TOWSON UNIVERSITY
OFFICE OF GRADUATE STUDIES

TOWARDS THE DESIGN OF STANDARDIZED FRAMEWORKS TO IMPROVE INFORMATION SECURITY AND PRIVACY IN HEALTHCARE: A CASE STUDY OF TWO LARGE NATIONAL HEALTHCARE PROVIDERS

by

Brian S. Coats

A Dissertation

Presented to the faculty of

Towson University

in partial fulfillment

of the requirements for the degree

Doctor of Science, Applied Information Technology

Department of Computer Science

Towson University
Towson, Maryland 21252

May, 2014

TOWSON UNIVERSITY

COLLEGE OF GRADUATE STUDIES AND RESEARCH

DISSERTATION APPROVAL PAGE

This is to certify that the dissertation thesis prepared Brian S. Contu entitled "TOWARDS THE DESIGN OF STANDARDIZED FRAMEWORKS TO IMPROVE INFORMATION SECURITY AND PRIVACY IN HEALTHCARE: A CASE STUDY OF TWO LARGE NATIONAL HEALTHCARE PROVIDERS" has been approved by this committee as satisfactory completion of the requirement for the degree of Doctor of Science in Information Technology.

Dr. Subrata Acharya Chair, Dissertation Committee	Subrata Acharya Signature	06/13/2014 Date
Dr. Jinjun Feng Committee Member	Signature	06/11/2014 Date
Dr. Michael P. McGuire Committee Member	Signature	6/13/2014 Date
Dr. Joyoni Chakrabarty Committee Member	Signature	6/12/2014 Date
Dr. Peter J. Murray External Committee Member	Signature	6/13/14 Date
Dr. Janet Y. DeLaney Dean, College of Graduate Studies and Research	Janet Y DeLaney Signature	6/13/14 Date

Acknowledgements

It is a pleasure to recognize and thank those individuals that enabled me to complete this dissertation. I would like to start by thanking Dr. Subrata Acharya for her willingness to serve as my faculty advisor and dissertation committee chair. I am most appreciative of the guidance and advice Dr. Acharya provided to me over the years. Further, I would also like to convey my gratitude to the other members of my dissertation committee, Dr. Joyram Chakraborty, Dr. Jinjuan Feng, Dr. Michael McGuire, and Dr. Peter Murray, for their involvement and helpful feedback. Lastly but most importantly, I would like to thank my family for their unrelenting encouragement and support as I completed this program while also juggling a flourishing career and a continually growing family. There are no words adequate enough to express my love and appreciation for my wife, Jessica, and my amazing daughters, Kallissa, Alexis, Katrina, and Tessa - thank you so much for your understanding and patience over these past four years.

Abstract

TOWARDS THE DESIGN OF STANDARDIZED FRAMEWORKS
TO IMPROVE INFORMATION SECURITY AND PRIVACY IN HEALTHCARE:
A CASE STUDY OF TWO LARGE NATIONAL HEALTHCARE PROVIDERS

Brian S. Coats

Integrity, efficiency, and accessibility in healthcare aren't new issues, but it has been only in the more recent years that they have 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. However, 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. Healthcare providers are under increasing pressure to derive answers to this issues and while integrity, efficiency, and accessibility have their own unique considerations, their solutions must also compliment one other to truly be effective. This research will converge on these issues by addressing compliance with the Health Insurance Portability and Accountability Act, electronic health record adoption and the federal Meaningful Use program, and pervasive electronic access for patients; all from the healthcare provider's perspective. Using standardized frameworks, this research proposes technological solutions for how accessibility, efficiency, and integrity in healthcare information security can be improved.

Table of Contents

List of Tables

List of Figures

Dissertation

Chapter 1. Introduction

The concept of providing patients electronic access to their health information has been a national objective with growing attention. The Affordable Care Act of 2010 was one of the more recent and significant strides that, among other priorities, made electronic access to patient medical data a national priority [1]. Furthermore, over the course of the last two decades the federal government has passed a number of laws to not only facilitate patient access but greatly enhance the exchange of medical information between all relevant parties: patients, providers, and payers. However, 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.

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. In the case of healthcare providers enabling patient access to their electronic health record, the Health Insurance Portability and Accountability Act (HIPAA) has provided many guidelines to

ensure the integrity of electronic protected health information (ePHI). As depicted in Figure 1, integrity is at the foundation, followed by efficiency, and finally accessibility at the pinnacle. Each higher layer is dependent on those layers below it to reach the ultimate goal of accessibility in the form of pervasive electronic access for patients.

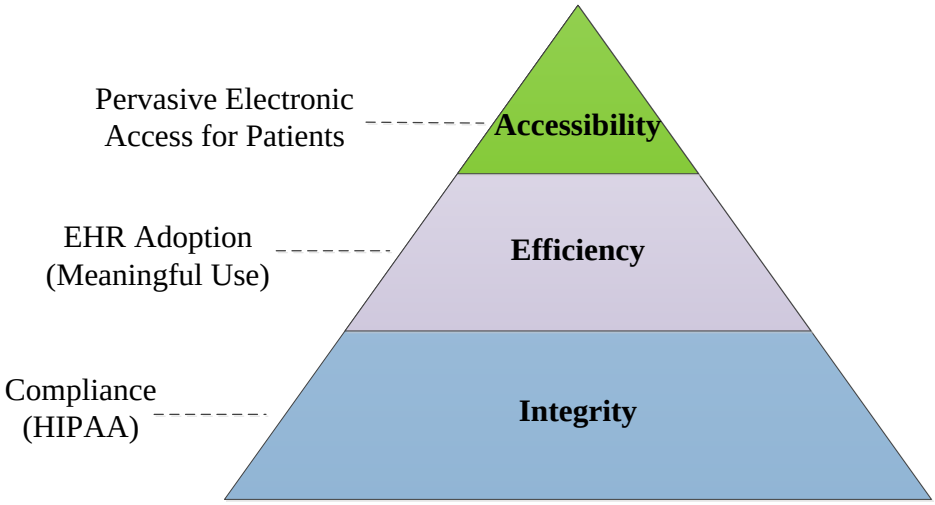

Figure 1. Proposed Research Topics

The HIPAA, the Health Information Technology for Economic and Clinical Health (HITECH) Act, and the National Strategy for Trusted Identities in Cyberspace (NSTIC) are some of the most significant federal actions related to achieving effective electronic healthcare access for patients nationally. HIPAA aims to use information technology (IT) to improve health insurance coverage and portability while also lowering costs and improving its quality [2]. 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 [3]. Finally, the White House's NSTIC initiative is aimed at addressing the usability and security concerns of electronic access by making the patient its central focus. NSTIC is singularly tasked with creating an "Identity Ecosystem" of interoperable technology

standards and policies related to digital identities to be used across all sectors to provide increased security and privacy, but most importantly ease of use for individuals [4]. All 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.

While the road to Health Insurance Portability and Accountability Act (HIPAA) compliance and EHR adoption is proving elusive, organizations clearly understand the importance and necessity of completing these undertakings. This problem is by no means trivial as it represents an extremely complex set of issues that naturally require equally complex analysis to derive viable solutions. The distributed and privatized nature of healthcare in the United States, in conjunction with the vast variety of healthcare entities, makes a systematic, exhaustive examination of every possible solution with every possible healthcare organization impractical if not impossible. As such, this research employed a case study approach to perform a detailed contextual analysis for a limited number of use cases. This approach enabled the ability to break this very complex problem down into more manageable pieces to identify the underlying issues and attempt to offer a path forward. During the design phase of the research, two specific use cases were identified to perform the associated data gathering and analysis of the case study. The use cases chosen were with two national healthcare providers. The use cases involved applying each of this research's proposed frameworks in one of the healthcare provider’s environments. These uses cases then provided a real-world evaluation of this research by measuring quantifiable impacts to those organizations. Further, by using these use cases, the case study was able to offer implications for how accessibility,

efficiency, and integrity in healthcare delivery can be improved through the application of the proposed information security frameworks.

1.1. Background and Motivation

The Health Insurance Portability and Accountability Act (HIPAA), established in 1996, provided broad guidelines for how health information should be secured, both within a healthcare provider's environment and when it is shared between disparate entities [5]. This legislation was arguably the most significant law related to the exchange of healthcare information on a national scale. The ability for patients, healthcare providers, and insurance companies to share and distribute health information between any and all necessary parties is a critical component to improving access to healthcare resources. One of HIPAA's primary goals is to enable this exchange of health information by creating uniformity, while maintaining privacy and security. Commonly known as the Administrative Simplification, this objective has proven anything but simple to achieve. Given the ever growing dependence of IT within all public and private domains, it was originally 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 more than eight years after the originally expected completion date, health institutions around the country are still attempting 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 [6]. 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. Unfortunately while the guidelines exist, HIPAA compliance has not occurred as quickly or completely as the federal government originally planned. Many healthcare providers are still struggling to achieve compliance while being threatened with significant penalties.

HIPAA compliance is mandated at both the federal and state level for all covered entities that work with 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 penalties of up to $25,000 per individual, per violation and criminal penalties of up to $250,000 and 10 years in prison. In 2010, over 2,700 corrective actions were required to be taken by healthcare entities based on complaints reviewed by the Department of Health & Human Services (HHS) [7]. More recently in 2013, the number of complaints filed has ballooned to 14,300 with almost 3,500 having corrective actions issued. Even with the HIPAA regulations having numerous punitive legal and financial reasons to have secure information environments, there have been tens of thousands of reported violations, since the industry has still yet to have 100% of healthcare providers achieve 100% compliance.

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 [8]. By way of this standardization, healthcare entities can exchange data much faster, securely, and more accurately to offer better patient care. 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 significant efficiency improvement opportunities that HIPAA affords, it only strengthens the case that there are tangible benefits for assisting healthcare providers to become compliant faster and with less effort.

The sluggishness of HIPAA compliance is paralleled by the delayed adoption of EHR systems by healthcare organizations. The provisions of the Administrative Simplification require the standardization of ePHI transactions to improve efficiency while also safeguarding the privacy and security of their data [9]. 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 Q1 2014 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 [10]. While a high percentage of providers have started the process of adopting an EHR system, very few have actually completed the process.

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 the 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 Health Information Technology for Economic and Clinical Health (HITECH) Act. This legislation provided the healthcare community a "transformational opportunity to break through the barriers to progress" [11]. HITECH 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 [12]. Stage 1 was just the first of an anticipated 3 stages to ensure full EHR adoption nationally. In 2013, the requirements for Stage 2 were released and entities can begin receiving payment for meeting this stage in 2014. Looking ahead, the Stage 3 requirements are already being circulated in a proposed form and it is tentatively scheduled for implementation in 2015. While HHS is offering incentives for early adoption, they are also circling back and levying penalties on providers if they haven't met the Stage 1 requirements 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 from inception in 2011 through May 2012 [13]. These reports, summarized in Table 1, 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.

			PROGRAM TOTALS			
Incentive Program		**Provider Type**	**Providers Registered**	**Providers Paid**	**% of Registrants Paid**	**Amounts Paid**
MEDICARE	Medicare	EP	163,748	58,530	35.7%	$994,993,305
		Hospital	202	89	44.1%	$133,465,560
		Total	**163,950**	**58,619**	**35.8%**	**$1,128,458,864**
	Medicare/ Medicaid	Hospital	3,373	958	28.4%	$1,753,110,807
		Total	**3,373**	**958**	**28.4%**	**$1,753,110,807**
		Total Hospitals	**3,575**	**1,047**	**29.3%**	**$1,886,576,367**
	Total		**167,323**	**59,577**	**35.6%**	**$2,881,569,672**
MEDICAID	Medicaid	EP	81,029	40,700	50.2%	$851,916,194
		Hospital	87	60	69.0%	$137,147,375
		Total	**81,116**	**40,760**	**50.2%**	**$989,063,569**
	Medicare/ Medicaid	Hospital	3,373	2,043	60.6%	$1,700,955,353
		Total	**3,373**	**2,043**	**60.6%**	**$1,700,955,353**
		Total Hospitals	**3,460**	**2,103**	**60.8%**	**$1,838,102,728**
	Total		**84,489**	**42,803**	**50.7%**	**$2,690,018,922**
Grand Total			**248,439**	**102,380**	**41.2%**	**$5,571,588,594**

Table 1. National Totals for Meaningful Use Payouts

(data for Table 1 taken from Centers for Medicare & Medicaid Services report [13]*)*

The gap between the number of registered providers and those that are actually getting paid demonstrates that EHR adoption and attestation are considerable challenges. It is important to note that the Stage 1 requirements only mandate a very partial implementation of an EHR with only some basic functionality having been adopted. It does not require that providers actually have an EHR system fully implemented and are

using it exclusively. This point just further exemplifies the struggles providers are experiencing with EHR adoption.

HIPAA and EHR implementations will surely increase the effectiveness and integrity of how data is utilized by healthcare providers and likewise exchanged with insurers. However, these programs focus very little on how patients can gain access to their own information. HITECH approaches the issue of patient access in its Meaningful Use program however the guidelines are extremely vague and generic as they have no stipulations for usability measures, merely that access provisions must exist. In addition to the regulatory and financial pressures created by HHS, the White House is now creating yet another impetus. In April 2011 the White House released its final draft of the National Strategy for Trusted Identities in Cyberspace (NSTIC). This strategy will force the healthcare industry to structure their identity access approaches to use a distributed model. All federal government agencies, including the HHS, are intimately involved in the development of NSTIC so it is imperative that healthcare providers ensure they are strategically aligned for participation. The NSTIC is laying a good foundation for cross-industry collaboration for easier user access. Unfortunately, the healthcare industry is considerably behind the curve compared to many of the other participating industries as it relates to identity assurance and federated identity practices [14]. The overwhelmingly private and distributed nature of healthcare providers in the United States has encouraged silos of technology adoption instead of a culture of collaboration and interoperability between providers and patients. The requirement of electronic access to medical information is a foregone conclusion but how to make this simple yet secure is still a long way off.

Regardless of the specific motivation, the need for security in healthcare providers' information technology environments is unquestioned. As such, each and every healthcare organization spends considerable time, effort, and money to establish technical and functional safeguards in an attempt to achieve an acceptable level of security for their systems. Likewise, healthcare providers are under increasing pressure to enable widespread access to their EHR systems for the patients they serve; the meaningful use incentive programs are perhaps the most significant driver encouraging this access.

1.2. Research Objectives

The goal of this research is to present a layered solution that bridges the gap from regulation to implementation 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. This research converges on these issues by addressing HIPAA compliance, EHR Adoption and the federal Meaningful Use program, and pervasive electronic access for patients; all from the healthcare provider's perspective. Using a case study approach, this research evaluated the proposed frameworks with two use cases in national healthcare providers' computing environments. These use cases provided a method to measure the effectiveness of the proposed solutions in real-world application.

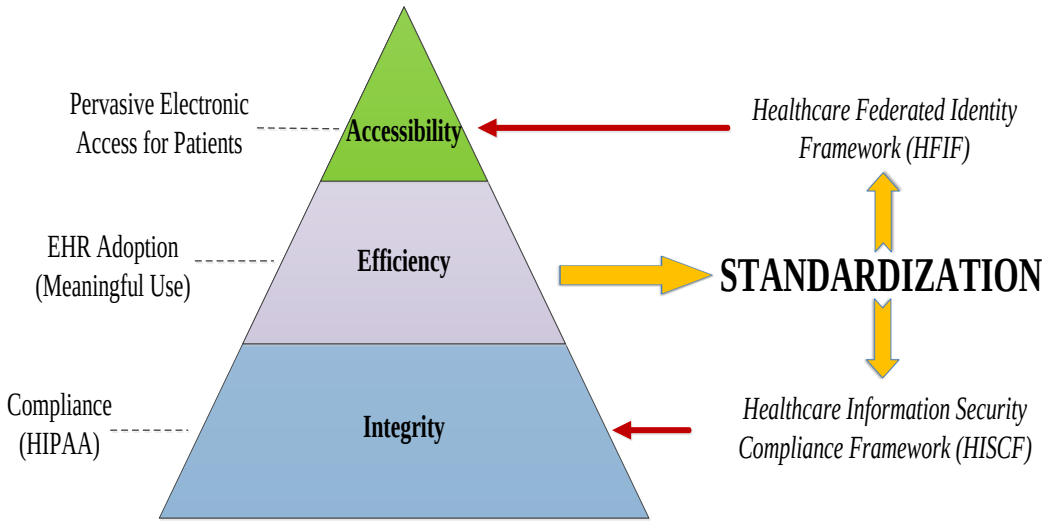

Figure 2. Proposed Convergence of Research Topics

Specifically, this research aims to lessen these challenges related to integrity, efficiency, and accessibility by providing answers to the following critical questions in healthcare information technology:

1. How do organizations verify that their security measures are functioning adequately and comprehensively address the requirements for federal compliance?
2. How do organizations provide documentation that the measures have been tested and work as intended whether for audit or attestation purposes?
3. How can healthcare providers enable easy access to their EHR systems for patients while preserving security and privacy but also be financially viable?
4. How can patients access their medical information for all healthcare providers in a similar fashion, without needing provider-specific credentials?

This research submits the answers to these questions are a set of comprehensive frameworks for healthcare providers to follow to assess and implement both effective and

complete information security policies and procedures. This research aims to fill 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. Furthermore, this research attempts to provide a practical, scalable solution to the credential issuance issue that must be overcome to have effective, widespread patient access to EHR systems. This research suggests that the cause of an organization's inability to consistently achieve HIPAA compliance, implement an EHR, and provide electronic patient access is not due to absence of technological solutions. As discussed at length in Chapter 2, the core barrier faced by healthcare providers is the difficulties surrounding implementation of said technologies. *The specific problem being addressed by this research is the lack of comprehensive, openly available frameworks for organizations to follow for healthcare information security compliance and usable federated identities and the effect on the implementation of these critical topics.*

1.3. Summary

The stage is set for the healthcare industry to provide a better quality of care delivery through the more effective and available exchange of ePHI between all appropriate parties while also ensuring security and privacy to their patients. It is now incumbent of the healthcare providers to implement the strategies, comply with the regulations, and offer the electronic services that patients have been eagerly awaiting. This is the crossroads that many healthcare providers find themselves at without a clear map of how to reach the destination. In response, this dissertation presents two key frameworks that propose to be comprehensive and actionable solutions to take an organization from requirement analysis to implementation.

