Compliance-Driven Architecture for Healthcare Industry

Syeda Uzma Gardazi and Arshad Ali Shahid
Department of Computer Science,
National University of Computer & Emerging Sciences (FAST-NU or NUCES),
Islamabad, Pakistan, PC 44000

***Abstract*—The United States (US) healthcare organizations are continuously struggling to cope-up with evolving regulatory requirements e.g. Health Information Technology for Economic and Clinical Health Act (HITECH) and International Organization for Standardization (ISO) 9001: 2015. These requirements are not only affecting the US healthcare industry but also other industries as well e.g. software industry that provides software products and services to healthcare organizations. It is vital for software companies to ensure and comply with applicable regulatory requirements. These evolving regulatory requirements may affect all phases of software development lifecycle including software architecture. It is difficult for Software architects to transform and trace regulatory requirements at software architecture level due to the absence of software design and architectural mechanisms. We have composed architectural mechanisms from given set of information security regulations i.e. Health Insurance Portability and Accountability Act (HIPAA) non-functional requirements, and these composed mechanisms were used to initiate initial architecture for the Electronic Health Record (EHR) and/or Health Level Seven (HL7). At next, style was selected for compliant and non-compliant software architecture. A layer of compliance was introduced in existing layered style that intends to help software companies to track compliance at software architecture level. Further, we have evaluated compliance-driven EHR architecture vs. non-compliant EHR architecture using a large healthcare billing and IT company with offices on three continents as a case study.**

Keywords*—Compliance-driven; architectural mechanisms; ISO 9001:2015; ISO 27001:2013; HIPAA; HITCH; software architecture; Logic-based Compliance Advisor (LCA); architectural evaluation

I. Introduction

It is vital for the United States (US) healthcare industry to ensure compliance with applicable standards and regulation e.g. Health Insurance Portability and Accountability Act (HIPAA) and Office of Inspector General (OIG) guideline, etc. The federal government of USA has started an audit process to evaluate the effectiveness of compliance program. In order to meet the technology requirements, the US federal government is continuously implementing the regulatory requirements e.g. HIPAA. These regulatory requirements are not only affecting the US healthcare industry but other industries as well. For example, software industry provides software products and services to the healthcare industry. The software product is highly affected by users, policies, and rules and regulations. It is essential for software companies to ensure compliance with requirements while developing and providing software to the US healthcare industry. A regulatory requirement extracted from regulation or standard can either belong to functional requirement category or non-functional requirement category [1]. The regulatory requirements may continuously affect all phases of software development lifecycle including software architecture phase. [2]. In now a days, software development process models' architecture is built, iteratively along with the software requirements [3]. Ghanavati has proposed a compliance framework to cope up with evolving regulatory requirements and it was validated using a case study [4].

As defined by SEI, tactic/mechanism is a reusable building block that can be used to define a design decision that can influence and control CA/QA response at architectural building block. A tactic is produced based on a set of NFRs that revels the solution for that architectural mechanism. At next level architecture is instantiated using that architectural mechanism along with NFRs [5].

Software architecture and requirements are directly related and stability in architecture is considered difficult to handle [6][8][9]. "Twin Peaks" model was proposed by Nuseibeh an improved version of iterative incremental model to demonstrate concurrent development of software's requirements and architecture. It is vital to evaluate effectiveness of architecture and it can be done at any stage of architecture lifetime as a standard part of development cycle. As suggested by Clements et al., architectural evaluation can hold either at development stage or maintenance stage [10].

The Software Engineering Institute (SEI) has introduced a number of methods and these have been applied on large number of projects of different sizes for years to evaluate architectures. Examples include Attribute-based Tradeoff Analysis Method (ATAM), Software Architecture Analysis Method (SAAM), Active Review for Intermediate Designs (ARID) and Attribute-Based Architectural Styles (ABAS) [11][12][13][14]. We have reviewed and applied ATAM and SAAM using a case study in evaluation section.

It is essential to bridge the gap between compliance of and software architecture. Failing to accommodate regulatory requirements will result in a non-compliant aware architecture and it possibly results in to violation of regulation and penalty imposed by governing agencies.

We have found that most of the work to ensure compliance is done at requirements level and there is still a need to reduce the gap between regulatory compliance and architecture. The research objectives being addressed in this paper include the following:

- HIPAA Compliance using ISO Quality and Security Management framework
- Introduction of additional attributes named as Compliance Attributes (CA) to address regulatory requirements which are architectural in nature
- Compliance-driven mechanisms for HIPAA, ISO and HITECH compliance
- Interaction between QAs and CAs
- CA impact on style
- Evaluation of proposed compliance-driven software architecture
- Empirical evaluation of proposed compliance-driven software architecture

We have used the US based Healthcare Billing Transcription Company (HTBIC) with a remote office located in AJK, US and Poland as a case study. HTBIC develops software and third party medical billing and transcription services for US healthcare industry. Recent studies showed that healthcare providers prefer to use electronic health records (EHR) on smart devices [15]. Further, EHR share data using HL7 layer. HTBIC was required to develop compliance-driven smartphone based EHR to meet customers need while ensuring that this product ensures compliance with all controlling and legal requirements. The remaining paper is organized as:

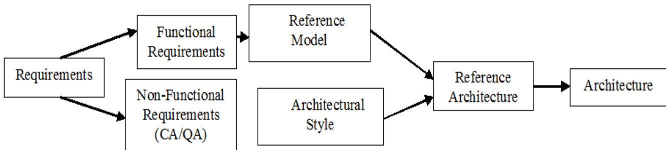


Fig. 1. Compliance-driven Software Architecture process

Section 2 gives a review about HIPAA and compliance attributes from HIPAA regulation. Further, we suggested a few compliance architectural mechanisms to represent and trace these compliance attributes at software architecture level. In Sections 4, 5, 6 and 7, we proposed reference model, compliance-driven styles along with compliance-driven software architecture using a case study that embodies regulatory requirements using architectural mechanisms as shown in Figure 1. Finally, compliance-driven architecture was evaluated and results and conclusion were discussed in the last section.

