiếp cận linh hoạt để biểu diễn các ràng buộc theo ngữ cảnh, đồng thời đưa ra các lưu ý khi triển khai [33]. Song song với ABAC, xu hướng "chính sách dưới dạng mã" (policy-as-code) nhấn mạnh việc tách logic chính sách ra khỏi mã ứng dụng để chính sách dễ đọc, dễ kiểm thử và dễ quản lý phiên bản. Một cách triển khai thường gặp là kiến trúc PEP/PDP: PEP đóng vai trò điểm thực thi tại nơi phát sinh yêu cầu truy

cập (chặn/cho phép), còn PDP là thành phần đánh giá chính sách và trả về quyết định dựa trên dữ liệu đầu vào và bộ chính sách hiện hành. OPA là một công cụ tiêu biểu cho hướng tiếp cận này, hỗ trợ viết và quản lý chính sách dưới dạng mã, đồng thời thuận tiện tích hợp với nhiều dịch vụ khác nhau [34]. Về mặt vận hành, các mô hình trên giúp quyết định quyền truy cập ngay tại thời điểm phát sinh yêu cầu. Tuy nhiên, nếu mục tiêu là theo dõi tuân thủ sau truy cập, hệ thống vẫn cần ghi lại "dấu vết quyết định" (chẳng hạn ngữ cảnh đầu vào, phiên bản chính sách đã áp dụng và kết quả cho phép/từ chối), rồi đối chiếu với nhật ký truy cập thực tế để phục vụ kiểm toán và truy vết.

Mô hình	Ưu điểm	Hạn chế	Ghi chú trong EHR
RBAC	Dễ hiểu, dễ quản trị theo vai trò; phù hợp phân quyền cơ bản	Khó mô tả ngữ cảnh (ca trực, quan hệ điều trị); dễ phát sinh ngoại lệ	Thường dùng làm lớp quyền nền [32]
ABAC	Linh hoạt, mô tả theo thuộc tính và ngữ cảnh; giảm nở vai trò	Cần quản trị thuộc tính tốt; policy phức tạp, khó debug	Phù hợp ràng buộc theo khoa/phòng, mục đích [33]
PEP/PDP + OPA	Tách policy khỏi ứng dụng; policy-as-code dễ kiểm thử/phiên bản hóa	Cần thiết kế điểm chặn (PEP) và bối cảnh đầu vào; phụ thuộc chất lượng log/ngữ cảnh	Hữu ích khi nhiều ứng dụng cùng dùng chính sách [34]

Bảng 2.1. So sánh các mô hình kiểm soát truy cập thường được sử dụng

2.1.3.3. Hạn chế khi đưa mô hình vào tuân thủ EHR

ABAC/PEP–PDP giúp mô tả và thực thi chính sách theo ngữ cảnh, nhưng khi áp dụng vào tuân thủ EHR thì thường phát sinh hai vấn đề chính: đầu vào ngữ cảnh và bằng chứng sau truy cập. Tài liệu NIST SP 800-162 mô tả rằng, ABAC đưa ra quyết định bằng cách đối chiếu các thuộc tính của chủ thể, đối tượng, hành động và điều kiện môi trường với chính sách đang áp dụng [33]. Trong EHR,

những thuộc tính dùng để kết luận tuân thủ lại thường thay đổi theo thời điểm và nằm ở nhiều nguồn khác nhau (quan hệ điều trị, ca trực, sự đồng ý của bệnh nhân, ngoại lệ khẩn cấp…). Vì vậy, nếu dữ liệu ngữ cảnh không được đồng bộ và đảm bảo chất lượng, chính sách rất dễ bị áp dụng thiếu nhất quán [33]. Thêm vào đó, cơ chế thực thi thường chỉ chặn hoặc cho phép tại một số điểm truy cập; trong khi thực tế hệ thống có thể có nhiều luồng truy cập khác nhau, nên việc bao phủ đầy đủ cũng là một thách thức khi triển khai.

Cuối cùng, để phục vụ tuân thủ, việc ra quyết định tại thời điểm truy cập vẫn chưa đủ, còn cần "dấu vết" để kiểm tra lại về sau: quyết định dựa trên ngữ cảnh nào, áp dụng chính sách phiên bản nào, và có khớp với nhật ký truy cập thực tế hay không. Hướng dẫn log management của NIST nhấn mạnh rằng log muốn dùng cho kiểm toán/điều tra cần được quản lý theo hướng chuẩn hóa, đồng bộ thời gian, bảo vệ khỏi sửa hoặc xóa và lưu giữ phù hợp [39].

2.1.3.4. Ứng dụng thực tế ở Việt Nam: Phân cấp còn rời rạc, khó kiểm chứng

Trong thực tế triển khai ở Việt Nam, nhiều cơ sở thường ưu tiên làm từng bước: trước hết ưu tiên số hoá vận hành (HIS, xét nghiệm, chẩn đoán hình ảnh…), sau đó mới dần mở rộng sang liên thông dữ liệu và giám sát tuân thủ. Báo cáo nghiên cứu của UNDP khi khảo sát tại Lạng Sơn, Bình Thuận và Tây Ninh mô tả khá rõ việc triển khai hồ sơ sức khỏe điện tử còn gặp nhiều điểm nghẽn về kết nối và chia sẻ dữ liệu; dữ liệu và phần mềm chuyên ngành có xu hướng phân tán theo từng mảng, khiến việc đồng bộ và khai thác chéo gặp nhiều trở ngại [54]. Khi hệ thống và dữ liệu bị phân tán, việc kiểm chứng tuân thủ cũng thường trở nên nặng hơn. Mỗi hệ thống có thể tự phân quyền và tự ghi nhật ký, nhưng để trả lời đầy đủ các câu hỏi kiểm toán như ai truy cập hồ sơ nào, truy cập trong bối cảnh nào và có hợp lệ hay không thì thường phải tổng hợp và đối chiếu từ nhiều nguồn. Nhìn ở tầm hệ thống, báo cáo PHSSR/WEF về Việt Nam cũng chỉ ra tình trạng trùng lặp hoặc phân mảnh của các hệ thống thông tin y tế do thiếu một chiến lược quốc gia toàn diện về e-Health [55]. Ngoài ra, khảo sát về mức độ ứng dụng công

nghệ y tế số tại 5 bệnh viện công tuyến cao ở Việt Nam cho thấy việc chia sẻ dữ liệu lâm sàng ra ngoài đơn vị theo chuẩn HL7 chưa phải là thực hành phổ biến, phản ánh rằng liên thông liên cơ sở vẫn còn là điểm yếu [56].

2.1.4. Quản lý danh tính (IAM)

2.1.4.1. OAuth 2.0, OpenID Connect và JWT

Trong kiến trúc EHR hiện đại, lớp IAM đóng vai trò nền tảng cho xác thực và ủy quyền, giúp hệ thống biết chính xác ai đang truy cập và người đó được phép làm gì. OAuth 2.0 chuẩn hóa cơ chế ủy quyền truy cập bằng token, nhờ đó ứng dụng có thể truy cập tài nguyên thay mặt người dùng cho mà không cần chia sẻ mật khẩu. OpenID Connect (OIDC) được xây dựng trên OAuth 2.0 để bổ sung lớp xác thực danh tính và thống nhất đăng nhập giữa các hệ thống. Trong khi đó, JWT thường được dùng làm định dạng token gọn nhẹ, thuận tiện cho việc mang theo "claims" và kiểm tra chữ ký để xác thực tính hợp lệ. Nhờ các chuẩn này, nhiều hệ thống EHR có thể tích hợp ứng dụng theo mô hình bên thứ ba (ví dụ SMART trên FHIR), nhưng vẫn giữ được cơ chế quản lý định danh và quyền truy cập theo hướng tập trung [35], [36], [37], [30].

2.1.4.2. IAM nguồn mở và các khả năng phù hợp cho các cơ sở vừa và nhỏ

Trong quá trình triển khai, nhiều tổ chức chọn các giải pháp IAM nguồn mở như Keycloak để giảm chi phí nhưng vẫn đáp ứng được những nhu cầu nền tảng: quản lý người dùng, nhóm/vai trò, SSO và liên kết với các nguồn danh tính khác (federation/brokering) [38]. Khi đặt Keycloak ở trước cổng FHIR hoặc cổng API, luồng xác thực và cấp quyền giữa ứng dụng và dịch vụ EHR thường được chuẩn hóa hơn vì mọi yêu cầu đều đi qua cơ chế phát hành token và kiểm tra token tập trung. Ngoài ra, Keycloak cũng có cơ chế ghi nhận sự kiện xác thực/ủy quyền (ví dụ đăng nhập, cấp token, lỗi xác thực…), nên có thể xem như một điểm tập trung để thu thập dấu vết ở lớp IAM, hỗ trợ đối chiếu khi cần [38].

2.1.4.3. Hạn chế: IAM không tự mình tạo ra giám sát tuân thủ

IAM chủ yếu giải quyết xác thực và ủy quyền, tức là xác định ai đang truy cập và truy cập với phạm vi quyền gì (thông qua cơ chế token/claims trong OAuth 2.0 và JWT) [35], [37]. Tuy nhiên, trong EHR, tuân thủ không chỉ là đúng quyền kỹ thuật mà còn phụ thuộc ngữ cảnh nghiệp vụ như quan hệ điều trị, ca trực, mục đích sử dụng hoặc ngoại lệ khẩn cấp; các yếu tố này thường không nằm trong token nên IAM khó tự kết luận truy cập có hợp lệ hay không. Ngoài ra, tuân thủ cần bằng chứng để kiểm tra lại về sau. Log của IAM thường chỉ phản ánh đăng nhập hoặc cấp token, trong khi kiểm toán truy cập EHR cần nhật ký ở nhiều lớp và phải được quản lý đủ tin cậy. NIST SP 800-92 nhấn mạnh log muốn phục vụ kiểm toán/điều tra cần được thu thập, chuẩn hóa, đồng bộ thời gian, bảo vệ khỏi sửa/xóa và lưu giữ phù hợp [39].