In Chapter 2, a thorough review will be presented of what research has already been performed in the areas of Health Insurance Portability and Accountability Act (HIPAA) compliance assessment and EHR adoption frameworks, as well as models for providing pervasive patient access to EHRs. This literature review will include peer-reviewed conference proceedings and workshops, journal articles, federal government publications, and industry-recognized whitepapers. By first examining the work that has already been completed, what is still left unaddressed will begin to frame the actual problem this dissertation strives to solve. Chapter 2 will also provide context for where this dissertation's research fits into the larger landscape of information security in healthcare.

Chapter 3 will begin by articulating the specific objectives of this dissertation research. Next, an explanation of how this research's proposed solutions were designed will be offered along with the methodology used to perform and validate the research. Finally, the entirety of both of the two key frameworks produced by this research, the Healthcare Information Security Compliance Framework and the Healthcare Federated Identity Framework, will be lay bare.

In Chapter 4, the case study findings will be presented. This will include the actual results produced from implementing the Healthcare Information Security Compliance Framework and Healthcare Federated Identity Framework over the last few years at two national healthcare providers will be presented. This chapter discusses the tangible contributions this research has made in the use cases by dramatically improving their security and privacy compliance while increasing patient accessibility as well as assisting in one of the hospital's award of the Meaningful Use Stage 1 certification.

Chapter 5 provides a discussion of the use case results presented in Chapter 4 and what inferences can be drawn from them. Furthermore, the implications of these results not only to the partner hospitals but potentially to other hospitals and the healthcare industry at large are covered.

The final chapter will provide a summary overview of the entire dissertation research in an organized narrative. This chapter will highlight the products of this research and their context and significance to the landscape of information security in healthcare. Future research implications and suggestions will be discussed to outline what related 'holes' still remain within healthcare information security.

Chapter 2. Literature Review

Information security has perpetually been a hot topic for all industries. The specific subject of healthcare information technology (HIT) and healthcare information security (HIS) has sparked a vast amount of research over the last few decades and is reflected in a wide array of peer-reviewed scholarly papers and journal articles. Furthermore, much attention has been given to the difficulties faced in HIT and HIS related to Health Insurance Portability and Accountability Act (HIPAA) implementation and assessment, EHR adoption, and patient accessibility. After a thorough examination of a substantial amount of the related literature, clear shortcomings became evident in the technological solutions as many researchers lamented some common problems and searched for answers.

2.1. Challenges

2.1.1. HIPAA - Soaring Implementation Costs

Healthcare providers and payers have been attempting to achieve Health Insurance Portability and Accountability Act (HIPAA) 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 nationally. As early as 2003 when the final regulations for both HIPAA rules had been released, healthcare legal expert George Annas [15] was already predicting HIPAA implementations to be "costly, inconsistent, and frustrating". Annas went on to state that "HIPAA consultants" were quickly becoming necessary for hospitals, health plans, and physician practices in order to understand how to comply with "long, complex" unclear regulations. By 2009, Appari et al [6] still echoed that

sentiment by offering that providers have pressure to hire external consultants as "there is a high degree of uncertainty associated with the interpretation of regulations [HIPAA] and organizations lack adequate in-house resources". In 2005, the Department of Health & Human Services (HHS) was already 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 [16]. By 2009, HIMSS sponsored research suggested that the actual nationwide implementation costs for providers would be closer to $40 billion [6]. Most recently in 2013, the Department of Health and Human Services had re-estimated this figure to have grown to a national average of $114 million to $225 million in the first year and a recurring annual cost of $14.5 million, per healthcare provider [17]. 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 are creating financial burdens drastically higher than originally anticipated. Many providers and researchers argue the HHS is still significantly underestimating the actual compliance costs [18].

2.1.2. HIPAA - Deadlines Missed

Surmounting costs aside, the original schedule set by the Privacy and Security Rules required compliance by 2003 and 2005 respectively [8]. Unfortunately these compliance goals were not met by most healthcare organizations around the country. In 2008, the Centers for Medicare and Medicaid Services performed a review of HIPAA covered entities (CEs) and their compliance only with the Security Rule. This review demonstrated that CEs continued to struggle with meeting all aspects of the regulations, specifically in the areas of risk assessment, currency of policies and procedures, security

training, workforce clearance, workstation security, and encryption [19]. Even in 2013, Solove [20] discusses the still present gap in HIPAA compliance by all CEs and offers that "in addition to the dynamism of HIPAA, compliance is not something that is ever completely solved". He continues that it is not a one-time implementation but rather a daily challenge to maintain. As such, healthcare entities are faced not only with just becoming HIPAA compliant at single point in time, but they must achieve and maintain compliance perpetually. Therefore it is critical for these organizations to have clear and comprehensive guidelines to follow for maximum efficiency in their efforts.

2.1.3. HIPAA - Difficulties Ensuring Data Integrity

Fichman et al [21] note that because ePHI is personal by nature this compounds public fears and concerns related to data breaches. Healthcare providers must work hard to gain the trust of their patients and work even harder to maintain that trust. Data breaches have severe consequences for providers ranging from fines, embarrassment, reputational damage, and remediation costs [22]. HHS, as part of the Health Information Technology for Economic and Clinical Health (HITECH) Act, has implemented a new data breach notification process that requires healthcare entities to publically post breach announcements for cases involving 500 or more individuals [23]. Similarly, HITECH also increased the severity of the fines up to $1.5 million for HIPAA violations related to both inadvertent and willful disclosure of patient data. While the penalties are dramatically increasing and organizations are investing in security protection and assessment tools, the reality is there is still a significant gap between the regulations and practice. In the first two years since the HHS installed the Breach Notification Rule, over 10 million patients' data were inappropriately disclosed [7]. A number of issues have

been identified as the reason for healthcare organization's limited success with implementing security practices that are effective and compliant with the HIPAA directives. These issues include superficial implementations that don't align technology and business practices [24], the tendency to be reactive instead of proactive due lack of active, established security programs [25], and security measures being implemented piece meal instead of a comprehensive, complimentary approach [26]. Xia et al [26] portray compliance as "a snapshot of security about whether an organization exhibits controls". They offer that organizations are more driven by compliance than true data security. Johnson et al [27] caution that organizations that employ security assessment models with a "check-the-box" mentality do not have true assurance their security measures are effective; it is only through comprehensive testing and auditing that the measures are vetted. Aral et al [28] make the apt distinction that actual security is defined by how well the security controls used for compliance are deployed and function.

2.1.4. EHRs - New Way of Doing Business

For healthcare providers, one of the major steps towards fully meeting the HIPAA regulations is the implementation of an EHR system. As of December 2011, HIMSS reported that while over 90% of healthcare providers were in some stage of implementing an EHR solution, only 66 hospitals or just over 1% nationally, had actually achieved Stage 7 – the final EHR adoption stage [29]. By Q1, 2014 these figures had risen to 95% of all healthcare providers that started an EHR implementation but the completion rate had only increased to 3%. Furthermore, even with the federal government offering anywhere from $100,000 to over $2 million per provider, per year just to demonstrate the 'meaningful use' of even a partial EHR implementation, only about 41% of providers

have cashed in [13]. Over $5.5 billion has already been paid to healthcare providers participating in the Meaningful Use program, but almost another potential $8 billion is being left unclaimed. Clearly providers are being given the proper motivation to implement EHR systems but they are finding themselves ill-equipped to take the necessary steps to accomplish the task. HealthLeaders Media rated EHR adoption, specifically meeting Meaningful Use requirements, the #8 issue for healthcare providers in the United States in 2011 [30].

There are a variety of reasons why EHR 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. EHRs require all healthcare transactions to be handled electronically and this is a significant change for many entities [31] [32]. Additionally, not only do EHRs require transactions to be electronic but it mandates 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 [33] [34].

The transition from paper to electronic data storage and exchange, introduces a myriad of new security and privacy concerns that many healthcare providers previously didn't have to consider [35]. Baumer et al [36] contend that the "impact of security breaches of company protocols that inadequately protect stored records are much more significant [with electronic medical records] than with paper records" and they create a noticeably increased opportunity. Many experts theorize EHR adoption is being stymied

because healthcare providers are viewing patient access to EHR as an exponential increase in the opportunity for data leakage [37] [38]. Aside from strictly EHR access, patients and practitioners alike are interfacing with ePHI in an ever increasing variety of ways thus creating additional security challenges. PwC predicted that in 2013 the healthcare industry will be faced with substantially new privacy and security difficulties coping with the Bring Your Own Device (BOYD) phenomenon. PwC named this #8 in their annual top ten issues for healthcare report and estimated that only 46% of hospitals have a security strategy to address this impending problem [39]. As such, the need for reliable security and privacy assessment and testing within healthcare organizations is significant.

2.1.5. EHRs – Providing Electronic Patient Access

EHR systems will afford significant cost savings to healthcare providers by streamlining and standardizing their exchange and storage of ePHI. These systems will also enable better access to patient data by all parties - providers, insurers, and patients themselves. But with this increased access, healthcare providers are presented with the challenge of ensuring both privacy and security are preserved [40] [41]. Additionally, providers have the daunting task of making the process of patients gaining electronic access to their data uncomplicated and straightforward. The recent Meaningful Use Stage 2 objectives specifically mandates that hospitals grant patients access to view, download, and transmit their health information online within 36 hours of discharge; Eligible Professionals (EP) have to do this within 4 business days [42]. Unfortunately, little to no guidance is given for how this should be accomplished, only that access provisions must exist. Therefore, providers are faced with granting timely, simple, wide-

spread access to their EHR systems, while guaranteeing the integrity of the data. The healthcare information technology industry has long discussed the issue and challenges of providing patient access, with very little in the way of solutions [43] [44].

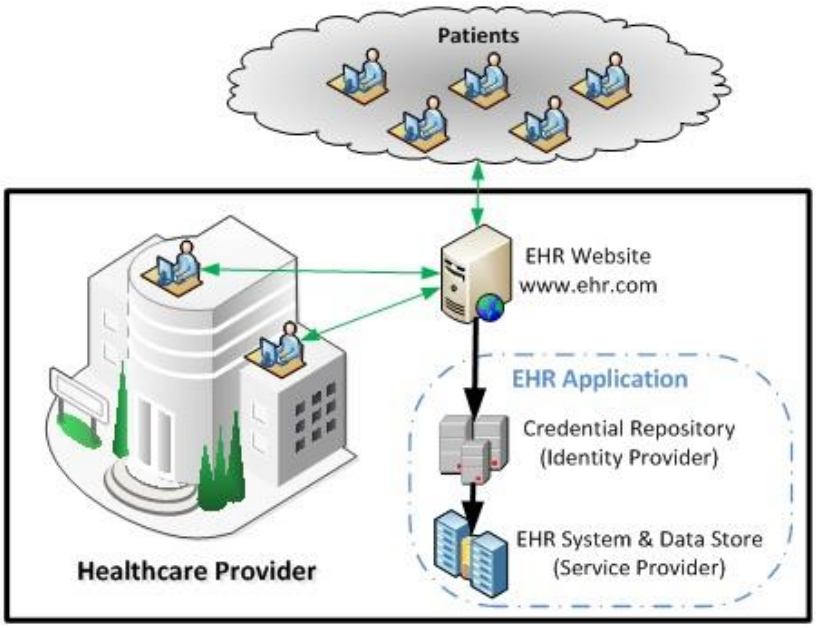

Figure 3. Proposed Traditional EHR Access Model

2.1.6. Patient e-Access – Digital Credential Management is Nontrivial

A key component of providing EHR access is how users will validate their identity. In a traditional scenario, this issue would be addressed by each EHR system creating its own, unique data stores and corresponding security controls for accessing their respective data. Similarly, authentication for these systems would involve using a credential stored locally within the system being accessed, as depicted in Figure 3. Therefore healthcare providers employing this traditional model must issue their users some credential, such as a username and password that is stored within the healthcare provider's local EHR system. Consequently, when the user attempts to access said EHR system they must enter the corresponding credential for that system. The effort and

complexity associated with the establishment, issuance, and maintenance of digital identities and corresponding credentials creates both a usability barrier for patients as well as an efficiency barrier for healthcare providers [45] [46].

Internationally, the majority of countries that have broad national EHR implementations have largely embraced the traditional authentication model [46]. The Netherlands has a national registry where all citizens are registered and possess a solitary digital identity [47]. This single identity paired with a national public key infrastructure (PKI), provides a secure authentication model for a single, national EHR deployment. Sweden has a very similar model as they also have a national EHR deployment. Sweden's nationwide health information network utilizes a single identity repository, the National Patient Summary system [48]. This system leverages smart cards as credentials instead of traditional soft-factor authentication like a username and password. While these single Identity Provider deployments have scaled for European countries that have national health programs, they become impractical for a largely distributed health system such as in United States. In the United States each healthcare provider is responsible for establishing and maintaining their own EHR system and by extension credential repository. Further, even the solutions adopted by the European countries that work well within that particular country start to break down when considering international interoperability. Weber-Jahnke et al [49] submit that there are only standards for interoperability between countries with respect to back-end data exchanges but not on the front-end for user access. In order to consider accommodating international interoperability, the scope of the credential repository needs to likewise not be restricted by national boundaries [50]. To this end, while in many cases, like the United States, the

traditional EHR access model of having one credential repository for one EHR system becomes impractical, it universally becomes impractical on an international stage. Sherlock et al [51] conclude for EHR systems to function optimally, they must be able to interoperate and the only current structure that can facilitate this exchange is a cloud-type solution. Zhang et al [52] concur with the assessment that the Cloud is the logical progression for EHRs to interoperate and patients to have ubiquitous access but a viable solution has been yet to be developed.

2.1.7. Patient e-Access – Single Credential vs. Provider-Specific

To compound the difficulty of credential issuance, if an individual interacts with multiple healthcare providers, they are required to have provider-specific credentials for each EHR system. Beard et al [53] point out this specific issue of fragmentation of an "individual patient's health information across the system" of numerous healthcare organizations is a critical obstacle for providing comprehensive access for patients. Beard et al identify the need to resolve this issue and offer the solution must be either through some form of an aggregated or federated access model. At the most basic level, the usability of an EHR system by a patient starts with being able to log in. Baker et al [54] acutely state that regardless of the security mechanism and its theoretical effectiveness, the primary issue should be usability or users simply won't use it. Requiring patients to contact each of their healthcare providers to establish unique credentials is appreciably more cumbersome and confusing compared to using a single, familiar credential for all EHR systems.

Another aspect to consider is that a healthcare provider establishing and maintaining the technical and support systems needed to issue credentials becomes an

intensive and costly undertaking. Li et al [55] conclude that the complexity and effort required to deploy secure yet easily accessible systems has become a barrier to the deployment of EHR systems. Therefore the traditional access approach, depicted in Figure 3, becomes inefficient and impractical compared to using a preexisting infrastructure that has very little associated cost and effort to utilize. For providers that are starting or have already begun to address identity access and management in their environments, it is critical that the technical and organizational solutions being adopted are scalable and able to easily interoperate throughout the entire healthcare industry and beyond. Hassol et al [56] conducted a survey of over 4,000 members of a health system in the United States related to patient experiences and attitudes to a patient EHR. The findings reveal that while over 80% of their respondents had a very positive experience and attitude related to accessing their EHR, only around 60% found the information to be acceptably complete. The lack of context within the patients' overall medical history with all providers was the key component that contributed to this negative impression. Pratt et al [57] report similar findings from studies related to patients' satisfaction with EHR systems. The findings indicate that patients were "frustrated by their inability to manage it all [medical history]" at one location, creating a very fragmented user experience.

2.2. Current Solutions

2.2.1. Self-Assessment Practices Lacking

As much of the published literature confirms, the core challenge that healthcare providers face with meeting Health Insurance Portability and Accountability Act (HIPAA) compliance, while also ensuring effective security, is simply the creation of a

plan to assess and test their environments. Further, once the assessments and tests are complete, the organizations also need a remediation plan in the form of an implementation guide to react to any issues discovered. 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 [58]. This guide gets closer to the concept of mapping regulation to implementation but still does not provide specific actionable recommendations. Unfortunately this is as close as the industry comes to have a publically available HIPAA compliance implementation guide for organizations to follow. Very recently in 2013, Wang et al [59] offer that theoretically organizations are provided reasonable steps to achieve HIPAA compliance and adequate ePHI protection but "in practice, organizations find this guidance too vague". 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. Middleton et al [60] contend that the lack of strong standards for entities to follow is slowing the progress of reaching HIPAA compliance and by extension EHR adoption. Middleton et al goes on to say that even if every health practitioner was committed to HIPAA compliance, it is critical that "we engineer adoption strategies that scale" and every provider "must not be forced to rediscover best practices for implementing." The published recommendations are at a very abstract level and require much interpretation to formulate an actual

implementation strategy. Massey et al [61] explain that regulatory phrases are not technical specifications therefore mappings must be created between the HIPAA regulations and actual implementation requirements.

In 2013, Lambrinoudakis [62] performed an extensive review and evaluation of available compliance frameworks for numerous security and privacy requirements including those set forth in HIPAA. He concluded that there are "significant gaps in compliance [frameworks]" and he goes on to specifically name HIPAA as an example of federal regulations that are in need of much more detailed guidance for entities trying to meet the mandates. Also in 2013, Kwon et al [63] performed an empirical study, based off a survey conducted by HIMSS and Kroll, a national leader in healthcare information security [64], of 243 hospitals in the United States, which demonstrated an entity's ability to address HIPAA (among other regulations) is directly related to the operational maturity of information security within the organization. Kwon et al state that without clear direction and no practical assessment guidance, the issues of compliance and security become the individual organization's responsibility to determine what an adequate approach is for their environment. This research submits that an entity's ability to achieve HIPAA compliance shouldn't be dependent on having a highly fluent IT staff that can competently navigate the regulations and design a tailored compliance solution. Furthermore, this research purport, as echoed by the numerous experts referenced, an open source, freely available compliance assessment solution is missing in the academic literature. With this a lack of readily accessible, comprehensive, and meaningful guidance, many entities have difficulty determining the best path for them to follow to satisfy each requirement.

