HIPAA Compliance: How do we get there? A Standardized Framework for Enabling Healthcare Information Security & Privacy

B. Coats and S. Acharya, *Towson University*, A. Saluja and D. Fuller, *Lexington Hospitalists Inc*.

Abstract – This research identifies the critical need for a standardized framework to establish and maintain compliance of security and privacy in healthcare organizations. In response to this need, this research proposes the design and development of a novel standardized framework for establishing and maintaining security and privacy compliance in information systems for health care organizations and clinical practices. Furthermore, to validate our solution we have tested the proposed framework against a real-world HIMSS 6[1] healthcare organization (and its partnering clinical practices). Finally, the proposed approach, design and methodology could act as learning and training guide for health care personnel and information security administrators in their efforts to build and maintain a security preserving and privacy aware healthcare system.

Index terms – HIPAA, Compliance, Healthcare Information Security

I. Introduction

One of the primary goals of the Health Insurance Portability and Accountability Act (HIPAA) of 1996 was to employ Information Technology (IT) to improve health insurance coverage and portability while also lowering costs and improving its quality [2]. This goal, commonly known as the Administrative Simplification, has proven anything but simple to realize. Given the ever growing dependence of IT within all public and private sectors, it was anticipated that the adoption and full compliance with HIPAA would be completed by 2006, just 3 years following the final revisions of the HIPAA Privacy and Security Rules. Now six years after the original expected completion date, health institutions around the country are still struggling to achieve full compliance. As of the 2006 deadline, research published by the Healthcare Information Management Systems Society (HIMSS) estimated that only 64% of U.S. healthcare entities were fully compliant with the Privacy Rule and only 19% were fully compliant with the Security Rule [3]. Each rule initially afforded entities roughly 3 years from publication to implementation. In practice, these implementations have taken at least 2 and 3 times as long as originally anticipated and the clock is still running for many organizations.

Considerable efforts have been expended towards achieving HIPAA compliance by healthcare organizations. This endeavor has proved challenging with the absence of standardized, federally provided, implementation plans. Each HIPAA covered entity has been forced to approach the task from their localized, individual perspective and hence the figurative wheel is being reinvented again and again. Further, each one of these entities is spending vast amounts of time, resources, and funds towards the same goal. With no clear direction, it takes significant effort to determine what needs to be done and how to do it even before organizations can get to the point of actual implementation. As such, most healthcare organizations are expending significant and superfluous effort in the assessment and planning stages. This point is acknowledged at the highest levels of the federal government and articulated in a report by the President's Council of Advisors on Science and Technology (PCAST) [4]. The report states that organizations with successful health IT deployments were required to use expensive, organizationally tailored solutions, incurring substantial resources for implementation.

To this end, the purpose of this research is to create a standardized guideline for healthcare information security, with universal adaptability for any organization. A clear, comprehensive guide for HIPAA compliance will afford businesses and institutions a cost-effective solution for the task all HIPAA covered entities are mandated to undertake. In addition to providing a recipe for success for HIPAA compliance, plug-and-play style tools will be developed for organizations in order to test the security of their environments. These tools will generate critical information both during the assessment stages as well as post-implementation to ensure continued compliance. Beyond the abstract and technical contributions, this research also significantly addresses the human technology interaction within an organization. All technical, functional, and administrative personals will gain invaluable training and awareness in order to establish, preserve and maintain security and privacy of information in their respective healthcare systems.

In order to validate the results of this research, a collaborative partnership was formed with a medium to large size healthcare system to enable interaction with real-world business practices, policies, and healthcare personnel. The collaboration involves guiding the healthcare system through all phases of the proposed framework. The results of the examination, assessment,

ISBN 1-933510-95-1/$15.00

and training of the organization will demonstrate the strength, effectiveness and completeness of the proposed academic research. To summarize, the salient contributions of this research to the healthcare information technology industry are:

- The creation of a standardized healthcare information security guideline for HIPAA compliance,
- A suite of security testing tools for assessment and ongoing compliance,
- The development of security awareness training procedures and manuals (administrative, functional, and technical), and
- Finally, the evaluation of the proposed research on a typical HIMSS 6[1] healthcare organization and its partnering hospitals and clinical practices.