2.1.4.4. Thực tế ở cơ sở vừa và nhỏ: SSO có tồn tại nhưng thiếu cơ chế tuân thủ

Ở các cơ sở vừa và nhỏ, SSO/IAM thường được ưu tiên triển khai sớm để giảm gánh nặng quản trị tài khoản và thống nhất đăng nhập. Các chuẩn như OAuth 2.0, OpenID Connect và JWT cung cấp nền tảng kỹ thuật cho việc xác thực và ủy quyền tập trung [35], [36], [37], [38]. Tuy nhiên, các tài liệu và hướng dẫn liên quan đều cho thấy IAM chủ yếu trả lời câu hỏi về danh tính và quyền kỹ thuật, trong khi đánh giá tuân thủ trong EHR còn cần bằng chứng truy cập gắn với ngữ cảnh nghiệp vụ và khả năng kiểm tra lại về sau.

Theo hướng dẫn về quản lý nhật ký, để phục vụ kiểm toán/điều tra, log cần được thu thập và quản lý đủ tin cậy (chuẩn hóa, đồng bộ thời gian, bảo vệ tính toàn vẹn và lưu giữ phù hợp) [39]. Vì vậy, trong nhiều trường hợp, dù đã có SSO, điểm cần cải thiện vẫn nằm ở chỗ thiếu cơ chế giám sát và đối chiếu dựa trên nhật ký để kiểm chứng tuân thủ một cách nhất quán [39].

2.1.5. SIEM và quản lý nhật ký

2.1.5.1. Quản lý nhật ký theo NIST SP 800-92

Quản lý nhật ký là một nền tảng quan trọng cho an toàn thông tin: giúp phát hiện sự cố, hỗ trợ điều tra sau sự kiện và cung cấp bằng chứng phục vụ kiểm toán, tuân thủ. NIST SP 800-92 nhấn mạnh các yêu cầu mang tính thực tiễn của quản lý log, từ việc xác định các nguồn nhật ký quan trọng, tổ chức thu thập và chuẩn hóa định dạng, đồng bộ thời gian giữa các hệ thống, đến bảo vệ nhật ký khỏi bị chỉnh sửa/xóa và thiết kế chính sách lưu giữ phù hợp với rủi ro [39]. Ở các hệ thống quy mô lớn, SIEM thường được dùng như lớp tập trung để thu thập nhật ký từ nhiều nguồn, liên hệ các sự kiện và tạo cảnh báo dựa trên quy tắc hoặc mô hình phân tích. Nhờ đó, log không chỉ phục vụ vận hành kỹ thuật mà còn hỗ trợ trả lời các câu hỏi kiểm toán cơ bản như ai đã làm gì, vào thời điểm nào, trên hệ thống nào và theo chuỗi sự kiện ra sao [39].

2.1.5.2. SIEM: kiến trúc, xu hướng nghiên cứu và bài học triển khai

Về mặt kiến trúc, các hệ thống SIEM thường xoay quanh một chuỗi chức năng khá ổn định: thu thập log/sự kiện từ nhiều nguồn, chuẩn hoá và lưu trữ, sau đó tương quan các sự kiện để tạo cảnh báo và báo cáo phục vụ vận hành an toàn thông tin. Các tổng quan về SIEM cũng mô tả SIEM như một nền tảng trung tâm có khả năng thu thập, tổng hợp, lưu trữ và tương quan sự kiện từ hạ tầng được quản lý, từ đó hỗ trợ xử lý cảnh báo và báo cáo an ninh [40]. Ở góc độ xu hướng, các nghiên cứu tổng quan ghi nhận SIEM đang dịch chuyển dần từ vai trò giám sát/cảnh báo thuần túy sang các mục tiêu rộng hơn như đáp ứng yêu cầu kiểm toán và tuân thủ, đồng thời kết hợp nhiều kỹ thuật phân tích dữ liệu hơn để nâng hiệu quả phát hiện [41]. Tuy vậy, bằng chứng triển khai thực tế ở quy mô lớn vẫn còn hạn chế: một systematic review về SIEM cho biết trong tập bài báo được phân tích, khoảng một nửa là các đề xuất mới tại thời điểm công bố, còn phần được kiểm chứng trong kịch bản thực tế chiếm tỷ lệ thấp hơn [41].

Từ góc nhìn triển khai, các tổng quan này gợi ý một bài học quan trọng: SIEM chỉ thực sự hữu ích khi dữ liệu đầu vào được chuẩn hoá và có ngữ cảnh đủ tốt để việc tương quan/cảnh báo bớt "nhiễu", đồng thời giúp người vận hành giải thích được vì sao một hành vi bị coi là rủi ro hay vi phạm [41].

2.1.5.3. Hạn chế của SIEM khi đánh giá tuân thủ EHR

Khi đưa SIEM vào bài toán tuân thủ trong EHR, khó khăn thường gặp nhất là thiếu ngữ cảnh nghiệp vụ để hiểu đúng ý nghĩa của cảnh báo. Một yêu cầu truy cập API có thể hoàn toàn hợp lệ nếu người dùng đang tham gia điều trị hoặc đang thực hiện nhiệm vụ được phân công; nhưng cũng cùng hành vi đó lại có thể trở thành vi phạm nếu truy cập ngoài phạm vi điều trị hoặc sai mục đích. Trong khi đó, nhiều nguồn log phổ biến lại thiên về thông tin kỹ thuật như endpoint, trạng thái phản hồi, mã lỗi hay thông tin phiên, mà thiếu các chi tiết giúp kết luận tuân thủ như vai trò theo nghiệp vụ, khoa/phòng, quan hệ điều trị, lý do truy cập hoặc tình huống khẩn cấp. Vì vậy, cảnh báo dễ rơi vào tình trạng khó giải thích và khó dùng như căn cứ kiểm tra tuân thủ. Ngoài vấn đề ngữ cảnh, các tổng quan về SIEM cũng chỉ ra những điểm vướng quen thuộc khi triển khai, chẳng hạn cảnh báo giả vẫn nhiều, thiếu dữ liệu gán nhãn để đánh giá mô hình, và kết quả khó được kiểm chứng ngoài môi trường thử nghiệm [40], [41]. Với các cơ sở vừa và nhỏ, rào cản còn nằm ở chi phí và nguồn lực vận hành: lưu trữ log, duy trì hệ thống và có người theo dõi, tinh chỉnh cảnh báo thường không đơn giản.

2.1.6. Anchor Hash

2.1.6.1. Chuỗi băm và ghi nhật ký giả mạo

Một thách thức quan trọng trong giám sát tuân thủ là độ tin cậy của bằng chứng. Nếu nhật ký có thể bị chỉnh sửa hoặc xóa sau khi ghi, thì việc kết luận tuân thủ sau đó sẽ khó thuyết phục. Vì vậy, nhiều nghiên cứu đề xuất cơ chế ghi nhật ký theo hướng chống giả mạo, trong đó phổ biến là dùng chuỗi băm để liên

kết các bản ghi: mỗi bản ghi mới phụ thuộc vào giá trị băm của bản ghi trước, nhờ đó các thay đổi về sau có thể bị phát hiện. Trong các công trình nền tảng, Kelsey và Schneier (1999) trình bày hướng tiếp cận về secure audit logs, đặt nền cho ý tưởng kiểm tra tính toàn vẹn của nhật ký; Ma và Tsudik (2008) tiếp tục mở rộng theo hướng ghi nhật ký chuyển tiếp an toàn hơn, tăng khả năng chống sửa đổi trong quá trình lưu trữ và vận hành [42], [43].

2.1.6.2. Cơ chế anchor hash định kỳ và đánh dấu thời gian

Trong bối cảnh đề tài, anchor hash có thể hiểu là việc định kỳ tổng hợp giá trị băm của chuỗi nhật ký (ví dụ theo giờ hoặc theo ngày) rồi ghi nhận giá trị này tại một nơi lưu trữ khó sửa đổi, chẳng hạn một dịch vụ ghi nhận độc lập hoặc dịch vụ đánh dấu thời gian. Cách làm này giúp tăng khả năng đối chiếu về sau: nếu nhật ký nội bộ bị can thiệp, có thể so sánh lại với giá trị đã được ghi nhận trước đó để phát hiện sai lệch. Bên cạnh việc đặt mốc bằng giá trị băm, đánh dấu thời gian cũng là một bước quan trọng để chứng minh dữ liệu đã tồn tại tại một thời điểm nhất định. RFC 3161 mô tả giao thức Time-Stamp Protocol (TSP), là cơ chế phổ biến để cấp tem thời gian cho dữ liệu băm nhằm hỗ trợ kiểm chứng về sau [44].

2.1.6.3. Hạn chế và vấn đề vận hành

Về mặt vận hành, cơ chế băm/anchor hash thường kéo theo thêm việc quản lý khóa, quy trình đối soát định kỳ và yêu cầu đồng bộ thời gian, lưu giữ dữ liệu bài bản. Nếu log đến từ nhiều nguồn mà định dạng và dấu thời gian không nhất quán, hoặc khối lượng log quá lớn so với nguồn lực xử lý, thì "có cơ chế chống sửa" cũng chưa chắc biến log thành bằng chứng dễ dùng cho kiểm toán. NIST SP 800-92 nhấn mạnh đúng các vướng mắc này: nhiều nguồn log, khác định dạng, khác timestamp và khối lượng log lớn khiến thu thập–lưu trữ–phân tích trở nên phức tạp; đồng thời log cũng cần được bảo vệ tính bí mật/toàn vẹn/sẵn sàng của log, và đảm bảo phải có quy trình phân tích đều đặn thì mới tạo ra giá trị [39].

Ở góc độ kỹ thuật, Trong Schneier & Kelsey (Secure Audit Logs to Support Computer Forensics, 1999), họ nêu rất rõ các giới hạn quan trọng: không có biện pháp nào bảo vệ được các bản ghi được tạo ra sau khi máy đã bị chiếm quyền; và mật mã chủ yếu giúp phát hiện can thiệp sau này chứ không thể ngăn xóa log nếu không có cơ chế ghi kiểu write-once [42]. Vì vậy, băm/anchor hash phù hợp để tăng độ tin cậy của bằng chứng, nhưng thường chỉ là một mảnh trong chuỗi giải pháp lớn hơn: vẫn cần lớp thu thập - chuẩn hóa - phân tích và các quy tắc tuân thủ ở phía trên để phát hiện vi phạm và giải thích được sự kiện.