2.2.2. Comprehensive OR Cost-Effective

Further demonstrating the lack of self-assessment guidance 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 include questionnaires for self-assessment and intensive penetration testing for onsite assessments [64] [65]. 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. The Health Information Trust (HITRUST) Alliance has created their *Common Security Framework (CSF)* to serve as a holistic solution to this significant need. HITRUST presents their CSF as a "comprehensive and flexible framework that remains sufficiently prescriptive in how control requirements can be scaled and tailored for healthcare organizations of varying types and sizes" [66]. Furthermore the CSF includes federal regulations and standards such as HIPAA, Payment Card Industry Data Security Standards (PCI DSS), and Control Objectives for Information and Related Technology (COBIT) as well as recommendations from NIST, the Federal Trade Commission (FTC), and the International Organization for Standardization (ISO). The scope of the CSF in fact exactly matches the need of a prescriptive, standardized solution for healthcare organizations to follow. As such, it is not surprising that the CSF is the most widely adopted security framework by the healthcare industry in the United States [67].

Unfortunately, the CSF like the consulting firms, comes with a substantial price tag for an annual subscription to access their framework content and information and have very limited (ranges from 10-20 annually depending on subscription tier) 'tickets' for working with a knowledgeable professional about how to implement the CSF.

Outside of healthcare, the concept of establishing standardized frameworks is very common. NIST has established the Risk Management Framework (RMF) to provide a systematic approach for managing organizational risk across all industries and sectors [68]. The framework can be applied to either new or existing information systems to evaluate risk as well select, implement, assess, and monitor mitigating controls to risk. Similarly, the Financial Services Roundtable, a collaborative body made up of the leadership of the nation's largest financial institutions, saw the need to create a standardized approach for information security within the financial industry. As a result, the verbose Banking Industry Technology Secretariat (BITS) Security Program was created that shared information security best practices and successful strategies [69].

Up to this point a comprehensive solution, like the CSF, RMF, or BITS Security Program, has not been presented in an open academic format for the healthcare industry such that organizations can perform both the abstract style assessment using questionnaires and surveys as well as conduct the active penetration testing themselves. 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 aside from the

man-hours to perform the assessment. Therefore as it stands today, 2 basic options have developed, either 'pay to play' by contracting with one of the private security assessment firms that specialize in HIPAA compliance or establish a subscription to HITRUST's CSF, or alternately use the NIST guideline and muddle through alone. With many organizations' considerable budget constraints, the latter option of proceeding independently using the existing guidance tends to become the common option [63]. Additionally, without an apparent plan or timeline to follow, it becomes extremely difficult for organizations to generate realistic cost estimates for their compliance efforts and likewise secure the necessary budgetary commitments [70]. This results in enormous wastes of capital, time, and energy for the healthcare provider. This point has been demonstrated consistently since the first HIPAA implementations began. Consequently, national cost estimates of HIPAA efforts have well eclipsed a factor of ten higher than what regulators estimated when the law was first enacted.

Only further complicating the HIPAA compliance landscape, the final rules of the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 introduced significant changes to the prior HIPAA regulations. While designed to encourage the development of health information exchanges these changes are still requiring additional attention and therefore cost and effort to be extended to HIPAA compliance. As part of these changes, the rules expanded the types of entities that are covered by HIPAA [71]. Previously, HIPAA only dealt with healthcare providers, health plans, and healthcare clearinghouses. The final rules released in January 2013 now defines covered entities as any vendor that creates, transmits, receives, or maintains ePHI. Furthermore, these additional entities can now be held civilly and criminally liable.

Aside from new entities being covered, even those entities that had achieved or were close to achieving HIPAA compliance coming into 2013 are now having to evaluate and accommodate the considerable additions and changes to the regulations [72]. The result of these recent changes have even more entities scrambling to become HIPAA compliant and effectively taking the cumulative percentage of all covered entities' compliance further away from the 100% target.

2.2.3. Lack of Scalability and Availability

When examining the potential solutions for providing electronic patient access to EHRs there are numerous existing models to consider although this research submits that a viable solution has yet to be developed that is scalable, cost-effective, and easily available to virtually everyone. This electronic identity situation has many healthcare providers finding themselves poorly positioned to enable the types of distributed access that EHR systems are supposed to facilitate [73] [74]. The regulations and programs that are driving EHR adoption, including HIPAA and Meaningful Use, provide virtually no direction on how to tackle these enormous usability and efficiency challenges. The federal program National Strategy for Trusted Identities in Cyberspace (NSTIC) is aggressively working to establish interoperable technology standards and policies for sharing identity information potentially anywhere in the public or private sectors [75]. The Department of Health and Human Services, the agency responsible for HIPAA and Meaningful Use, is intimately involved in the development of NSTIC. This strategy will compound the need for healthcare entities to entirely restructure their approaches for identity and access management from centralized to distributed models.

It is important to note that numerous organizations and foundations are likewise working in the identity space related to portable digital identities [76]. Considerable work is being done in the higher education community by Internet2 and the InCommon Federation. This work is aimed to enable member universities access to other universities' and governmental resources using a single digital identity housed at the home institution. InCommon has been working extensively with federating technologies for the last decade and by no accident has become the first trust framework the Federal Identity, Credential, and Access Management (FICAM) agency has approved for LOA 1-2 access for federal resources [77]. Unfortunately, while InCommon on behalf of higher education has made significant strides towards interoperable digital identities, the majority of the population of the United States does not have a relationship with a higher education institution in order to have credentials issued from that source. Furthermore, relationships with higher education institutions are not free and therefore this potential solution would prove cost-prohibitive for much of the population. This research offers that InCommon's successes need to be built upon and used as a model for other industries outside of the higher education community. In the private sector, the Open Identity Exchange (OIX) is working closely with FICAM to advance private trust frameworks and identity portability to access federal resources using OpenID [78] [79]. Elsewhere, Verizon has recently developed a Software as a Service (SaaS) offering to perform external authentication service, similar to those proposed by this research, specifically for healthcare organizations [80]. However, similar to the InCommon Federation, Verizon’s solution has a cost associated either for the patient as they would be required to be a

Verizon customer or by the healthcare provider on behalf of all their patients to enable the service.

Even once an Identity Provider has been determined as viable, it is equally as critical to determine what technological standard can be easily leveraged by both the Identity Provider and the healthcare provider(s). Dagdee et al [81] propose a hybrid access control methodology to solve the identity registration and credential issuance problem for certain types of care delivery. This methodology would allow the traditional credential methods but also allow authorization credentials (AC) to be used. The AC would be based on a person's role in the delivery of care, like a practitioner or emergency personnel, such that if a system could assert the person's identity was connected to one of the appropriate roles, their specific identity wasn't required to be pre-registered before gaining access to the EHR system. Even with the AC method proposed, Dagdee et al [81] admit that the most commonly used access control mechanisms are based on a specific person's digital identity and pre-registration of the associated credential in an EHR. Further, they articulate that continued work is needed in creating a flexible, scalable "infrastructure for the issue and management of credentials." They further submit that it is the issue of traditional credential registration and issuance that is fueling the need for alternative and hybrid approaches to be considered. Katehakis et al [82] proposed a similar role-based solution to facilitate EHR access, but once again name credential issuance as a barrier for adoption.

The majority of the proposed access frameworks for EHR systems involve using PKI for the authentication mechanism as some of the European countries have done [83] [52]. Wright et al [84] propose a very secure authentication model that involves PKI but

they ignore the issue of how the security tokens are to be distributed. Hu et al [85] also offer a hybrid PKI solution that very aptly meets the security and privacy requirements of HIPAA but also requires each healthcare provider to issue smartcards to each of their patients. Adding to the challenge of token-based authentication, whether soft or hard tokens, is the associated costs. Tanimoto et al [86] admit that with all PKI's benefits, it is rarely deployed on large scales because of its significantly higher cost structure compared to other forms of authentication. Certainly scalability needs to be considered when evaluating solutions. This research would contend that theoretically these PKI solutions are viable but in reality they are both cost prohibitive and logistically impossible.

In response to the disjointed data presentation and management issue, Bhatti et al [87] present a federated EHR framework that allows users to pass from one EHR system to another. Their solution leverages Security Assertion Markup Language (SAML) and Extensible Accessible Control Markup Language (XACML) in conjunction with the well-established Federated Database System (FBDS) [88] architecture. While they were able to create successful prototypes of a federated EHR environment, a key deficiency that they conceded was the patient credential issuance and management effort. Daglish et al [89] agree that a critical issue to be addressed in patient access to health records is the establishment of credentials for users from a trusted source.

In the literature reviewed, all distributed access models either cite credential distribution as being a critical issue to address or merely ignore this component of the access workflow altogether. For this reason, this research gives special focus to the credential issuance and maintenance topic. The vehicle for credential distribution and the cost to establish and support said credentials are all directly related to a solution's true

scalability. This research proposes specifically how a federated authentication model can be replicated using an open source style architecture to leverage credentials held by a larger population of patients while significantly lowering costs to the healthcare provider.

The recognition of the need for standardized frameworks for healthcare information security is widespread throughout the healthcare industry and federal government, even within the White House. This point is specifically acknowledged and articulated in a 2010 report by the President's Council of Advisors on Science and Technology (PCAST) [90]. The report stated that organizations with successful health IT deployments were required to use expensive, organizationally tailored solutions that required substantial resources to implement and identified the need for more widely adopted standards. Whether it is HIPAA compliance, EHR systems and Meaningful Use, or distributed electronic patient access, every healthcare entity is approaching these issues independently. This approach is continuing to prove both costly and timely, and ultimately the general public feels the impact by way of diminished quality of healthcare delivery. The fundamental objectives of all these regulations and programs provide for valuable improvements to the overall health care in the United States. Unfortunately these benefits can only be realized when the programs are completed and at present the necessary steps are proving extremely challenging for healthcare organizations. Based on the experts presented in this literature review, there is agreement in healthcare information technology that the roads to HIPAA compliance and EHR adoption are riddled with pitfalls and obstacles. There is clear acknowledgement in the industry that more standards are needed and better guidance required to make these journeys easier and quicker for healthcare providers. This research examines these needs, both

hypothetically and in current practice, and offers solutions that have been implemented within national healthcare providers' environments.

Chapter 3. Research Methodology

3.1. Research Focus

Organizations have both ethical and financial motivations to provide their customers the guarantees and benefits that the Health Insurance Portability and Accountability Act (HIPAA) and EHR systems afford. As a result, healthcare providers are spending massive amounts of time and money on their implementations. Chapter 2 explained in depth the genuine need for comprehensive, widely available frameworks for organizations to leverage both for healthcare information security compliance and federated identities for patient access to EHRs. While improved electronic patient accessibility is the ultimate goal, this can only be accomplished once integrity and efficiency have been accomplished. This research purports that the solution must be comprehensive, cost-effective, and interoperable to truly be successful and viable.

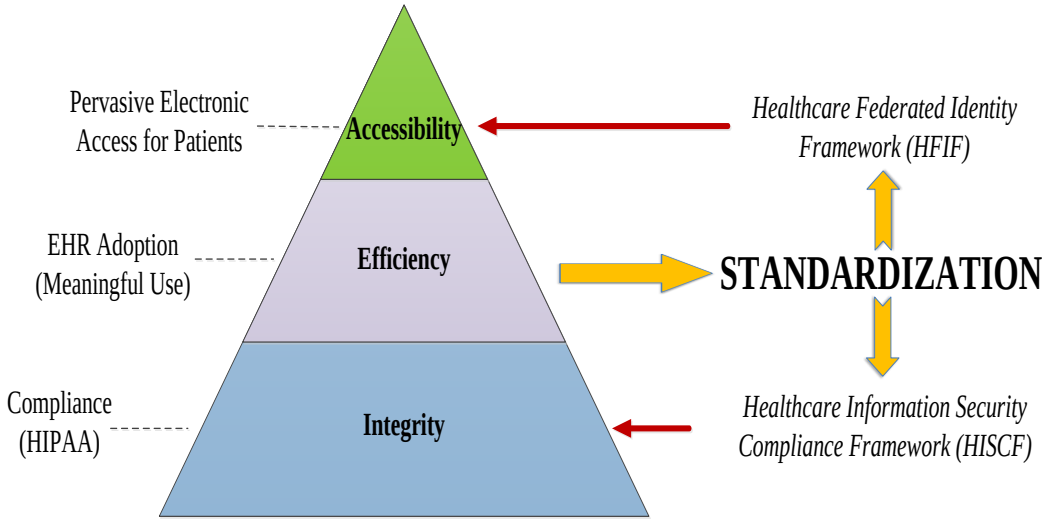

Figure 4. Proposed Solution

This research's goal is to address the following critical questions related to integrity, efficiency, and accessibility in healthcare information technology:

1. How do organizations verify that their IT security measures are functioning adequately and comprehensively address the requirements for federal compliance?
2. How do organizations provide documentation that the measures have been tested and work as intended, either for audit or attestation purposes?
3. How can healthcare providers enable easy access to their EHR systems for patients while being financially viable and also preserving security and privacy?
4. How can patients access their medical information for all healthcare providers in a similar fashion, without needing provider-specific credentials, to move towards ubiquitous electronic access?

By focusing on these questions, this research intends to derive technological solutions that are generic enough for widespread adoption but also carefully designed to satisfy the applicable federal regulations related to privacy and security. Specifically, the key objectives of this research are:

- The creation of the overarching Healthcare Information Security Compliance Framework (HISCF) to offer direction for organizations to plan and execute their overall HIPAA compliance efforts including Meaningful Use attestation,
- The creation of the Healthcare Information Security Guide (HISG) to provide comprehensive implementation level guidance for satisfying HIPAA regulations,
- The creation of a set of assessment surveys, based off the guidelines set forth in the HISG, that comprehensively evaluate an organization's information technology architecture as well as policies and practices,

- The creation of the Healthcare Information Security Testing Directive (HISTD) and a collection of open source security testing software for organizations to actively test their environment then mitigate any findings,
- The creation of the Healthcare Federated Identity Framework (HFIF) that will position healthcare providers to enable distributed electronic access to patient data, and
- A set of identity assurance profiles for Cloud Identity Providers to follow to ensure their practices conform to industry standards and meet HIPAA guidelines;
- Enhanced security and privacy for a national healthcare provider that will enable qualification for Meaningful Use Stage 1.

3.2. Research Design

When considering the 3 basic goals of this research - integrity, efficiency, and accessibility in healthcare - it became clear that any technology solution would require a delicate balance of these 3 areas in order to be viable for practical application. As such, integrity and accessibility quickly became the 2 pillars and motivations of the solutions, while efficiency became the measure of success. Integrity (or compliance) was the first of the 2 foundational elements tackled. In a very basic sense, the design approach was to determine how an organization could measure and achieve compliance (ensure integrity) in an efficient manner. Once integrity had been addressed, the research's attention shifted to how to make healthcare access more easily attainable and efficient. These efforts resulted in the creation of 2 unique frameworks that aim to bring together integrity, accessibility, and efficiency for a healthcare provider's organization.

3.2.1. Assumptions, Limitations, and Delimitations of the Research

In all research studies there are assumptions made, limitations encountered, and delimitations imposed. This research was no exception and it is important to present and explain those characteristics before delving into the proposed solutions.

There were a number of unprovable factors that were simply accepted as true within the context of this research. Identifying these assumptions was a key step in determining the proper approach to the problems targeted by this research. First and foremost, the assumption was made that the regulations set forth by the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act will continue to be a requirement for healthcare providers and they will not be drastically contradicted or repealed in the future. Without these regulations, much of this research becomes irrelevant to healthcare providers and the healthcare industry at large. Additionally, this research assumed the implementation configurations and practices documented in the 'key sources' tables – Table 2 and Table 3 – have in fact been vetted and represent 'best practices' for IT. No additional vetting of these recommendations was made to verify their legitimacy in actual practice. The next assumption made was that the hospitals engaged as part of this research are suitably representative of a common healthcare provider in the United States. These hospitals were used extensively as models of typical healthcare providers during both the design and implementation of the proposed solutions and thereby could potentially 'color' the results and suggested conclusions if this assumption was inappropriate. The next set of assumptions was related to the interactions with the healthcare providers' IT leadership and staff, as well as the respective practitioners. This

research's proposed solutions hinge on the assumption that all parties involved are cooperative, forthcoming, and honest. From the IT leadership and staff's perspective, it is critical that what is reported and disclosed in the questionnaires and other reviews be accurate and complete. Furthermore, what information and actual technology is made available for inspection and testing must be all encompassing of the organization and not a selective representation. This information should be held confidentially and non-disclosure agreements created to ensure the quality of the data is not compromised. From the practitioners' perspective, the surveys should be conducted anonymously and confidentially so there participants can answer honestly without reservation. In the application of this research presented in Chapter 4, these steps were taken to preserve the integrity of the findings. Another assumption was that both the individual(s) coordinating the implementation of the framework as well as those collecting data for the various assessments are in fact competent to serve in those roles and complete those tasks. The assumption of competency also impacts the quality of data collected and thereby has direct impact on the results produced. The last assumption is the related to how the proposed solutions' success or failure was measured. As it specifically relates to the proposed compliance framework, success was measured by an organization's ability to pass an external audit after applying the framework to their environment. It was assumed that if an organization could pass an external audit, this was a strong indicator that the framework was effective and successful.

