HIPAA and QMS based architectural requirements to cope with the OCR audit program

Syeda Uzma Gardazi and Arshad Ali Shahid
Computer Science Department
National University of Computer & Emerging Sciences
Islamabad, Pakistan
uzma.gardazi@gmail.com and arshad.ali@nu.edu.pk

Christine Salimbene, Esq.
Legal Department
Healthcare IT Company
United States
csalimbene@gmail.com

***Abstract*—The United States legislation known as the Health Insurance Portability and Accountability Act of 1996 (HIPAA) is aimed at strengthening patient rights, increasing efficiency and decreasing administrative costs in the healthcare industry. Under HIPAA all Covered Entities are required to ensure compliance with certain privacy and security rules concerned with protecting private patient health information. Building upon the objectives of HIPAA, the American Recovery and Reinvestment Act (ARRA) of 2009, in Section 13411 of the Health Information Technology for Economic and Clinical Health (HITECH) Act, required the Department of Health and Human Services (HHS) to conduct periodic audits of Covered Entities against HIPAA Security Rule. This paper presents and evaluates a new approach which might be used by Covered Entities to achieve compliance with HIPAA by adopting the ISO 9001 guidelines. A United States based Healthcare IT Company (UHITC) with a backup office in Pakistan was taken as a case study for this approach. UHITC develops software for mobile devices along with providing third party medical billing services. In connection with its achieving ISO 9001 certification since 2004, UHITC had already developed a company-wide quality audit protocol based on the ISO 9001 standard. For purposes of conforming the ISO standards to the HIPAA audit protocol in a streamlined fashion, UHITC examined the HIPAA requirements to determine whether the existing protocol could be tailored to achieve HIPAA compliance. In order to accomplish this evaluation, the two standards were compared by cross-mapping their components. The comparison revealed that the controls mentioned in the ISO 9001 guideline meet or exceed the HIPAA Security Rule for 36% of the implementation requirements. UHITC was also able to increase customer satisfaction by achieving compliance with HIPAA Security Rule using a quality management system (QMS) model. At the next level, Compliance Attributes (CA) were derived from these requirements and classified as architectural and non-architectural in nature. A new approach to define compliance oriented software architecture using compliance tactic was also proposed.**

Keywords- HIPAA, ISO, HIPAA compliance and QMS intermapping, software architecture and OCR Audit Program

I. INTRODUCTION

United States legislation requires healthcare service provider entities to adhere to certain privacy and security rules. In order to enforce this mandate, the US federal government has initiated a program to conduct audits of 150 Covered Entities by the end of December 2012.

A. Health Insurance Portability and Accountability Act (HIPAA)

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a federal law that applies throughout the United States [1]. HIPAA sets forth a security rule that governs the security of patient health information (PHI). This security rule is divided into four sections: administrative safeguards; physical safeguards; technical safeguards; and organizational requirements.

The HIPAA Security Rule aims at strengthening the integrity and confidentiality of PHI, as that term is defined in 45 CFR § 164.501. The HIPAA Security Rule has divided requirements into the following two categories:

- required clauses (R):

Covered Entities are responsible to ensure compliance with these requirements. The term "Covered Entity" is defined as in 45 CFR 160.103 and refers to those healthcare service providers that are subject to the jurisdiction of HIPAA.

- addressable clauses-labeled by HIPAA as being "addressable" (A):

Covered Entities are responsible to decide how and to what extent they have to ensure compliance with these requirements.

Although Covered Entities are mandated to comply with HIPAA requirements, the legislation does not provide any specific security framework for the Covered Entities to follow. One possible solution for Covered Entities could be to integrate HIPAA requirements into an existing management system with minimum additional load. This paper proposes one way of doing so.

B. ISO 9001:2008 quality management system (QMS)

The International Organization for Standardization (ISO) is a non-governmental organization which develops and publishes international standards and serves as a bridge between the public and private sectors. ISO standards provide recognized benchmarks for companies doing business around the world. ISO 9001 is a particular standard which sets forth universal requirements for establishing and maintaining a QMS. Going forward, we will refer to the ISO 9001:2008 standard (reference number ISO 9001:2008(E)) as the ISO 9001 guideline. A company that is ISO 9001

978-0-7695-4727-5/12 $26.00 © 2012 IEEE
DOI 10.1109/MUSIC.2012.50

certified, has demonstrated its ability to develop and produce quality products or services on time [2].

C. Comparison of Standards.

The HIPAA Security Rule is divided into following four areas:

- Administrative Safeguard requirements
- Physical Safeguard requirements
- Technical Safeguard requirements
- Organizational requirements

Whereas, the ISO standard defines quality standard into following eight areas:

- Scope
- Normative References
- Terms and Definitions
- QMS
- Management Responsibility
- Resource Management
- Product Realization
- Measurement, Analysis and Improvement

The HIPAA requirements have been cross-mapped with the ISO requirements to identify similarities.