2.2. Summary of the Literature Review

Tổng hợp các nhóm tài liệu cho thấy:

(i) các tiêu chuẩn và khung tuân thủ như HIPAA, ISO và NIST đều nhấn mạnh yêu cầu kiểm soát truy cập và quản lý nhật ký như một phần bắt buộc để phục vụ kiểm toán và truy vết;

(ii) FHIR/SMART đóng vai trò quan trọng trong liên thông dữ liệu và tạo nền tảng để ghi nhận, kiểm tra hoạt động theo ngữ nghĩa y tế;

(iii) các mô hình RBAC/ABAC cùng xu hướng chính sách dưới dạng mã hỗ trợ đưa ra quyết định truy cập ngay tại thời điểm thực thi;

(iv) SIEM giúp tập trung thu thập và tương quan sự kiện, nhưng khi áp dụng cho EHR thường gặp khó ở khâu gắn log kỹ thuật với ngữ cảnh nghiệp vụ để kết luận tuân thủ. Đáng chú ý, các tổng quan về SIEM cũng cho thấy số lượng nghiên cứu có đánh giá thực nghiệm trong môi trường thực tế còn hạn chế [41], trong khi các báo cáo về an ninh y tế ghi nhận quy mô sự cố/vi phạm ở mức đáng kể và thiên về nhóm xâm nhập hệ thống; chẳng hạn DBIR 2024 ghi nhận System Intrusion chiếm 83% các vụ trong ngành chăm sóc sức khỏe, và dữ liệu dài hạn cho thấy tỷ lệ rò rỉ do hack/sự cố CNTT tăng từ 4% lên 81% (2010–2024), với ransomware là một mối đe doạ nổi bật [45], [46].

Văn bản/chuẩn (Việt Nam)	Yêu cầu trọng tâm	Hàm ý kỹ thuật	Chức năng trong hệ thống đề xuất
Thông tư 46/2018/TT-BYT [28]	Ghi vết thao tác người dùng trên bệnh án điện tử	Thu thập log đầy đủ và liên kết theo người dùng, hồ sơ, thời điểm	Chuẩn hóa log EHR; truy vấn theo người dùng, hồ sơ, thời điểm
Nghị định 13/2023/NĐ-CP [25]	Bảo vệ dữ liệu cá nhân; kiểm soát truy cập và xử lý đúng mục đích	Chính sách truy cập gắn với mục đích và bối cảnh; phải truy vết được việc sử dụng dữ liệu	Bộ quy tắc kiểm tra tuân thủ; báo cáo vi phạm theo mục đích và phạm vi dữ liệu
Quy chế ATTT/ANM Bộ Y tế (QĐ 326/2024) [50]	Theo dõi hoạt động hệ thống, lưu nhật ký, phục vụ giám sát và xử lý sự cố	Gom log về một điểm, lọc theo quy tắc, tạo cảnh báo và bảo toàn bằng chứng	Pipeline log tập trung; rule engine; dashboard; bảo toàn log bằng hash chain
Luật ANM 2018 và NĐ 53/2022 [26], [27]	Giám sát an ninh mạng và ứng phó sự cố	Theo dõi truy cập bất thường; cung cấp nhật ký phục vụ điều tra khi có yêu cầu	Chỉ báo cảnh báo theo quy tắc; xuất báo cáo phục vụ kiểm tra

Bảng 2.2. Liên hệ các yêu cầu pháp lý của Việt Nam và ý nghĩa kỹ thuật đối với hệ thống giám sát tuân thủ.

Tại Việt Nam, các đánh giá gần đây cũng cho thấy nghiên cứu về hệ thống y tế số trong bệnh viện còn khá hạn chế, đặc biệt là nghiên cứu triển khai và đánh giá vận hành. Điều này làm cho khoảng cách giữa các quy định/tiêu chuẩn và thực tiễn tuân thủ càng rõ ràng hơn, đặc biệt là ở các cơ sở vừa và nhỏ [52].

Nhóm giải pháp	Đã làm được	Hạn chế thường gặp	Hàm ý cho đồ án
Khung tuân thủ (HIPAA/ISO/NIST)	Định nghĩa yêu cầu bảo mật, audit, quản trị rủi ro	Mô tả ở mức nguyên tắc; triển khai phụ thuộc tổ chức	Cần biến yêu cầu thành quy tắc kiểm tra trên log
FHIR/SMART & AuditEvent	Chuẩn hóa dữ liệu, hỗ trợ tích hợp ứng dụng và mô tả sự kiện audit	AuditEvent không tự suy luận đúng/sai theo chính sách nội bộ	Chuẩn hóa log theo bối cảnh EHR để kiểm chứng tuân thủ
RBAC/ABAC/Policy-as-code	Ra quyết định truy cập linh hoạt theo vai trò/thuộc tính	Khó quản trị thuộc tính và ngoại lệ nghiệp vụ; thiếu vòng kiểm chứng sau truy cập	Kết hợp enforcement + evidence để truy vết và đối soát
SIEM & phân tích log	Thu thập/tương quan sự kiện, cảnh báo theo luật/mẫu	Thiếu ngữ cảnh nghiệp vụ; chi phí vận hành; cảnh báo giả [41]	Tối giản use-case, ưu tiên cảnh báo có ý nghĩa tuân thủ
Tamper-evident logging (hash chain)	Bảo vệ toàn vẹn, bắt buộc phải có bằng chứng kiểm toán	Không tự phát hiện vi phạm; cần quản lý khóa/thời gian	Dùng để tăng độ tin cậy bằng chứng cho pipeline giám sát

Từ các tài liệu đã khảo sát, có thể thấy khi đặt vào bối cảnh cơ sở y tế vừa và nhỏ vẫn còn một vài điểm chưa thật sự trọn vẹn:

- Nhiều hướng tiếp cận hiện nay mới giải quyết tốt từng phần riêng lẻ, chẳng hạn có IAM/SSO để quản lý đăng nhập, có phân quyền để kiểm soát truy

cập, hoặc có log để ghi nhận hoạt động. Tuy vậy, việc nối các mảnh này lại thành một quy trình liền mạch : từ chính sách, đến thực thi, rồi đến kiểm chứng tuân thủ dựa trên bằng chứng vẫn chưa dễ thực hiện một cách nhất quán.

- Với SIEM và các giải pháp giám sát đầy đủ, rào cản thường nằm ở nguồn lực. Không chỉ là chi phí công cụ, mà còn là dung lượng lưu trữ, công vận hành và nhân sự theo dõi, tinh chỉnh cảnh báo. Vì vậy, nhiều cơ sở có xu hướng chỉ triển khai ở mức tối thiểu, hoặc ưu tiên vận hành trước rồi mới tính đến giám sát tuân thủ bài bản.

- Ở lớp bằng chứng, nhật ký đôi khi đã được ghi lại nhưng chất lượng chưa đủ để dùng cho kiểm toán/điều tra: dữ liệu phân tán ở nhiều hệ thống, thiếu chuẩn hoá, thiếu đồng bộ thời gian, hoặc chưa có cơ chế đảm bảo tính toàn vẹn để đối chiếu về sau.
- Cuối cùng, các bằng chứng đánh giá trong bối cảnh cơ sở vừa và nhỏ vẫn còn hạn chế. Nhiều công trình về SIEM chủ yếu dừng ở mức đề xuất hoặc thử nghiệm nhỏ, nên việc khẳng định hiệu quả khi áp dụng rộng rãi trong thực tế vẫn cần thêm dữ liệu và đánh giá [41].

2.3. Contribution of Research

Dựa trên các điểm còn thiếu ở phần trên, đề tài này hướng tới một vài đóng góp theo hướng thực tế hơn:

- Trước hết, đề tài đặt mục tiêu xây dựng một cách nhìn về giám sát tuân thủ dựa trên chính sách cho hệ thống hồ sơ bệnh án điện tử, trong đó trọng tâm là làm sao để những hoạt động truy cập có thể được kiểm chứng lại bằng dấu vết cụ thể.

- Tiếp theo, đề tài phác thảo một kiến trúc kết hợp điểm thực thi (PEP), nơi ra quyết định (PDP) và quy trình thu thập – phân tích nhật ký, đồng thời ưu tiên một số kịch bản tuân thủ cốt lõi để triển khai gọn và dễ vận hành hơn.
- Để tăng độ tin cậy của bằng chứng, đề tài đưa thêm cơ chế anchor hash và ghi nhật ký chống giả mạo theo chu kỳ, nhằm giúp việc đối chiếu và phát hiện can thiệp vào nhật ký trở nên rõ ràng hơn.
- Cuối cùng, đề tài định hướng triển khai theo hướng tối giản và tận dụng các thành phần nguồn mở, để phù hợp hơn với điều kiện hạ tầng và nhân lực của các cơ sở y tế vừa và nhỏ.

CHƯƠNG 3. PHƯƠNG PHÁP NGHIÊN CỨU VÀ THIẾT KẾ HỆ THỐNG

3.1. Thiết kế nghiên cứu và cách tiếp cận

Đồ án được triển khai theo hướng nghiên cứu thiết kế (research-by-design), trong đó mục tiêu của nhóm không chỉ dừng ở việc khảo sát hay mô tả hiện trạng mà hướng đến tạo ra một giải pháp kỹ thuật có thể triển khai, vận hành và kiểm chứng trong một bối cảnh đại diện. Lựa chọn này xuất phát từ nhu cầu thực tế khi các cơ sở y tế phải triển khai và vận hành các hệ thống hồ sơ/bệnh án điện tử, đồng thời ngày càng cần có cách chứng minh việc kiểm soát truy cập và truy vết theo hướng có thể kiểm toán. [48], [49], [28] Với đặc trưng đó, nhóm lựa chọn Design Science Research Methodology (DSRM) làm khung phương pháp chủ đạo, bởi DSRM nhấn mạnh tiến trình nghiên cứu theo chuỗi bước rõ ràng: nhận diện vấn đề, xác lập mục tiêu cho giải pháp, thiết kế và phát triển hiện vật, trình diễn trong bối cảnh sử dụng, đánh giá theo tiêu chí đo được và tổng kết đóng góp. Cấu trúc này giúp đồ án vừa đảm bảo tính học thuật (có quy trình, có lập luận, có đánh giá), vừa bám sát yêu cầu triển khai giải pháp trong môi trường khách hàng. [60]

Trong bối cảnh đề tài phát triển hệ thống tự động giám sát tuân thủ chính sách bảo mật EHR cho cơ sở y tế nhỏ và vừa, phạm vi của nhóm không nhằm xây dựng một hệ thống EHR hoàn chỉnh từ đầu, mà tập trung tạo ra một lớp giám sát tuân

thủ có thể tích hợp với EHR sẵn có (hoặc các hệ thống quản lý khám chữa bệnh tương đương). Định hướng này phù hợp với thực tế triển khai đa cơ sở, nơi mỗi đơn vị có thể khác nhau về quy trình và hạ tầng, trong khi vẫn cần một cách đánh giá tuân thủ dựa trên bằng chứng thống nhất. [25], [28] Từ đó, nhóm diễn giải tuân thủ theo cách tiếp cận dựa trên bằng chứng vận hành: hệ thống không kết luận dựa trên cảm tính hay khảo sát tự khai, mà dựa trên các dấu vết có thể kiểm chứng trong quá trình vận hành như định danh người dùng, hành vi truy cập, quyết định uỷ quyền và thao tác nghiệp vụ, vốn được ghi nhận dưới dạng log. Về phương pháp, nhóm coi log là nguồn dữ liệu quan sát trung tâm: log được thu thập và chuẩn hoá, các sự kiện được liên kết theo ngữ cảnh (ai – làm gì – trên tài nguyên nào – lúc nào – theo quyền gì), sau đó đối soát với các quy tắc để đưa ra kết luận tuân thủ và hình thành bằng chứng kiểm toán. Cách tiếp cận này phù hợp với tinh thần của hướng dẫn quản trị log trong an toàn thông tin, nơi log được xem là nền tảng cho giám sát, điều tra và kiểm toán. [61].