Aside from the assumptions made to this research, there were limitations that presented factors beyond control and could potentially impact the validity of the proposed solutions and their results. The first limitation, which may in fact be the most important

to recognize, is that this research conducted a comparative review of other standards and methodologies but it was not exhaustive. The sheer volume of standards for all aspects of IT and corresponding recommendations and guides for how to implement these standards made an exhaustive review impractical, if not impossible. This research focused specifically on the National Institute for Standards and Technology (NIST) introductory guide for HIPAA – Special Publication 800-66 revision 1 – as a baseline for meeting HIPAA regulations. From this, an examination was done of how to satisfy the NIST guidelines using technical implementation recommendation put forth by NIST, other federal agencies, and private organizations. In addition to not being an exhaustive review of all standards and implementation guides, the proposed solutions were not vetted by an external entity. While this vetting process would be extremely beneficial to substantiate the validity of the proposed solutions, there were no reasonable opportunities to have this done due to the cost associated to such an exercise. Furthermore, as there are no freely available frameworks that dealt with these topics, as discussed in Chapter 2, it was not feasible to compare and contrast this research's proposed frameworks with other solutions to measure both effectiveness and completeness. It is due to this limitation that the assumption of measuring success by way of an external audit was derived. Similarly, the proposed solution was not tested exhaustively as time and practicality did not permit. As such, the effective sample size used to validate this research was 1 hospital per proposed framework. A description of each hospital engaged in the evaluation of these frameworks is provided in Chapter 4. It is important to state that the more organizations that apply the proposed solutions set forth by this research, the more the findings could

substantiate the success and relative effectiveness of this research. This point will be discussed further in Chapter 5.

The last area to discuss prior to presenting the proposed solutions is the delimitations imposed on this research to constrain its scope. It is important to recognize that this research limited its focus on HIPAA compliance to solely the Security and Privacy Rules set forth in Parts 160 and 164 of the federal regulations. Furthermore, only those regulations and requirements detailed in the key sources listed in Table 2 were considered in scope for this research. Similarly, when designing the proposed solutions, only HIPAA compliance was considered and other parts of the Federal Information Security Management Act (FISMA), of which HIPAA is part, as well as other potential compliance requirements such as PCI-DSS and COBIT were regarded as out of scope. The research also considered all applications and services not hosted internally to the target organization to be out of scope. These external systems, even though potentially used by the target healthcare provider, were excluded from this study except for the transmission medium used to access these systems to the extent of the boundary of the provider's network.

The assumptions, limitations, and delimitations mentioned directly impacted the scope and design approach of this research's proposed solutions. Understanding what these factors are and their impact on this research provides a context for the aims of this research and the methodology applied to achieve them.

3.2.2. Healthcare Information Security Compliance Framework

A federal grant from the Department of Health & Human Services (HHS), that begun in early 2011, connected Towson University and a large federally-funded regional

trauma center and national healthcare provider located in central Pennsylvania national healthcare provider (specific identity of the hospital has been suppressed due to non-disclosure agreement of grant). Part of the deliverables of this grant was to assess the Pennsylvania Hospital's HIPAA compliance and to respond to any shortcomings. As a result of this original need, the Healthcare Information Security Compliance Framework (HISCF) concept was first developed with the very specific goal of creating a HIPAA compliance assessment plan for a hospital. During the early discovery and research stage of the grant, it became very apparent that there was a clear lack of implementation level guidance on how to achieve HIPAA compliance and furthermore how to assess it. It became equally evident that the research and work associated with bringing this large national hospital into compliance could be leveraged to create and propose a standardized, reusable model that other organizations could potentially benefit from.

3.2.2.1. Framework Creation Process

With the goal of creating a standardized method for assessing an organization's HIPAA compliance and addressing any findings, it became apparent there were key steps to accomplish this task. The first step was to create a comprehensive set of all the HIPAA regulations, consisting of the Security and Privacy Rules, as well as any other requirements laid out by HHS related to HIPAA, including the revisions to HIPAA spelled out in the Health Information Technology for Economic and Clinical Health (HITECH) Act. Once all the requirements had been defined, the next step was analyzing their technical implications and what implementation decisions would have relevance to compliance. Following this general analysis, research was done on what guidance NIST, HHS, and other federal agencies had provided to date, and what guidance private

organizations like the Healthcare Information Management Systems Society (HIMSS) had produced both from a regulation and implementation perspective. At this point, all the regulations and requirements had been documented, their technical implications identified, and the existing guidance reviewed. It was during this step that the gap of actual implementation guidance was continually observed.

The next steps were to perform an examination of how HIPAA and other types of security and privacy assessments were being accomplished at other healthcare organization as well as and non-healthcare entities. This research formed the basis for the creation of the HISCF. The HISCF at its very core is an internal information security audit using the HIPAA regulations as the effective measurement of success or failure.

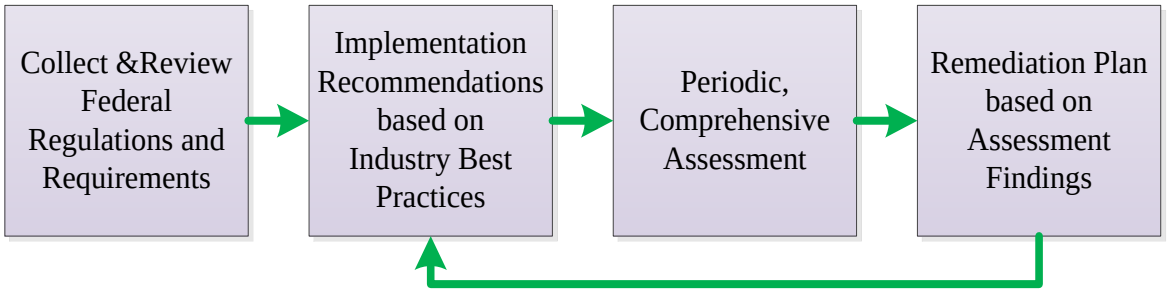

Figure 5. Conceptual Basis of Proposed HISCF

Starting with the conceptual basis shown in

Figure 5, each step of the process was expanded into phases of actual tasks. The result was the formation of the framework shown in Figure 6. The proposed compliance framework consists of three primary phases enabling complete HIPAA compliance at its conclusion. 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. While the phases and associated 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 assessment guides and instruments are organizationally relevant.

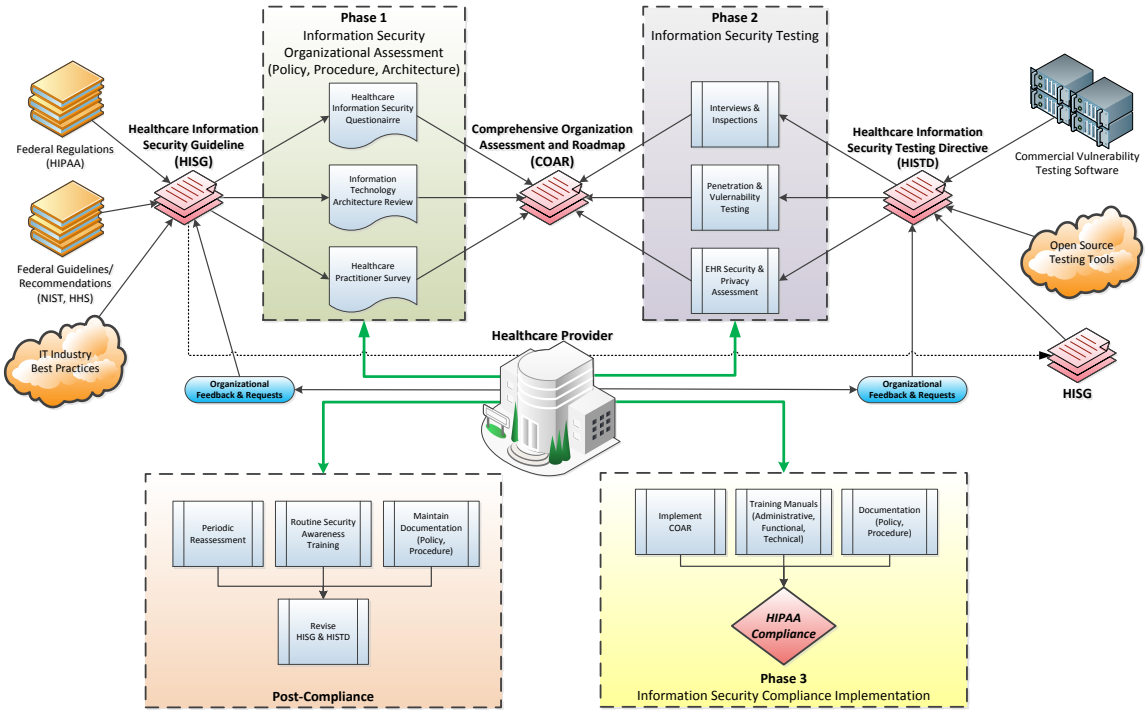

Figure 6. Proposed Healthcare Information Security Compliance Framework

NIST acknowledges 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 [91]. 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.

3.2.2.2. Healthcare Information Security Guide (HISG)

Many of the various activities laid out in the framework rely on the creation of the Healthcare Information Security Guide (HISG). The HISG is an invention of this research to serve as the cumulative, comprehensive reference manual for healthcare providers to use both for implementation assistance as well as later for assessment. In conjunction with the research performed while creating the HISCF, the basic content of the HISG was likewise compiled. The complete HISG can be found in Appendix 3. 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). The key documents used to gather these regulations and requirements are shown in Table 2.

Federal Government Agencies
National Archives and Records Administration
Federal Register, Vol. 78, No. 17, Part II – 45 CFR Parts 160 and 164
Department of Health and Human Services
42 CFR parts 412, 412, and 495: Medicare and Medicaid Programs; Electronic Health Record Incentive Program Stage 2; Health Information Technology: Standards, Implementation Specifications, and Certification Criteria for Electronic Health Record Technology, 2014 Edition; Revisions to the Permanent Certification Program for Health Information Technology; Final Rules
45 CFR parts 160 and 164: Modifications to the HIPAA Privacy, Security, Enforcement and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act: Other Modifications to the HIPAA Rules: Final Rule
Center for Medicare and Medicaid Services
"Regulations and Guidance," available at https://www.cms.gov/home/regsguidance.asp
"HIPAA Security Series – Security Standards: Technical Safeguards," available at http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/techsafeguards.pdf
"CMS System Security and e-Authentication Assurance Levels by Information Type," available at http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Downloads/System-Security-Levels-by-Information-Type.pdf
"CMS EHR Meaningful Use Overview," available at https://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Meaningful_Use.html
"Logical Access Controls and Segregation of Duties," available at http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/downloads/WP02-Logical_Access.pdf
Office of Management and Budget
"M-04-04: E-Authentication Guidance for Federal Agencies," available at http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy04/m04-04.pdf
National Institute of Standards and Technology

An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule (SP800-66 rev1)
"Risk Management Framework (RMF)" available at http://csrc.nist.gov/groups/SMA/fisma/framework.html

Table 2. Key Sources of Regulations and Requirements for Information Security

Once the regulations were documented, research was performed to determine actual implementation suggestions that meet those regulations. The specific implementation recommendations incorporate standards and best practice guides provided by NIST, the National Security Agency (NSA), the Department of Homeland Security, and a myriad of public guides and private industry whitepapers. The key material used to generate these recommendations and practices came from the documents listed in Table 3.

Federal Government Agencies
Department of Homeland Security - Federal Network Security Branch
"Continuous Asset Evaluation, Situational Awareness, and Risk Scoring Reference Architecture Report (CAESARS)," available at http://www.dhs.gov/xlibrary/assets/fns-caesars.pdf
National Institute of Standards and Technology
Guide for Conducting Risk Assessments (SP800-30 rev1)
Risk Management Guide for Information Technology Systems (SP800-37 rev1)
Managing Information Security Risk: Organization, Mission, and Information System View (SP800-39)
Creating a Patch and Vulnerability Management Program (SP800-40 ver2)
Guidelines on Firewalls and Firewall Policy (SP800-41 rev1)
Guidelines on Securing Public Web Servers (SP800-44 ver2)
Guide to Securing Legacy IEEE 802.11 Wireless Networks (SP800-48 rev1)
Guide for Assessing the Security Controls in Federal Information Systems and Organizations (SP800-53A rev1)
Recommendation for Key Management, Part 1: General (Draft SP800-57 part1 rev3)
Electronic Authentication Guide (SP800-63 rev1)
Guide to Intrusion Detection and Prevention Systems (IDPS) (SP800-94)
Technical Guide to Information Security Testing and Assessment (SP800-115)
Guidelines for Securing Wireless Local Area Networks (WLANs) (SP800-153)
National Security Agency – Central Security Service
"Security Configuration Guides" available at http://www.nsa.gov/ia/mitigation_guidance/security_configuration_guides/index.shtml
Office of Government-wide Policy
"Federal Identity, Credential, and Access Management," available at http://www.idmanagement.gov/pages.cfm/page/ICAM
Private Organizations
Healthcare Information Management Systems Society (HIMSS)

"Guidelines for Establishing Information Security Policies at Organizations with Computer-based Patient Record Systems," available at http://www.himss.org/content/files/CPRIToolkit/version6/v7/D38_CPRI_Guidelines-Information_Security_Policies.pdf
"HIMSS Application Security Questionnaire (HIMSS ASQ)," available at http://www.himss.org/content/files/ApplicationSecurityv2.3.pdf
Medical Universities
Johns Hopkins University
"Information Technology Policies," available at http://www.it.johnshopkins.edu/policies/itpolicies.html
University of California
"Guidelines for HIPAA Security Rule Compliance University of California," available at http://www.universityofcalifornia.edu/hipaa/docs/security_guidelines.pdf
State Governments
State of California. Office of Information Security
"California Information Security Risk Assessment Checklist (CA ISRAC)," available at http://www.cio.ca.gov/OIS/Government/documents/docs/RA_Checklist.doc
State of Maryland. Department of Information Technology
"Information Security Policy," available at http://doit.maryland.gov/support/Documents/security_guidelines/DoITSecurityPolicyv3.pdf
State of North Carolina. Statewide HIPAA Assessment Team
"North Carolina HIPAA Impact Determination Assessment (NC HIDA)," available at http://hipaa.dhhs.state.nc.us/hipaa2002/amicovered/doc/ImpactDeterminationQuestionnaire-Step2-2.doc

Table 3. Key Sources of Implementation Recommendations and Practices

Once the information, guidelines, and requirements from all these sources was compiled, they were distilled into a concise, comprehensive guide that covers four key policy areas - disaster recovery and business continuity; risk mitigation; operations management; and logical access - and four major technical 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 as a remediation plan for any shortcomings.

3.2.2.3. Phase 1 – Information Security Organizational Assessment

The goal of Phase 1 is to carry out a high-level assessment involving a thorough review of all policies, procedures, practices, and architectural designs. This stage is

broken into three parts - the Healthcare Information Security Questionnaire, the Information Technology Architecture Review, and the Healthcare Practitioner Survey. These three instruments are designed to measure information security compliance from both technical and functional perspectives. The grant's project director provided quality checks on the instruments to ensure their appropriateness and completeness for the areas the instruments were designed to assess - no external quality evaluation was performed.

3.2.2.3.1. Healthcare Information Security Questionnaire (HISQ)

Computing environments by their nature have intrinsic risks that require some form of mitigating action to minimize the potential for harm. These vulnerabilities are essentially any attribute or characteristic of the environment that can be exploited to violate established security policies or cause a deleterious effect. Organizations therefore should have vulnerability assessment plans that are executed routinely to detect, identify, measure, and understand the risks present in their information technology environments [92]. The Healthcare Information Security Questionnaire (HISQ) is designed to comprehensively assess the organization's information security policies, procedures, and practices. The HISQ represents the bulk of the Phase 1 assessment as it evaluates the organization's compliance with the baseline requirements of the HISG. The complete HISQ can be found in Appendix 4. The questionnaire itself was designed by creating sets of dichotomous and semantic differential questions to determine how the organization's policies, procedures, and practices compared to those laid out in the HISG. The assessment is divided into the same 4 key policy subjects as well as 4 overarching technical areas described in the HISG.

There are 4 key policy areas that the HISQ examines in specific detail: Disaster Recovery and Business Continuity; Risk Management; Operations Management; and Logical Access. These aspects of information technology cut across an organization's strategic and operational practices. Both HIPAA and Meaningful Use clearly lay out numerous requirements in these critical areas. The policy sections of the HISQ are presented in the form of a questionnaire that in most cases asks straightforward, single choice answers. This area is typically completed by the healthcare provider's IT leadership or their representative as it covers the overall organization's IT policies and established procedures.

The technical assessment is likewise divided into the areas of Network, Application, Database, and Infrastructure. In contrast to the policy review, the technical sections are best completed by IT engineers or someone intimately familiar with the technical configuration of the organization IT environment. The technical sections allow for much more free form answers to accommodate and capture environment-specific details. Many of the questions posed in the technical section are directed at specific implementation choices and details compared to the more general inquiries of the policy and procedure sections. The results assist in providing a comprehensive evaluation of the entire technical architecture, policies, and practices of the healthcare provider. The vulnerability assessment matrix shown in Table 4 depicts how the technical portion of the HISQ covers each aspect of the HIPAA Security Rule guidelines.

HIPAA Security Rule Section	Network	Applications	Database	Infrastructure
164.308(a)(1) – Security Management	X	X	X	X
164.308(a)(2) – Security Responsibilities	X	X	X	X
164.308(a)(3) - Workforce Security	X	X		X

HIPAA Security Rule Section	Network	Applications	Database	Infrastructure
164.308(a)(4) – Access Management	X	X	X	
164.308(a)(5) – Security Awareness and Training	X	X	X	X
164.308(a)(6) – Incident Response	X	X	X	X
164.308(a)(7) – Contingency Plan	X	X	X	X
164.308(a)(8) – Organizational Evaluation	X	X	X	X
164.308(b)(1) - Business Associate Contracts or Other Arrangements	X	X	X	X
164.310(a)(1) – Facility Access Controls	X			X
164.310(b) – Workstation Use				X
164.310(c) – Workstation Security				X
164.310(d)(1) – Device and Media Controls				X
164.312(a)(1) – Access Controls	X	X	X	X
164.312(b) – Audit Controls	X	X	X	X
164.312(c)(1) – Data Integrity		X	X	
164.312(d) – Person or Entity Authentication	X	X	X	X
164.312(e)(1) – Transmission Security	X			

Table 4. Proposed Vulnerability Assessment Matrix per Technical Area

The HISQ is designed as a questionnaire, not a survey, and it is expected to be filled out in its entirety just once, but collaboratively, using the appropriate technical and leadership resources from across the organization. It is also recommended that the questionnaire be completed through a series of iterative drafts whereby there are active discussions about both the questions and answers. This will ensure there is good understanding of both the question be asked and the response given.

