From Regulations to Practice: Achieving Information Security Compliance in Healthcare

Subrata Acharya, Brian Coats, Arpit Saluja, and Dale Fuller

Computer and Information Sciences, Towson University, Towson, MD, USA
CIMS, Johns Hopkins Medical Institute, Baltimore, MD, USA
University of Pittsburgh Medical Center Altoona, Altoona, PA, USA
sacharya@towson.edu,
bcoats1@students.towson.edu,
asaluja1@jhmi.edu,
dfuller@altoonaregional.org

Abstract. Access to healthcare is not a new issue, but it has been only in the last few years that it has gained significant traction with the federal government passing a number of laws to greatly enhance the exchange of medical information between all relevant parties: patients, providers, and payers. This research focuses specifically on these issues by examining industry compliance to the Health Insurance Portability and Accountability Act, electronic health record adoption, and the federal Meaningful Use program; all from the healthcare provider's perspective. While many plans have been made, guidelines created, and national strategies forged, there are significant gaps in how actual technology will be applied to achieve these goals. The goal of this research is to bridge the gap from regulation to practice in a number of key technological areas of healthcare information security. Using standardized frameworks, this research proposes how accessibility, efficiency, and integrity in healthcare information security can be improved.

Keywords: Meaningful Use, HIPAA Compliance, Assessment.

1 Introduction

When considering healthcare accessibility, two other issues quickly come to the forefront: efficiency and integrity. Every solution a healthcare provider evaluates related to access, must address these other areas adequately to warrant consideration. The issue of efficiency refers to the organizational impact of delivering and maintaining the chosen solution. Topics such as scalability, support infrastructures, cost, time to market, and functionality all fall under the umbrella of 'efficiency'. Likewise, the area of integrity covers both the privacy and security of the underlying data being accessed.

The Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act are some of the most significant federal actions related to achieving effective electronic

T. Tryfonas and I. Askoxylakis (Eds.): HAS 2014, LNCS 8533, pp. 209–220, 2014.

healthcare access nationally. HIPAA aims to use information technology (IT) to improve health insurance coverage and portability while also lowering costs and improving its quality [1]. Similarly, one of the major aspects of HITECH was designed to provide an incentive program for healthcare providers to implement and utilize electronic health record (EHR) systems to further the original goals of HIPAA [2]. Both of these laws and programs are intended to improve electronic healthcare access but many organizations are struggling to implement them and therefore the industry at large is not fully realizing their theoretical cumulative benefits.

Healthcare providers and payers have been attempting to achieve HIPAA compliance for nearly a decade. The sluggishness of HIPAA compliance is paralleled by the delayed introduction of EHR systems by healthcare organizations. The provisions of the Administrative Simplification, which is part of HIPAA, require the standardization of ePHI transactions to improve efficiency while also safeguarding the privacy and security of their data [3]. In order to achieve this standardization of ePHI and its transactions, many healthcare providers have or are in the process of implementing EHR systems. HIMSS Analytics, the authoritative source on EHR/EMR adoption trends, reports as of Q4 2013 almost 95% of 5,458 providers in the United States were in some stage of an EHR implementation but less than 3% had a complete deployment covering all possible aspects - data capture, storage, access, reporting, and exchange [4]. A high percentage of providers have started the process of adopting an EHR system but very few have actually completed the process.

While the road to HIPAA compliance and EHR adoption is proving elusive and costly, organizations clearly understand the importance and necessity of completing the undertakings. The lack of comprehensive, openly available frameworks for organizations to follow for healthcare information security compliance has become quite obvious. This research aims to fill some the implementation gaps that become readily apparent to all organizations that work towards providing patient access to EHR systems, while working within the HIPAA regulations. To this end, this research provides a comprehensive solution for healthcare providers to assist in the completion of the required attestation for Meaningful Use dictated by the U.S. Department of Health & Human Services (HHS). The product of this research will help organizations successfully review and assess their organization's technology policies and procedures and provide recommendations of how to mitigate potential findings. Specifically, the key contributions of this research to the healthcare information technology industry are:

- The creation of a comprehensive implementation guide for information security policies and procedures at an organizational level,
- A set of assessment tools for healthcare providers to self-evaluate the completeness and effectiveness of their current policies and procedures for attestation and ongoing compliance, and
- Enhanced security and privacy for a national healthcare provider that enabled qualification for Meaningful Use Stage 1.