Do dữ liệu y tế là dữ liệu nhạy cảm, đồng thời việc triển khai thực tế trên nhiều cơ sở vượt quá phạm vi của một đồ án tốt nghiệp, nhóm lựa chọn chiến lược đánh giá trong môi trường giả lập có kiểm soát. Mục tiêu của đánh giá không phải chứng minh năng lực tấn công hay phòng thủ, mà tập trung chứng minh giải pháp có thể đo lường và chứng minh mức độ tuân thủ theo cách nhất quán và có thể giải thích. Cụ thể, nhóm thiết kế đánh giá để làm rõ ba năng lực cốt lõi: (i) thu thập và chuẩn hoá bằng chứng từ nhiều nguồn log theo một mô hình sự kiện thống nhất; (ii) thực thi kiểm tra tuân thủ dựa trên các luật/quy tắc có thể diễn giải và truy vết; và (iii) xuất cảnh báo, báo cáo tuân thủ theo ngữ cảnh vận hành của từng cơ sở. Với cách thiết kế này, đồ án được đặt đúng vai trò của một lớp giám sát tuân thủ: không thay thế hệ thống EHR, mà cung cấp cơ chế quan sát, đối soát và tạo bằng chứng để hỗ trợ quản trị rủi ro và kiểm toán trong thực tế.

3.2. Thiết kế hệ thống và phương pháp thu thập dữ liệu phục vụ giám sát tuân thủ

Xét ở góc độ kiến trúc, hệ thống được thiết kế theo nguyên tắc tách lớp giám sát khỏi lõi EHR để phù hợp mô hình triển khai cho nhiều cơ sở. Thay vì can thiệp sâu vào mô hình dữ liệu nội tại của từng EHR, giải pháp đứng ở các điểm giao tiếp và điểm quyết định chính sách để vừa kiểm soát, vừa quan sát và ghi nhận bằng chứng. Lựa chọn này nhằm giảm mức xâm lấn khi tích hợp và giúp triển khai thuận lợi hơn trong bối cảnh các cơ sở nhỏ và vừa có thể khác nhau về hạ tầng, quy trình vận hành, cũng như nền tảng EHR đang sử dụng. Khi lớp giám sát được đặt tại các điểm giao tiếp và điểm ra quyết định chính sách, việc quan sát và kiểm soát được thực hiện theo cùng một nguyên tắc, đồng thời giảm phụ thuộc vào mô hình dữ liệu nội tại của từng hệ thống EHR. Trên cơ sở đó, kiến trúc được tổ chức theo chuỗi định danh và xác thực, lớp cổng truy cập, lớp quyết định chính sách, lớp ứng dụng EHR và lớp giám sát tuân thủ. Cách tổ chức nhiều lớp giúp giảm rủi ro do cấu hình không đồng nhất giữa các cơ sở, đồng thời bảo đảm hệ thống vẫn hoạt động được ngay cả khi EHR của khách hàng khác nhau về công nghệ và mô hình dữ liệu.

Commented [1]: sài từ dễ hiểu hơn ở đoạn này

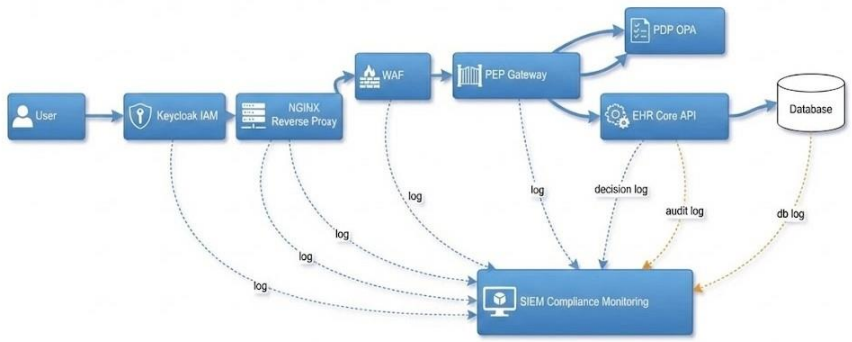


Figure 3.1. Overall architecture of the proposed compliance monitoring system for SME healthcare facilities.

3.2.1. Lớp định danh và xác thực dựa trên chuẩn, bảo đảm tính truy vết

Giải pháp sử dụng OpenID Connect làm lớp xác thực trên nền OAuth 2.0 để chuẩn hóa luồng đăng nhập, phát hành token và duy trì thông tin định danh xuyên suốt các request về sau. Theo cách tiếp cận này, sau khi người dùng được xác thực thành công, hệ thống phát hành token và các request về sau sẽ mang theo token để các thành phần phía sau có thể nhận biết được ai đang truy cập, thay vì mỗi thành phần phải tự xây dựng cơ chế xác thực riêng. [62]. OpenID Foundation

Trên cùng nền đó, OAuth 2.0 đảm nhiệm phần uỷ quyền, tức là xác định phạm vi truy cập của client đối với tài nguyên thông qua access token, đồng thời phân tách rõ các vai trò như chủ sở hữu tài nguyên, client và resource server. Việc tách bạch này giúp luồng truy cập rõ ràng hơn và thuận lợi cho việc ghi nhận, đối soát khi cần truy vết theo phiên và theo hành vi truy cập.[63]. RFC Editor

Commented [2]: thay từ khác đồng nghĩa

Trong đồ án, các token được biểu diễn theo định dạng JSON Web Token (JWT). Nói cách khác, JWT là định dạng gọn nhẹ để mang các claim cần thiết (ví dụ thông tin định danh và phạm vi quyền), phù hợp khi truyền qua HTTP header và có thể đảm bảo tính toàn vẹn bằng chữ ký hoặc MAC. [64]. RFC Editor

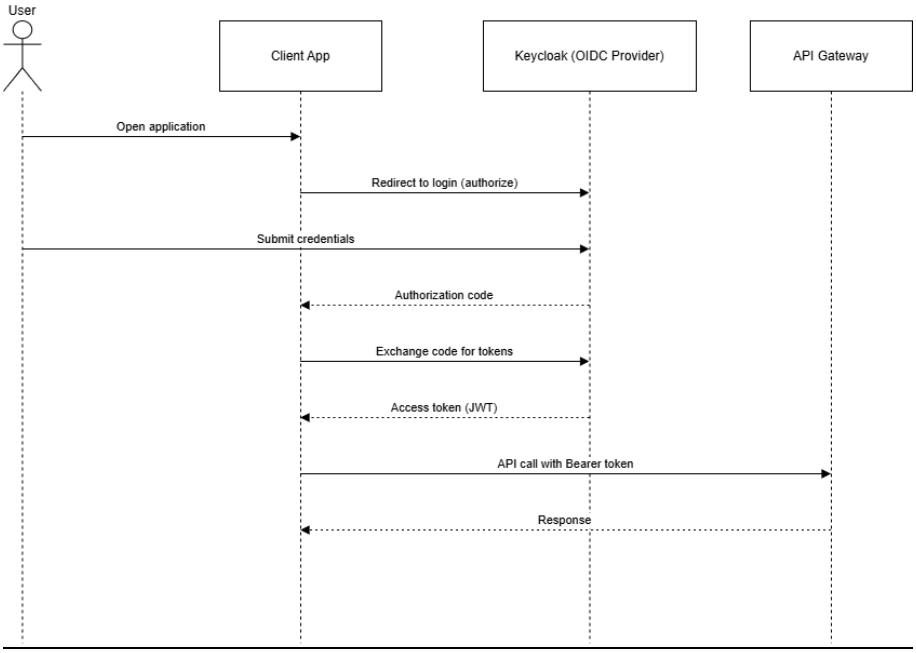


Figure 3.2. OpenID Connect based authentication and token issuance flow.