The rest of the paper is as follows: section II presents the significance and importance of this research; in Section III we layout the stages and methodology of both the academic research and collaborative industrial project; Section IV describes the status of the project and the application of the academic framework to the real-world environment.; finally, Section V provides a summary of goals of this research, its relevance, and how this research is already being applied and benefiting a typical national healthcare organization.

II. Background and Related Work

HIPAA compliance is mandated at both the federal and state level for all covered entities that work with electronic protected health information (ePHI). Compliance with federal and state regulations is an unavoidable requirement of doing business in the United States. As such, entities found in violation of HIPAA are subject to both civil and criminal penalties. In 2010, over 2,700 corrective actions were required to be taken by healthcare entities based on complaints reviewed by the U.S. Department of Health & Human Services (HHS) [5]. The most recent resolution agreement example posted by HHS was with the University of California at Los Angeles Health System (UCLAHS), in July of 2011, for violations of the Security and Privacy Rules. The penalties levied by HHS on UCLAHS included $865,000 in fines, required employee sanctions, and independent monitoring for 3 years [6]. Other posted cases had similar penalties, some with fines in excess of $1 million. Aside from complying with HIPAA for the sake of regulation and threat of penalty, one of the primary objectives of HIPAA that can be realized by health organizations is the Administrative Simplification. HHS has created national standards for electronic health care transactions, code sets, and many other aspects of capturing ePHI data [7]. By way of this standardization, healthcare entities can exchange data much faster, securely, and more accurately to offer better patient care. The Administrative Simplification will further benefit patient care by enabling the acceleration of the inquiry and response times for eligibility verification, claim status, and service requests. From a different angle, the national standards will greatly improve fraud detection capabilities as all payers and providers will effectively be speaking the same 'language' and there will be less ambiguity and confusion with how claims are categorized and processed. At the local organization level, the HIPAA implementations will provide an opportunity for many organizations to renovate or possibly replace antiquated systems and streamline their business processes. It is uncommon for organizations to perform exhaustive analysis of their policies and practices without some form of external motivation. The HIPAA Administrative Simplification will supply this driver and subsequently enable organizations to increase their efficiency for both internal and external activities.

With the many motivations to implement the HIPAA guidelines, healthcare providers and payers have been attempting to achieve compliance for nearly a decade. In 1998, shortly after HIPAA's signing, the research firm Gartner Group estimated the implementation of HIPAA would collectively cost healthcare providers $5 billion and health plans $14 billion. By 2005, HHS was estimating that the costs could be at least 3 times the original amount for providers and as much as 10 times the original amount for health plans [8]. In 2009, HIMSS sponsored research suggested that the actual implementation costs for providers would be closer to $40 billion [3]. This trend indicates a considerable cost increase that in some cases could prove crippling, especially for smaller entities. The costs of these implementations have deviated even more than their timelines and creating financial burdens drastically higher than originally anticipated. Surmounting costs aside, the original schedule set by the Privacy and Security Rules required compliance by 2003 and 2005 respectively [9]. Clearly these compliance goals have not been met by most healthcare organizations around the country. While the road to HIPAA compliance is proving elusive and costly, organizations clearly understand the importance and necessity of completing the undertaking. HIPAA will ultimately ensure better privacy and security of ePHI data. Organizations have both ethical and financial motivations to provide their customers the guarantees that HIPAA requires and are spending massive amounts of time and money on their implementations. It is critical for these organizations to have clear and comprehensive guidelines to follow for maximum efficiency in their efforts.

There are a variety of reasons why HIPAA implementations have proved more expensive and taken considerably longer than originally anticipated by federal regulators and healthcare organizations alike. One of the fundamental challenges that many healthcare