The remainder of the paper is as follows: Section 2 presents the significance of the research to the healthcare industry and what related work has already been performed; Section 3 describes the framework itself; Section 4 describes how this research is

already being applied and benefiting a typical national healthcare organization; finally Section 5 summarizes the goals of this research and its importance to the landscape of information security in healthcare.

2 Background and Related Work

Over the last few years, the healthcare industry has been giving information security special attention with such a focus being put on the implementation of electronic health record (EHR) systems. From the federal government's perspective, EHR systems are the solution to achieving many of the security and privacy measures that HIPAA laid out more than 10 years ago. The federal government has proved its national commitment to universal implementation of EHRs by enticing healthcare providers to start using EHR technology with very lucrative 'carrots' for both hospitals and private practices. In 2009, the federal government passed the HITECH Act which authorizes incentive payments through both Medicaid and Medicare to private practices and hospitals that use certified EHR technology to accomplish specific objectives in care delivery. The incentive program has been labeled 'Meaningful Use' as it rewards providers for demonstrating their meaningful use of EHR systems. In 2011 and 2012, EPs that met the Stage 1 requirements of Meaningful Use could have earned over $100,000 and hospitals over $2 million between Medicaid and Medicare [5]. Stage 1 was just the first of an anticipated 3 stages to ensure full EHR adoption nationally. The requirements for Stage 2 have been released and entities can begin receiving payment for meeting this stage in 2014. Looking ahead, the Stage 3 requirements are already out in a proposed form and it is tentatively scheduled for implementation in 2015. While HHS is offering incentives for early adoption, they are also levying penalties if Stage 1 hasn't been met by 2015.

The financial attraction for healthcare providers to participate in the HHS' Meaningful Use programs is evident, but still many providers have been unable to capitalize on the opportunity. The Centers for Medicare & Medicaid Services (CMS) released reports in June 2012 on the performance of the incentive programs through May 2012 [6]. These reports detailed how nationwide only slightly better than a 35% of all healthcare providers that have registered for the incentive programs are actually receiving the benefits of the Medicare program and barely over 50% are receiving benefits for the Medicaid program. The gap between the number of registered providers and those that are actually getting paid demonstrates that EHR adoption and attestation are considerable challenges.

In an effort to provide organizations a standardized approach for addressing the HIPAA regulations, the National Institute for Standards and Technology (NIST) produced special publication 800-66 that focused on the implementation of the HIPAA Security Rule [7]. This guide gets closer to the concept of mapping regulation to implementation but still does not provide specific actionable recommendations. Unfortunately there are no publically available HIPAA compliance assessment frameworks for organizations to follow. With a lack of clear direction, many entities have difficulty determining the best path for them to follow to satisfy each

requirement. Further demonstrating this point is the emergence of numerous consulting firms that offer HIPAA compliance assessment. These companies offer both self and onsite assessment solutions. Kroll and Clearwater are both premier international security firms that offer HIPAA compliance services. Both of these companies state their assessment process includes questionnaires for self-assessment and intensive penetration testing for onsite assessments [8, 9]. These companies further state that their questionnaires and testing is based on the guidelines laid on in the NIST 800-66 publication and the HIPAA regulations themselves. The idea of having actionable plans based off these various publications as well as other industry best practices is not a novel concept in of itself. However, up to this point a solution has not been presented in an open academic format such that organizations can perform both the abstract style assessment from questionnaires and surveys as well as the active penetration testing without assistance. What is also missing from the current commercial offerings is the ability to see specifically the derivation of the all the assessment mechanisms so that they can be updated and adapted if and when regulations are added or changed. This mapping information, tying regulation to practice and assessment, is proprietary to the commercial offerings as it effectively constitutes the entire value of their engagements. Therefore as it stands today, 2 basic options have developed either contract with one of the private security assessment firms that specialize in HIPAA compliance or use the NIST guideline and muddle through alone. With many organizations' budget constraints, unfortunately the latter option tends to become the common option but ultimately 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 [10]. This point has been demonstrated consistently since the first HIPAA implementations began. Consequently, national cost estimates of HIPAA efforts have eclipsed a factor of ten higher than what regulators estimated when the law was first enacted.

This research aims to lessen this challenge by providing a comprehensive guide for healthcare providers to follow to implement effective and complete information security policies and procedures. Further, using this research's assessment tools, organizations can evaluate and document the state of their current information security policy and procedure. The operational aspects are given specific attention in the assessment tools to help organizations complete the required Meaningful Use attestation.