Trong triển khai tham chiếu, nhóm lựa chọn Keycloak làm nền tảng IAM vì hệ thống này hỗ trợ đầy đủ các endpoint theo chuẩn OpenID Connect và phù hợp với mô hình SSO cho ứng dụng web. Nhờ vậy, nhóm giảm được phần công tự phát triển các chức năng IAM cơ bản, đồng thời khi tích hợp cho từng cơ sở có thể chủ yếu cấu hình realm, client và role thay vì phải chỉnh sửa mã nguồn ứng dụng.[65] Keycloak

3.2.2. Lớp cổng truy cập và điểm quyết định chính sách, tách enforcement khỏi application code

Để việc kiểm soát truy cập được tập trung và dễ quan sát hơn, đồ án đặt một reverse proxy phía trước EHR Core nhằm gom các luồng request về một điểm. Nhờ đó, hệ thống thuận lợi hơn trong việc gắn thông tin định danh, kiểm soát header, ghi log truy cập và điều phối request đến các dịch vụ phía sau. Theo hướng dẫn của NGINX, reverse proxy có thể chuyển tiếp request đến upstream server, sửa đổi request header và điều chỉnh cơ chế buffering, vì vậy phù hợp khi đóng vai trò là "cổng vào" của hệ thống. [66] NGINX Docs

Về uỷ quyền, đồ án áp dụng mô hình quyết định chính sách tách rời, trong đó Policy Decision Point (PDP) đảm nhiệm việc đánh giá luật và Policy Enforcement Point (PEP) thực thi kết quả cho phép hoặc từ chối. Cách tổ chức này phù hợp với mô hình Attribute Based Access Control (ABAC), vì ABAC đưa ra quyết định dựa trên thuộc tính của chủ thể, đối tượng, thao tác yêu cầu và điều kiện môi trường. Nhờ vậy, hệ thống có thể biểu diễn các ràng buộc theo ngữ cảnh vốn rất phổ biến trong y tế, chẳng hạn đúng vai trò, đúng khoa, đúng ca trực hoặc đúng quan hệ điều trị. [67]. NIST Publications

Open Policy Agent được sử dụng như policy engine theo hướng policy as code, cung cấp ngôn ngữ khai báo và API để tách logic chính sách khỏi mã ứng dụng. Cách làm này giúp nhóm dễ cập nhật chính sách theo từng cơ sở mà không cần sửa trực tiếp EHR Core. [68]. openpolicyagent.org

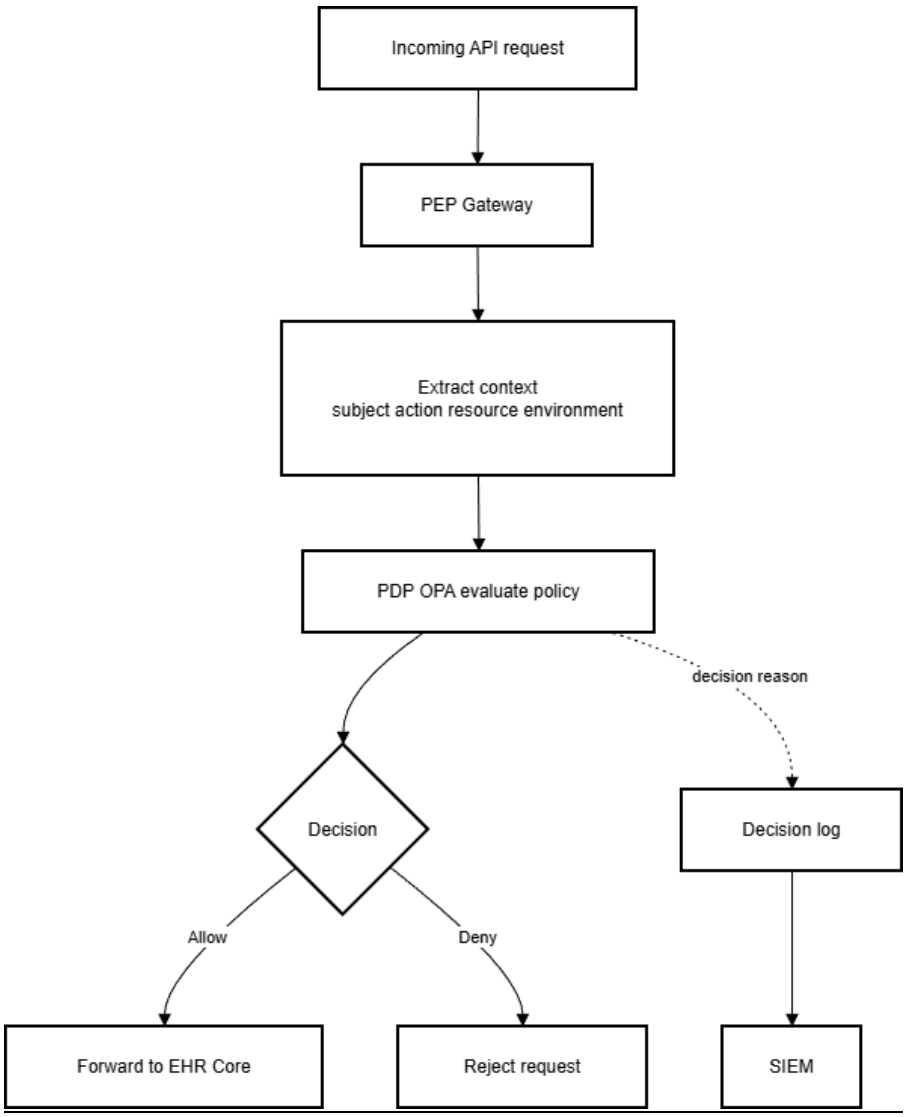


Figure 3.3. Policy enforcement workflow using PEP and PDP with decision logging.

Để tránh nhầm lẫn trong quá trình triển khai và đánh giá, hệ thống phân biệt hai lớp luật. Thứ nhất là lớp luật enforcement theo thời gian thực, thường nằm trong policy module của PDP, có nhiệm vụ trả lời ngay việc cho phép hay từ chối truy

cập dựa trên vai trò và các thuộc tính ngữ cảnh. Thứ hai là lớp luật tuân thủ ở tầng giám sát, được thực thi theo cơ chế hậu kiểm trên log nhằm kết luận mức tuân thủ và tạo báo cáo. Hai lớp luật này bổ trợ cho nhau: enforcement giúp giảm rủi ro truy cập trái phép ngay tại thời điểm truy cập, còn giám sát tuân thủ giúp đo lường và chứng minh mức độ đáp ứng kiểm soát theo thời gian

3.2.3. Thu thập log như bằng chứng, chuẩn hoá theo mô hình sự kiện kiểm toán

Dữ liệu đầu vào phục vụ giám sát tuân thủ là log được thu thập từ nhiều thành phần khác nhau, bao gồm lớp IAM, reverse proxy, lớp uỷ quyền, lớp ứng dụng EHR và khi cần có thể bổ sung log truy vấn ở tầng dữ liệu. Cách thu thập theo hướng đa nguồn giúp hệ thống tái dựng được chuỗi hành động đầy đủ theo phạm vi giám sát, từ bước đăng nhập cho đến các thao tác truy xuất dữ liệu, đồng thời hạn chế tình trạng thiếu ngữ cảnh nếu chỉ dựa vào một nguồn log đơn lẻ. Hướng dẫn quản trị log của NIST cũng nhấn mạnh rằng log cần được thu thập, lưu trữ, bảo vệ và phân tích như một quy trình hoàn chỉnh để phục vụ giám sát và kiểm toán, thay vì chỉ ghi log nhằm mục đích gỡ lỗi. [61]

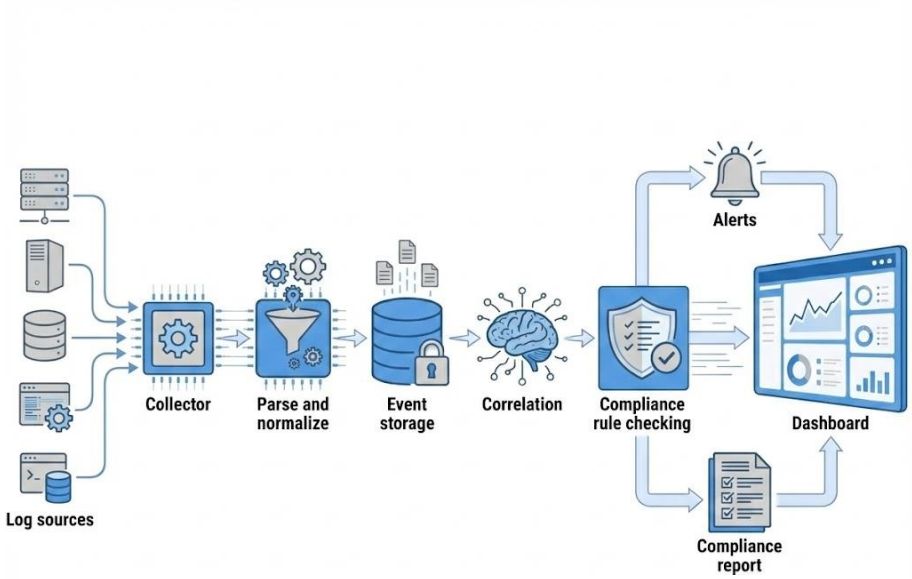


Figure 3.4. SIEM based compliance monitoring pipeline from log collection to compliance reporting.

Ngoài các nguồn log vận hành cốt lõi, nhóm bổ sung thêm một nguồn sự kiện phản ánh các truy cập bất thường ở tầng web để làm rõ năng lực giám sát và cảnh báo, vốn là một phần quan trọng khi chứng minh các kiểm soát an toàn đang được thực thi đối với dịch vụ EHR. Theo đó, hệ thống tích hợp WAF nhằm ghi nhận tốt hơn các request nghi ngờ và tạo thêm bằng chứng về cơ chế phát hiện, cảnh báo truy cập bất thường. WAF được cấu hình dựa trên bộ luật OWASP Core Rule Set, là tập luật phổ biến thường được triển khai cùng ModSecurity hoặc các WAF tương thích để nhận diện các mẫu tấn công điển hình ở tầng ứng dụng web [69]. Cần nhấn mạnh rằng việc đưa WAF vào kiến trúc không nhằm kiểm tra năng lực kiểm thử xâm nhập, mà nhằm bổ sung một nhóm sự kiện quan trọng phục vụ đánh

giá tuân thủ, cụ thể là khả năng ghi nhận và cảnh báo truy cập bất thường đối với dịch vụ EHR.

Để báo cáo tuân thủ có thể so sánh giữa các cơ sở và thuận lợi cho kiểm toán, các bản ghi cần được chuẩn hoá theo cùng một cách mô tả sự kiện, thay vì giữ nguyên các định dạng log khác nhau theo từng thành phần hoặc từng sản phẩm. Vì vậy, nhóm chuẩn hoá các bản ghi sự kiện theo hướng bám gần tư duy AuditEvent của HL7 FHIR. Theo đặc tả này, AuditEvent mô tả các sự kiện liên quan đến vận hành, quyền riêng tư, bảo mật và phân tích hiệu năng, qua đó phục vụ mục đích kiểm toán và chứng minh các cơ chế bảo vệ đang hoạt động đúng. [70].

Trên nền đó, hệ thống trích xuất các trường tối thiểu gồm thời điểm, tác nhân, hành động, đối tượng dữ liệu và kết quả, sau đó lưu vào kho log để phục vụ liên kết sự kiện và đối soát luật tuân thủ ở các bước tiếp theo.