II. HIPAA Compliance Attributes (CA)

HIPAA is a United States' federal law that ensures confidentiality, integrity and availability of protected health information (PHI). PHI is defined in 45 CFR § 164.501. Covered Entity as defined in 45 CFR 160.103 is required to take necessary steps to ensure compliance with these HIPAA required ("R") clauses and addressable ("A") clauses. Covered Entities are mandated to comply with HIPAA required requirements but do not provide any specific framework. This paper proposes that HTBIC can integrate HIPAA requirements in its exiting ISO 9001:2015 Quality Management System (QMS) to reduce HIPAA compliance implementation overhead.

A. Identification, prioritization and cross-mapping of ISO 9001: 2015, ISO 27001: 2013 and HIPAA requirements

Requirement elicitation is the first step of software development life cycle. Requirements are categorized as functional requirements or non-functional requirements. A non-functional requirement is a condition that affects the behavior of the software and functional requirement specifies what software will do?. Regulatory requirements are cross-section of functional and non-functional requirements and covered entities are required to ensure compliance with these requirements e.g. HIPAA requirements. Quality Attributes (QA) are devises derived from requirements which are architectural in nature after identification of architectural requirements. With respect to software architecture, defined QAs address many generic architectural requirements and there is a need to defined attribute for specific needs like-regulatory requirements, PHI. Hence, we have developed attributes for this purpose named Compliance Attributes (CA) that address the additional HIPAA requirements which are architectural and are derived from the federal regulations set forth in HIPAA [16]. Some regulatory requirements can be mapped to existing QA, some required additional CA definition, and some are solely fulfilled by CA. For example, encryption requirement can be mapped on security QA. Whereas, HIPAA rule stringent this requirement by imposing that encryption method should be FIPs 140-2 compliant/validated (NIST SP 800-66 HIPAA Security Rule). Additional Compliance Attributes are introduced to address regulatory requirements which are also architectural in nature. Compliance Attributes are assigned high priorities which are derived from required HIPAA requirements and medium priority are assigned to those which are directly extracted from addressable HIPAA requirements.

HIPAA aimed at strengthening patient rights, increasing efficiency, and decreasing administrative cost. It is essential for all covered entities under HIPAA to protect PHI. On the other hand, ISO 9001:2015 is a Quality Management System (QMS) standard. The ISO 9001:2015 standard can be used for any company from product manufacturers to service providers and it is not specific to any product or industry. Rather than specify requirements for your final product – what you produce – ISO 9001 focuses further "upstream" on the processes, or how you produce.

We have compared HIPAA and ISO 9001:2013 to identify cross-mapping between these standard and regulation. Basic purpose of mapping is to find out whether compliance with one standard results in satisfaction of other or not. The ISO 9001:2015 controls meets or exceed the HIPAA Standards for 20% of the implementation requirements, where, the ISO 27001: 2013 controls meet or exceed the HIPAA Standards for 50% of the implementation requirements [17]. It is concluded that ISO 27001:2013 provides 30% better mechanisms to achieve HIPAA compliance than ISO 9001:2013 as shown in Table 1.

TABLE I. COMPARISON SUMMARY -OPERATORS FOR COMPARISON STANDARDS

Requirements	**Designation**	**Meaning**
Overlap	ISO~HIPAA	HIPAA and ISO requirements are same for the covered topic.
	ISO>HIPAA	The ISO requirements include HIPAA requirement along with additional requirements for the covered topic.
	HIPAA>ISO	HIPAA requirement includes at least one requirement not included in ISO requirements for the covered topic. The ISO Quality standard does not fully contain the HIPAA Standard.
Not found	!HIPAA	Requirement not found in the HIPAA standard. In this case ISO requirement will be greater than HIPAA (ISO>!HIPAA).
	!ISO	Requirement not found in the ISO 9001 standard. In this case HIPAA requirement will be greater than ISO requirement (HIPAA>!ISO).

B. *Devising Compliance Attributes (CA) and compliance utility tree for evaluation:*

Compliance attributes (CA) can be derived from law or other formally legally imposed requirements and it is architectural (AR) in nature to which a system must conform. Whereas compliance utility trees provide a tactic for translating the business requirements into attributes scenarios which is later used by ATAM for evaluation.

Tables 2 and 3 shows the HIPAA compliance utility tree for EHR architecture and prioritized quality and compliance attributes realized as scenarios. The three levels are defined as below:

HIPAA regulation and ISO 9001:2015 Standard		
Description	***Comparison***	***Percentage***
HIPAA and ISO 9001 requirements are same for the covered topic.	ISO9~HIPAA	15%
The ISO 9001 requirements include HIPAA requirement along with additional requirements for the covered topic.	ISO9>HIPAA	5%
HIPAA requirement includes at least one requirement not included in ISO 9001 requirements for the covered topic. The ISO 9001 Quality standard does not fully contain the HIPAA Standard.	HIPAA>ISO9	80%
ISO 27001:2013 Standard and HIPAA regulation		
HIPAA and ISO 27001 requirements are same for the covered topic.	ISO2~HIPAA	45%
The ISO 27001 requirements include HIPAA requirement along with additional requirements for the covered topic.	ISO2>HIPAA	5%
HIPAA requirement includes at least one requirement not included in ISO 27001 requirements for the covered topic. The ISO 27001 Quality standard does not fully contain the HIPAA Standard.	HIPAA>ISO2	50%

- the compliance level,
- quality level, and
- scenarios level [11].

The compliance and quality level are used to identify cross-mapping quality attributes against compliance attributes, if possible. The scenarios are defined at last level and ranked based on importance, AR and difficulty level.