organizations face, especially smaller ones, is the introduction or transition to e-Business. HIPAA requires all healthcare transactions to be handled electronically and this is a significant change for many entities. Additionally, not only does HIPAA require transactions to be electronic, all data must be standardized. Local code sets must now be replaced with a national code set. The standardization and normalization of all protected health information that an organization possesses or interacts with can prove to be a colossal task. Certainly the biggest hurdle to overcome is simply the creation of an assessment, testing, and implementation plan. While many government agencies, private foundations, and industry consortiums have established high level guidelines and recommendations of how to address each of the HIPAA Rules, there is no nationally mandated implementation plan or standardized framework for organizations to follow. Each entity is responsible for reviewing the guidelines and determining the appropriate solution. The published recommendations are at a very abstract level and require much interpretation to formulate an actual implementation strategy. With a lack of clear direction, many entities have difficulty determining the best path for them to follow to satisfy each requirement. Furthermore, without an apparent plan or timeline, it becomes extremely difficult for organizations to generate realistic cost estimates for their compliance efforts and likewise secure the necessary budgetary commitments. This point has been demonstrated consistently since the first HIPAA implementations began. National cost estimates of HIPAA efforts are approaching a factor of ten higher than what regulators estimated when the law was first enacted. The contributions of this research will fill a gap that becomes readily obvious to all organizations that work with the HIPAA regulations. The objective of this research is to produce a standardized guideline for HIPAA compliance along with a suite of security testing tools and security awareness training that any healthcare organization can easily adapt to their environment with minimal effort and achieve maximum success.

III. Framework

While HIPAA compliance is a federal government mandate, no governmental agency has created a specific plan for organizations to evaluate and correct themselves. If HIPAA compliance was easy to assess and corrective actions were known, the compliance statistics would reflect the fact and likewise be considerably better. As such, a standardized guideline for healthcare information security is desperately needed to ease the implementation burden of HIPAA. Our proposed standardized framework consists of three primary phases, as depicted in Figure 1, guaranteeing complete HIPAA compliance. The framework is designed to take an organization from the initial recognition of the need for compliance all the way through to implementation of any necessary changes to their environment.

A. Phase 1

Phase 1 is a high-level assessment involving a thorough review of all policies, procedures, practices, and architectural designs. This first stage has three major tasks: to create the Healthcare Information Security Guideline (HISG), to perform an assessment of the organization, and to produce a Comprehensive Organization Assessment and Roadmap (COAR) report. While the tasks are performed sequentially, there are feedback loops at almost every stage to reflect findings and feedback of successive steps to the preceding steps to ensure the resultant HISG and COAR are organizationally relevant.

The first task of Phase 1 is the creation of the HISG, which is essentially a general guideline for any healthcare organization to follow in order to achieve HIPAA compliance. The HISG is the culmination of the actual HIPAA regulations, federal recommendations from the National Institute for Standards and Technology (NIST) and the Department of Health and Human Services (HHS), and IT industry best practices. Once the information, guidelines, and requirements from all these sources are compiled, they are distilled into a concise, comprehensive guide that is divided into four major areas of information technology: Network, Database, Applications, and Infrastructure. The HISG then serves as the emblematic ruler that the healthcare organization is evaluated against and appropriate recommendations are derived from for the organization. One of the practical applications of this research is for organizations to effectively start their HIPAA compliance activities at this point in the framework, using the HISG that this research has produced.

The next undertaking of Phase 1 is to gather information about the organization's IT environment and current security practices. The specific assessments to be performed will be an overall Healthcare Information Security Assessment (HISA), an evaluation of human technology interaction, and finally, an Information Technology Architecture Assessment (ITAA). The HISA will be produced by initially creating a Healthcare Information Security Questionnaire (HISQ), based off of the HISG. This questionnaire will then be sent to the central IT department for the organization to be completed. The HISA is created based on the responses given to the HISQ. The human technology interaction will be evaluated through the creation of a survey targeted at healthcare providers. The survey will cover the healthcare personnel's perception of the current IT practices, their understanding of requirements and procedures in place, and their specific interactions with ePHI data. After the survey has been created and

completed by the organization's staff, the results will be compiled and evaluated. These results will be presented in a Healthcare Provider Analysis report. The final assessment area is of the organization's IT architecture. This review will involve obtaining network diagrams, data center diagrams, network device configurations, and other documents that depict how the network and infrastructure architecture is implemented. The analysis of these diagrams and documents will be captured in the ITAA report. Each of these assessments will produce a list of potential findings and a corresponding recommendation for corrective actions. The findings and recommendations will be the basis for the creation of a Comprehensive Organization Assessment and Roadmap (COAR) report.

The last step of Phase 1 of the project is the creation of the COAR report. The recommendations from the assessment stage will be combined with the guidelines laid out in the HISG created in the initial step to produce a clear summary of actionable items specific to the organization. The COAR will eventually serve as a detailed implementation guide for the organization to follow in order to achieve HIPAA compliance. At the end of Phase 1, the COAR initially provides only an abstract assessment and guide for the organization. The next phase performs a practical evaluation of the areas covered in the first phase and amends the COAR as necessary.