3.2.2.3.2. Information Technology Architecture Review (ITAR)

In addition to the completing the HISQ, the organization submits to a full examination of their IT architecture. This review involves obtaining network diagrams,

data center diagrams, network device configurations, and other documents that depict how the network and infrastructure architecture is implemented. The topology of the environment is scrutinized specifically for appropriate isolation and segregation of ePHI data on the organization's network. The complete ITAR specification can be found in Appendix 5.

The HIPAA regulations specifically address transmission security in §164.312(e)(1) by the following statute, "implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network" [5]. The regulation goes on to state that there are 2 key components of ensuring the security of ePHI during transit: integrity controls and encryption. The primary purpose of integrity controls is to ensure the ePHI data isn't modified in any way during transmission. Encryption serves to disguise the true content of data such that it is not easily readable or decrypted without proper authorization. These 2 security measures are the basic foundation of providing secure transmissions. If an unauthorized entity can't read the contents of a transmission or alter or delete any portion of it, the authenticity and confidentiality of the transmission is ensured. While the concepts are straightforward, successfully achieving them can be challenging.

There are a number of fundamental approaches that are effective across almost all environments. It is important to acknowledge that before making architectural decisions related to the technical aspects of transmission security, it is imperative that operational needs, functional and financial, be considered. It is easy for the technical staff typically tasked with the implementation of the HIPAA technical safeguards to lose sight of how

the technology will actually be used in practice. If the chosen measures provide the appropriate levels of security but are impractical to utilize, the overall solution is ineffective. Further, in such cases the likelihood of both intentional and accidental misuse or circumvention of the organization's security will increase dramatically.

The ITAR performs a thorough analysis of the IT architecture and provides an evaluation using the following considerations:

- ***Usability:*** Are the systems functional as needed for normal business operations? Can users reasonably reach the data they need from the locations they need operationally?
- ***Security:*** Are systems that hold ePHI data appropriately isolated and segregated on the network? Are all points of egress and ingress appropriate?
- ***Dependability:*** Are there single points of failure within the architecture that will adversely affect business continuity in a disaster recovery situation? Does the network topology minimize the possibility of throughput bottlenecks that could impact system performance?

3.2.2.3.3. Healthcare Practitioner Survey (HPS)

The last assessment in Phase 1 is the Healthcare Practitioner Survey. This assessment evaluates the organization's human-technology interaction by the healthcare practitioners. The survey covers 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. It is not uncommon for an organization's published and intended IT security practices to not directly correspond to how their users are actually functioning [27]. This assessment's purpose is to provide a check and balance for

established policy and procedures that were examined in the HISQ. The survey is designed to be short but engaging, consisting of 25 'yes-no' questions related to the practitioners' awareness of the healthcare provider's IT policies and practices. The survey should be presented electronically and completed anonymously to encourage honesty and frankness. Once the survey has been completed, the results are compiled and evaluated. The complete HPS, including the results that are presented in Chapter 4, can be found in Appendix 6.

3.2.2.3.4. Phase 1 Conclusion

The findings of each of the assessments are combined to produce a cumulative Phase 1 summary, presented as the Comprehensive Organization Assessment and Roadmap (COAR). After creating the COAR, Phase 2 performs a practical evaluation of the areas covered in the first phase and amends and expands the COAR as necessary.

3.2.2.4. Comprehensive Organization Assessment and Roadmap (COAR)

The COAR is effectively the framework's master report of the results of both Phase 1 and Phase 2. At the conclusion of Phase 1, an initial draft of the COAR is produced that contains the results of the all the Phase 1 assessments, along with any recommended mitigating actions. A thorough organization review of the COAR is very useful at this stage, prior to beginning Phase 2. Each question of each questionnaire and survey for all Phase 1 assessments contains a cross-reference to both the HIPAA statute and the corresponding section of the HISG. As such, the recommendations from the Phase 1 assessments can be easily combined with the guidelines laid out in the HISG, to produce a clear set of actionable tasks. Phase 2 shifts the assessment style from abstract to practical. Following the completion of Phase 2, the COAR will be revised to include

the results from those assessments as well. Once the results of Phase 2 are included, the COAR will serve as a detailed implementation guide for the organization to follow in order to achieve HIPAA compliance.

3.2.2.5. Healthcare Information Security Testing Directive (HISTD)

When considering an evaluation of information security, an organization must first establish what the actual objectives are for the environment being examined. After the security objectives have been established, the actual test plan or methodology can be drafted. It is important to recognize that an effective testing plan must be easily repeatable. It is in the repetition of the security tests and surveys that many issues can be identified using comparative analysis of prior test results. Many times issues or vulnerabilities are not immediately obvious during the course of normal examination but when compared to prior test results, anomalous conditions can be much more readily recognized.

The proposed security testing plan, the HISTD, which can be found in its entirety in Appendix 7, divides the testing techniques into five key areas: target identification and analysis; target vulnerability validation; password cracking; business process testing, and application assessments. The identification and analysis testing is centered on network discovery, port and service identification, and vulnerability scanning. The vulnerability validation category consists of a variety of penetration tests on the different components of the organization information technology environment. The password cracking area is focused very specifically on testing the strength of passwords within the organization. The business process testing portion, much like the Healthcare Practitioner Survey, provides an examination of how technology is actually being used in normal business

operations to ensure security controls are not being circumvented in actual practices. The final testing technique of application assessments is intended to provide in-depth application security testing beyond typical penetration testing.

Unfortunately no single security test can be used to validate all systems and services from all perspectives. As such, it is necessary to use an assortment of tools to achieve a truly complete assessment. This research has focused on creating a collection of testing tools that can provide a comprehensive set of tests with the minimal amount of overlap. The collection of tools configured and preloaded on the two Tester Virtual Machines (VMs) are shown in Table 5. Additionally, the tests have been preconfigured and automated as much as possible to minimize the amount of effort necessary to conduct the testing.

Since security testing is a very fluid and changing process, it is recommended that all organizations establish an information security testing environment to become acquainted with the testing tools and run simulated tests to perfect the organization's testing plan. Figure 7 depicts a basic testing environment that was created by this research and can be utilized by any healthcare organization. Having a dedicated testing sandbox environment can be helpful to show how each type of test is performed and understand their impact to the systems being tested. It is important to perform all types of security testing from both an internal and external perspective. In order to truly validate adequate security exists within the environment the conditions of the tests must match or be relevantly comparable to the scenario being tested.

VM 1	
Operating System - Ubuntu 11.10 [93]	
Testing Tools	
Nessus 5.0 [94]	*Vulnerability Scanning*
VM 2	
Operating System - BackTrack 5 R3 [95]	
Testing Tools	
NMap [96]	*Network Enumeration and Port Scanning*
THC-AMap [97]	*Protocol Detection*
Enum4Linux [98]	*Windows Enumeration*
Swaks [99]	*SMTP Testing*
SSLScan [100]	*Encryption Testing*
Bluediving [101]	*Bluetooth Penetration Testing*
AirCrack [102]	*Wireless Penetration Testing*
SMAP [103]	*SIP Scanning for VoIP*
OneSixtyONe [104]	*SNMP Scanning*
SQLMAP [105]	*SQL Injection and Database Takeover Testing*
Armitage [106]	*Exploitation testing*
THC-Hydra [107]	*Password Cracking*
W3af [108]	*Exploit testing*
Uniscan [109]	*Website Vulnerability Scanning*
Nikto [110]	*Web Application Testing (White box, Black box)*
Burpsuite [111]	*Web Application Testing (White box, Black box)*

Table 5: Proposed Security Testing VM Configurations

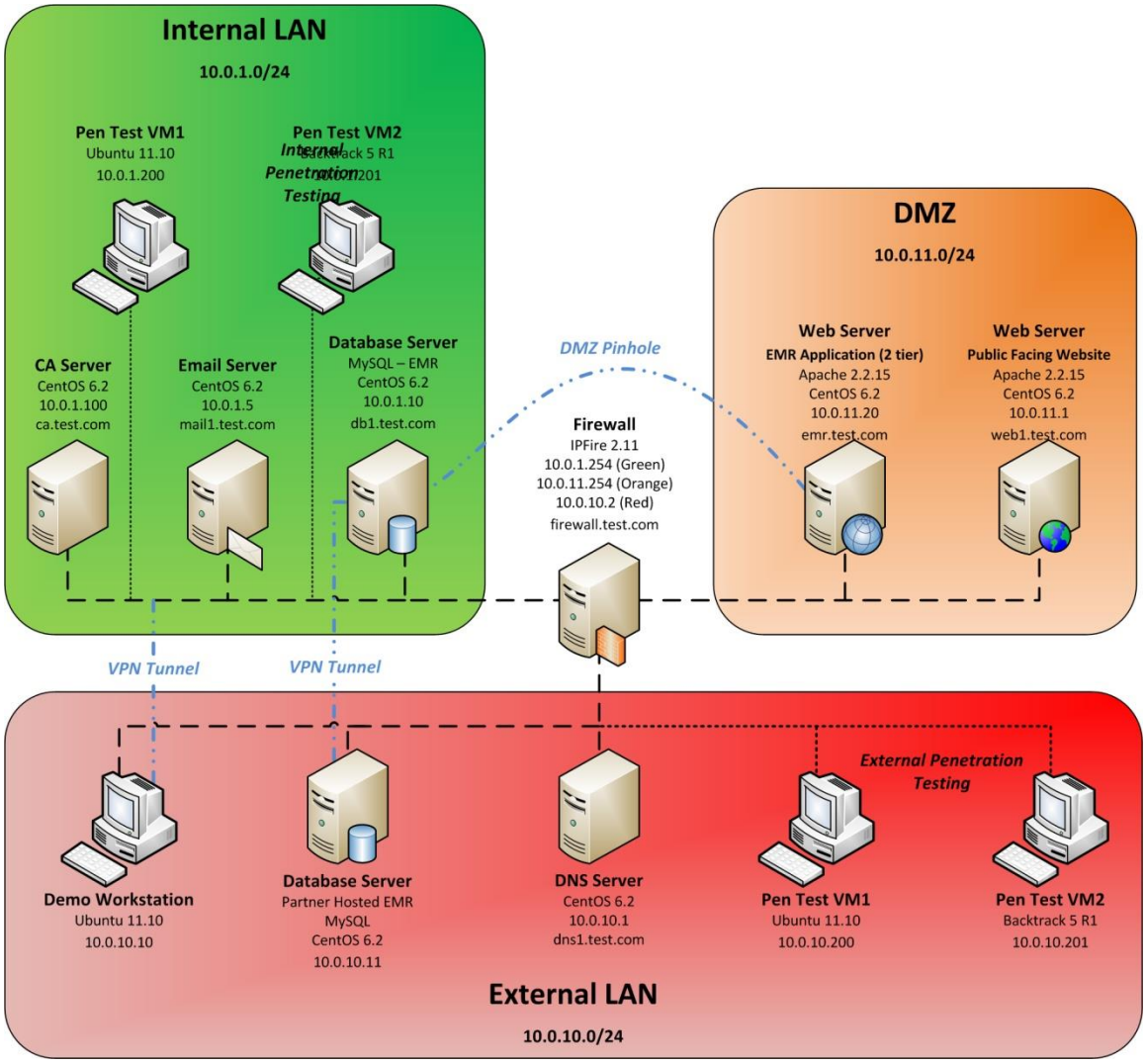

Figure 7. Proposed Security Testing Environment

3.2.2.5.1. Target Identification and Analysis

For the target identification and analysis tests, the systems on the network segment being tested will be cataloged including each system's operating system (OS) information and patching status as well as any open ports or active services. Network discovery can be performed using either an active scanning tool or passively using a network sniffer. While the passive approach tends to make the lesser impact to the performance of the network or scanned machine, it takes considerably longer and the results are bound by what events are actually taking place. Active scanning usually

yields but more comprehensive results and allows the scans to be targeted to look for specific characteristics, regardless of a system's current activity. It is important to recognize that discovery scanning can be an intensive process and potentially have significant impact on the systems it is scanning and in cases of older systems, cause system failures. Network discovery can be helpful to detect unauthorized systems present on an organization's network. It is important to note that scanning should not be limited just to the wired network. A number of wireless scanners exist that can very effectively collect relevant data about wireless devices and the local wireless network that wouldn't normally apply to a traditional wired network. The wireless scanning should not only include all 802.11 channels but also Bluetooth and a general radio frequency (RF) spectrum analyzer [91].

Once the connected systems have been identified for a particular network segment, these hosts are further examined using a port scanner to see which ports are open and what services are running on those ports. The port scanning process can also perform OS fingerprinting. The last test of this group is to perform vulnerability scanning. The types of checks vulnerability scanners can perform depends on the tool but they typically can identify out of date software, missing patches, and various errors with configurations. Unfortunately, vulnerability scanning has a number of limitations that are important to recognize. First, vulnerability scanning is much like virus scanning as it relies on a repository of signatures and therefore can only detect documented issues. This requires frequent updating of the repository to be able to discover the latest vulnerabilities. Secondly, these scans usually have a high false positive error rate and thus require an experienced information security individual to effectively interpret the

results. These weaknesses ultimately limits the scanning process as there are considerable portions of these tests that are labor intensive and cannot be automated [112]. The network-based scans generate significantly more network traffic that network discovery and port/service scanning and can prove harmful to the hosts being scanned. When the vulnerability scanning is complete, the tests in first stage of the security testing plan will have produced a comprehensive report of the organization's connected systems and including information about their OS, active services, and any vulnerability they have.

3.2.2.5.2. Penetration Testing

With the information generated in the first round of the testing, the next stage will continue to search for vulnerabilities and demonstrate the exposures created when they are exploited. Penetration testing will simulate real-world attacks and provide information about how the system, application, or network will respond to malicious attacks. Penetration testing also can help provide information about effective countermeasures to attacks, how to detect an attack, and the appropriate response. Penetration testing is very labor intensive, much like vulnerability scanning, and as such typically requires a professional with considerable skill to conduct the testing successfully without damaging the targeted system [113]. The majority of the tests performed as part of this security testing framework fall into the penetration testing category.

3.2.2.5.3. Password Cracking

After the penetration testing stage is complete, a series of password cracking tests are performed. There are a couple general approaches for password attacks: dictionary

attacks, brute force, and rainbow table attacks. Typically password cracking involves obtaining the hash of the actual password, either from the target system directly or using a network sniffer. Once the hash is obtained, the attacks take different approaches in an attempt to generate a matching hash to discover the actual password. While an attack could be directed at a system service or application, these attacks are typically not as efficient and take considerably longer to conduct. Using this approach, you are limited to response times of the target system or application per attempt, as well as the round trip network time, to determine if the attack was successful. While the time associated with a single attack is extremely small, when millions of credentials are being attempted, the compounded time usually makes this approach unattractive. By having a copy of the hash you are trying to recreate, the attack is only limited to the processing capabilities of the system performing the attack. Different from penetration testing, password cracking can be effectively performed offline to remove the possibility of any impact on the target system, network, or application. The objective of password cracking is to determine how predisposed an organization's password policies are to being compromised. In cases where passwords are determined to be vulnerable, their respective strength can be augmented to achieve appropriate entropy.

3.2.2.5.4. Business Process Testing

While examining each component of an IT environment is a critical exercise, it is also important to examine entire processes to verify each component is being used appropriately during normal business practices. It is possible that not all security capabilities of each component are actually employed in practice or exceptions have been 'built-in' to processes that circumvent the safeguards the components could normally

exert. Clearly, EHR security is a crucial element of any healthcare organization's overall security framework. To this end, the ways in which EHR systems are used in normal practice serve as excellent candidates for process testing scenarios. From a process perspective, EHR security can be examined in three key areas: access, transmission, and storage.

- **Access** – this category deals specifically with the functional areas related to authentication, authorization, and delegation. More specifically this area handles who can have access to data, which data they can access, what type of actions they can take on that data, and who they can provide some degree of access to the data as well.
- **Transmission** – this category covers how data is moved in an electronic medium. This area covers where data can be access from, where that data can be sent to, how the data is formatted while being moved, how data is presented to the user, and what mechanisms can be used to send the data.
- **Storage** – this category accounts for how data is captured and preserved. This area deals with how data can be added, modified, or deleted, how the data is validated upon entry, the format of how data is stored electronically, how the data is preserved, and how data integrity is ensured.

There are 4 examples of business process testing presented in the HISTD that can be found in Appendix 7. These examples depict the information flow analysis used and how each step in the flow is tested. These examples include authentication to an EHR system from a wired connection, authentication to an EHR system from a wireless connection, accessing ePHI in an EHR system, and lastly writing ePHI in an EHR system.

3.2.2.5.5. Application Review and Testing

This part of the HISTD involves an extensive review, categorization, and analysis of all enterprise applications. Each application is examined to determine if it interacts with ePHI and if so, in what way and for what function or purpose. This final type of testing is directed specifically at an organization's applications that capture, access, or transmit ePHI. This type of testing involves both *white box* and *black box* approaches. White box testing takes the perspective of an internal user such that the tests assume a working knowledge of how the application works. Conversely, Black box testing assumes the attacker has no familiarity with application or how it is designed and implemented. These types of tests and attacks include injection attacks, file descriptor attacks, data corruption attempts, and intentional misuse of the application beyond the organization's published policies and procedures. Application testing, along with all the other parts of the vulnerability validation-testing phase are used to evaluate systems during actual use. Therefore, the closer the tests are to normal conditions, the more useful the results of the tests will be in discovering potential risks.

3.2.2.6. Phase 2 - Information Security Testing

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.

3.2.2.6.1. Interviews and Inspections

The interviews and inspections stage of Phase 2 is aimed at providing an opportunity to inspect various components of the IT environment including physical security controls for the data center and other locations where ePHI data is stored. While this was evaluated in Phase 1, these inspections should serve as the effective penetration tests of the physical computing environment. The onsite visits should involve interviews with all appropriate personnel of the organization, both within the IT department, and administration, and leadership.