D. Importance and relevance of mobile technology in healthcare field.

Recently the trend to access electronic health records (EHR) using mobile devices e.g. IPad, IPhone or Android phone has been tremendously increased among healthcare providers [3]. Understanding the need of hour, UHITC has also developed mobile oriented practice and revenue cycle management software, applications and websites for private physician offices and hospitals throughout the US. Due to size and portability features of mobile devices, probability of possible data breaches has been increased. UHITC as a Covered Entity under HIPAA regulation is required to ensure HIPAA compliance within their processes including the development of mobile specific software and websites. The important consideration for UHITC is to continue adopting a HIPAA compliant processes approach to devise HIPAA compliant software and applications for mobile-device-minded practices. In section IV, this paper discusses how UHITC has ensured compliance of its processes with HIPAA using ISO 9001 standard.

II. UHITC's Existing Internal Audit Protocol

A. ISO In General

The operations of a US Healthcare IT Company's, (UHITC) back office located in Pakistan were used as a case study. UHITC formulates software for use by professionals in the US healthcare industry and develops and customizes its software for mobile devices along with desktop systems. As evidence of its ability to provide quality products and services, UHITC has attainted ISO 9001:2008 certification status. In connection with developing the processes which were used to attain its ISO certification, UHITC implemented an internal quality audit protocol which encompasses all functions of various departmental activities related to UHITC's QMS, and includes processes required to comply with applicable US governmental regulations such as HIPAA. The UHITC QMS was created in order to establish a quality management policy with corresponding objectives and also to establish the means to achieve those objectives. ISO 9001 standard has provided a starting point for developing a QMS for UHITC. ISO 9001:2008 standard requires that its adopters incorporate following documentation levels:

- Documentation Level 1: creating a company quality manual that addresses quality policy, organizational structure, management responsibilities etc. and that explains how to address each of the clauses in ISO 9001:2008 (including determinations that a control is not applicable).
- Documentation Level 2: establishing quality procedures that delineate activity tasks and assign particular responsibilities.
- Documentation Level 3: instituting quality work instructions that detail the methods and guidelines to be used in performing the tasks.
- Documentation Level 4: maintaining records and forms that contain evidence and control mechanisms to show compliance and results.

The ISO 9001 guideline requires companies to implement an effective QMS for controlling the processes used to develop and produce/deliver products and/or services. The term "process" is defined as "a set of interacting activities, which transforms inputs into outputs." Compliance with these standards implies that there are certain elements every QMS must have in place. Effective implementation of QMS according to ISO 9001 standard will ultimately result in the delivery of quality products and services to the customer on time.

HIPAA Security Rule 45 CFR 160, 162, and 164 has been published by HHS. This regulation provides specific organizational, administrative, physical and technical requirements to ensure security of patient health information. In comparison with the ISO 9001, the HIPAA Security Rule does not provide the same level of guidance for demonstrating compliance with it. In this paper, HIPAA Security Rule requirements were mapped against ISO 9001 requirements to identify similarities to achieve HIPAA compliance.

B. The ISO Protocol at UHITC

In accordance with maintaining its certification, the UHITC ISO 9001 Team, through its Management Representative (MR) ensures that UHITC periodically conducts audits of different departments to determine whether:

- UHITC's processes conform to the requirements of ISO 9001 and to those QMS requirements established by the organization, and
- The effectiveness and maintenance of its QMS are up-to-the requirements set by ISO 9001.

The ISO team within UHITC is responsible for the planning, scheduling, execution and reporting of the Internal

Audit Protocol. As defined in ISO manual Ref 5.2.2, the MR serves as liaison with external parties on matters relating to the QMS. As required by the ISO 9001 standard, the MR is responsible for planning and scheduling the Internal Audits. The Internal Audits are then regularly carried out at least once a year; activities are audited more frequently if processes affecting QMS are changing. Internal Audits are then regularly carried out at least once a year.