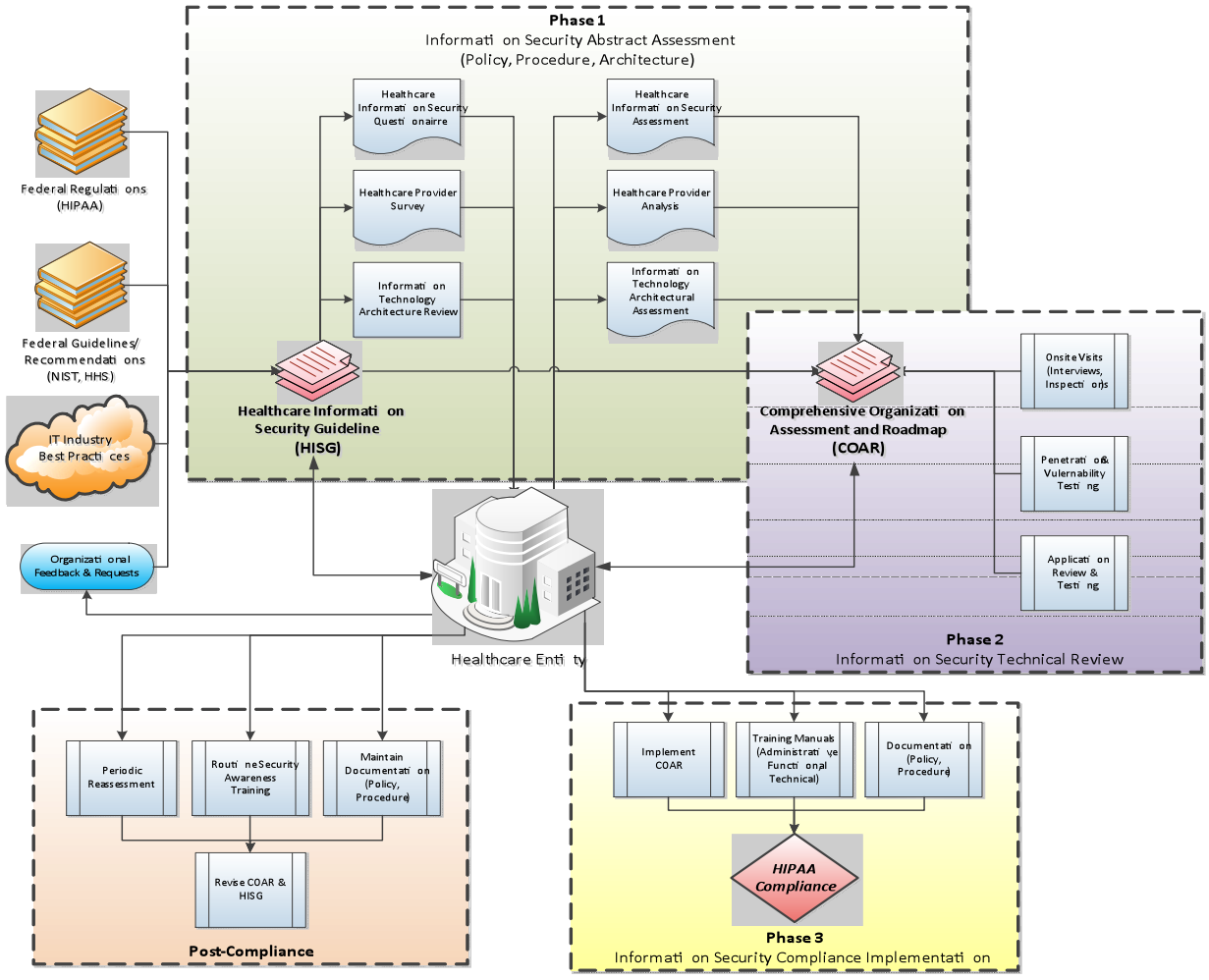

Figure 1: Project Framework Diagram

B. Phase 2

Phase 2 is a detailed, hands-on technical review and assessment of the IT environment. This phase measures and analyzes the actual performance of the systems and practices both against the theoretical goal of the HISG and the reported state of the organization provided in the assessment stage of Phase 1. The variances found in this effort will be reflected in the COAR with appropriate mitigating actions. The technical review will include onsite visits, penetration and vulnerability testing, and a comprehensive review and assessment of all enterprise applications. The onsite visits will consist of interviews with the personnel of the organization, both within the IT