3.3. Phương pháp phân tích dữ liệu và cơ chế đánh giá tuân thủ theo từng cơ sở y tế

3.3.1. Tham số hoá theo hồ sơ cơ sở để tránh kết luận "một chuẩn cho tất cả"

Vì đề tài được định vị theo hướng triển khai cho nhiều cơ sở, nhóm đưa vào khái niệm hồ sơ cơ sở như một tập tham số mô tả cách từng cơ sở vận hành và áp dụng chính sách trong thực tế. Hồ sơ này bao gồm các thành phần cốt lõi như hệ vai trò nghiệp vụ, cách phân chia khoa phòng, nhóm hành động nghiệp vụ tương ứng với các API hoặc chức năng trong EHR, các điều kiện ngữ cảnh đặc thù (ví dụ ca trực), cũng như những ngoại lệ được xem là hợp lệ theo quy chế nội bộ của từng đơn vị. Trên thực tế, chính sự khác nhau giữa các cơ sở khiến việc đánh giá tuân thủ bắt buộc phải đặt trong ngữ cảnh. Ví dụ, tại cơ sở A, điều dưỡng có thể được phép xem một phần thông tin hành chính để phục vụ tiếp nhận; trong khi ở cơ sở B, hành vi này chỉ được chấp nhận khi điều dưỡng có phân công trực tiếp liên quan đến bệnh nhân. Do đó, nhóm không xem việc hai cơ sở cho ra kết quả tuân

thủ khác nhau là mâu thuẫn, mà coi đây là yêu cầu quan trọng mà một hệ thống giám sát đa cơ sở cần đáp ứng, tức là đánh giá đúng theo chính sách và cách vận hành của từng nơi.

Ở tầng enforcement, các tham số trong hồ sơ cơ sở được đưa vào PDP dưới dạng thuộc tính để ABAC có thể áp dụng luật theo đúng ngữ cảnh. NIST mô tả ABAC như một phương pháp uỷ quyền dựa trên thuộc tính của subject, object, operation và có thể bao gồm thêm điều kiện môi trường; đây là cơ sở để nhóm biểu diễn các ràng buộc ngữ cảnh vốn rất phổ biến trong nghiệp vụ y tế. [67]. NIST

Ở tầng giám sát tuân thủ, hồ sơ cơ sở tiếp tục đóng vai trò "khung diễn giải", quyết định cách hệ thống hiểu các sự kiện thu thập được. Chẳng hạn, hồ sơ sẽ quy định nhóm hành động nào được xem là "truy cập hồ sơ", nhóm hành động nào tương ứng "xuất dữ liệu", và ngưỡng nào được xem là bất thường dựa trên năng lực vận hành cũng như quy trình làm việc của từng cơ sở.

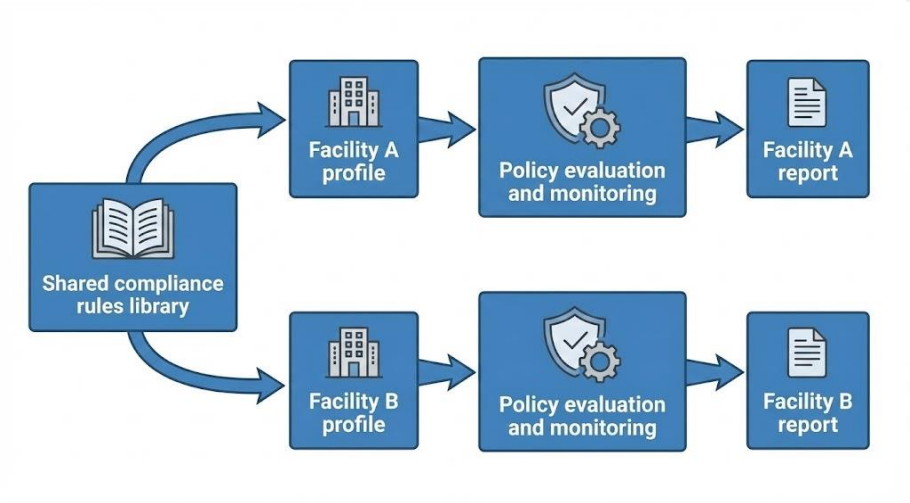


Figure 3.5. Multi facility compliance evaluation using site profiles and parameterized rules.

3.3.2. Liên kết sự kiện và đối soát luật, tạo kết luận tuân thủ có thể giải thích và kiểm toán

Quy trình phân tích trong SIEM được thiết kế theo hướng tái dựng chuỗi hành động của người dùng, thay vì xử lý từng dòng log một cách rời rạc. Khi phát sinh một thao tác nghiệp vụ, các sự kiện liên quan được gom theo các khoá tương quan như người dùng, phiên làm việc, token id hoặc request id, từ đó hình thành một phiên hành vi đủ bối cảnh theo phạm vi giám sát để mô tả diễn biến của một lần truy cập. [40], [41]. Trên mỗi phiên hành vi, việc tách hai tầng giúp tránh tình trạng kết luận tuân thủ dựa trên các sự kiện không đủ tin cậy về mặt định danh và uỷ quyền, đồng thời đảm bảo mỗi kết luận đều truy ngược được về luật và bằng chứng cụ thể. Ở tầng thứ nhất, các điều kiện nền tảng liên quan đến định danh và uỷ quyền theo chuẩn được kiểm tra dựa trên tính hợp lệ của bằng chứng truy cập. Cụ thể, hệ thống đối chiếu các thông tin như issuer/audience, thời hạn hiệu lực, phạm vi quyền (scope) và các claim định danh cần thiết, đồng thời kiểm tra cơ chế bảo vệ tính toàn vẹn của token theo các yêu cầu tương ứng của OpenID Connect, OAuth 2.0 và JWT. Bước này giúp bảo đảm các sự kiện truy cập có thể truy vết và đối chiếu thống nhất trước khi chuyển sang đánh giá tuân thủ ở mức kiểm soát. [62], [63], [64]. Ở tầng thứ hai, các điều kiện tuân thủ được đối soát theo từng nhóm kiểm soát, chẳng hạn nhóm kiểm soát truy cập, nhóm kiểm toán và nhóm giám sát an ninh. Mỗi kết luận vi phạm được gắn với luật cụ thể và trỏ đến bằng chứng tương ứng trong chuỗi sự kiện, nhờ đó kết quả đánh giá có thể được giải thích, kiểm tra lại và sử dụng như một phần của hồ sơ kiểm toán khi cần.

Cách tổ chức luật tuân thủ được xây dựng theo tư duy nhóm kiểm soát thường gặp trong các bộ kiểm soát an toàn thông tin, trong đó Access Control và Audit and Accountability là hai nhóm đặc biệt quan trọng đối với hệ thống xử lý dữ liệu nhạy cảm [71]. Việc bám theo cấu trúc nhóm kiểm soát giúp báo cáo tuân thủ dễ theo dõi hơn đối với các cơ sở nhỏ và vừa, vì cơ sở có thể nhận ra vấn đề nằm ở

nhóm nào, thiếu do chưa ghi nhận log đầy đủ, do chính sách truy cập chưa phù hợp, hay do chưa có cơ chế theo dõi và cảnh báo bất thường. Theo hướng này, báo cáo không chỉ tổng hợp kết quả, mà còn hỗ trợ xác định phần cần cải thiện và đi kèm bằng chứng cụ thể.

3.3.3. Bảo toàn bằng chứng log ở mức "tamper evident" trong phạm vi đồ án

Trong đánh giá tuân thủ, giá trị của log phụ thuộc trực tiếp vào mức độ tin cậy của log. Nếu log có thể bị xóa hoặc chỉnh sửa mà không để lại dấu hiệu, hệ thống sẽ rất khó sử dụng log như bằng chứng khi cần kiểm tra hoặc đối chiếu. Vì vậy, trong phạm vi triển khai, giải pháp bổ sung cơ chế bảo toàn bằng chứng theo hướng tamper-evident, lấy mục tiêu ưu tiên là phát hiện và ghi nhận dấu hiệu can thiệp để bảo vệ giá trị bằng chứng kiểm toán, thay vì theo đuổi mô hình đòi hỏi hạ tầng và quy trình vận hành phức tạp.

Hướng tiếp cận được dùng dựa trên ý tưởng liên kết log theo chuỗi băm nhằm tạo tính toàn vẹn theo hướng về phía trước: mỗi bản ghi mới được gắn với bản ghi trước đó thông qua giá trị băm, khiến việc sửa hoặc xoá một bản ghi ở giữa chuỗi dễ tạo ra sai lệch có thể phát hiện. Các nghiên cứu kinh điển về secure logging đã chỉ ra cách tổ chức này giúp việc can thiệp vào log sau khi xâm nhập trở nên khó che giấu, vì thay đổi sẽ làm đứt mạch liên kết giữa các bản ghi. [72]. USENIX

Trên cơ sở đó, hệ thống thực hiện đối soát theo chu kỳ và phát cảnh báo mức nghiêm trọng cao khi phát hiện dấu hiệu sai lệch, chẳng hạn đứt chuỗi băm hoặc không khớp tại các mốc đối soát. Cách làm này giúp yêu cầu "bằng chứng kiểm toán phải đáng tin" được chuyển thành một điều kiện kiểm tra cụ thể và có thể theo dõi trong chính hệ thống giám sát.

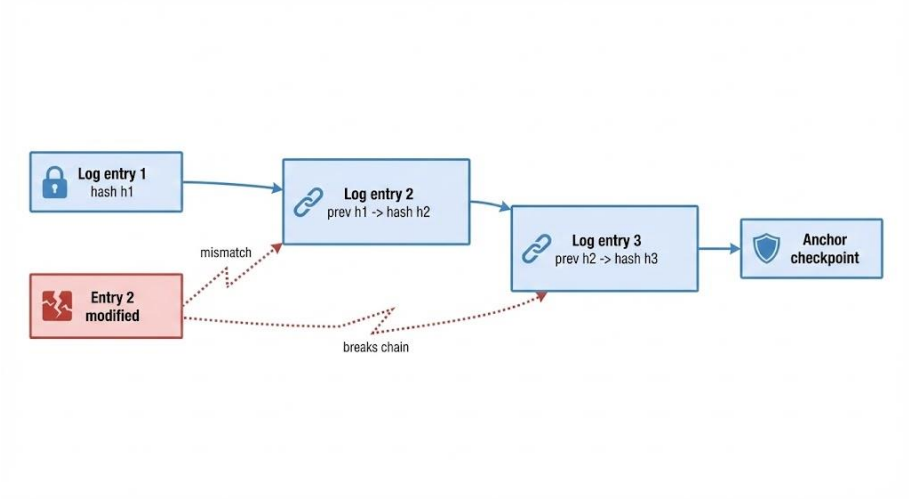


Figure 3.6. Tamper evident logging concept using hash chaining and periodic anchoring.