TABLE II. SUMMARY OF UTILITY TREE RANKING

Ranking Description	**Term**	**Count**
Importance level states either the requirement is required or addressable. Required ("R") term is used to refer required requirements, and Addressable ("A") are used to refer addressable requirements.	R A	17 18
Requirement is architectural in nature using Yes ("Y") and No ("N").	Y N	28 7
Degree level is used to represent the difficulty level to achieve that scenario using: High ("H"), Medium (M), Low ("L") and Not applicable ("N/A")	H M L	6 15 7
	N/A	7

The HIPAA Security Rule requirements are categorized and ranked in below Table 3:

TABLE III. HIPAA COMPLIANCE ATTRIBUTE SCENARIOS FOR THE LOGIC-BASED COMPLIANCE ADVISOR (LCA)-BASED ELECTRONIC HEALTH RECORDS ("EHR")

TRANSMISSION SECURITY [164.312(E)(1)]

Requirements	**Attribute Name**	**Type**	**Ranking (Importance, AR and Difficulty)**
The EHR should provide a function to generate and verify a hash value to ensure integrity of PHI during transmission.	Integrity Controls	CA	A, Y, M
In this scenario the EHR should be able to encrypt/decrypt PHI according to FIPS standard while sending message over internet.	Network Protection	CA	A,Y, L

ACCESS CONTROL [164.312(A)(1)]

Requirements	**Attribute**	**Type**	**Ranking (IM, AR, D)**
The EHR should be capable to create a unique user ID and assign appropriate rights to this user ID.	Identification	CA	R, Y, M
The her should be capable to assign and allow emergency access to authorized user ID(s) during an emergency.	Break-the Glass / Security	CA/ QA	R, Y, M
The EHR should provide an option to lock session after specific time period of inactivity.	Automatic Lock/ Security	CA/ QA	A, Y, M
The EHR should be capable to encrypt and decrypt PHI (data at rest) using an algorithm approved by NIST/FIPS.	Encryption and Decryption	CA	A, Y, M

III. Devising Architectural Mechanisms (AM) for CAs

In this section we will define compliance-driven architectural mechanisms [19] to achieve CA at software architecture level.

A. *AM 1 Access Control*

The Department of Health and Human Services (HHS) under 45 CFR § 164.304 defined means necessary to read, write, modify, or communicate data. Covered Entities (CE) or Business Associates (BA) should consider multiple factor for administrative access e.g. two-factor authentication to enhance HIPAA compliance [18].

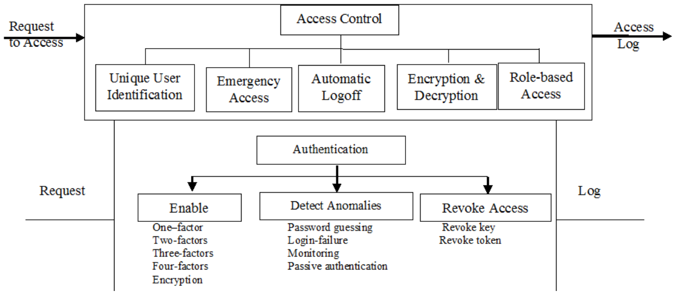


Fig. 2. Summary of access mechanisms in support of Authentication

Above tactic can be called as access control tactic under HIPAA. Stimulus is request to access and response is "access log". The relationship between stimulus, response, and access mechanisms is show in Figure 2.

Non-compliance of above CA will result in:

- Risk
- Non-Risk
- Sensitivity
- Tradeoff

Risk (R1): Unauthorized PHI disclosure, Non-Risk (NR1): Authorized PHI disclosure, Sensitivity (S1): Security and Trade-off (T1): Performance

Reasoning: The Department of Health and Human Services, hereinafter referred as "HHS", on May 27, 2011, issued a notice of proposed rulemaking, ("Proposed Rule"), to modify the HIPAA standard for accounting of disclosures of PHI. The purpose of these modifications is to implement the statutory requirement under the HITECH Act to require covered entities and business associates to account for disclosure of PHI to carry out treatment, payment, and healthcare operations if such disclosures are through an electronic health record.

B. *AM 2 Encryption*

As per HIPAA security rule, Entities should render PHI through the use of technology or methodology specified in the guidance issued under section 13402(h)(2) of HHS Pub. L.111-5 to secure PHI and avoid breach.

Stimulus is device/media assignment request and response is encryption status report. We represent the encryption tactic along with stimulus and response in Figure 3.

Non-compliance of above CA will result in:

- Risk
- Non-Risk
- Sensitivity
- Trade-off

Risk (R1): Unauthorized PHI disclosure, Non-Risk (NR1): Legitimate access to EPHI, Sensitivity (S1): Security and Trade-off (T1): Performance

Reasoning: Strong security measures must be put in place to safeguard PHI.

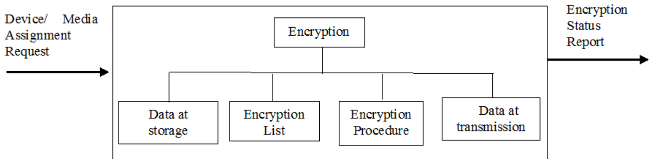


Fig. 3. Encryption AM

C. *AM 3 Incident Management (IM)*

HITECH does require notification of certain breaches of unsecured PHI. We represent the incident management tactic along with stimulus and response in Figure 4.

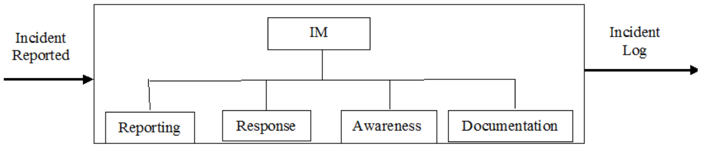


Fig. 4. Incident Management AM

Non-compliance of above CA will result in:

- Risk
- Non-Risk
- Sensitivity
- Trade-off

Risk (R1): Unauthorized PHI disclosure, Non-Risk (NR2): Authorized PHI disclosure, Sensitivity (S1): Security and Trade-off (T2): Availability

Reasoning: Limited access of PHI should be allowed to authorize users only.