3.2.2.6.2. Penetration and Vulnerability Testing

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 the future as part of the organization's continued compliance efforts. This stage will simulate real-world attacks and provide information about how the system, application, or network will respond to malicious attacks. The penetration and vulnerability testing also can help provide information about effective countermeasures to attacks, how to detect an attack, and the appropriate response. Business process testing is an important aspect of this stage. This aspect examines entire processes to verify each technological component is being used appropriately during normal business practices. Many information security breaches are actually caused by a failure to use a system as designed or the procedure doesn't match the policy [114].

3.2.2.6.3. EHR Security and Privacy Assessment

The last task of Phase 2 is to perform an in-depth review of the organization's EHR systems specifically. This assessment examines both the security and privacy policies and practices. The complete EHR Security and Privacy Assessment can be found in Appendix 8. The evaluation instrument is a survey that is completed by the leadership responsible for the technical support of the EHR system. The survey is broken into 3 main sections - organization policies and practices, functional implementation, and technical implementation. The first part, organizational policies and practices, covers topics such as how staff is trained on HIPAA privacy requirements, security awareness training, the presence and application of acceptable use policies, how ePHI releases are handled, and how data alteration/deletion is guarded against. The functional implementation section covers how the EHR system is used in normal operations. Questions for this section cover how the business practices for how ePHI is captured, accessed, and transmitted. The last area of the survey, technical implementation, examines how the EHR system was deployed technically including the system architecture, how patch management is addressed, presence of intrusion detection and prevention, and finally network location and safeguards. The information captured within this survey provides a complete portrayal of whether the organization has enacted adequate security and privacy controls for their EHR systems.

3.2.2.6.4. Phase 2 Conclusion

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.

3.2.2.7. Phase 3 – Implementation

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.

3.2.2.8. Post-Compliance

With the completion of the third phase, the entire framework will likewise be completed. The designed result of the framework will first and foremost be the achievement of HIPAA compliance for the organization. In the efforts to attain compliance, there will also be the potential for a number of other tangible

accomplishments. This framework will create a standardized Healthcare Information Security Guide 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 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 framework 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 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.

3.2.3. Healthcare Federated Identity Framework

While healthcare providers must address information security compliance in their computing environment, they are simultaneously being faced with having to provide their patients electronic access to their health information. The Meaningful Use guidelines dictate that healthcare providers accomplish this feat within 36 hours of providing care to all their patients. As part of the same federal grant that created the Healthcare Information Security Compliance Framework, the central Pennsylvania (PA) hospital was also keenly interested in achieving Meaningful Use Stage 1. Similarly, another large

national hospital in Maryland with a national trauma and cardiac care center (specific identity of the hospital has been suppressed due to non-disclosure agreement), was similarly interested in solving this patient access dilemma for Meaningful Use attestation.

3.2.3.1. Framework Creation Process

In response to these needs, a thorough analysis of industry standards related to federated authentication and portable identities was performed. Immediately a wide variety of similar work being performed in other industries became evident. Unfortunately, as discussed in Chapter 2, none of the current solutions seemed scalable when cost or availability was considered. This became especially apparent when multiple healthcare providers tried to interoperate so as to provide a homogenous experience for their common patients. Ultimately, this research took a number of mature, proven technologies, standards, and architectural solutions and derived an alternative trust framework for exchanging identity information between the multiple healthcare providers and the Cloud. This research proposes a comprehensive structure that healthcare providers can use to integrate their EHRs with the Cloud for identity validation, while meeting compliance guidelines for security and privacy.

In order to build a viable framework, a series of key steps had to be taken. First, an analysis of how authentication fits into the larger scheme of application access needed to be performed. This examination provided the basis for how to create a portable access model such that a digital credential of one system could be used to access another disparate system, such as an EHR. The next step was to determine how an assignment of trust could be assigned to that digital credential so that another system, such an EHR, has a level of confidence in who is accessing the system. To ensure compatibility with the

federal government standards and regulations, including the Health Insurance Portability and Accountability Act (HIPAA), the definitions and requirements for establishing trust described in the National Institute of Standards and Technology (NIST) e-Authentication specifications [115] were used. With trust requirements defined, the next step was to design implementation profiles for creating and managing credentials so as to introduce varying degrees of trust and assurance for the different identities the providers manage or interact with. Using these profiles, Healthcare providers can then establish trust relationships with external authentication systems or Identity Providers. These trust arrangements work within the Health Insurance Portability and Accountability Act (HIPAA) compliance guidelines to meet the Meaningful Use objectives while preparing providers to become engaged in cross-industry initiatives such as the National Strategy for Trusted Identities in Cyberspace (NSTIC). With the steps up to this point serving as the foundation, the framework then needed to determine the appropriate technologies to connect external credentials and identities with autonomous systems. In order to specifically leverage and connect the Cloud as the external authentication system, this framework examined the possible technologies that could be implemented easily and on the largest scale. Furthermore, this research had to develop a method by which the Cloud identities could be mapped to actual patients in a healthcare provider's EHR system. The last part of the framework was to examine the healthcare providers' role in support of a Cloud-connected system. This research suggests that by improving the usability and thereby accessibility of an EHR system, there are residual benefits to the healthcare provider related to support requirements. Each of the steps in building this framework are covered at length in the subsequent sections.

3.2.3.2. Creating a Portable Access Model

There are 3 fundamental issues that need to be addressed when establishing digital identities and configuring applications to leverage those identities:

- Who does the digital identity belong to?
- How does the individual prove their identity?
- What should the user be allowed to access or do in the relevant application?

These issues are more technically referred to as identity management (IdM), authentication, and authorization. IdM is the underlying processes and systems that establishes and keeps track of who an individual is and allows other systems to relate a digital identity to an actual person. It is critical to recognize that an individual possess any number of identifiers that make up their digital identity. The IdM system correlates and tracks those identifiers across all systems. Authentication and authorization are many times incorrectly used interchangeably or combined as a single issue called 'access' but they are 2 very distinct steps. Authentication is how an individual proves who they are. On the other hand, authorization addresses what privileges that individual should have, such as being able to view or modify data in an application. The distinction is critical when considering a portable access model.

Authorization decisions must inherently be made at the application level but authentication can almost always be externalized from the resource being accessed. Examining the authentication event closer, there are 3 sub-components: the user, known as the Subject, with possession of a credential; an authentication system that can validate said credentials, known as the Identity Provider (IdP); and the application that recognizes the identity, known as the Service Provider (SP). As Figure 3 shows, traditional systems

have the credential repository or IdP built into the application itself. This model creates a dependency that in order to access that application the corresponding internal credential must be used. A key objective of this research is to break this dependency. More simply, this research proposes that EHR applications need to be able to use other identity stores to validate credentials, beyond those stored in the local EHR database. Fortunately, this basic functionality is supported by all the major commercial offerings in some fashion and the real effort lies in getting EHR systems to work effectively and appropriately with external systems. Therefore as healthcare providers address electronic access to their EHR systems, the challenge of authentication can be essentially outsourced to other vendors and organizations that have already made significant investments in this arena.

Leveraging the ability to separate the authentication process from the EHR application, this research proposes a framework by which authentication of a single EHR system can not only be configured to a single external authentication system but in fact to use any number of authentication systems. In this model, the authentication event can be performed by any trusted Identity Provider. The basic function of an IdP is to be an authoritative source for establishing and maintaining both identities and credentials. An IdP could be a commercial vendor such as Verizon, Comcast, or AT&T that has a business relationship with individuals. Similarly, an IdP could be a company such as Google, Yahoo!, Microsoft, or MySpace, that offers free services but also tracks relevant identity information. It is important to point out that while all of these IdPs can authenticate an individual, it is critical that the identity management system at the local healthcare provider have the ability to map the external IdP's identifier to a user in the local system. For example, many of the free IdPs use an email address as the core

identifier for users in their systems. An EHR system is likely to use something entirely different such as a Social Security number, Patient Number, or similar style identifier. Therefore the healthcare provider's IdM system needs to know how to map that external identifier to the internal identifier. It is also important to acknowledge that not all Identity Providers have the same security requirements for establishing identities and credentials. Consequently, not all Identity Providers can be extended the same amount of implicit trust that the user has proved their identity. In fact, it is this concept of varying trust or levels of assurance (LOA) that is central to regulating external credentials appropriately for EHR access.

3.2.3.3. Defining Trust in an Identity

When examining trust in an identity, there are 2 fundamental aspects that define assurance: 1) the degree of confidence in the vetting process for establishing the identity and matching credential, and 2) the degree of confidence that the user of the credential is the owner of the credential. The higher the level of confidence in both of these areas, the higher the level of assurance a system can have when using the associated credential. Depending on the needs or requirements of the system to be accessed, the appropriate LOA can be required of the credentials being used. The proposed framework involves creating identity assurance profiles with varying LOA that map directly to the National Institute of Standards and Technology's (NIST) e-Authentication specifications.

In 2003, the Federal Government's Office of Management and Budget (OMB) released memorandum M-04-04, *E-Authentication Guidance for Federal Agencies*. This document laid out four distinct levels of assurance related to electronic identities used for electronic transactions [116]. These levels are:

- Level 1: Little or no confidence in the asserted identity's validity.
- Level 2: Some confidence in the asserted identity's validity.
- Level 3: High confidence in the asserted identity's validity.
- Level 4: Very high confidence in the asserted identity's validity.

OMB mandated that NIST establish technical standards for the implementation of each level of assurance. NIST subsequently created the *Electronic Authentication Guideline* which now acts as the regulatory standard for all electronic authentication for resources of federal agencies [115]. In 2008 the Federal Identity, Credential, and Access Management (FICAM) subcommittee of the General Services Administration Office of Government-wide Policy was established to improve electronic access to government resources [117]. These improvements included internal access, access with other government partners and agencies, external business partners, and with the American population at large. Consequently, one of the specific tasks FICAM performs is the evaluation of identity authentication models for possible adoption or integration by the Federal Government. Hence the guidelines laid out by both FICAM and NIST serve as the obvious benchmark that other industries could use to establish their own e-authentication requirements and provide the foundation for new trust frameworks.

The Centers for Medicare & Medicaid Service has issued specific requirements dealing with e-authentication and levels of assurance when accessing ePHI covered by the HIPAA [118]. The Centers for Medicare & Medicaid Services (CMS) has determined the equivalent of NIST LOA Level 2 identity assurance is needed for accessing your own PHI and Level 3 for accessing PHI about someone else. This means potential IdPs for EHR systems would need to ensure an identity assurance equivalent to

Level 2 or 3 depending on the type of access. This research lays out identity assurance profiles for Levels 1-3 that satisfy the NIST guidelines so Identity Providers can guarantee which LOA each of their credentials can reliably assert. An implicit trust can then be achieved with all recognized IdPs that assert a particular LOA credential since all IdPs would be using the same standardized identity assurance profiles. These arrangements would culminate in a many-to-many relationship between EHR systems and Identity Providers. Furthermore, if Cloud Identity Providers participated in this scheme, patients could leverage their existing Cloud credentials to access their medical information as shown in Figure 8. This results in patients being able to use the same, familiar Cloud credential to access EHR systems at different healthcare providers. As mentioned, the authentication event is just one of 3 aspects of access that need to be addressed but it represents a key user interaction point in the process. By taking advantage of existing Cloud credentials, healthcare providers can not only provide their patients with a familiar user experience but also effectively offload the username/password creation and maintenance effort. Password resets have traditionally been one of the largest technical support issues for organizations. This framework outsources this support issue to the Cloud.

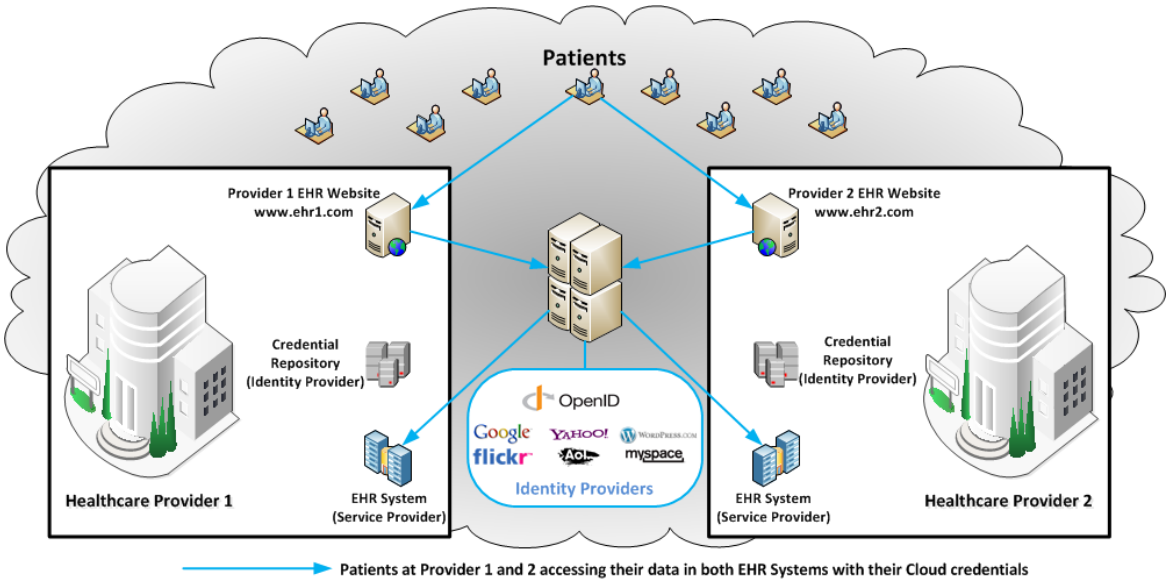

Figure 8. Proposed Federated EHR Access Model using the Cloud

Usability underpins this solution's entire premise. While patient authentication is essentially just the first step in providing access, it can be a crippling area if not approached properly. This research lays out a solution for healthcare providers to get out of the 'username/password business'. The existing Identity Providers in the Cloud are investing billions of dollars cumulatively every year towards usability. Much of their usability efforts are centered on making their services easy to use and prevalently placed throughout the Internet. Basic authentication functionality such as looking up a username or resetting a password is fundamental to the Cloud and is constantly being refined and improved. Healthcare providers can simply leverage this incredible investment instead of trying to emulate and duplicate it. Further, these Cloud Identity Providers enable entities to leverage their services for absolutely no cost beyond the man-hours required to configure the integration.

While the concept of Identity Providers and Service Providers operating within a common identity assurance framework is extremely compelling, there clearly needs to be

some level of governance to ensure its practical viability. This governance body would be responsible for establishing a certification process by which potential member healthcare providers could verify they are able to interoperate with Identity Providers while ensuring the security and privacy of the sensitive data they possess. The certification process for IdPs would be tiered to accommodate different criteria depending on the LOA of the credentials the IdP holds. With common profiles to follow, effectively any organization could participate as an Identity Provider including public organizations, private companies, or even healthcare providers themselves.

3.2.3.4. Criteria for Identity Profiles

Many of the criteria apply to all the LOA profiles used by Identity Providers. The higher the LOA of the identity to be asserted, the more scrutiny that must be given to how the identity was established, how the credentials issued, how the user asserts their identity, and the general integrity of the business practices of the IdP. A summary of the identity assurance profiles can be found in Table 6 and while a summary explanation of each criteria follows, the full proposed profile criteria specification can be found in Appendix 9.

Category	Criteria	LOA 1	LOA 2	LOA 3
A. Organizational Requirements	1. Certification	♦	♦	♦
	2. Legal Status	♦	♦	♦
	3. Liability Provisions	♦	♦	♦
	4. Policies and Practices	♦	♦	♦
B. Infrastructure Guidelines	1. Software Security		♦	♦
	2. Physical Security		♦	♦
	3. Network Security		♦	♦
C. Identity Creation and Proofing	1. Identity Establishment		♦	♦
	2. Identity Proofing		♦	♦
	Existing Relationship		♦	♦
	In-Person Proofing		♦	♦
	Remote Proofing		♦	♦
	3. Record Retention		♦	♦

Category	Criteria	LOA 1	LOA 2	LOA 3
D. Identity Management Practices	1. LOA Classification per Identity	♦	♦	♦
	2. Consistent Data Definitions	♦	♦	♦
	3. Informed Consent	♦	♦	♦
E. Credential Management	1. Subject Interactions		♦	♦
	2. Revocation		♦	♦
	3. Reissuance		♦	♦
	4. Record Retention		♦	♦
F. Authentication Guidelines	1. Unique Identifier	♦	♦	♦
	2. Minimum Entropy of Authentication Secret	14 bits	20 bits	64 bits
	3. Protection of Authentication Secrets	♦	♦	♦
	4. Assertion Security	♦	♦	♦
	5. Multi-Factor Authentication			♦
G. Risk Mitigation	1. Acceptable Use Policies	♦	♦	♦
	2. Business Continuity		♦	♦
	3. Attack Resistant	♦	♦	♦
	4. Single Sign-on (SSO)	♦	♦	♦
	5. Credential Sharing Resistant	♦	♦	♦

Table 6. Summary of Criteria for Proposed Identity Provider LOA Profiles

The Organizational Requirements category covers the basic guidelines each IdP must meet or follow if they are to obtain certification for any level of assurance. It is necessary for the IdPs to demonstrate they are a legitimate entity and should indeed be recognized as an authoritative source of identity for other organizations. Further, IdPs must establish they can provide appropriate levels of liability for their actions. Lastly, IdPs must ensure they have documented policies and procedures and their practices are consistent with those documents.

The Infrastructure Guidelines category establishes guidelines for the Identity Provider's IT environment. All IdPs must ensure adequate software security by keeping all relevant software up to date and patched. This includes software used for: transactions of identities, credentials, and assertions; the authentication process; credential issuance and maintenance; and identity data storage. IdPs must be able to

similarly demonstrate appropriate physical and network security exists at their respective locations where identity data is stored.

The next category deals with how identities are created, vetted, and proofed. For IdPs asserting LOA 2 or 3 identities, processes must exist to verify the data they collect is based on public records or government-issued IDs. As this data will be the basis for which the digital identity will be established, it is critical that it is vetted before it is used for transactions outside of the Identity Provider. Once the identity has been registered, the IdP must perform identity proofing by ensuring that the collected information reflects an actual person, that the information can uniquely distinguish a single individual within the IdP's system, and that the person requesting the registration matches the identity being registered. The last part of this category covers the requirements for record retention of the registration process and how the identity was vetted and proofed.