3 Methodology

The proposed compliance framework [11] consists of three primary phases that culminate in complete HIPAA compliance for the healthcare provider. A well-documented and repeatable compliance framework will greatly speed up the assessment and testing process, yield more consistent results, present less risk to the normal business operations of the organization, and minimize the resources needed to perform the testing [12]. This research offers a comprehensive solution to organizational assessment and information security testing by providing step-by-step instructions for

how to plan and perform information security compliance assessment and testing, how to analyze the results of the tests, and ultimately how to correct and mitigate any findings. 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. Further, the framework provides a post-compliance phase to ensure the healthcare provider maintains their compliance perpetually.

Phase 1 is a high-level assessment involving a thorough review of all policies, procedures, practices, and architectural designs. This first stage uses the Healthcare Information Security Guideline (HISG) produced by this research, to perform an organizational assessment of the healthcare provider. These assessments include a thorough review of the technical architecture, policy, and procedures. The results of these assessments and recommended mitigating actions are combined 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 COAR is organizationally relevant. The COAR will eventually serve as a detailed implementation guide for the organization to follow in order to achieve HIPAA compliance. The next phase performs a practical evaluation of the areas covered in the first phase and amends the COAR as necessary.

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 are reflected in the COAR with appropriate mitigating actions. The technical review includes onsite visits, penetration and vulnerability testing, and a comprehensive review and assessment of all enterprise applications. The onsite visits consist of interviews with the personnel of the organization, both within the IT department and administration. It also involves 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 is engaged to conduct penetration and vulnerability testing on the network and infrastructure portions of the organization. All associated testing is documented in the Healthcare Information Security Testing Directive (HISTD). The HISTD ensures the testing is 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 are conducted in this phase. Each application is examined to determine if it interacts with ePHI and if so, in what way and for what function or purpose. 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 has been methodically examined and evaluated.

The final phase involves taking the findings of the first two phases captured in the COAR 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 organization will have successfully achieved HIPAA compliance. In the efforts to attain compliance, there will also be a number of other tangible accomplishments. This framework presents 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 framework will provides a series of valuable tools for periodic testing of the security configurations. These tools will produce important actionable information as well as save time and effort in regards to the ongoing penetration and vulnerability testing procedures. Lastly, this framework will impart extremely useful training and awareness of security to the organization at all levels. The assessment exercises alone will orient the healthcare practitioners, technical staff and administration alike on the current 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 educates 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.

4 Case Study

In order to validate the effectiveness of this research, it was vital that both the assessment tools and implementation guide be utilized in an actual healthcare provider's environment. In 2011 a partnership was formed with a national HIMSS Stage 6 [13] hospital (Hospital X) for a mutually beneficial relationship. The arrangement allowed this research to be field tested and the hospital would be provided a comprehensive assessment of their entire environment, including specific, actionable tasks to remedy any deficiencies uncovered. The partnership was scoped for a 3 year engagement, with roughly 1 year allocated per phase of a larger information technology assessment framework.

4.1 Organizational Assessment

Starting with Phase 1, a high-level assessment, involving a thorough review of all technology practices and architectural designs, was performed [14]. The information technology staff was interviewed extensively and asked both dichotomous and semantic differential questions. The measurement scale used to quantify the responses is based on the percentage the organization is in compliance with the guidelines laid out in the HIPAA guidelines [15] and NIST's recommendations [16] for HIPAA implementations. The measurement scale used to quantify the responses is based on the percentage the organization is in compliance with the guidelines laid out in the HIPAA guidelines [15] and NIST's recommendations [16] for HIPAA implementations. 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. 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.