D. *Business Continuity (BC)*

Stimulus is BC request and response is BC report. We represent the BC tactic along with stimulus and response in Figure 5.

Non-compliance of above CA will result in:

FAIR We are deeply indebted to Higher Education Commission (HEC) and Mr. Haq (CEO MTBC) for all the unforgettable generous support during Framework and Software Architecture for Information Assurance and Regulatory Compliance (FAIR) research process.

- Risk
- Non-Risk
- Sensitivity
- Trade-off

Risk (R2): PHI is not available to authorized users, Non-Risk (NR3): PHI availability, Sensitivity (S1): Security and Trade-off (T2): Availability

Reasoning: PHI should be accessible to authorize users only.

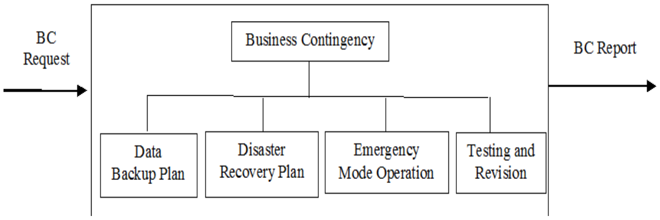


Fig. 5. Business Continuity AM

E. *Generic HIPAA Compliance Architectural Tacti*

The below mentioned section represents HIPAA Security Rule requirements as tactics:

Stimulus

Source

- Authorized User e.g. consultant
- Un-authorized User e.g. hacker

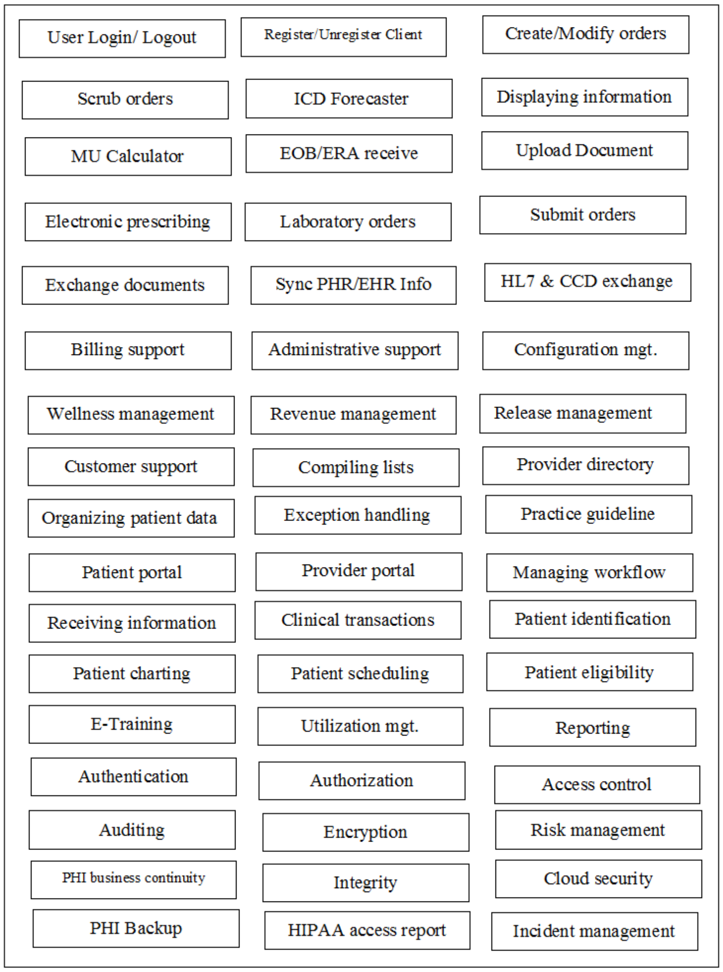
Type

- PHI Breach among covered entities
- Other types of PHI Breach

Ten AM were formulated for twenty eight CA but only four named access control, encryption, incident management, business continuity, accounting of PHI access and integrity were presented in this paper.

IV. Reference Model

A reference model is a higher level framework to represent interlinked components part of any concepts to ensure effective communication (see Figure 6).



User Login/ Logout	Register/Unregister Client	Create/Modify orders
Scrub orders	ICD Forecaster	Displaying information
MU Calculator	EOB/ERA receive	Upload Document
Electronic prescribing	Laboratory orders	Submit orders
Exchange documents	Sync PHR/EHR Info	HL7 & CCD exchange
Billing support	Administrative support	Configuration mgt.
Wellness management	Revenue management	Release management
Customer support	Compiling lists	Provider directory
Organizing patient data	Exception handling	Practice guideline
Patient portal	Provider portal	Managing workflow
Receiving information	Clinical transactions	Patient identification
Patient charting	Patient scheduling	Patient eligibility
E-Training	Utilization mgt.	Reporting
Authentication	Authorization	Access control
Auditing	Encryption	Risk management
PHI business continuity	Integrity	Cloud security
PHI Backup	HIPAA access report	Incident management

Fig. 6. Reference Model for EHR and HL7

V. Selection of Architecture Styles

Software architects use a number of commonly known "styles" to develop the architecture of a system. Architectural style is a set of design rules that identify the kinds of components and connectors that may be used to compose a system or subsystem, together with local or global constraints on the way the composition is done" (Shaw & Clements, 1996). Component types may also be distinguished by their package in the ways they interact with other components. Packaging is usually implicit which tends to hide important properties of the components. To clarify the abstractions we isolate the definitions of these interaction protocols in connectors (e.g., processes interact via message-passing protocols; UNIX filters interact via data flow through pipes). The connectors play a fundamental role in distinguishing one architectural style from another and have an important effect on the characteristics of a particular style.