3.4. Giới hạn nghiên cứu và phạm vi áp dụng

Trong quá trình thực hiện đề tài này, nhóm đã nhận thấy có một số hạn chế cần được nêu rõ như:

Thứ nhất, vì không có điều kiện tiếp cận dữ liệu y tế thật từ các bệnh viện với lý do bảo mật về pháp lý và dữ liệu riêng tư của bệnh nhân, vì vậy nên nhóm em đã thực hiện đánh giá trong môi trường giả lập bằng cách thiết kế ra trang web Hồ sơ bệnh án điện tử EHR gần giống với dữ liệu thật khoảng 80%, và kết quả thử nghiệm cho thấy rằng hệ thống hoạt động tốt trong việc thu thập hành vi người dùng, ngữ cảnh và chuẩn hóa dữ liệu, liên kết các sự kiện trong EHR và kiểm tra tuân thủ. Tuy nhiên, chưa thể khẳng định hoàn toàn khi triển khai hệ thống thực tế bên ngoài, bởi ngoài đời thực có rất nhiều yếu tố phức tạp hơn. Ví dụ như mỗi nhà cung cấp phần mềm EHR sẽ có cách ghi log cho hệ thống của họ khác nhau, mỗi bệnh viện có cách chia mạng nội bộ khác nhau hoặc quy trình khám chữa bệnh ở mỗi bệnh viện cũng có thể khác nhau.

Thứ hai là chất lượng kết quả phân tích của hệ thống sẽ phụ thuộc vào việc các hệ thống nguồn như phần mềm EHR, Keycloak, Database phải được cấu hình đúng để ghi log đầy đủ hay không. Mặc dù hệ thống của nhóm là hệ thống giám sát được thiết kế để chuẩn hóa và đồng bộ dữ liệu log sau khi thu thập nhưng nếu hệ thống nguồn không ghi lại một sự kiện đúng với thời điểm mà người dùng thực

hiện truy cập ngay từ đầu, thì hệ thống giám sát sẽ không có cách nào khôi phục được thông tin đó. Ví dụ như máy chủ Keycloak ghi nhận thời gian đăng nhập sai lệch so với thực tế, việc xâu chuỗi các sự kiện giữa đăng nhập và truy cập dữ liệu sẽ bị ảnh hưởng. Đây là một trong những hạn chế có thể xảy ra và cần được khắc phục từ phía cấu hình các hệ thống nguồn trước khi triển khai [61]

Thứ ba, mặc dù hệ thống nhóm được thiết kế để linh hoạt và phù hợp với các cơ sở y tế vừa và nhỏ khác nhau, nhưng trong thực tế, mỗi phòng khám hoặc trung tâm y tế đều có quy trình làm việc và cách tổ cũng có thể khác nhau. Ví dụ như ở phòng khám đa khoa A, bác sĩ nào cũng có thể xem hồ sơ của tất cả bệnh nhân vì chỉ có 1 phòng khám duy nhất, nhưng ở phòng khám B có nhiều chi nhánh hơn thì bác sĩ ở chi nhánh 1 không được xem hồ sơ bệnh nhân của chi nhánh 2. Vì vậy, trước khi triển khai hệ thống tại một cơ sở cụ thể thì vẫn cần có giai đoạn khảo sát ban đầu để tìm hiểu rõ ràng và chính xác nghiệp vụ của các cơ sở y tế vừa và nhỏ đó. Hiện tại quy trình khảo sát và thiết lập của nhóm em vẫn đang thực hiện thủ công với sự hỗ trợ của công cụ AI, chưa thể xây dựng thành một quy trình tự động hoàn toàn.

Thứ tư, hệ thống sử dụng các tiêu chuẩn quốc như NIST SP 800-53 [30] làm nền tảng để xây dựng khung phân loại và bộ luật kiểm tra tuân thủ. Tuy nhiên, các tiêu chuẩn này được viết theo ngữ cảnh pháp lý của các nước phương tây trong khi các cơ sở y tế vừa và nhỏ tại Việt Nam cần tuân thủ theo các văn bản pháp luật trong nước như Nghị Định 13/2023/NĐ-CP về bảo vệ dữ liệu cá nhân và Thông Tư 46/2018/TT-BYT về quản lý hồ sơ bệnh án điện tử.Vì vậy, cần có thêm một bước chuyển đổi các điều khoản trong văn bản pháp luật Việt Nam sang các luật kỹ thuật mà hệ thống có thể hiểu và thực thi được. Ví dụ: Điều 9 của Nghị Định 13/2023 quy định: “Việc xử lý dữ liệu cá nhân nhạy cảm phải có sự đồng ý của chủ thể dữ liệu” cần được chuyển thành một luật kỹ thuật mà hệ thống có thể hiểu được. Hiện tại, việc chuyển đổi này đang thực hiện thủ công với sự hỗ trợ của các mô hình AI. Tuy nhiên, đây vẫn là quá trình khá tốn thời gian và đòi hỏi người thực hiện phải hiểu cả về luật pháp lẫn kỹ thuật.

REFERENCES

[1] thuvienphapluat.vn – Quyet dinh 5349 QD BYT 2019 phe duyet Ke hoach trien khai ho so suc khoe dien tu 428071. https://thuvienphapluat.vn/van-ban/The-thao-Y-te/Quyet-dinh-5349-QD-BYT-2019-phe-duyet-Ke-hoach-trien-khai-ho-so-suc-khoe-dien-tu-428071.aspx

[2] xaydungchinhsach.chinhphu.vn – nhung diem moi quan trong trong luat kham benh chua benh sua doi 119230203112956887. https://xaydungchinhsach.chinhphu.vn/nhung-diem-moi-quan-trong-trong-luat-kham-benh-chua-benh-sua-doi-119230203112956887.htm

[3] vanban.chinhphu.vn. https://vanban.chinhphu.vn/?pageid=27160&docid=205022

[4] baohiemxahoi.gov.vn – hoat dong bo nganh lien quan. https://baohiemxahoi.gov.vn/tintuc/Pages/hoat-dong-bo-nganh-lien-quan.aspx?CateID=0&ItemID=23491

[5] chiefhealthcareexecutive.com – small hospitals and clinics emerge as big targets for cyberattacks. https://www.chiefhealthcareexecutive.com/view/small-hospitals-and-clinics-emerge-as-big-targets-for-cyberattacks

[6] ruralhealthinfo.org – cybersecurity attacks. https://www.ruralhealthinfo.org/rural-monitor/cybersecurity-attacks

[7] cyberinsurancenews.org – healthcare cybersecurity medicaid cuts small hospitals 2025. https://cyberinsurancenews.org/healthcare-cybersecurity-medicaid-cuts-small-hospitals-2025/

[8] chinhphu.vn – default. https://chinhphu.vn/default.aspx?pageid=27160&docid=193779

[9] ncsgroup.vn – rhysida tuyen bo tan cong ransomware vao prospect medical de doa ban du lieu. https://ncsgroup.vn/rhysida-tuyen-bo-tan-cong-ransomware-vao-prospect-medical-de-doa-ban-du-lieu/

[10] ponemonsullivanreport.com – the protected health information crisis in healthcare. https://ponemonsullivanreport.com/2024/05/the-protected-health-information-crisis-in-healthcare/

[11] blackbookmarketresearch.com – 2024 State of the Cybersecurity Industry 01 12 23. https://blackbookmarketresearch.com/images/2024-State-of-the-Cybersecurity-Industry-01-12-23.pdf

[12] claroty.com – Clarotys state of cps security report healthcare exposures 2025. https://claroty.com/blog/clarotys-state-of-cps-security-report-healthcare-exposures-2025

[13] nvlpubs.nist.gov – nistspecialpublication800 92. https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-92.pdf

[14] dl.acm.org – 984334.984339. https://dl.acm.org/doi/epdf/10.1145/984334.984339

[15] ahima.org – healthcare data governance practice brief final. https://www.ahima.org/media/pmcb0fr5/healthcare-data-governance-practice-brief-final.pdf

[16] enisa.europa.eu – ENISA Report Cybersecurity for SMES Challenges and Recommendations. https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Report%20-%20Cybersecurity%20for%20SMES%20Challenges%20and%20Recommendations.pdf

[17] link.springer.com – s13677 025 00831 z. https://link.springer.com/article/10.1186/s13677-025-00831-z

[18] mdpi.com – 11 4 98. https://www.mdpi.com/2227-9709/11/4/98

[19] thuvienphapluat.vn – Nghi dinh 13 2023 ND CP bao ve du lieu ca nhan 465185. https://thuvienphapluat.vn/van-ban/Cong-nghe-thong-tin/Nghi-dinh-13-2023-ND-CP-bao-ve-du-lieu-ca-nhan-465185.aspx

[20] link.springer.com – s12910 022 00758 z. https://link.springer.com/article/10.1186/s12910-022-00758-z

[21] U.S. Department of Health & Human Services, 45 CFR § 164.312 - Technical safeguards, HIPAA Security Rule. https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-C/section-164.312

[22] ISO, ISO 27799 - Health informatics - Information security management in health, International Organization for Standardization. https://www.iso.org/standard/62777.html

[23] NIST, SP 800-53 Rev. 5: Security and Privacy Controls for Information Systems and Organizations, 2020. https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

[24] NIST, SP 800-137: Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations, 2011. https://csrc.nist.gov/publications/detail/sp/800-137/final

[25] Government of Vietnam, Decree No. 13/2023/ND-CP on personal data protection, 2023. https://vanban.chinhphu.vn/?classid=0&docid=207759&pageid=27160 (Alternative PDF: https://files.thuvienphapluat.vn/uploads/FileLargeTemp/2023/4/17/13_2023_ND-CP_465185.pdf)

[26] Vietnam National Assembly, Law No. 24/2018/QH14 (Cybersecurity Law), 2018. https://vanban.chinhphu.vn/?docid=206114&pageid=27160 (Alternative: https://thuvienphapluat.vn/van-ban/Cong-nghe-thong-tin/Luat-an-ninh-mang-2018-351416.aspx)