The following flowchart explains the six key steps of the internal audit protocol:

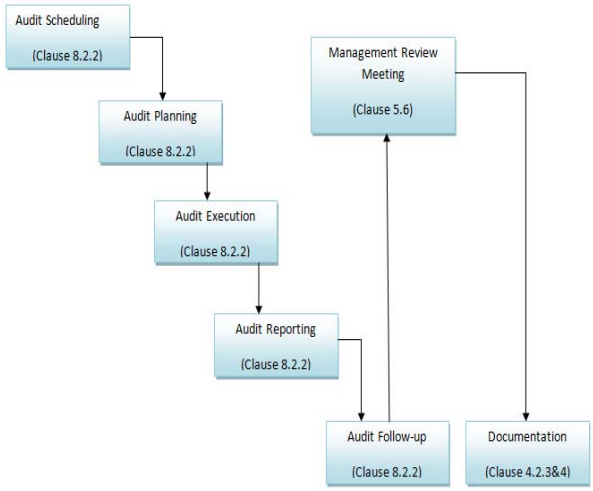

Figure 1. ISO Internal Audit Protocol Flow Chart

The audit protocol contains the following six key activities [4]:

- Audit Schedule: The audit schedule is prepared annually, usually at the beginning of the year.
- Audit Planning: An audit plan containing all the activities corresponding to the QMS is prepared and distributed. This plan identifies the time and location for all these activities.
- Audit Execution: The audits are then executed by the audit teams which are made up of members of different organizational departments or functions. While conducting the audit, auditors seek to determine whether documented protocols and instructions meet the requirements of the standard; verify whether the protocols and instructions are being implemented and assess whether the process/activity/operation meets the customer's quality requirements.
- Audit Reporting: On completion of the audit, the audit team compiles and submits to the MR and to the Auditees the following:
    - The findings of the audit;
    - Complied audit non-conformities and
    - Their corrective action requests (CAR)
- Audit Follow-up: The same auditors conduct a follow-up audit to determine if the corrective and preventive action has been implemented and to assess its effectiveness. When there is objective evidence that the corrective and preventive action is effective, the audit is closed out. If more work is needed to fully implement the corrective and preventive action, a new follow-up date is agreed upon.
- Management Review Meeting: UHITC senior management has established a Management Review committee to co-ordinate and controls the activities of the QMS of services provided by different organizational departments, and to periodically review and evaluate the performance of the same.

III. HIPAA EVALUATION REQUIREMENT COMPLIANCE BY IMPLEMENTING QMS AUDIT PROTOCOL

The HIPAA evaluation requirement requires Covered Entities to periodically review and evaluate the mandatory administrative, physical and technical safeguards to review and document their compliance with their security policy and other federal requirements. Covered Entities must specifically assess the need for a new evaluation based on any changes to their security environment since their last evaluation. In its initial attempt to comply with the HIPAA evaluation (§164.308(a)(8)) requirement, UHITC, utilized its existing ISO QMS protocol to formulate a framework for this required HIPAA compliance protocol, thus providing the case study for the authors herein. From this point onward, the authors will be referred to as "we." This utilization of the ISO QMS protocol as the foundation for the HIPAA evaluation protocol was effectuated by first conducting a comparative mapping of the two standards.

A. HIPAA and ISO 9001Inter-relationship

A QMS is set up by a company in order to establish a quality policy and quality objectives and also to establish the means to achieve those objectives. ISO 9001 guidelines create a list of requirements for organizations to consider when defining their QMS. ISO 9001 guidelines provide a starting point for companies that intend to develop their own QMS.

Because the HIPAA Security Rule does not provide an adequate mechanism for demonstrating compliance with it, this paper suggests that a healthcare organization could use its QMS to ensure that HIPAA Security Rule requirements are properly added and implemented. To do so, a careful analysis of HIPAA Security Rule clauses against ISO 9001 guidelines has to be performed. After identification of appropriate controls the next important step is to demonstrate compliance. In our case study, UHITC has to assure that these controls are properly implemented, managed, reviewed and improved in a timely fashion as required.

B. Comparative Assessment

During the comparative mapping preparation, the standards were compared based on match in the scope and intention of the clauses. The table below demonstrates the results of this comparison.

TABLE I. 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).

IV. SOFTWARE ARCHITECTURE FOR HEALTHCARE INDUSTRY

Software architecture development is an increasingly important field in the healthcare industry. The first stage of software architecture is requirement elicitation. There are two major types of requirements known as functional and non-functional requirements [5]. Functional requirements directly affect the behavior of the software/system. Whereas non-functional requirements are the criteria that affect the operations/behavior of the system. Compliance requirements are a cross-section of both functional and non-functional requirements that are extracted from regulations and standards. For example, the additional requirements are put in place by HIPAA. Therefore, entities operating in the healthcare industry are mandated to comply with HIPAA.