A. Option 1(Data-centered architecure style):

On the basis of performance quality attribute blackboard data-cantered architecture style was selected for EHR and represented in Figure 7 [20]. Components communicate through a shared database.

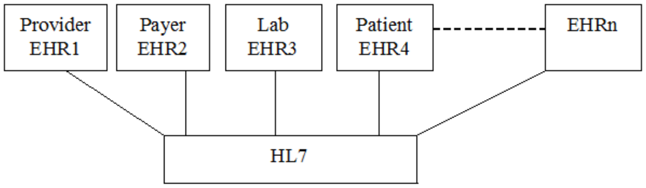


Fig. 7. Blackboard style for LCA-based EHR

B. Option 2:

On the basis of performance quality attribute and security compliance attribute client-server along with event-based implicit invocation were selected and represented in Figure 8. The invocation style is applicable to store the information in the log table and execute logics using Logic-based Compliance Advisor (LCA). Further, we have restructured layered architecture style by providing an additional layer of Compliance.

- Client-Server Style
- Layered Style
- Event-based Implicit Invocation Style

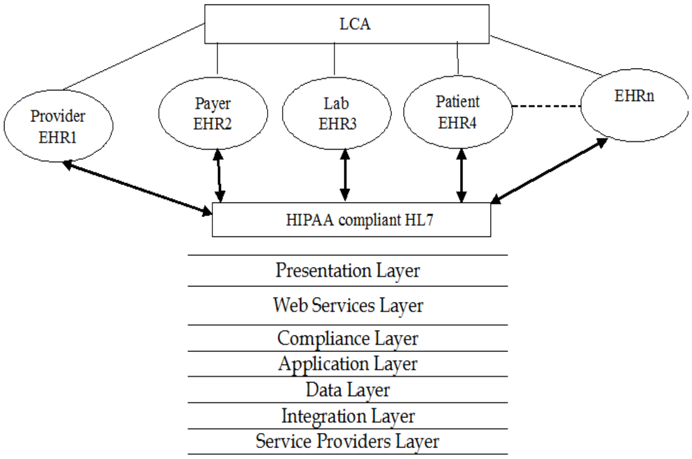
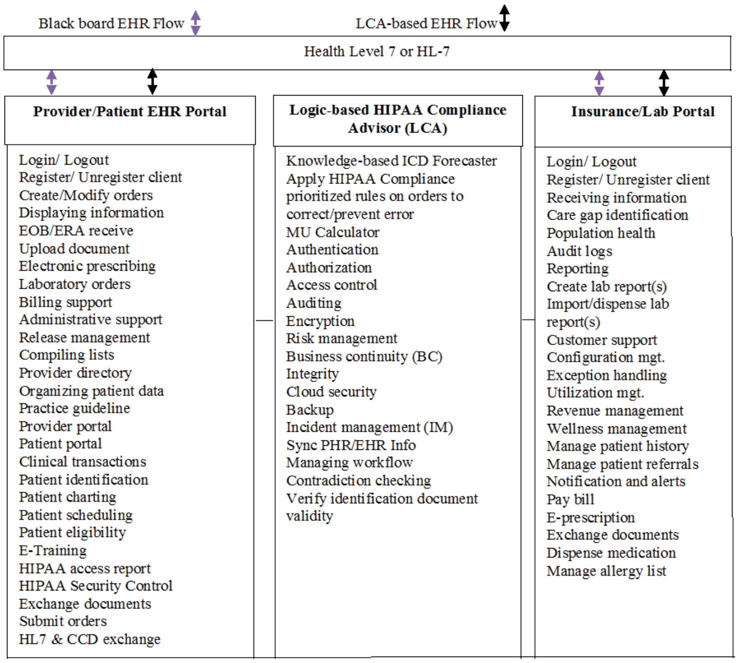


Fig. 8. Client-Server architecture style for LCA-based EHR.

In this before submitting the claim to HTBIC on submit command the rule procedure and function executes. In this it executes all the compliance rules including HIPAA rules on the order/claim. The LCA-based EHR does prioritize the rules and also maintain log which affect performance of the software. At next level, we will formulate reference model [24].

VI. Reference Architecture

A reference architecture is a template solution for a particular domain where the key elements and their relations provide guideline for software architecture. On the basis of reference model and architecture style we formulated reference architecture. Figure 9 shows the reference architecture for LCA-based EHR. Three major entities named as Provider/Patient EHR portal, LCA and Insurance/Lab portal contains different components identified earlier in reference model. The actual data of the medical claim consists of information about diagnosis, also known as diagnosis code (DxCode), information about procedures/treatment, also known as Current Procedure Terminology (CPT), information about patient demographics and some other information which is required by insurance for making payments. This data is stored in a relational database of the EHR portal, LCA will pick that data directly from the relevant and execute the logics before submitting the data to insurance/lab company. Reference model is merged with Option 2 style to produce reference architecture as shown in Figure 9.



Provider/Patient EHR Portal

Login/ Logout
Register/ Unregister client
Create/Modify orders
Displaying information
EOB/ERA receive
Upload document
Electronic prescribing
Laboratory orders
Billing support
Administrative support
Release management
Compiling lists
Provider directory
Organizing patient data
Practice guideline
Provider portal
Patient portal
Clinical transactions
Patient identification
Patient charting
Patient scheduling
Patient eligibility
E-Training
HIPAA access report
HIPAA Security Control
Exchange documents
Submit orders
HL7 & CCD exchange

Logic-based HIPAA Compliance Advisor (LCA)

Knowledge-based ICD Forecaster
Apply HIPAA Compliance prioritized rules on orders to correct/prevent error
MU Calculator
Authentication
Authorization
Access control
Auditing
Encryption
Risk management
Business continuity (BC)
Integrity
Cloud security
Backup
Incident management (IM)
Sync PHR/EHR Info
Managing workflow
Contradiction checking
Verify identification document validity

Insurance/Lab Portal

Login/ Logout
Register/ Unregister client
Receiving information
Care gap identification
Population health
Audit logs
Reporting
Create lab report(s)
Import/dispense lab report(s)
Customer support
Configuration mgt.
Exception handling
Utilization mgt.
Revenue management
Wellness management
Manage patient history
Manage patient referrals
Notification and alerts
Pay bill
E-prescription
Exchange documents
Dispense medication
Manage allergy list

Fig. 9. Reference Architecture for EHR and HL7

VII. Reference Architecture

In the software architecture components and connector are used to bind. The components are also called software elements and are held together by connectors. These connectors define the relationship between different components. The major emphasis is on components and interaction among them instead of the details make up by the subcomponents.