department and administration. It will also involve inspections of various components of the IT environment including physical security controls for the data center and other locations where ePHI data is stored. In addition to the onsite visits, the IT staff will be engaged to conduct penetration and vulnerability testing on the network and infrastructure portions of the organization. All associated testing will be performed using automated tools. By creating and utilizing an automated tool, the testing can be standardized and easily repeated not only during the current review period but in future as part of the organization's continued compliance efforts. Additionally, an extensive review, categorization, and analysis of all enterprise applications will be conducted in this phase. Each application will be examined to determine if it interacts with ePHI and if so, in what way and for what function or purpose. Further, every application will be independently assessed against the HISG and all findings reported with corresponding recommendations. Once each of the technical reviews is complete, the final task of this phase is to update the COAR report with all the findings and corrective actions identified in this phase. At the conclusion of this phase, the organization's entire IT environment will have been methodically examined and evaluated.

C. Phase 3

The final phase involves taking the findings of the first two phases and performing corrective actions as appropriate. Phase 3 is the implementation stage including changes related to technical configurations, policy, procedures, training, and documentation.

At the start of the implementation phase, an implementation plan will be drafted, based off of the final COAR. While the findings and recommendations laid out in the COAR will provide specific tasks to complete, a plan needs to be developed of how to put those changes into operation. Meetings with stakeholders, IT staff, and administrative staff will be necessary to create an effective plan including an appropriate timeline. Once the plan has been developed, the actual implementation can be scheduled and started. In addition to the technical, policy, and procedural changes covered in the COAR implementation plan, this phase will also ensure that necessary documentation is created for both the impending changes and the preexisting environment. Further, this phase will include any necessary training – administrative, technical, or functional – related to the changes implemented, new procedures, and general security awareness training of the organization moving forward.

With the completion of the third phase, the entire project will likewise be completed. The result of the project will first and foremost be the achievement of HIPAA compliance for the organization. In the efforts to attain compliance, there will also be a number of other tangible accomplishments. This project will create a standardized Healthcare Information Security Guideline that can be referenced and updated for perpetuity. The HISG will serve as a critical resource for evaluating future enhancements and changes to the environment and ensure compliance is maintained. Additionally, the project will produce a series of valuable tools for periodic testing of the security configurations. These tools will provide important actionable information as well as save time and effort in regards to the ongoing penetration and vulnerability testing procedures. Lastly, this project will afford extremely useful training and awareness of security to the organization at all levels. The assessment exercises alone will orient the healthcare providers, technical staff and administration alike on the current updated state of their IT environment. It is often the case in HIPAA compliance efforts, that the simple lack of knowing how to measure compliance can greatly delay the entire effort. This research is also an exercise of educating organizations as to what compliance requires, how these requirements translate into their specific environment, and how to satisfy them quickly, efficiently, and at a significantly reduced cost compared to tackling this effort alone.

IV. Case Study

While the academic process of developing the HISG produced a standardized approach for evaluating and ensuring HIPAA compliance, it needed to be legitimized through actual application in a real-world environment. This validation was realized through a collaborative partnership with a typical regional healthcare system that has achieved HIMSS Stage 6 [1] certification – only 248 hospitals/systems have achieved the certification in the United States. The healthcare system is being provided the benefit of a comprehensive assessment of their entire environment, including specific, actionable tasks to remedy any deficiencies uncovered in compliance.

The project is a three year engagement, with roughly one year allocated per phase of the framework. Phase 1 of the project has recently been completed. Each stage of the framework was completed for Phase 1, including the 3 assessments. For each assessment, an initial draft, with any potential findings, was presented to the organization for their review and acceptance. The healthcare system either accepted the findings or disputed them and provided supporting documentation that demonstrates the finding was not valid. Following the review and acceptance process, the complete COAR report was produced and submitted to the organization for final review and acceptance.

Phase 1 of the project yielded a significant number of critical findings within the organization's environment.