A. Identification, prioritization and comparsion of healthcare requirements and set of Compliance Attributes (CA)

In software architecture after identification of requirements, Quality Attributes (QA) are derived from these identified requirements which are not compliance requirements. QAs on their own do not address the additional federal regulatory/compliance requirements that are in place to protect certain data, namely PHI. Accordingly, for those entities operating in the healthcare industry, there is a need to develop attributes that address the additional requirements. These additional attributes or HIPAA Compliance Attributes (CA) are derived from the specific federal regulations set forth in HIPAA. High priority has been assigned to those CA which are directly extracted from required regulatory HIPAA requirements as compared to other CA. Medium priority has been assigned to those CA which are directly extracted from addressable regulatory HIPAA requirements as compared to other CA.

HIPAA Security Rule clauses have been assessed against ISO 9001 guideline clauses. First, the scope and intention of the clauses were reviewed. At the next level, we determined the extent to which ISO 9001 guideline clauses would facilitate in availing compliance with HIPAA requirements. We found a good match in a few cases when some ISO 9001 guideline clauses (concerning legal compliance) have been mapped to the HIPAA as a whole entity and vice versa. As we are comparing regulation versus standard, it is expected that 100% mapping is not possible. HIPAA and ISO 9001:2008 are complementary in terms of covered entity's operations. The particular mappings indicate whether there is an equivalent match or whether the ISO 9001:2008 clause exceeds or falls short being able to support a demonstration of compliance with the HIPAA requirement. We also specify whether a requirement is architectural (AR) in nature, i.e., where the architectural requirement describes a condition or capability to which a system must conform. These requirements can be derived from users, regulations, standards, specifications, or other formally imposed document. The below mentioned section shows how specific HIPAA Security Rule requirements are compared to ISO 9001 guideline:

1) Administrative Safeguards

CA#1: HIPAA requires that Covered Entities should implement risk analysis, risk management; sanction policy and information security activity review requirements. These requirements may map indirectly with ISO requirements. We are considering these requirements as architectural requirements based on the assumption that these requirements will be provided as software product feature in the software which automatically ensure compliance.

HIPAA Clause	ISO 9001 Clause	Comparison
Security Management Process (§164.308(a)(1))	Competence, Training and Awareness (6.2.2), Design and Development (7.3) and Production and Service Provision (7.5)	HIPAA>ISO, AR=Yes & Priority=High

CA#2: HIPAA requires that Covered Entities should nominate/assign resources to ensure compliance within the company.

HIPAA Clause	ISO 9001 Clause	Comparison
Assigned Security Responsibility (§164.308(a)(2))	Competence, Training and Awareness (6.2.2)	ISO~HIPAA, AR=No & Priority=High

CA#3: This HIPAA requirement defines a specific requirement titled as clause 6.2 (Human Resource). In this clause employee training details are also discussed.

HIPAA Clause	ISO 9001 Clause	Comparison
Workforce Security (§164.308(a)(3))	Competence, Training and Awareness (6.2)	ISO>HIPAA, AR=Yes & Priority=Medium

CA#4: ISO 9001 does not specifically define Information Access Management requirement.

HIPAA Clause	ISO 9001 Clause	Comparison
Information Access Management (§164.308(a)(4))	Competence, Training and Awareness (6.2.2), Design and Development (7.3) and Production and Service Provision (7.5)	HIPAA>ISO, AR=Yes & Priority= Medium

CA#5: ISO 9001 does not specifically address Security Awareness and Training requirement.

HIPAA Clause	ISO 9001 Clause	Comparison
Security Awareness and Training (§164.308(a)(5))	Competence, Training and Awareness (6.2.2)	ISO~HIPAA, AR=No & Priority= Medium

CA#6: ISO 9001 does not specifically address Security Incident Procedures requirement.

HIPAA Clause	ISO 9001 Clause	Comparison
Security Incident Procedures (§164.308(a)(6))	Human Resource (6.2) , Design and Development (7.3) and Production and Service Provision (7.5)	HIPAA>ISO, AR=No & Priority=High

CA#7: ISO 9001 refers to record retention and data availability requirement.

HIPAA Clause	ISO 9001 Clause	Comparison
Contingency Plan (§164.308(a)(7))	Control of Documents & Records (4.2.3 & 4.2.4), Human Resource (6.2) , Design & Development (7.3) and Production and Service Provision (7.5)	ISO~HIPAA, AR=No & Priority=High

CA#8: ISO 9001 requires that entities conduct internal audits after planned intervals.

HIPAA Clause	ISO 9001 Clause	Comparison
Evaluation (§164.308(a)(8))	Internal Audit (8.2.2), Monitoring and Measurement of Processes and Products (8.2.3 and 8.2.4)	HIPAA>ISO, AR=No & Priority=High

CA#9: ISO 9001 discuss the agreement requirement but HIPAA exceeds this requirement. At this point, we are assuming that BAA is an online setup.