The Identity Management section deals with how the Identity Provider defines, asserts, and releases identity information. The IdP must classify each digital identity it holds to a specific LOA and ensure there is no chance for identities to inadvertently have their LOA elevated. Each IdP will also need to conform to a standard set of data definitions for the identity data that will be shared with EHR systems to ensure interoperability. Before releasing data to an EHR system, the IdP must present the user with the specific data that will be released, allow the user to consent to the release, and then record the consent for non-repudiation. Informed consent has been an ever growing issue with transactions on the Internet and it is a critical component of any trust framework.

The Credential Management category deals with how credentials are used in transactions. IdPs are required to ensure users reassert their identity for each transaction in some fashion. Additionally, IdPs will ensure any credentials that are no longer valid for any reason will be revoked immediately. If a credential is ever reissued, the user must reestablish their identity by providing information from prior transactions such as by using pre-registered questions with responses not easily determined by anyone other than the user. The final aspect of this category is the requirement for IdPs to maintain a record of all credential management activities including issuance, revocation, expiration, and reissuance for a period not less than 180 days beyond the age of the credential. This level of documentation is needed for IdPs to sufficiently establish non-repudiation for the user's activities.

The Authentication Guidelines section stipulates how the authentication process must work on the IdP for the different levels of assurance. First and foremost, IdPs have to ensure all credentials they issue are unique and only correspond to a single individual. While a user could possibly have multiple credentials to validate themselves, no set of credentials can be held by more than one user. Depending on the LOA, the authentication secret - commonly a password - needs to meet a certain degree of entropy or resistance to guessing. Entropy is achieved by making the authentication secret have adequate complexity parameters, limit the age and reuse of the secret, and limit the number of invalid attempts before the credential is disabled. For LOA 1, the minimum entropy for the authentication secret is 14 bits or 1 in 16,384 (2^{14}) chance of being guessed. For LOA 2, the minimum entropy is 20 bits and LOA 3 is 64 bits. The higher the LOA, the higher the resistance to guessing is required. It is a requirement for all

LOA's that IdPs store the authentication secrets using industry-standard encryption algorithm to provide adequate protection while at rest. Similarly, IdPs must guarantee all communications between the user and the IdP are also encrypted. Lastly, IdPs that assert LOA 3 identities must utilize a form of multi-factor authentication while validating the user.

Risk mitigation is the final category of the profile. Each IdP must have acceptable use policies that their users are periodically informed of and the users' agreement to said policies is recorded. Additionally, IdPs must take steps to ensure business continuity by minimizing the chance of system failures. In the event there was a failure, IdPs must guarantee the failure wouldn't cause an inaccurate identity assertion being sent to an EHR system. IdPs must also be able to ensure that their authentication systems are resistant to various attacks including replay and eavesdropping. If IdPs use any type of single sign-on (SSO) technologies, they must utilize industry-standard techniques and encryption must be used to ensure their integrity. The final risk mitigation requirement is the IdP must demonstrate measures have been taken to resist credential sharing, either accidental or intentional.

3.2.3.5. Connecting the Cloud

The identity assurance profiles provide all parties a known set of rules by which to operate. However, beyond the profiles it is critical that organizations adopt an established internet standard to facilitate the sharing and exchanging of identity information. While there are more than a few options available, the prominent standards that have emerged are:

1) OpenID

2) Security Assertion Markup Language (SAML)
3) OAuth
4) WS-Trust

While any and all of these technologies can provide a similar solution, this research purports that OpenID is the most suitable identity standard available. As such, the OpenID identity standard has been incorporated into this framework to provide the foundation for identity creation and credential distribution. OpenID consists of the most common Identity Providers available on the Internet including Google, Yahoo!, Flickr, MySpace, and AOL. In addition to Google and Yahoo, its corporate members add companies such as Microsoft, PayPal, Symantec, and Verizon to create a foundation with significant market share in the digital identity space. Over a billion OpenID enabled accounts exist and are being used by more than 50,000 websites today [119]. By choosing a standard that is already in use by so many individuals and sites, the barriers for entry and user acceptance are significantly lower than other alternatives. The Federal Government has recognized OpenID as an important standard with which to interoperate. FICAM has approved an OpenID profile that is certified for LOA 1 authentication for Federal Government resources [78]. The creation of a profile for LOA 2 and LOA 3 for use with the government is well underway; further signifying the wide adoption of the standard by the public and private sectors.

3.2.3.6. Mapping Patients to Cloud Identities

While the OpenID standard facilitates the authentication event, organizations must also address how the OpenID identity is connected or mapped to the organization's record of that identity. The mapping process can have user involvement or not,

depending on the data held by the external IdP and the degree of trust extended to how the data was vetted as belonging to the user. A base solution offered by the framework is a user-driven registration process as shown in Figure 9 through Figure 14. This process begins at the healthcare provider's EHR login page or patient portal.

Figure 9. Example Patient Portal

From this page, the patient would choose to register themselves with the EHR site by clicking the "Register via your Cloud Account" link. The patient would be directed to a simple registration page, hosted by the healthcare provider, which would ask the patient to enter a few pieces of known identifiable information, as depicted in Figure 10.

Figure 10. Proposed Registration via the Cloud - Step 1

The information entered on this page allows the user to uniquely identify themselves to the healthcare provider while providing a degree of confidence that it is indeed the patient registering on the site. Once the healthcare provider has verified the

information against its records, the site will notify the patient that their identity has been established.

Figure 11. Proposed Registration via the Cloud - Step 2

The patient will then choose a Cloud Account of their choice to link to the confirmed identity. Once the patient has selected an OpenID provider (a Cloud Account), they are directed to that Cloud service's authentication page and prompted to enter those credentials.

Figure 12. Proposed Registration via the Cloud - Step 3

Once the credentials have been verified by the OpenID provider, a data release consent page will be presented to the patient.

Figure 13. Proposed Registration via the Cloud - Step 4

This page will describe which specific pieces of information the healthcare provider is requesting from the Cloud account. Once the patient has consented to the release of the information, the mapping is complete.

Figure 14. Proposed Registration via the Cloud - Step 5

This simplistic approach is used extensively within the Cloud today by many merchants and web resources, presenting options such as 'Register with Google' or 'Register with Facebook'. Healthcare providers would essentially be doing a similar type registration process by letting their patients attach a Cloud credential to their identity in the provider's EHR. With the Cloud credential mapped to an EHR identity, patients could then log into the EHR application using that credential. The patient portal or EHR authentication page would simply have a link to "Sign in via the Cloud", similar to Figure 15.

Figure 15. Proposed Patient EHR - Sign in via the Cloud

After a patient clicks the link they would be directed to then choose a Cloud Account (an OpenID provider), similar to Figure 16.

Figure 16. Proposed Authentication via the Cloud

Once the OpenID provider was selected, the patient would be presented with the respective OpenID provider's authentication screen, as seen in Figure 12, the same screen presented by the OpenID provider as part of the registration process. After successful authentication, the patient would be redirected back directly into the EHR application.

Figure 17. Sample Patient EHR

Using this model, different patients could be using their Cloud account of choice from any one of the different OpenID providers to gain access to the same EHR system. This approach affords healthcare providers flexibility for authentication to their system such that patients will be able to use credentials they use on a daily basis for access to many other electronic resources in their personal life. Further, for all healthcare providers that implemented this solution, common patients of those providers could use the same set of credentials to access their respective EHR across all of those providers. This type of pervasive access to EHR systems across the industry is exactly the direction that the federal government and patients alike are starting to demand.

3.2.3.7. Provider Support for Cloud-Connected Systems

In addition to potentially improving the usability and user acceptance of a hospital's EHR, the proposed solution could potentially reduce the healthcare provider's support requirements related to electronic patient access. While all systems require some degree of support, the proposed solution could dramatically reduce a provider's support requirements and therefore provide cost savings by simplifying the process by which patient log into EHRs and other applications. Having patients use credentials they use on a very regular basis compared to a very occasional and sporadic basis offers a significant simplification. The provider would still need to have resources to help those patients to establish a Cloud identity that do not already have one or to assist patients that use their Cloud credentials very little.

To quantify the reality of this potential support reduction, it is important to capture information about whether support related to electronic authentication by patients for Cloud-connected systems has been reduced. It is this research's recommendation that

an organization adapt their normal support procedures to record what support is for Cloud-connected systems and what support is for other systems. This information can then be used to generate metrics for support requirements for both systems that have been integrated with the HFIF and those that have not. Similarly, those applications and systems that have been integrated can be compared historically before and after the integration to determine the impact the HFIF integration had to each respective application's support requirements.

This research tackles real issues faced by the healthcare industry today. Billions of dollars are being spent every year, in each of the covered areas: accessibility, efficiency, and integrity. This research suggests that all of these issues can be addressed and improved upon using standardized frameworks across the industry. Ultimately, other healthcare entities can hopefully leverage the findings of this research to achieve HIPAA compliance, EHR adoption, and pervasive electronic access for patients, quicker and cheaper to enable enhanced patient care.

Chapter 4. Research Evaluation and Analysis

In order to validate the effectiveness of this research, it was vital that both frameworks be implemented in an actual healthcare provider's environment. As mentioned in Chapter 3, this research was fortunate to have cooperative agreements with 2 national healthcare providers to provide that opportunity. The large central Pennsylvania hospital was engaged for evaluation of the Healthcare Information Security Compliance Framework (HISCF) and the large Maryland hospital was engaged to pilot the Healthcare Federated Identity Framework (HFIF). Both entities are national hospitals with the PA hospital having over 500 licensed beds and more than 400,000 patient admissions (combined inpatient and outpatient) every year, while the Maryland healthcare provider has over 800 beds and more than 350,000 patient admissions (combined inpatient and outpatient) each year. Each of these hospitals interact with a significant number of patients annually and are both faced with the daunting and costly challenges of achieving Health Insurance Portability and Accountability Act (HIPAA) compliance and providing patient access to electronic health records.

4.1. Case Study of Healthcare Information Security Compliance Framework

Since the HISCF was largely borne out of a federal grant of which a key deliverable was compliance assessment, the PA hospital was very eager to participate in its implementation even though they had already obtained certification as a HIMSS Stage 6 Hospital. This partnership between the Pennsylvania hospital and Towson University started in 2011 and promised the hospital would be provided a comprehensive assessment of their entire IT 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 the larger information technology assessment framework. The HISCF, depicted in Figure 6, is designed to take an organization from the initial recognition of the need for Health Insurance Portability and Accountability Act (HIPAA) compliance all the way through to implementation of any necessary changes to their environment. Along the way to compliance, specifically in Phase 2, a comprehensive security audit is performed that partially satisfies the necessary attestation for Meaningful Use.

4.1.1. HISCF - Phase 1

Starting with Phase 1, a high-level assessment, involving a thorough review of all technology practices and architectural designs, was performed. The information technology staff was engaged to assist in the completion of both the HISQ and ITAR.

4.1.1.1. Healthcare Information Security Questionnaire (HISQ) Execution

The HISQ was presented to a single point of contact in the Pennsylvania hospital's IT group. This individual, a senior security engineer, then worked with the appropriate staff within the 52 member IT department to complete each part of the questionnaire. Once the initial draft of the HISQ responses was completed, a series of interviews were conducted to review the responses for clarity and consistency. The responses were also reviewed by the hospital's Chief Information Officer (CIO) for additional validation. 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 HISG with is directed based on the HIPAA guidelines [5] and National Institute for Standards and Technology (NIST) recommendations [9] for HIPAA implementations.

4.1.1.1.1. HISQ - Policy Assessment Findings

The policy and procedure review results for each of the 4 policy areas had a number of similarities that cut across many of the technology areas of the organization. The common theme was that the healthcare provider had addressed most of the needed areas to some degree but not completely, seemed to emerge very quickly from the results.

4.1.1.1.1.1. Disaster Recovery and Business Continuity

In the area of Disaster Recovery and Business Continuity, the organization had only partially implemented a DRP plan and the portions that did exist need significant updating. The hospital had been rapidly growing over the last few years and their patient counts had been equally increasing. As such, disaster recovery and business continuity planning had not been given the appropriate degree of attention.

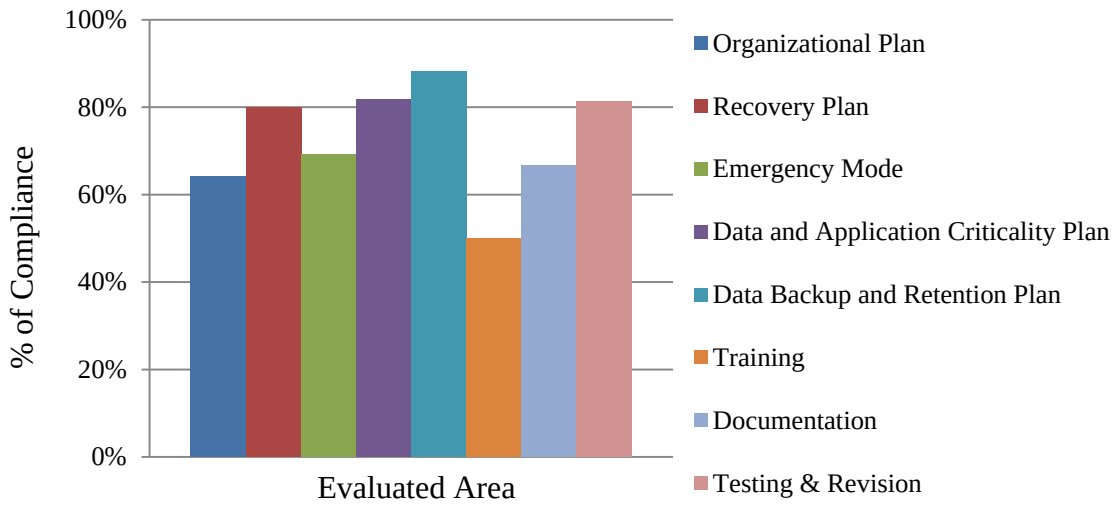

Figure 18: Disaster Recovery & Business Continuity Results from Pennsylvania Hospital Use Case

Based on the assessment findings shown in Figure 18, the organization's overall compliance with disaster recovery and business continuity rated 77% adequate. As expected, some areas were more complete than others. The organization scored over

80% in compliance for their recovery plan, their data and application criticality plan, their data backup and retention plan, and testing and revision process. However, the organization DRP policy, their emergency mode plan, DRP training, and documentation were all below 70% compliance with training only rating 50%. Some of the specific key findings in this area included the lack of backup copies of data being kept at an off-site facility. There was also no documentation for DRP training and the training that did exist was pretty limited. Another issue uncovered was that fact that there are single points of failure within both the recovery and emergency mode plans. Specific key responsibilities had no delegation accommodations therefore if a specific person is not available, those responsibilities and functions cannot be performed. This was a significant flaw in the organization's current DRP procedures.

4.1.1.1.1.2. Risk Management

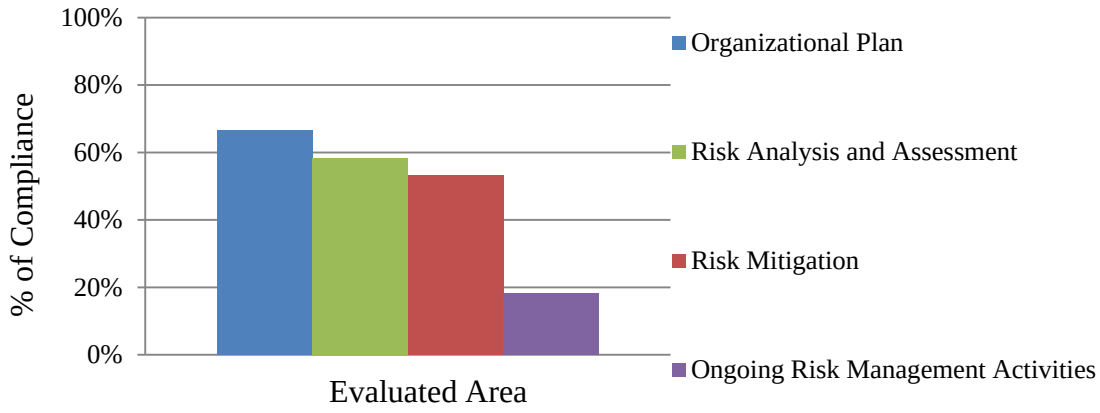

Figure 19. Risk Management Results from Pennsylvania Hospital Use Case

The results for Risk Management shown in Figure 19 were considerably worse than the other 3 areas. Overall the organization rated just 52% in compliance. The ongoing risk management activities were by far the least adequate area, scoring just 18%. The hospital had very little proactive risk monitoring in place. Most risk mitigation

efforts were reactive once an issue has been uncovered. Similar to DRP, the organization had partially developed plans for risk analysis and assessment as well as mitigation. Unfortunately none of these programs were fully implemented nor were they comprehensive enough to be in compliance all HIPAA guidelines.