We have introduced a new concept of compliance-driven software architecture in which components and connector are bind to ensure compliance at software architecture level. On the basis of reference model and architecture style we formulated reference architecture. Figure 10 shows the reference architecture for EHR. Three major entities named as Provider, HTBIC and Insurance contains different components identified earlier in reference architecture phase. Provider, HTBIC and Insurance components are connected through connectors named as I1, I2, I3, I4, I5 and I6. Figure 10 represents a CA behaviour of LCA in EHR system [25].

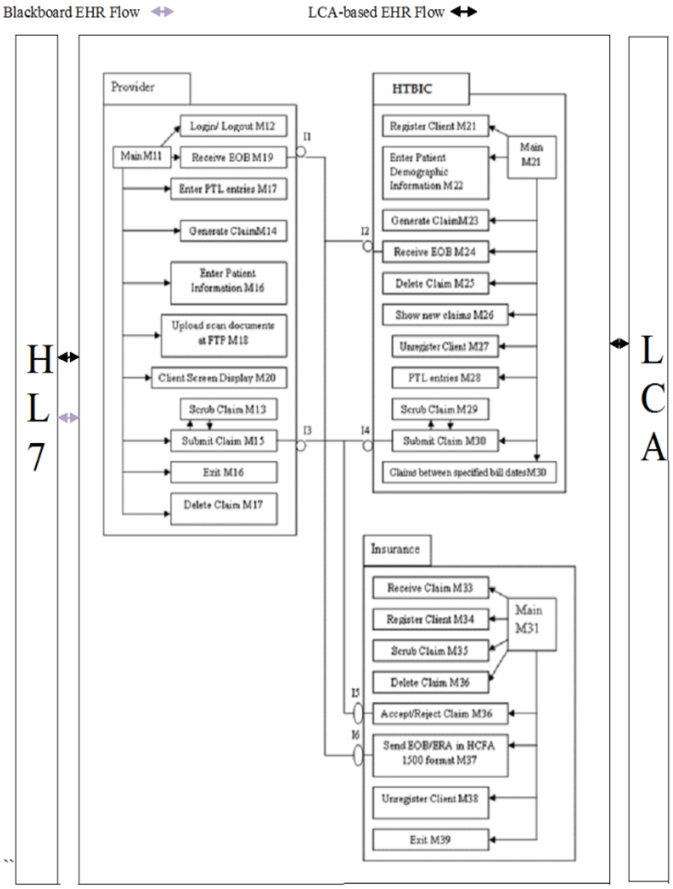


Fig. 10. EHR and HL7 Software Architecture

VIII. Compliance-Driven Software Architecture (CSA) Evaluation

A. *To what extent the CA justify the choice of the architecture?*

We have reviewed different software architecture evaluation methods and selected SAAM and ATAM to evaluate compliance-driven software architectures as these are scenario-based techniques that supports modifiability, security, performance, variability and achievement of functionality goals. Further, these techniques use thought experiments, walk through scenarios, assessment by experts' approaches to evaluation. SAAM was selected to assess modifiability in architecture along with attributes and ATAM was used to evaluate multiple attributes [19]. Qualities only have meaning within a context and SAAM specifies context through scenarios.

B. *Scenario-based evaluations of Blackboard Electronic Health Records ("EHR") using SAAM*

Compliance Scenario#1 (CS 1)

- Description: Controlled substances e-perception should be digitally signed before submission.
- Type (Direct/ Indirect): Indirect
- Changes: All components that call submit prescription must be modified.

Compliance Scenario#2 (CS 2)

- Description: Interception of and tampering with communication
- Type (Direct/ Indirect): Indirect
- Changes: Use Secure Socket Layer (SSL) transport layer security

Compliance Scenario#3 (CS 3)

- Description: Denial of service (DOS), sending large amount of data based on spoofed identifier
- Type (Direct/ Indirect): Indirect
- Changes: Implement server monitoring for high traffic from a particular user.

Blackboard EHR scenario-based analysis identified a number of severe software architecture level limitations to achieve HIPAA compliance as compared to LCA-based EHR (see Table 4) e.g. Accounting of disclosure and access control, etc.

TABLE IV. SCENARIO-BASED EVALUATION OF EHR AND HL7 ARCHITECTURES USING SAAM

Architecture Option	Scenario Type	Count	Scenario CS#
Option 1: Blackboard EHR	Direct	3	4, 5, 6
	Indirect	3	1, 2, 3
Option 2: LCA-based EHR	Direct	5	1, 4, 5, 6
	Indirect	1	2, 3

C. *Scenario-based evaluations using ATAM*

Trade-off between compliance and QA while choosing a particular tactic and style

We have selected two architectural styles for EHR to achieve performance and compliance attributes, respectively. Theses styles were mapped at architecture level and now we will evaluate them using ATAM to determine the useful characteristics of each of the architectural options using ATAM. ATAM determined the compliance architectural trade-off points, which helped to finalize architecture for HIPAA compliance.