HIPAA Clause	ISO 9001 Clause	Comparison
Business Associate Contracts (§164.308(b)(1))	Customer Property (7.5.4)	HIPAA>ISO, AR=Yes & Priority=High

2) Physical Safeguards

CA#10: ISO 9001 section 6.2 partially discusses this HIPAA requirement.

HIPAA Clause	ISO 9001 Clause	Comparison
Facility Access Controls (§164.310(a)(1))	Human Resource (6.2)	HIPAA>ISO, AR=No & Priority= Medium

CA#11: ISO 9001standard does not directly address this HIPAA requirement.

HIPAA Clause	ISO 9001 Clause	Comparison
Workstation Use (§164.310(b))	Human Resource (6.2) and Service Provision (7.5)	HIPAA>ISO, AR=Yes & Priority= High

CA#12: ISO 9001 guideline does not directly address this HIPAA requirement.

HIPAA Clause	ISO 9001 Clause	Comparison
Workstation Security (§164.310 (c))	Human Resource (6.2) and Service Provision (7.5)	HIPAA>ISO, AR=Yes & Priority= High

CA#13: ISO 9001 guideline does not directly address this HIPAA requirement. We assume that device access is controlled using third party software e.g. GFI End Point Security.

HIPAA Clause	ISO 9001 Clause	Comparison
Device and Media Controls(§164.310 (d)(1))	Human Resource (6.2) and Service Provision (7.5)	HIPAA>ISO, AR=Yes & Priority= High

3) Technical Safeguards

CA#14: ISO 9001 guideline does not directly address this HIPAA requirement.

HIPAA Clause	ISO 9001 Clause	Comparison
Access Control (§164.312(a)(1))	Human Resource (6.2) and Service Provision (7.5)	HIPAA>ISO, AR=Yes & Priority= High

CA#15: ISO 9001 guideline emphasize on the requirement of audit after specific intervals. This requirement is architectural in nature and can be directly mapped on software.

HIPAA Clause	ISO 9001 Clause	Comparison
Audit Controls (§164.312(b))	Human Resource (6.2), Service Provision (7.5) and Internal Audit (8.2.2)	HIPAA~ISO, AR=Yes & Priority= High

CA#16: ISO 9001 guideline does not specify the HIPAA integrity requirement.

HIPAA Clause	ISO 9001 Clause	Comparison
Integrity (§164.312(c)(1))	Human Resource (6.2) and Service Provision (7.5)	HIPAA>ISO, AR=Yes & Priority= Medium

CA#17: ISO 9001 guideline does not specify this HIPAA requirement.

HIPAA Clause	ISO 9001 Clause	Comparison
Person and Entity Authentication (§164.312(d))	Human Resource (6.2) and Service Provision (7.5)	HIPAA>ISO, AR=Yes & Priority= High

CA#18: ISO 9001 guideline does not specify this HIPAA requirement.

HIPAA Clause	ISO 9001 Clause	Comparison
Transmission Security (§164.312(e)(1))	Design and Development (7.3) and Service Provision (7.5)	HIPAA>ISO, AR=Yes & Priority= Medium

4) Organizational Requirements

CA#19: ISO 9001 guideline require that entities review the customer requirement and document exact final requirements before supplying the product.

HIPAA Clause	ISO 9001 Clause	Comparison
Business Associate Contracts (§164.312(a)(1))	Product requirements are defined (7.2.2 a)	ISO~HIPAA, AR=No & Priority= High

CA#20: ISO 9001 guideline does not specify this HIPAA requirement.

HIPAA Clause	ISO 9001 Clause	Comparison
Requirements for Group Health Plan (§164.312(b)(1))	Not found	HIPAA>!ISO, AR=No & Priority= Medium

CA#21: ISO 9001 guideline requires that the documentation should be properly controlled.

HIPAA Clause	ISO 9001 Clause	Comparison
Policies and Procedures (§164.316(a))	Control of Documents (4.2.3)	ISO~HIPAA, AR=No & Priority= High

CA#22: ISO 9001 guideline requires that the documentation and records should be properly controlled.

HIPAA Clause	ISO 9001Clause	Comparison
Documentation (§164.316(b)(1))	Control of Documents (4.2.3) and Control of Records (4.2.4)	ISO~HIPAA, AR=No & Priority= High

TABLE II. SUMMARY OF COMPARISON OF ISO 9001 AND HIPAA STANDARDS

	ISO 9001:2008	Percentage
ISO~HIPAA	7	31.82%
ISO>HIPAA	1	4.55%
HIPAA>ISO	14	63.63%

The controls specified in the ISO 9001 guideline meet or exceed the HIPAA Security Rule for 36% approximately of the implementation requirement. Accordingly, it is possible for UHITC to use its QMS to ensure that HIPAA Security Rule requirements are properly added and implemented. Any additional HIPAA requirements would be added to the organization's quality system procedures (QSP). Whereas, 55% of HIPAA requirements are architectural in nature.