Considering the partner healthcare system is a HIMSS Analytics Stage 6 Hospital [1], the findings were non-trivial and representative of typical hospitals in the United States. The top critical findings based on organizational impact are detailed below – in decreasing order of criticality – along with their recommended corrective actions.

A. Critical Findings

1. *Single points of failure* – Analysis of the network topology determined the organization had six significant single points of failure related to how the various buildings on campus were connected both to the institution's data center and the Internet. In some of the cases these single points of failure were due to a single physical transmission medium existing between buildings. The other cases were that not all buildings had redundant network paths to the internet or the data center. There were three instances where a disaster scenario in one building would segregate one or more buildings by extension from all other networks – internal or external. While a disaster scenario at a particular building is expected to directly impact that building's connectivity, such an impact should not be entirely debilitating to ancillary buildings. Single points of failure create an organizational risk to both contingency planning and business continuity, both of which are required – §164.308(a) (7) – within the HIPAA regulations [2]. Redundancy within the network can be achieved using a variety of hardware and/or software solutions that will be detailed in the COAR.

2. *Disaster recovery (DR) and emergency plans* – Only a third of the Healthcare Provider Survey respondents definitively stated that disaster recovery and emergency plans exist and are periodically tested. The majority, 63%, of the responses indicated that it was unclear whether plans exist or are tested. This was reiterated by the responses provided to the HISQ by the organization's technical staff. The lack of awareness of a DR plan is akin to not having a plan altogether since the majority of personnel have not reviewed or tested the plan. Business continuity is a HIPAA regulation [2] – §164.308(a) (7) – of which disaster recovery and emergency plans are a critical component. Disaster recovery plans must be established and periodically tested in order to be fully compliant.

3. *Undue exposure in application architecture* – It was discovered that not all applications that interact with ePHI data utilized a 2 or 3-tier architecture. Numerous applications are not configured such that web services, application services, and database services are segregated from one another. In many cases all these services reside on the same physical machine and are directly accessible by internal and external hosts. The final ITAA will recommend that all ePHI data that will be accessed by users should be done via a 2 or 3-tier application architecture with the data store on an internal, inaccessible network segment. All efforts should be made to minimize the exposure each server has to non-administrative internal and external networks. Since all applications must inherently be accessed by internal and/or external users, some amount of exposure is necessary on generally accessible networks. Through a 2 or 3-tier architecture, the only way users can access ePHI data is via proxy through the web or application servers. This design minimizes the impact of a breach at a web server since no actual ePHI data resides on those servers.

4. *Undue exposure in network architecture* - The organization does not have an adequate demilitarized zone (DMZ) configuration that contains all publically accessible web servers. Many of the application's web servers reside in the same network subnets where the application and database servers are located. In order to minimize exposure, any web server that is publically accessible should reside in the DMZ and there should be no publically accessible machines outside of the DMZ. The DMZ should be segregated from all internal network segments and resources that hold ePHI data. Further all network segments besides the DMZ should be inaccessible from external networks. Network segmentation, such as a DMZ or in conjunction with a 2 or 3-teir application configuration, is an approach for decreasing exposure and ensuring systems and data is not unnecessarily accessible by internal and/or external hosts. Information access management is a specific requirement of the HIPAA administrative safeguards [2] – §164.308(a) (4).

5. *Use of shared accounts* – 16% of the Healthcare Provider Survey respondents stated that shared accounts were in use to some degree for ePHI-relevant applications. HIPAA regulations [2] – §164.312(a) (1) – mandate user accounts for ePHI applications be unique per individual for auditing and non-repudiation. The responses suggest that the majority of ePHI applications are using unique user accounts but not all. It is critical to review the authentication model for each ePHI application and implement user-specific accounts for any application that doesn't already employ that scheme.

6. *Automatic logoff* – About 12% of the survey responses stated automatic log offs do NOT occur for all ePHI applications. HIPAA regulations [2] – §164.312(a) (1) – require all applications that interact with ePHI to automatically log users off after a period of inactivity. According to the survey responses, a comprehensive review of all ePHI relevant applications is needed to ensure each application has this capability enabled. There was a specific comment that some applications within the hospital keep the original user logged in indefinitely, which precludes compliance.