Attribute-specific analysis:

Quality and compliance attributes are mapped against architectural options. If an attribute exists in an architecture option then it is represented by a mark (+). LCA-based EHR architecture is better than blackboard EHR architecture to ensure HIPAA compliance based on attribute analysis (see Table 5). Compliance scenarios along with risk, sensitivity and trade-off are mapped against architectural options. If a compliance scenario exists in an architecture option then it is represented by a mark (+). In ATAM, the term risk refers to is an architectural decision that may lead to objectionable consequences and similarly, a non-risk is an architectural decision that is considered safe. Sensitivity and trade-off terms are architectural choices that have consequence on one or more quality/compliance attributes, the former positively and the latter negatively.

TABLE V. ATTRIBUTE-SPECIFIC ANALYSIS OF COMPLIANCE-DRIVEN ARCHITECTURES

Attributes		Option 1 (Blackboard EHR)	Option 2 (LCA-based EHR)	CS#, AM#, R#, NR#, S3 and T#
QA1	Performance	+	-	NA
QA2	Availability	+	+	NA
CA1	Access Control	-	++	CS6, AM1, R1, NR1, S1, and T1
CA2	Encryption	+	+	CS2/CS3/CS5, AM2, R1, NR1, S1 and T1
CA3	Incident Management	-	+	NA
CA4	Risk Management	-	+	CS4, AM2, R1, NR1, S1 and T1
CA5	Business continuity	-	+	NA
CA6	Accounting of disclosure	-	++	NA
CA7	Integrity	-	+	CS1, AM6, R4, NR5, S1 and T1

Based on ATAM, we have come to the conclusion that LCR-based EHR has better ability to meet HIPAA compliance requirements as compared to the blackboard EHR.

IX. EMPIRICAL EVALUATION

Software evaluation technique: LCA-based EHR performance is real time as it is used by Providers, labs and Insurances, where employees are entering data with the help of EHR software and sharing it using HL7 standard. The blackboard EHR performed better in terms of time as it provides limited HIPAA compliance contains no additional compliance layer and doesn't maintain log as shown in Figure 11.

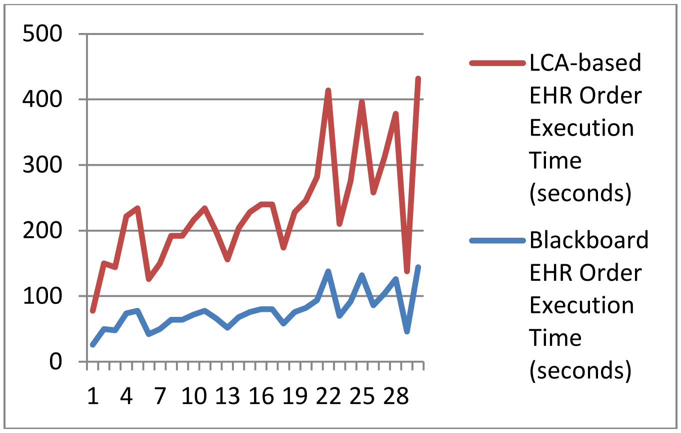


Fig. 11. Performance trend of blackboard EHR versus LCA-based HER

The relationship between execution time and logics applied can be shown by the equation 1 as mentioned below:

- Performance (seconds)= logic execution time/# of logics applied ----------------(1)
- The relationship between Order and Compliance can be shown by the equation 2 as mentioned below:
- # of Compliant Orders= Total Orders-Total Non-Compliant Orders ------------------(2)

It took approximately 0.7 second for an Order to apply 35 logics on it.

Compliance logic for electronic health records is shown in Table 6.

TABLE VI. COMPLIANCE LOGICS FOR ELECTRONIC HEALTH RECORDS ("EHR")

S no.	Logic Description	Passed	Failed	N/A	Regulation/Standard
1	Ensure confidential data are sent over an encrypted channel and ensure encryption is consistent with the FIPS 140-2 standard	2403	34	0	HITECH
2	Two-factor authentication is required for e-prescription (e-Rx) of a controlled substance to ensure Drug Enforcement Agency (DEA) rule requirement.	404	6	2	DEA
3	Convert primary account number (PAN) in unreadable format anywhere it is stored using encryption technique	23682	0	3517	PCI DSS
4	Provide a feature to account all types of PHI disclosures along with access report.	940	16	10	HITECH
5	Ensure that any personal information for which the organization is responsible is adequately protected in the country of destination when transferred across border and during transit (block country list is maintained)	27152	16	23	EU and UK Data Protection Act

X. Conclusion and Future Work

Software architecture is an iterative process and simultaneously carried-out along with the requirements phase. Architecture shall be compliant aware, where regulatory requirements should be bi-directional traceable to the architecture. It is also essential to bridge the gap between compliance and software architecture. Non-compliant aware architecture may result in to violation of regulation and penalty imposed by governing agencies. We have proposed compliance attributes to achieve HIPAA Security Rule compliance at software architecture level using compliance-driven mechanisms and styles. HTBIC needs to revise existing EHR procedures to bridge the compliance gap using ISO 9001:2015 process driven approach [26]. Further, two EHR architectures were evaluated and compliance of both software were measured. The blackboard EHR performed better in terms of time as it provides limited HIPAA compliance and doesn’t maintain log. The LCA-based EHR works better than blackboard EHR in terms of:

- improved data quality and compliance with healthcare IT industry standards/regulations compliance e.g. HIPAA,
- eliminated error-prone diagnosis and drug coding/delivery,
- monitored patient health remotely,
- 7 AMs are mapped on LCA based EHR,
- 2 AMs are mapped on black-board HER,
- ensure regulatory requirements with HIPAA compliant data, and
- better access log management.

Acknowledgment

The authors would like to thank HEC, Unique Healthcare Company and NUCES-FAST for their valuable contribution to the compliance-driven software architecture evaluation process.

Competing Interests

We declare that they have no competing interests.