However, based on research conducted by the SANS Institute reveals that the ISO 27001:2005 standard controls meet or exceed the HIPAA Security Rule for 74% of the implementation requirements [6].

Compliance evaluation

HIPAA compliance using QMS was evaluated using following two techniques:

Questionnaire technique:

We have evaluated these CA extracted from HIPAA using questionnaire technique. Based on this evaluation, we conclude that UHITC has implemented 63% requirements up to the mark. Whereas remaining 37% requirements implementation either needs to be revised or entirely changed to achieve the compliance with HIPAA Security Rule. UHITC complies with ISO standard requirements by 85%. Whereas remaining 15% requirements implementations either needs to be revised or entirely changed to achieve the compliance with this standard. Please see the % compliance trend in figure 2.

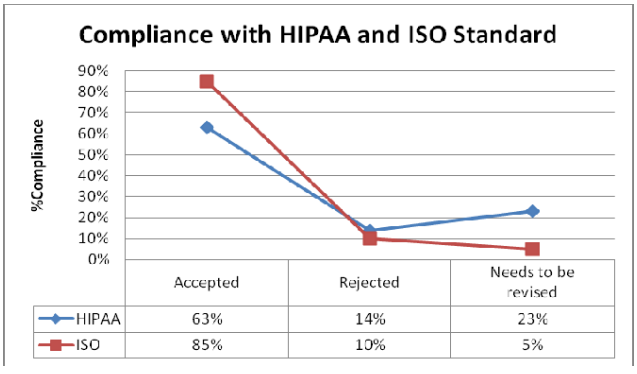

Figure 2. % Compliance of UHITC with HIPAA and ISO Requirements

Audit technique:

Two audits were conducted in year 2011 named as IA-1 and IA-2. IA-1 only focused on ISO 9001 standard whereas IA-2 also covered the HIPAA requirements. Please also see the NCRs trend for both the audits IA-1 and IA-2 in figure 3 and 4.

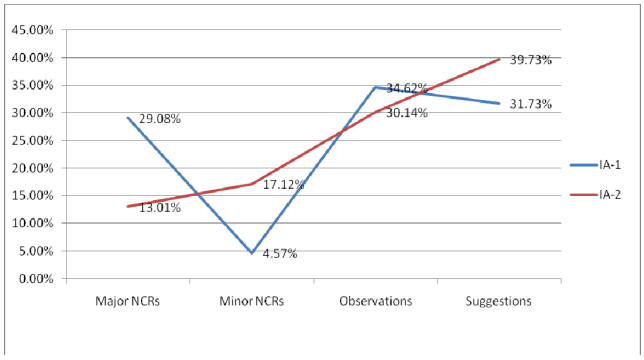

Figure 3. Non-Conformance Statistical Analysis

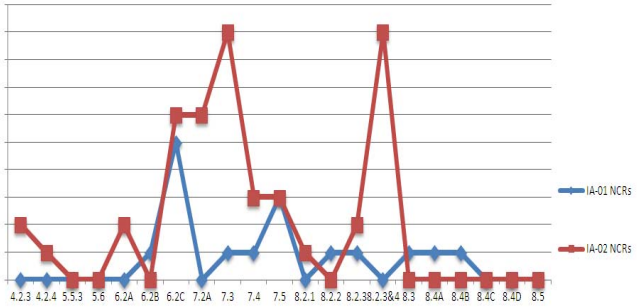

Figure 4. Non-Conformance Statistical Analysis

The overall NCRs trend was increased by 17% in IA-2 as shown in figure 5 because of following reasons:

- overall audit scope of ISO 9001 was extended by incorporating HIPAA requirements in the existing UHITC's QMS scope and
- as compared to IA-1, more departments were included in the scope of IA-2.

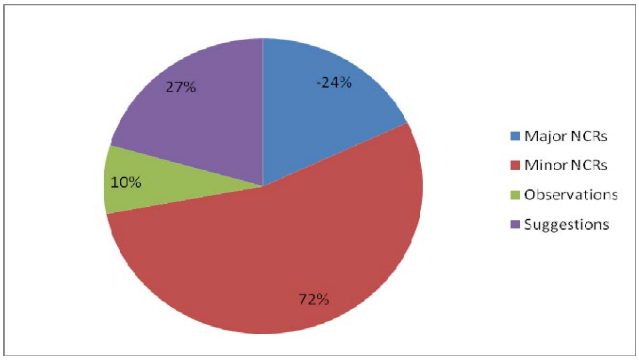

Figure 5. Non-conformance trend of IA-2

Due to an overall increase in number of identification and resolution of issues during the IA-2, the processes within UHITC further improved.