[27] Government of Vietnam, Decree No. 53/2022/ND-CP detailing a number of articles of the Cyber Security Law, 2022. https://vanban.chinhphu.vn/?classid=1&docid=206381&orggroupid=2&pageid=27160 (Alternative: https://thuvienphapluat.vn/van-ban/Cong-nghe-thong-tin/Nghi-dinh-53-2022-ND-CP-huong-dan-Luat-An-ninh-mang-398695.aspx)

[28] Ministry of Health, Circular 46/2018/TT-BYT regulating the use and management of electronic medical records, 2018. https://thuvienphapluat.vn/van-ban/Cong-nghe-thong-tin/Thong-tu-46-2018-TT-BYT-su-dung-va-quan-ly-ho-so-benh-an-dien-tu-391438.aspx

[29] HL7, FHIR Specification (R4/R4B/R5), Health Level Seven International. https://hl7.org/fhir/

[30] HL7, SMART on FHIR, Health Level Seven International. https://www.hl7.org/fhir/smart-app-launch/

[31] HL7, FHIR Resource: AuditEvent, Health Level Seven International. https://hl7.org/fhir/auditevent.html

[32] INCITS, ANSI INCITS 359-2012: Role Based Access Control, 2012. https://www.incits.org/standards/all-standards

[33] NIST, SP 800-162: Guide to Attribute Based Access Control (ABAC) Definition and Considerations, 2014. https://csrc.nist.gov/publications/detail/sp/800-162/final

[34] Open Policy Agent, OPA Documentation - Policy as Code, Open Policy Agent Project. https://www.openpolicyagent.org/docs/latest/

[35] IETF, RFC 6749: The OAuth 2.0 Authorization Framework, 2012. https://datatracker.ietf.org/doc/html/rfc6749

[36] OpenID Foundation, OpenID Connect Core 1.0, 2014. https://openid.net/specs/openid-connect-core-1_0.html

[37] IETF, RFC 7519: JSON Web Token (JWT), 2015. https://datatracker.ietf.org/doc/html/rfc7519

[38] Keycloak, Keycloak Documentation, Keycloak Project. https://www.keycloak.org/documentation

[39] NIST, SP 800-92: Guide to Computer Security Log Management, 2006. https://csrc.nist.gov/publications/detail/sp/800-92/final

[40] González-Granadillo, G.; González-Zarzosa, S.; Diaz, R., Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures, Sensors, vol. 21, no. 14, 4759, 2021. DOI: 10.3390/s21144759. https://doi.org/10.3390/s21144759

[41] López Velásquez, J.M.; Martínez Monterrubio, S.M.; Sánchez Crespo, L.E.; Garcia Rosado, D., Systematic review of SIEM technology: SIEM-SC birth, International Journal of Information Security, vol. 22, pp. 691–711, 2023. DOI: 10.1007/s10207-022-00657-9. https://doi.org/10.1007/s10207-022-00657-9

[42] Schneier, B.; Kelsey, J., Secure Audit Logs to Support Computer Forensics, ACM Transactions on Information and System Security, vol. 2, no. 2, pp. 159–176, 1999. https://doi.org/10.1145/317087.317092

[43] Ma, D.; Tsudik, G., A New Approach to Secure Logging, IACR Cryptology ePrint Archive, Report 2008/185, 2008. https://eprint.iacr.org/2008/185

[44] IETF, RFC 3161: Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP), 2001. https://datatracker.ietf.org/doc/html/rfc3161

[45] Verizon. (2024). Data Breach Investigations Report (DBIR) 2024. Verizon Business. https://www.verizon.com/business/resources/reports/dbir/

[46] Jiang, J. X., Ross, J. S., & Bai, G. (2025). Ransomware attacks and data breaches in U.S. health care systems. JAMA Network Open, 8(5), e2510180. https://doi.org/10.1001/jamanetworkopen.2025.10180

[47] Munoz Cornejo, G., Lee, J., & Russell, B. A. (2024). A thematic analysis of ransomware incidents among United States hospitals, 2016–2022. Health and Technology, 14, 1059–1070. https://doi.org/10.1007/s12553-024-00890-3

[48] Government Electronic Information Portal, 100% of hospitals must deploy electronic medical records before October 2025, March 19, 2025. https://baochinhphu.vn/100-benh-vien-phai-trien-khai-benh-an-dien-tu-truoc-thang-10-2025-102250319135405888.htm

[49] Ministry of Health, Decision 1150/QD-BYT dated April 3, 2025 approving the Plan to deploy electronic medical records, 2025. https://thuvienphapluat.vn/van-ban/Cong-nghe-thong-tin/Quyet-dinh-1150-QD-BYT-2025-phe-duyet-Ke-hoach-trien-khai-ho-so-benh-an-dien-tu-650763.aspx

[50] Ministry of Health, Decision 326/QD-BYT dated February 7, 2024 promulgating the Regulations on ensuring information security and network security of the Ministry of Health, 2024. https://thuvienphapluat.vn/van-

ban/Cong-nghe-thong-tin/Quyet-dinh-326-QD-BYT-2024-Quy-che-dam-bao-an-toan-thong-tin-an-ninh-mang-cua-Bo-Y-te-638785.aspx

[51] Viettel Threat Intelligence, Situation of information security risks in Vietnam in the first quarter of 2024, 2024. https://viettel.com.vn/media/viettel/documents/Final_Tinh_hinh_nguy_co_mat_ATTT_tai_Viet_Nam_quy_1_nam_2024_1.pdf

[52] Tran, D. M., Thwaites, C. L., Van Nuil, J. I., et al., Digital Health Policy and Programs for Hospital Care in Vietnam: Scoping Review, Journal of Medical Internet Research, 2022;24(2):e32392. https://doi.org/10.2196/32392

[53] Rule, A., Melnick, E. R., & Apathy, N. C., Using event logs to observe interactions with electronic health records: an updated scoping review shows increasing use of vendor-derived measures. Journal of the American Medical Informatics Association, 2023;30(1):144-156. https://academic.oup.com/jamia/article/30/1/144/6730799

[54] United Nations Development Programme (UNDP), Enhancing Digital Transformation in the Health Sector in Viet Nam: A Case Study on Application of Electronic Health Records in Lang Son, Binh Thuan and Tay Ninh Provinces, 2024. https://www.undp.org/vietnam/publications/enhancing-digital-transformation-health-sector-viet-nam-case-study-application-electronic-health-records-lang-son-binh-thuan-and

[55] World Economic Forum (PHSSR), Sustainability and Resilience in the Vietnamese Health System, PHSSR country report, 2021. https://www3.weforum.org/docs/WEF_PHSSR_Vietnam_Report.pdf

[56] Thwaites, C. L., Tran, D. M., et al., Status of Digital Health Technology Adoption in 5 Vietnamese Hospitals and Their Needs for Digital Transformation: Cross-Sectional Assessment. JMIR Formative Research, 2025;9:e53483. https://formative.jmir.org/2025/1/e53483

[57]A Design Science Research Methodology for Information Systems Research https://dl.acm.org/doi/10.2753/MIS0742-1222240302

[58] The Operational Role of Security Information and Event Management Systems https://ieeexplore.ieee.org/document/6924640

[59] Security and Privacy Controls for Information Systems and Organizations https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

[60] K. Peffers, T. Tuunanen, M. A. Rothenberger, and S. Chatterjee, "A Design Science Research Methodology for Information Systems Research," Journal of Management Information Systems, vol. 24, no. 3, pp. 45–77, 2007, doi: 10.2753/MIS0742-1222240302. Available: https://doi.org/10.2753/MIS0742-1222240302. Accessed: 07-Jan-2026. Indico

[61] K. A. Scarfone and P. M. Hoffman, "Guide to Computer Security Log Management," NIST Special Publication 800-92, Sep. 2006. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-92.pdf. Accessed: 07-Jan-2026. NIST Publications

[62] OpenID Foundation, "OpenID Connect Core 1.0," Final Specification. Available: https://openid.net/specs/openid-connect-core-1_0-final.html. Accessed: 07-Jan-2026. OpenID Foundation

[63] E. Hardt, "The OAuth 2.0 Authorization Framework," IETF RFC 6749, Oct. 2012. Available: https://www.rfc-editor.org/rfc/rfc6749.html. Accessed: 07-Jan-2026. RFC Editor

[64] M. Jones, J. Bradley, and N. Sakimura, "JSON Web Token (JWT)," IETF RFC 7519, May 2015. Available: https://www.rfc-editor.org/rfc/rfc7519.html. Accessed: 07-Jan-2026. RFC Editor

[65] Keycloak, “Securing applications and services with OpenID Connect,” Documentation. Available: https://www.keycloak.org/securing-apps/oidc-layers. Accessed: 07-Jan-2026. Keycloak

[66] NGINX, “NGINX Reverse Proxy,” Official Documentation. Available: https://docs.nginx.com/nginx/admin-guide/web-server/reverse-proxy/. Accessed: 07-Jan-2026. NGINX Docs

[67] V. C. Hu et al., “Guide to Attribute Based Access Control (ABAC) Definition and Considerations,” NIST Special Publication 800-162, Jan. 2014. Available: https://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.sp.800-162.pdf. Accessed: 07-Jan-2026. NIST Publications

[68] Open Policy Agent, “OPA Documentation,” Official Docs. Available: https://www.openpolicyagent.org/docs. Accessed: 07-Jan-2026. openpolicyagent.org

[69] OWASP Core Rule Set Project, “CRS Documentation,” coreruleset.org. Available: https://coreruleset.org/docs/. Accessed: 07-Jan-2026. CRS Project

[70] HL7, “AuditEvent,” FHIR Specification. Available: https://fhir.hl7.org/fhir/auditevent.html. Accessed: 07-Jan-2026. fhir.hl7.org

[71] NIST, “Security and Privacy Controls for Information Systems and Organizations,” NIST Special Publication 800-53 Revision 5, Sep. 2020. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf. Accessed: 07-Jan-2026. NIST Publications

[72] B. Schneier and J. Kelsey, “Cryptographic Support for Secure Logs on Untrusted Machines,” in Proc. 7th USENIX Security Symposium, Jan. 1998. Available:

https://www.usenix.org/publications/library/proceedings/sec98/full_papers/schneier/schneier.pdf