7. *Security awareness training* – Just under half of the survey respondents stated security awareness training is provided on a regular basis although almost as many responses indicated they were unsure if such training existed. The HIPAA law [2] – §164.308(a)(5) – requires routine security awareness training and based on the responses the indication is while training exists within a portion of the organization, it is not present within all units. A security awareness and training program needs to be established and implemented across the organization.

8. *Acceptable use policies* – Almost 53% of the Healthcare Provider Survey responses indicated they were unsure if such policies exist or are signed by ePHI relevant users. HIPAA regulations [2] – §164.308(a) (1) – mandate that acceptable use policies be created, users agree to them, and this agreement is documented prior to accessing ePHI data. Based on the responses the indication is while acceptable use policies exist within a portion of the organization, they are not pervasive through all units. Such policies need to be established that comprehensively define appropriate and inappropriate use, access, and disclosure of ePHI including sanctions for not following the policies.

9. *Reporting of unauthorized or inappropriate ePHI release* – Just less than half of the survey responses stated that procedures exist for reporting unauthorized or inappropriate releases of ePHI data and no responses contradicted the assertion. The other half of the responses were unsure whether such procedures existed or not. The HIPAA regulations [2] – §164.308(a) (6) – mandate procedures be established to report and react to ePHI data being released unintentionally. While no responses indicated procedures didn't exist, the lack of understanding by the staff about such procedures in of itself creates an implied deficiency. Any staff member that interacts with ePHI must understand how to identify an incident and what to do if and when they occur.

10. *Physical access controls* – Almost 23% of the Healthcare Provider Survey respondents stated that physical controls are not present in all ePHI relevant locations this indicates some areas either have no or insufficient controls for ingress/egress. The HIPAA law [2] – §164.310(a) (1) – require physical access be secure and monitored. Any areas that do not have these controls in place must be corrected.

B. Overall Assessment Results

After all assessments were completed and reviewed, each area was rated based on the organization's degree of compliance. Compliance scores were provided for each section and sub-section to give indications where technical and organizational changes may be necessary. The complete assessment breakdown and scoring of the HISA can be viewed at http://wp.me/P2fsKI-9. Additional human technology interaction results were derived from the submitted responses to the Healthcare Provider Survey.

While a significant number of findings were made related to the current policies, practices, and architecture of the organization' IT environment, the partner health system's level of compliance is on par with the industry averages. The industry averages, derived from HIMSS sponsored research [3], indicate most organizations are closer to full compliance to privacy than security. The case study organization mirrored this pattern with Privacy Rule compliance at 86% while the Security Rule compliance was approximately 71%. Similar to many healthcare entities, the organization is relatively close to compliance but not at the federally mandated 100% compliance.

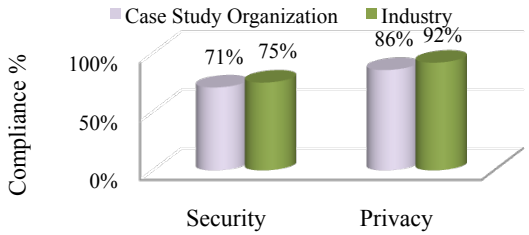

Figure 2: Overall Compliance Performance

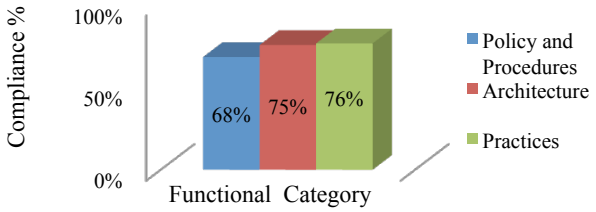

Figure 3: Compliance per Functional Category

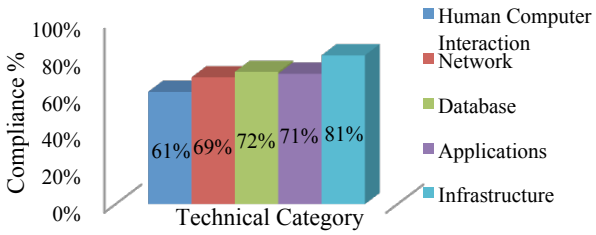

Figure 4: Compliance per Technical Category

Similarly, the organization has the most compliance issues with regard to the human technology interaction element of IT compared to the four solely technical areas.