NCR aging analysis: The average time to close a raised issue between IA-1 and IA-2 was reduced by 36% indicating that the responsible personnel/departments are closing the raised concerns with in less time as shown in figure 6.

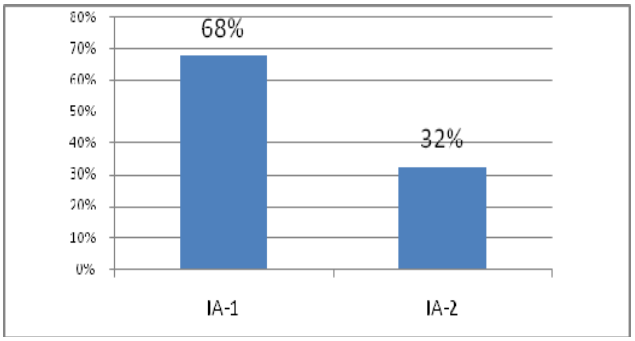

Figure 6. NCR aging trend

Customer Satisfaction: The client satisfaction trend shows that the client satisfaction has been increased during the year by 17% whereas the client dissatisfaction has been decreased by 45% indicating increased customer satisfaction. One of the reasons for improved satisfaction is that HIPAA requirements were mapped against ISO 9001 standard and implemented within UHITC. Further, UHITC's IT department uses compliance-driven software architecture for software development.

B. Architectural mechanism

After CA extraction from regulatory requirements, the next level is to devise appropriate compliance tactics to achieve these CA at software architecture level. A tactic can be defined as a design decision that can influence and control the CA response [7]. In this section we will emphasis defining the architectural tactic to achieve compliance at software architecture level using an example of accounting of disclosure compliance tactics.

TABLE III. SUMMARY OF COMPARISON OF CURRENT AND PROPOSED ACCOUNTING OF DISCLOSURE RULE

The Current Accounting of Disclosure Rule	The Proposed Accounting of Disclosure Rule
The current accounting of disclosure rule requires that entities covered under HIPAA should properly track and document the unauthorized disclosures of Protected Health Information (PHI).	The proposed accounting of disclosure rule requires that accounting of disclosure reports should be generated for patients using a Designated Record Set (DRS) in both the formats i.e. paper and electronic.
The current accounting of disclosure rule requires that an accounting of disclosures should be done in electronic and paper formats.	The proposed accounting of disclosure rule specifies that Covered Entities should provide the access report in electronic format only including the summary of disclosures made for the treatment, payment or health care operations purposes ("TPO").

The following tactic has been introduced for compliance, and can be called as accounting of disclosure tactic under HIPAA to achieve compliance with the proposed accounting of disclosure rule. Stimulus is request for access report generated by the patient and response is the access report in electronic format. We represent the relationship between stimulus, response and tactics in figure 7.

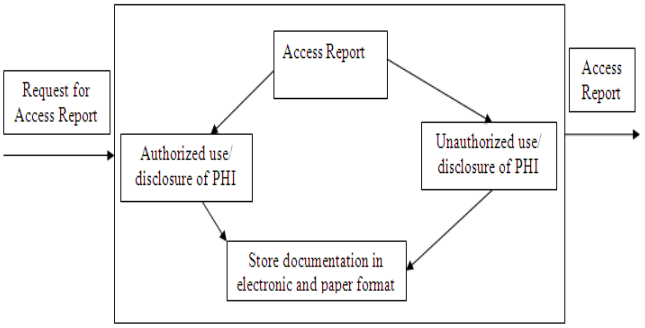

Figure 7. Hierarchy of accounting of disclosure tactics

The accounting of disclosure compliance tactic is divided the disclosure into two types named as authorized and unauthorized use/disclosure of patient information. Covered Entities are required to record and provide the access report of any type of use or disclosure of PHI upon receiving the request from individual. Further, secure PHI tactic display a number of methods to protect from breach. The relationship is shown in figure 8.