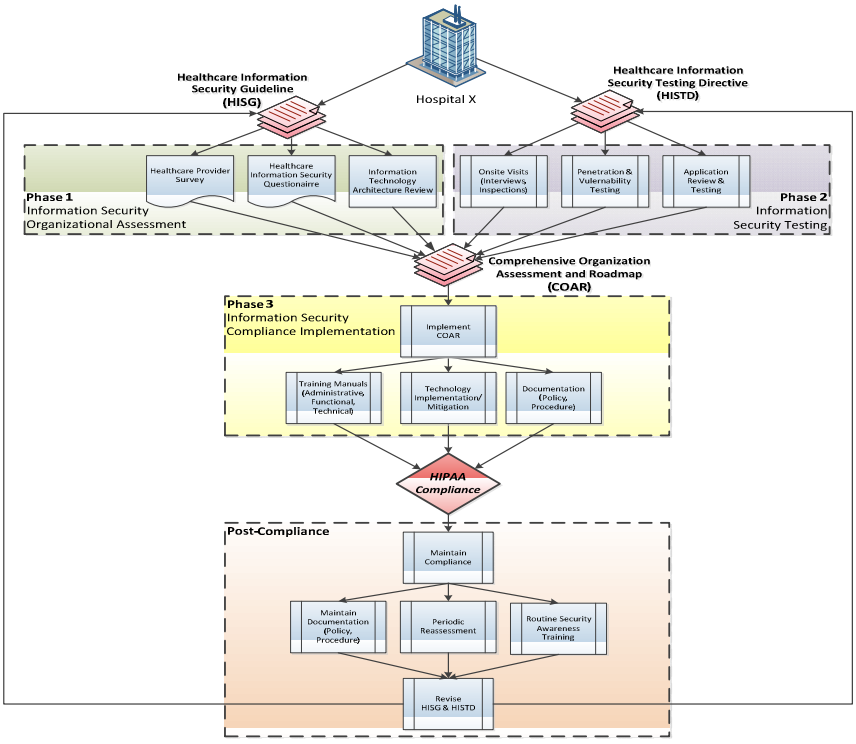

Fig. 1. Information Security Compliance Framework Implementation Flow Diagram

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 [17]; indicate most organizations are closer to full compliance to privacy than security. The partner hospital 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. 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 enact this type of change. 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.

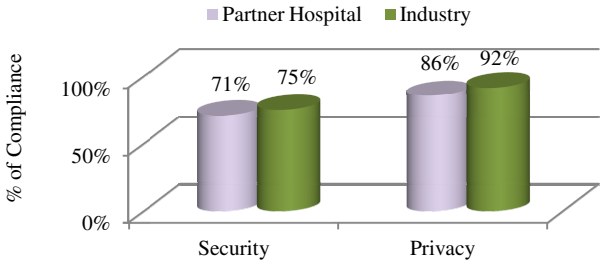

Fig. 2. Overall Compliance Performance

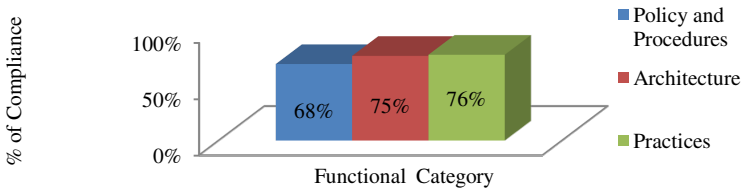

Fig. 3. Compliance per Functional Category

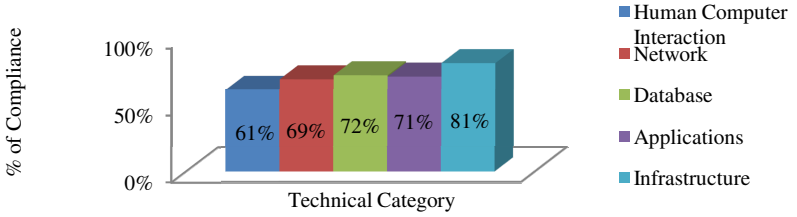

Fig. 4. Compliance per Technical Category

4.2 Security Testing Results

Phase 2 of the framework included a detailed, hands-on technical review and assessment of an organization's IT environment. The technical review included onsite visits, penetration and vulnerability testing, and a comprehensive review and assessment of all enterprise applications. At the conclusion of Phase 2, the organization's entire IT environment had been methodically examined, tested, and documented.

Table 1. Summary of Findings from Security Testing Phase

Subnet	Unique Hosts	Critical	High	Medium	Low	Totals
A	**98**	**66**	**234**	**406**	**93**	**799**
B	171	1583	2155	1611	415	**5764**
C	11	97	15	95	36	**243**
D	179	24	43	1025	195	**1287**
E	192	0	10	1114	187	**1311**
F	198	15	15	1146	196	**1372**
G	87	126	291	603	92	**1112**
H	26	359	436	219	50	**1064**
I	50	0	54	13	18	**85**
	1012	**2270**	**3253**	**6232**	**1282**	**13037**

Penetration testing and vulnerability scanning by their very nature are an exhaustive, iterative process that many times requires analysis from both operational and security perspectives. One of the most common issues that lead to vulnerabilities or exploitation is merely an ignorance that a particular host is present on the network or a host is running unnecessary or unexpected services [18]. The first step in any penetration test is to create a survey of the hosts that are present on the network and what services that are running. Many of these services are intentional and are functioning as expected. It is those hosts and related services that are unintentional that are of most significance for this initial survey. A number of intensive vulnerability scans were performed of Hospital X's environment. Initially the subnet A was examined exhaustively 98 hosts were discovered with 799 issues ranging from critical to low risk. Following this assessment, the decision was made to expand the network range being tested to include other subnets that held other production and development servers as well as clients and workstations. The expanded subnets included subnets B through I. The summary of the findings from both the initial assessment and the expanded testing can be seen in Table 1.