The functional area that requires the most improvement by the organization is policy and procedures. This deficiency is fairly common throughout all industry with

respect to IT and is also one of the hardest areas to correct. Changing policy and procedure requires changes to business practices and it is typically challenging for organizations to secure the leadership commitment and stakeholder buy-in to intact this type of change.

The project is currently in Phase 2, which includes tool design, testing, vulnerability assessment, and a comprehensive review and assessment of all enterprise applications. The results and findings of the technical evaluations will be incorporated with the Phase 1 COAR to form a final security guidelines report for the organization. Phase 3 will involve actually implementing the COAR and getting the organization to 100% HIPAA compliance.

V. Conclusions

The recognition of the need for a standardized framework for healthcare information security is widespread throughout the healthcare industry and federal government, all the way to the White House. Every healthcare entity approaching this issue independently is both costly and timely, and ultimately the general public feels the impact. The fundamental objectives of HIPAA provide for valuable improvements to the overall health care in the United States. Unfortunately these benefits can only be realized when HIPAA compliance is achieved and at present, compliance is proving to be extremely challenging for healthcare organizations.

The goal of this research is to bridge the gap from regulation to practice. In this effort, the research performed exhaustive reviews of countless governmental regulations, guidelines published by federal agencies and private consortiums, and public research related to HIPAA compliance. The findings of these efforts were combined with industry best practices for security and privacy in IT industry. The result of the pairing was the creation of a comprehensive healthcare information security guideline that will serve as an implementation roadmap for organizations to save time and money for their HIPAA compliance pursuit. Moreover, the research findings are being field tested in a typical regional healthcare system that is already well on its way to HIPAA compliance. The collaborative project associated to this research is providing real-world scenarios for the evaluation framework to be applied and validated. The case study organization has already acknowledged that the standardized guideline has identified issues within its environment as well as offered specific recommendations about how to remedy the problems. Ultimately, other healthcare entities can leverage the findings performed by this research, as the case study organization, to achieve compliance quicker and cheaper and quicker, and enable enhanced patient care.

VI. References

[1] HIMSS Analytics. (2011). "EMR Adoption Model," last accessed on November 2011. http://www.himssanalytics.org/hc_providers/emr_adoption.asp.

[2] United States. National Archives and Records Administration. (1996). "Title 45 – Public Welfare, Subtitle A – Department of Health and Human Services, Part 164 – Security and Privacy," retrieved August 2011, http://www.access.gpo.gov/nara/cfr/waisidx_07/45cfr164_07.html.

[3] Appari, A., Anthony, D.L., and Johnson, M.E. (2009). "HIPAA Compliance: An Examination of Institutional and Market Forces," last accessed on Nov. 2011, http://www.himss.org/foundation/docs/Appari_etal2009_HIPAAcompliance_20091023.pdf.

[4] United States. Executive Office of the President. President's Council of Advisors on Science and Technology. (2010). "Report to the President – Realizing the Full Potential of Health Information Technology to Improve Healthcare for Americans: The Path Forward, "retrieved February 2012, http://www.whitehouse.gov/sites/default/files/microsites/ostp/pcast-health-it-report.pdf.

[5] United States. Department of Health and Human Services. Center for Medicare and Medicaid Services. (2010). "Enforcement Results per Year," retrieved November 2011, http://www.hhs.gov/ocr/privacy/hipaa/enforcement/data/historicalnumbers.html.

[6] United States. Department of Health and Human Services. Office for Civil Rights. (2011). "Resolution Agreement," retrieved February 2012, http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/uclaagreement.html.

[7] United States. Department of Health and Human Services. Center for Medicare and Medicaid Services. (2004). "Regulations and Guidance," last accessed on November 2011. https://www.cms.gov/home/regsguidance.asp.

[8] Blue Cross Blue Shield Association. (2005). "HIPAA Return On Investment, " presented to the National Committee on Vital Health Statistics, Subcommittee on Standards and Security. http://ncvhs.hhs.gov/050406p1.pdf.

[9] United States. Department of Commerce. National Institute of Standards and Technology. (2008). "An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule (rev 1)," retrieved July 2011, http://csrc.nist.gov/publications/nistpubs/800-66-Rev1/SP-800-66-Revision1.pdf.