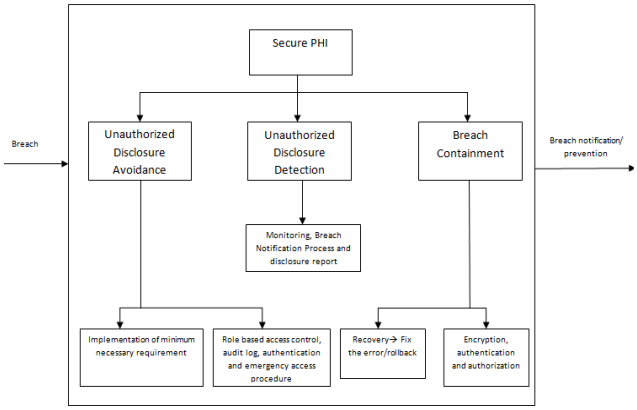

Figure 8. Hierarchy of secure PHI tactic

C. Architecture

One way is to follow the minimum necessary rule that requires providing only the minimally necessary information to the authorized individual after verification. Using the above tactic the following architecture [8 and 9] for access report was formulated:

Component Patient

Ports

- Port P1 (in→Receive_Electronic_Access_Report)
- Port P2 (out→ Generate_Access_Report_Request)

End Ports

Connectors

- Interface I1 (in)
- Interface I2 (out)

End Connector

End Component

Component Provider

Ports

- Port P3 (In→ Receive_Access_Report_Request)
- Port P4 (out→Generate_Access_Report, Notify_Business Associates)

End Ports

Connectors

- Interface I1 (out)
- Interface I2 (in)

End Connector

End Component

Connector Access_Report_Progress
Connects Patient with Provider
binds Generate_Access_Report_Request with Generate_Access_Report
notify_Provider with notify_Patient
End Connector

V. FUTURE WORK

Evaluate HIPAA & ISO 9001 compliant software architecture.

VI. CONCLUSION

HIPAA does not provide a specific security framework for those entities subject to its jurisdiction, but requires them nonetheless to address the requirements. This paper has suggested a way for Covered Entities to integrate HIPAA requirements into an existing QMS system with minimal additional load. ISO 9001 series provides Covered Entities with a mechanism that can be adopted by these companies. This paper has a proposed a new approach to achieve compliance with HIPAA requirements using QMS model. Compliance attributes, tactics and compliance-oriented software architecture were derived from HIPAA requirements. As per our analysis, the controls mentioned in ISO 9001 guideline meet or exceed the HIPAA Security Rule for 36% of the implementation requirements. The ISO 27001:2005 controls meet or exceed the HIPAA Security Rule for 74% of the implementation requirements.

It is concluded, then, that ISO 27001:2005 provides 38% better mechanism to achieve HIPAA compliance than ISO 9001:2008. Healthcare organization can still adopt ISO 9001guideline and processes based approach to achieve HIPAA compliance and improved customer satisfaction. UHITC was able to achieve the increase in client satisfaction by 17% and decreased in client dissatisfaction by 45%. HIPAA Security Rule also provides a process based model to achieve and ensure continuous compliance of its requirements. HIPAA requirements can be mapped against clauses mentioned in the ISO 9001 guidelines except a small number of requirements. Those exceptions can be dealt with by devising particular procedures to address the HIPAA requirement and then incorporating same into the existing ISO protocol.

ACKNOWLEDGMENT

The authors would like to acknowledge Mrs. Ishrat Hyder, the Higher Education Commission (HEC), and National University of Computer & Emerging Sciences (FAST-NUCES) for providing funding and required resources to complete this work. It would have been impossible to complete this effort without their continuous support.

REFERENCES

[1] HIPAA; Pub.L. 104-191, 110 Stat. 1936, enacted August 21, 1996

[2] 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.

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

[4] R.K. Mautz & H.A. Sharaf, The Philosophy of Auditing, American Accounting Association. & Dunn, J., 1996. Auditing Theory and Practice. 2nd ed. Prentice Hall, 1961.

[5] T. D. Breaux, A. I. Anton, Analyzing Regulatory Rules for Privacy and Security Requirements, IEEE Transactions on Software Engineering, 34(1), pp. 5-20, January 2008.

[6] Borkin, The HIPAA Final Security Standards and ISO/IEC 17799, SANS Institute Reading Room site, July 15, 2003.

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

[8] S. U. Gardazi and A. A. Shahid, "Survey of Software Architecture Description and Usage in Software Industry of Pakistan", IEEE ICET 2009.

[9] S. U. Gardazi, A. A. Shahid, Billing Compliance Assurance Architecture for Healthcare Industry (BCAHI), Computer Science Journal, 2010.

[10] http://www.zygma.biz/pdf/Zygma%20%2017799%20vs%20HIPAA%20white%20paper%20v1bis.pdf

[11] S. Ghanavati, D. Amyot, and L. Peyton, A Requirements Management Framework for Privacy Compliance. Proc. of the 10th Workshop on Requirements Engineering (WER'07), Toronto, Canada, May 2007, 149-159

[12] S. U. Gardazi, S. F. Gardazi, H. Khan and A. A. Shahid, "Motivation in Software Architecture and Software Project Management", IEEE ICET 2009.