Through analysis of the security testing results, it was discovered that many of the specific critical and high risk vulnerabilities were found repetitively throughout the environment. Of the 5253 critical and high risk issues found, they are made up only 446 unique vulnerabilities. This finding suggested that enterprise wide patching processes and schedules as well as standardized deployment configurations of servers and workstations could mitigate many of these issues very quickly and reliably. Hospital X's technical staff was able to validate these findings and corresponding mitigation steps to resolve nearly 90% of the findings in a matter of weeks. The final

phase of the compliance framework has just begun with the partner hospital. Phase 3 is the implementation stage and includes making changes related to technical configurations, policy, procedures, training, and documentation based on the findings of the earlier phases. Based on the findings that the assessments revealed in the earlier phases, a complete list of recommendations has been prepared and is under review by Hospital X. Once the mitigation recommendations have been analyzed, they will be incorporated into the COAR and become part of the compliance implementation plan. This will enable a final, detailed implementation plan to be prepared. The next step will be to have the healthcare provider review and approve the plan, then ultimately schedule and execute it.

5 Conclusion

The opportunity to apply this research at Hospital X proved to be an excellent exercise. Hospital X was struggling with getting their computing environment to 100% HIPAA compliance. Only just below the national average for compliance for the Security and Privacy rules at 71% and 86% respectively, they were well on their way to full compliance at the beginning of this collaboration. A significant factor that was prohibiting the organization from achieving complete compliance was their lack of a comprehensive procedure to evaluate their environment and reliably identify issues. Their approach to information security was much more reactive than proactive. This stance put their organization at risk legally, financially, and ultimately ethically. Furthermore, not having the ability to periodically assess and test their systems created an unawareness of where to focus their efforts to move forward. Beyond HIPAA, Hospital X was eager to satisfy the Meaningful Use objectives and complete the attestation to qualify for the more than $2 million annual incentive payment. Hospital X had begun an EHR implementation to some extent a number of years prior to the relationship, as they were already a HIMSS Stage 6 hospital, but were unsure of meeting all of the care delivery objectives to in order to complete the MU program.

This research was able to close the gap for Hospital X with regard to both HIPAA and Meaningful Use. Phase 1 of the Healthcare Information Security Compliance Framework provided a quantifiable starting point for the organization. At the completion of this assessment phase, it was clear where the deficiencies were in policy, procedure, and practice. Overall the hospital rated 68% compliant with regard to policy and formal procedures, only slightly better at 75% for architectural design, and approximately 76% for the organization's practices. These results provided a basis upon which to begin Phase 2, the Security Testing stage. The security testing process yielded even more issues with the computing environment by identifying 300 critical and high level findings across 98 production servers. Furthermore, another 5,253 critical and high level issues were found on 914 other systems (workstations and test/development systems) that were on the hospital's production network. Only 16% of the organization's systems did not have at least 1 issue that required attention. This was a concerning discovery as this meant 84% of the hospital's environment was exposed to some degree to unnecessary risk. While finding issues in an environment can oft times not be well received, the Hospital X staff were extremely receptive to working through the analysis of those findings and considering mitigating actions.

Certainly the goal of all organization's information technology staff is to create and maintain flawless, impenetrable systems. Unfortunately the reality is this goal is rarely reached and it is critical to have effective methods to continually evaluate all systems and practices to uncover issues when they are present.

Accessibility is a pillar of healthcare delivery. However, as soon as access is afforded, it is the ethical, legal, and financial responsibility of healthcare providers to ensure the integrity of the care delivery is upheld. HIPAA and EHR systems lay the foundation for satisfying these concerns. Unfortunately, these endeavors have proved challenging to accomplish with the absence of standardized, openly provided, implementation plans. Each HIPAA covered entity has been forced to approach these tasks from their localized, individual perspective and they are spending vast amounts of time, resources, and money trying to determine multiple paths towards the same goals. With a lack of 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. Technology has long thrived on the adoption of standards and this research contends that the issues of accessibility, integrity, and efficiency in healthcare information technology are no exception.