Authors’ Contributions

Syeda Uzma Gardazi (UG) proposed compliance attributes and compliance mechanisms. Arshad Ali Shahid (AS) verified these mechanisms and requirements. Further, UG formulated and evaluated compliance-driven software using a case study which was also verified by AS. All authors read and approved the final manuscript.

References

[1] Annie I. Antón, Julia B. Earp and Jessica D. Young., How Internet Users’ Privacy Concerns Have Evolved Since 2002., IEEE Security & Privacy, 8(1), pp. 21-27, January/February 2010.

[2] Aaron K. Massey, Paul N. Otto, Lauren J. Hayward, and Annie I. Antón. Evaluating EHR Requirements for HIPAA Compliance: A Case Study, Requirements Engineering Journal, Springer-Verlag, 15(1), 119-137, January 2010.

[3] B. Nuseibeh, "Weaving together requirements and architecture", IEEE Computer, 34(3):115-117, March 2001

[4] Travis D. Breaux, Annie I. Antón and Eugene H. Spafford., A Distributed Requirements Management Framework for Legal Compliance and Accountability, Computers & Security, Elsevier, 28(1-2), pp. 8-17, February-March 2009.

[5] S.Kim, D.K. Kim, L. Lu, S. Park, Quality-driven. Architecture Development Using Architectural Mechanisms, J. Syst. Softw. 82, Aug. 2009, pp. 1211-1231.

[6] Finkelstein, A.: Architectural Stability. http://www.cs.ucl.ac.uk/staff/a.finkelstein/talks.html (2000)

[7] Garlan, D.: Software Architecture: A Roadmap. In: A. Finkelstein (ed.): The Future of Software Engineering, ACM Press (2000) 91-101

[8] van Lamsweerde, A.: Requirements Engineering in the Year 00: A Research perspective. In: Proc. 22nd International Conference on Software Engineering, Limerick, Ireland (2000) ACM Press 5-19

[9] Nuseibeh, B.: Weaving the Software Development Process between Requirements and Architectures. In: Proceedings of STRAW 01 the First International Workshop from Software Requirements to Architectures, Toronto, Canada (2001)

[10] Clements, P., Kazman, R., and Klein, M.: Evaluating Software Architectures: Methods and Case Studies. Addison Wesley, Boston, USA (2002)

[11] Abowd, G., Bass, L., Clements, P., Kazman, R., Northrop, L., and Zaremski, A.: Recommended Best Industrial Practice for Software Architecture Evaluation (CMU/SEI-96-TR-025), Software Engineering Institute, Carnegie Mellon University (1996)

[12] Kazman, R., Abowd, G., Bass, and L., Webb, M.: SAAM: A Method for Analyzing the Properties of Software Architectures. In: Proceedings of the 16th International Conference on Software Engineering, Sorento, Italy. IEEE CS (1994) 81-90

[13] Clements, P.: Active Reviews for Intermediate Designs. Technical Report (CMU/SEI-2000-TN-009), Software Engineering Institute, Carnegie Mellon University (2000)

[14] Klein, M., and Kazman, R.: Attribute-Based Architectural Styles. Technical Report CMU/SEI-99-TR-22, Software Engineering Institute, Carnegie Mellon University (1999)

[15] R. Istepanian, S. Laxminarayan, C. S. Pattichis, M-Health: Emerging Mobile Health Systems. Springer. ISBN 978-0-387-26558-2, eds, 2005.

[16] Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191, 110 Stat. 1936 (1996), Codified at 42 U.S.C. § 300gg and 29 U.S.C § 1181 et seq. and 42 USC 1320d et seq.

[17] Achieving HIPAA Security Standards compliance by implementing an ISO/IEC 27000 series Information Security Management System, from Zygma partnership, 2005-12-04

[18] Qingfeng He and Annie I. Antón. Requirements-based Access Control Analysis and Policy Specification (ReCAPS), Information & Software Technology, Elsevier, 51(6), pp. 993-1009, June 2009.

[19] S.Kim, D.K. Kim, L. Lu, S. Park, Quality-driven. Architecture Development Using Architectural Mechanisms, J. Syst. Softw. 82, Aug. 2009, pp. 1211-1231.

[20] Garlan, D., Allen, R., and Ockerbloom: Exploiting Style in Architectural Design Environments. In: Proceedings of SIGSOFT’94, Foundations of Software Engineering, New Orleans, Louisiana, USA, ACM Press(1994)175-188

[21] Baldwin, C. Y., and Clark, K.B.: Modularity and Real Options. Working paper, Harvard Business School (1993)

[22] Syeda Uzma Gardazi, Christine Salimbene and Arshad Ali Shahid, HIPAA and QMS based architectural requirements to cope with the OCR audit program, 3rd FTRA International Conference on Mobile Ubiquitous, and Intelligent Computing (MUSIC), 26-28 June 2012, Vancouver, Canada.

[23] Syeda Uzma Gardazi, and Arshad Ali Shahid, Taking Compliance Patterns and Quality Management System (QMS) Framework Approach to Ensure Medical Billing Compliance, 2nd International Conference on Health Information Science (HIS 2013), HIS Volume 7798 of the series Lecture Notes in Computer Science (pp 78-92), 25-27 March 2013, London, UK.

[24] Syeda Uzma Gardazi and Arshad Ali Shahid, Software Architecture for Information Assurance, International Conference on Product Focused

Software Development and Process Improvement (PROFES), 21-23 June 2010, Limerick, Ireland.

[25] Syeda Uzma Gardazi and Arshad Ali Shahid, Billing Compliance Assurance Architecture for Healthcare Industry (BCAHI), Computer Science Journal (CSJ), April 2011.

[26] E. Naveh, A. Marcus, "When Does the ISO 9000 Quality Assurance Standard Lead to Performance Improvement? Assimilation and Going Beyond", IEEE Transactions on Engineering Management 51 (3): 352, 2004