There is overwhelming consensus in the healthcare industry that the spirit of HIPAA is positive and beneficial to both patients and providers. Likewise, the move from paper and film to EHR systems is clearly the natural evolution of health information storage and data exchange. It has not been so much of a struggle for most healthcare providers to find answers to the Why; it has been the How that has kept these issues at the forefront of the healthcare industry for over a decade. The complexity and reach of HIPAA and the Meaningful Use programs across the entire United States has provided a seemingly endless parade of motivations for finding better methods to ensure their implementation. The guides and tools this research has produced will surely assist healthcare providers with the initial implementation of these initiatives as well as better equip organizations to maintain their ongoing compliance.

References

1. United States. Department of Health and Human Services. Office of Civil Rights, HIPAA Administrative Simplification (2006), http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/adminsimpregtext.pdf (retrieved November 2011)
2. United States. Department of Health and Human Services. Center for Medicare and Medicaid Services, CMS EHR Meaningful Use Overview (2012), https://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Meaningful_Use.html (last accessed June 2012)
3. United States. Department of Commerce. National Institute of Standards and Technology, An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule (rev 1) (2008), http://csrc.nist.gov/publications/nistpubs/800-66-Rev1/SP-800-66-Revision1.pdf (retrieved July 2011)

4. HIMSS Analytics, EMR Adoption Trends (2012), http://www.himssanalytics.org/stagesGraph.asp (last accessed October 2012)
5. United States. Department of HHS. The Office of the National Coordinator for Health Information Technology, EHR Incentive Programs (2012), http://www.healthit.gov/providers-professionals/ehr-incentive-programs (retrieved February 2013)
6. United States. Department of HHS. CMS, Data and Reports (2012), http://www.webcitation.org/6EMwIm36I (retrieved July 2012)
7. United States. Department of Health and Human Services. Center for Medicare and Medicaid Services, HIPAA Security Series – Security Standards: Technical Safeguards (2007), http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/techsafeguards.pdf (retrieved September 2011)
8. Kroll, HIPAA Self Risk Assessment (2013), http://www.krollcybersecurity.com/hipaa-risk-assessment/ (last accessed on November 2013)
9. Clearwater Compliance, Achieve HIPAA HITECH Compliance (2013), https://www.hipaasecurityassessment.com/ (last accessed on November 2013)
10. Harle, C., Dewar, M.: Factors in Physician Expectations of a Forthcoming Electronic Health Record Implementation. In: Proceedings of the 45th Hawaii International Conference on System Sciences, pp. 2869–2878 (2012), doi:10.1109/HICSS.2012.277
11. Acharya, A., Coats, B., Saluja, A., Fuller, D.: A Roadmap for Information Security Assessment for Meaningful Use. In: Proceedings of the 2013 IEEE/ACM International Symposium on Network Analysis and Mining for Health Informatics, Biomedicine and Bioinformatics, Shanghai, China (2013)
12. United States. Department of Commerce. NIST, Technical Guide to Information Security Testing and Assessment (2008), http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf (retrieved June 2012)
13. HIMSS Analytics, EMR Adoption Model (2011), http://www.webcitation.org/6A1XGCtkJ (last accessed on November 2011)
14. Coats, B., Acharya, S., Saluja, A., Fuller, D.: HIPAA Compliance: How Do We Get There? A Standardized Framework for Enabling Healthcare Information Security & Privacy. In: Proceedings of the 16th Colloquium for Information Systems Security Education, Orlando, Florida (2012)
15. United States. National Archives and Records Administration, Title 45 – Public Welfare, Subtitle A – Department of HHS, Part 164 – Security and Privacy (1996), http://www.access.gpo.gov/nara/cfr/waisidx_07/45cfr164_07.html (retrieved April 2012)
16. United States. Department of Commerce. National Institute of Standards and Technology, An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, rev 1 (2008), http://csrc.nist.gov/publications/nistpubs/800-66-Rev1/SP-800-66-Revision1.pdf (retrieved July 2011)
17. Appari, A., Anthony, D.L., Johnson, M.E.: HIPAA Compliance: An Examination of Institutional and Market Forces (2009), http://www.himss.org/foundation/docs/Appari_etal2009_HIPAAcompliance_20091023.pdf (last accessed on November 2011)
18. United States. Department of Commerce. NIST, Technical Guide to Information Security Testing and Assessment (2008), http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf (retrieved June 2012)