4.1.1.1.1.3. Operations Management

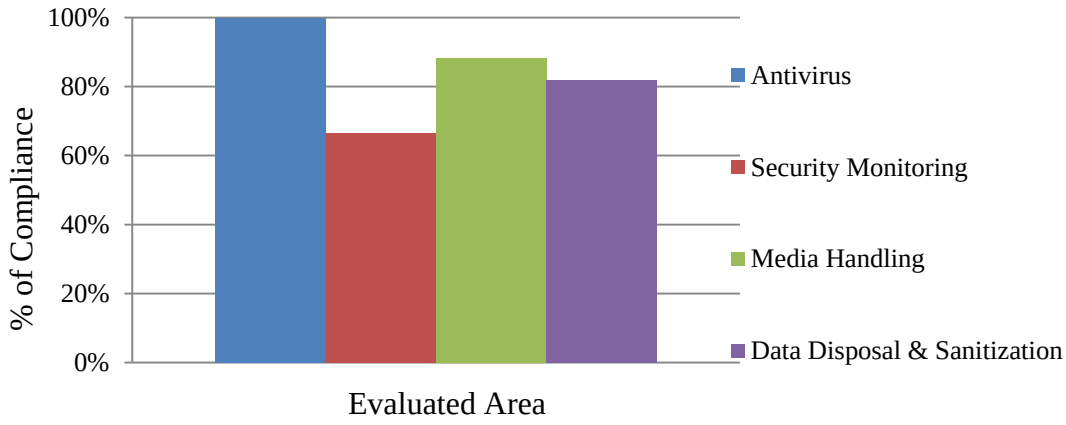

Figure 20: Operations Management Results from Pennsylvania Hospital Use Case

The healthcare provider had considerably more comprehensive policies and procedures related to operations management as shown in Figure 20. The antivirus program was 100% compliant and both media handling and data disposal had only very minor deficiencies. Security monitoring was in fact the only aspect of this area that had inadequacies of any significant degree. One of the main factors creating the issues related to security monitoring was that while they had a commercial intrusion detection and prevention system (IDPS) implemented, it had only been configured to monitor a very small segment of the organization's environment. Once the IDPS was fully configured this aspect should have come into compliance.

4.1.1.1.1.4. Logical Access

Logical access, shown in Figure 21, was measured at being 80% compliant overall. As with most areas assessed, plans for the various aspects of logical access had been developed and implemented but they were not comprehensive and were not up to date. It was discovered that many of the hospital's practices were not reflected in the policy nor were all the procedures mentioned in the policies actually in practice. Another key finding was that data could not be easily shared with external entities. While security of this data was sufficient, the logical access practices being employed created usability barriers and deficiencies. Further, due to the inflexible logical access issues, access to ePHI was not possible remotely. This situation also created an issue related to emergency access for business continuity during a disaster scenario.

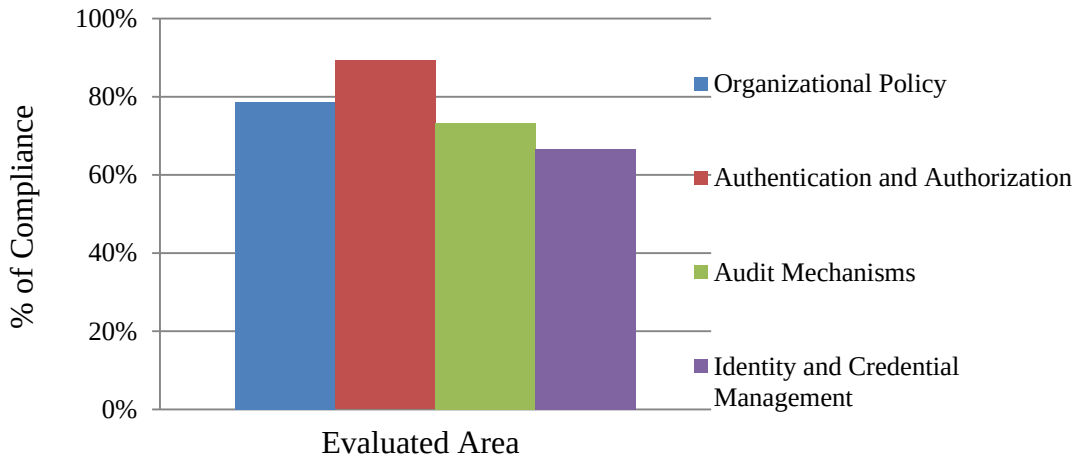

Figure 21: Logical Access Results from Pennsylvania Hospital Use Case

4.1.1.1.2. HISQ - Technical Assessment Findings

In addition to reviewing the policies and practices of the organization, the HISQ is designed to perform a technical assessment of information security. This portion of the questionnaire is divided into 4 main IT areas: Network, Applications, Database, and

Infrastructure. The relevant members of the healthcare's organization completed the questionnaire and those responses are denoted below. Only potential actionable issues were mentioned in this assessment. For any portion of the IT environment that is managed or hosted by a third-party, the assumption was made that those aspects of the environment were implicitly satisfactory and in compliance with all HIPAA regulations. A review of all third-party systems and management practices is out of scope for this assessment. For those potential issues that were identified, a description of the finding and the recommended corrective action to mitigate or remove the issues are provided. Regardless of whether a specific finding was cited with an actionable mitigating response, each area was scored based on how thoroughly and effectively it is being addressed within the current environment. The scoring determination was made from the series of responses given to each question, supplemental comments made in the Healthcare Practitioner Survey, and the general understanding of the environment based on all information provided. The complete results of the scoring are included in Appendix 10.

4.1.1.1.2.1. Network

1) Policies and Procedures

The response to the questionnaire indicated policies and procedures related to network operations and disaster recovery had not been adequately addressed. There seemed to be an indication that policies and procedures were once in place but they were no longer up to date with the current environment. Having comprehensive policies and procedures established, documented, and published for review would have addressed a number of HIPAA guidelines – §§164.308(a)(1), 164.308(a)(2), 164.308(a)(5),

164.308(a)(7) – related to the security management process, assigned security responsibilities, security awareness and training, and contingency planning. The questionnaire response indicated that acceptable use polices (AUP) were in existence but were not up to date. It is important to have documented and published acceptable use policies that all users agree to and this consent is recorded. Having an AUP in place further satisfies HIPAA guidelines – §§164.308(a)(1), 164.308(a)(5) – related to security management process as well as security awareness and training. The questionnaire response indicated that staff members were regularly receiving security alerts and advisories and likewise took the appropriate actions. That practice in part satisfies HIPAA guidelines related to security awareness and training - §164.308(a)(5).

2) Practices

The response to the questionnaire indicated that administrative credentials for network devices and applications were in some cases shared and in some cases unique to the staff member. The sharing of credentials, especially for administrative accounts with elevated privileges, is strongly discouraged. Without unique credentials the audit logging effectiveness is greatly reduced with respect to identity. The HIPAA technical safeguard guidelines related to access control – §164.312(a)(1) – clearly requires unique identifiers and credentials.

Since non-institutionally owned devices and PCs were allowed to access both the internal wired and wireless networks, it was critical that those machines had been scanned for risks prior to allowing full access to the network resources. Network access protection (NAP) and network admission control (NAC) software can provide the necessary safeguards required for security awareness and training – §164.308(a)(5). The

response indicated that software to perform NAP/NAC was licensed but not implemented.

The response further indicated that vulnerability scanning was performed but infrequently. It was crucial to regularly check the network for vulnerabilities and problems, and then address them in order to minimize the opportunity for accidental or malicious exploitation. The transmission security and regular evaluation requirements of HIPAA – §§164.308(a)(8), 164.312(e)(1) – necessitate regular penetration and vulnerability testing.

4.1.1.1.2.2. Database

1) Policies and Procedures

The response to the questionnaire indicated policies and procedures related to database operations and disaster recovery had not been adequately addressed. The responses indicated policies and procedures had either not been created or had not been completed. Having comprehensive policies and procedures established, documented, and published for review would have addressed a number of HIPAA guidelines – §§164.308(a)(1), 164.308(a)(2), 164.308(a)(5), 164.308(a)(7) – related to the security management process, assigned security responsibilities, security awareness and training, and contingency planning. The questionnaire response indicated that staff members were regularly receiving security alerts and advisories but were not taking the appropriate actions. Responding to security notices is a required practice to satisfy in part HIPAA guidelines related to security awareness and training - §164.308(a)(5).

2) Architecture

The response to the questionnaire indicated in some cases the database, application server, and web server all resided on the same physical machine. ePHI related applications that utilize databases should have use either a 2- or 3-tier architecture such that the database does not reside on the same physical server as either the application or web server. All efforts should be made to minimize the exposure each server has to non-administrative users and networks. Since all applications must inherently be accessed by internal and/or external users, some amount of exposure is necessary. 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 minimizes the impact of a breach at a web server since no actual ePHI data resides on those servers.

The response further indicated that there was no redundancy for databases within the environment. Redundancy should exist for databases as appropriate to the sensitivity or criticality of the data they hold. Having redundancy for databases that hold ePHI will assist in providing business continuity and satisfy the HIPAA regulations related to contingency planning – §164.308(a)(7).

Data encryption is critical for protection of ePHI. The response to the questionnaire denoted that encryption occurred only in some cases. In order to satisfy the HIPAA technical safeguards related to access control – §164.312(a)(1) – all ePHI data must be encrypted while at rest.

3) Practices

The response to the questionnaire indicated there was no monitoring or alert mechanism in place for databases. The indication was that activity logging was in place and was referenced reactively as required when an issue occurred. Having monitoring for

database activity is crucial to ensuring the security of ePHI data and knowing what is happening within the database. The monitoring should have the ability to alert the appropriate staff as well as either automatically or manually responding to events. HIPAA regulations – §164.312(b) – require adequate audit controls be in place for both non-repudiation and exception notification.

Administrative credentials for databases were shared among staff members according to the response. The sharing of credentials, especially for administrative accounts with elevated privileges, was strongly discouraged. Without unique credentials the audit logging effectiveness was greatly reduced with respect to identity. The HIPAA technical safeguard guidelines related to access control – §164.312(a)(1) – clearly requires unique identifiers and credentials.

4.1.1.1.2.3. Applications

1) Policies and Procedures

The response to the questionnaire indicated policies and procedures related to application operations and disaster recovery had not been adequately addressed. The response indicated policies and procedures had either not been created or had not been completed. Having comprehensive policies and procedures established, documented, and published for review would have addressed a number of HIPAA guidelines – §§164.308(a)(1), 164.308(a)(2), 164.308(a)(5), 164.308(a)(7) – related to the security management process, assigned security responsibilities, security awareness and training, and contingency planning. The questionnaire response indicated that staff members were not regularly receiving security alerts and advisories and likewise were not taking the appropriate actions. Distributing and responding to security notices is a required practice

to satisfy in part HIPAA guidelines related to security awareness and training - §164.308(a)(5).

2) Functionality

The response to the questionnaire indicated ePHI related applications had audit logging capabilities that produce easily reviewable logs. However, it was stated that the logs were not easily searchable and there was no central management of these logs. Audit logs that are centrally managed and searchable enable monitoring and alert functionality for proactive security. Adequate audit controls are a HIPAA requirement – §164.312(b) – including the ability to review and search exception reports.

The response further indicated that encryption was not used when ePHI data was transmitted between applications. Encryption is an effective way to safeguard the integrity of data while at rest and in transit. All methods used to transmit ePHI data between applications or within the application itself should use secure channels and some form of encryption. HIPAA regulations related to access control and transmission security – §§164.312(a)(1), 164.312(e)(1) – require encryption to be used when reasonable and appropriate.

All ePHI related applications should have the ability to check their data for accuracy, completeness, and validity. The response indicated that not every relevant application had this capability and furthermore SQL injection vulnerabilities had been identified for some applications. Invalid data can create both intentional and unintentional data pollution. Application and/or database level data checks should be used to mitigate the risk of compromised data integrity and address HIPAA regulations related to audit controls and integrity – §§164.312(b), 164.312(c)(1).

The possible methods of ePHI data extraction and transmission were not readily known according to the questionnaire response. It is a fundamental HIPAA requirement – §164.308(a)(8) to have an accurate understanding of how ePHI can be accessed and moved within the electronic environment of an organization. Without an adequate understanding of how users and applications interact with ePHI data it is impossible to take sufficiently secure measures to safeguard said data. All ePHI relevant applications should have all possible methods of ePHI data extraction or transmission secured and documented including aggregations of ePHI data outside of enterprise applications and databases.

3) Practices

The response to the questionnaire indicated that it was unknown whether administrative credentials for applications were shared or unique to the staff member. The sharing of credentials, especially for administrative accounts with elevated privileges, was strongly discouraged. Without unique credentials the audit logging effectiveness is greatly reduced with respect to identity. The HIPAA technical safeguard guidelines related to access control – §164.312(a)(1) – clearly requires unique identifiers and credentials.

4.1.1.1.2.4. Infrastructure

1) Policies and Procedures

The response to the questionnaire indicated policies and procedures related to infrastructure disaster recovery had not been adequately addressed. The response indicates policies and procedures had either not been created or had not been completed. Having comprehensive policies and procedures established, documented, and published

for disaster recovery would have addressed HIPAA contingency planning – §164.308(a)(7). The questionnaire response also indicated that an accurate inventory of all institutional hardware had not been created or was incomplete. Having a complete, accurate inventory of the organization's hardware will address in part the HIPAA regulations related to workstation use and security and device and media controls – §§ 164.310(a)(1), 164.310(b), 164.310(c).

2) Architecture

The response to the questionnaire indicated that there was redundancy for servers in some cases but not for all servers within the environment. Redundancy should exist for all servers as appropriate to the sensitivity or criticality of the data they hold, they interact with, or transmit. Having redundancy for servers and therefore the services or applications they hold will assist in providing business continuity and satisfy the HIPAA regulations related to contingency planning – §164.308(a)(7).

The response also indicated that servers were not located on segregated networks from both external hosts and internal user workstations. Network segmentation in conjunction with 2 or 3 tier application architecture allow for greater security through minimizing exposure. Managing information access and exposure is a HIPAA requirement – §164.308(a)(4).

No intrusion detection/prevention systems (IDS/IPS) was in place in the environment according to the responses. IDS and IPS provide many tools and techniques to monitor and react to intrusion events, detect and mitigate attacks, and provide notification of unauthorized system use. Most operating systems have some degree of IDS capabilities built-in but may need to be configured and enabled to provide the

functionality. An effective IDS/IPS strategy utilizes both the delivered capabilities of the operating systems as well as a stand-alone IDS/IPS application. Monitoring the servers and workstations of potential intrusions both electronic and physical is a requirement of providing adequate security – §164.310(a)(1).

3) Practices

The response to the questionnaire indicated that unregistered devices/machines were permitted to use NOS resources such as file and print sharing. This type of access implied NOS resources allow anonymous access which was not a secure practice. HIPAA regulations related to workstation security - §164.310(c) – require methods of access to be documented. Anonymous access greatly complicates the accurate recording of access activity.

The response further indicated that users had the ability to modify their PC/device configurations as well as install additional software. In such cases, it is important that users be trained on appropriate security best practices to help guard against unintentional compromises through the installation of malware or other hostile applications. For PCs and devices that have access to ePHI data, users' ability to modify the configuration and install software should be limited as operationally practical. The greater the capacity for users to modify their workstations increases the risk for compromise and likewise must be addressed as part of HIPAA regulations for workstation security – §164.310(c).

There were no measures in place to address ePHI data loss in the event a PC or mobile device was lost or stolen according to the response. At a minimum file encryption and strong device authentication should have been used to safeguard ePHI data if the device it was stored on was no longer in possession or control of the user originally

authorized to access it. Many mobile devices have the ability to complete delete their contents remotely if they are attempted to be broken into with brute force or other attacks. Data loss prevention (DLP) measures satisfy in part the HIPAA regulations related to device and media controls – §164.310(d)(1).

Server hardening is an industry best practice that was not being performed according to the response. Hardening ensures only the minimally necessary access and exposure for a server and the services or applications that it hosts. Many malicious attacks exploit unused, accessible resources on servers to compromise those systems.

4.1.1.2. Information Technology Architecture Review (ITAR) Findings

A number of phone interviews and exchange of emails were performed to gather information about the organization's IT architecture. Network diagrams, system configuration documents, and hardware specifications were examined as part of the architecture review. In contrast to the HISQ where the IT staff answered questions about the organization's policies or technical implementation decisions, the ITAR and subsequent analysis was performed by the team at Towson. Certainly in subsequent reassessments, the organization could perform this step themselves. The ITAR revealed there were a number of critical areas not addressed in the network design. The network topology was analyzed in detail and determined to be flat in crucial areas which indicates redundancy was not present in all areas. Further, network paths were not optimally designed for enhanced performance. The review also pinpointed a number of single points of failure within the network design thereby not sufficiently satisfying the HIPAA guidelines for contingency planning and business continuity – §164.308(a)(7).

It was documented that VLAN segmentation was not present throughout the network. VLAN segmentation is an essential technique to securing communications within an organization. One part of network segmentation is creating a DMZ in which all publicly accessible web servers are located. According to the review interviews, a DMZ existed but was not effective. Furthermore it was indicated that not all publicly accessible servers were located within the DMZ implying that portions of the internal network were reachable directly from external hosts. It was also indicated that internal VLANs were not always appropriately segregated from each other thereby enabling unnecessary accessibility to secure resources and data. VLAN segmentation is one aspect of ensuring systems and data is not unnecessarily accessible by internal and/or external hosts – §164.308(a)(4).

The review further determined that all applications and databases could have been accessed directly using a wireless connection. Wireless networks are inherently insecure due to the nature of the transmission medium and the inability to control where the transmission travels and therefore who can receive or intercept it. While there are measures possible to minimize wireless networks' vulnerabilities, they should be regarded as an insecure medium and only used for such applications and services that are tolerant to the intrinsic risk or required for operational necessity [120].

According to the interview responses, there was an absence of stand-alone intrusion detection/prevention systems (IDS/IPS) within the environment. IDS and IPS provide many tools and techniques to monitor and react to intrusion events, detect and mitigate attacks, and provide notification of unauthorized system use. Many network devices have some degree of IDS capabilities built-in but may need to be configured and

enabled to provide the functionality. An effective IDS/IPS strategy utilizes both the delivered capabilities of the network devices as well as a stand-alone IDS/IPS application. Monitoring the network is a requirement of providing adequate transmission security – §164.312(e)(1).

4.1.1.3. Healthcare Practitioner Survey (HPS) Findings

The focus group used for this survey was approximately 400 healthcare staff from the Pennsylvania hospital and its partner clinical practices. The group's population is diverse in gender, race, ethnicity, and creed. All members of the focus group were qualified physicians or physicians assistants at the hospital or clinical practices and appropriately familiar with the policies and practices of the hospital. The survey was completed anonymously to ensure honest, accurate responses as well as remove any undue bias from the analysis of said responses. The survey had a little over 10% response rate, resulting in 45 total responses received. The full results of the survey along with an analysis of the responses can be found in Appendix 6.

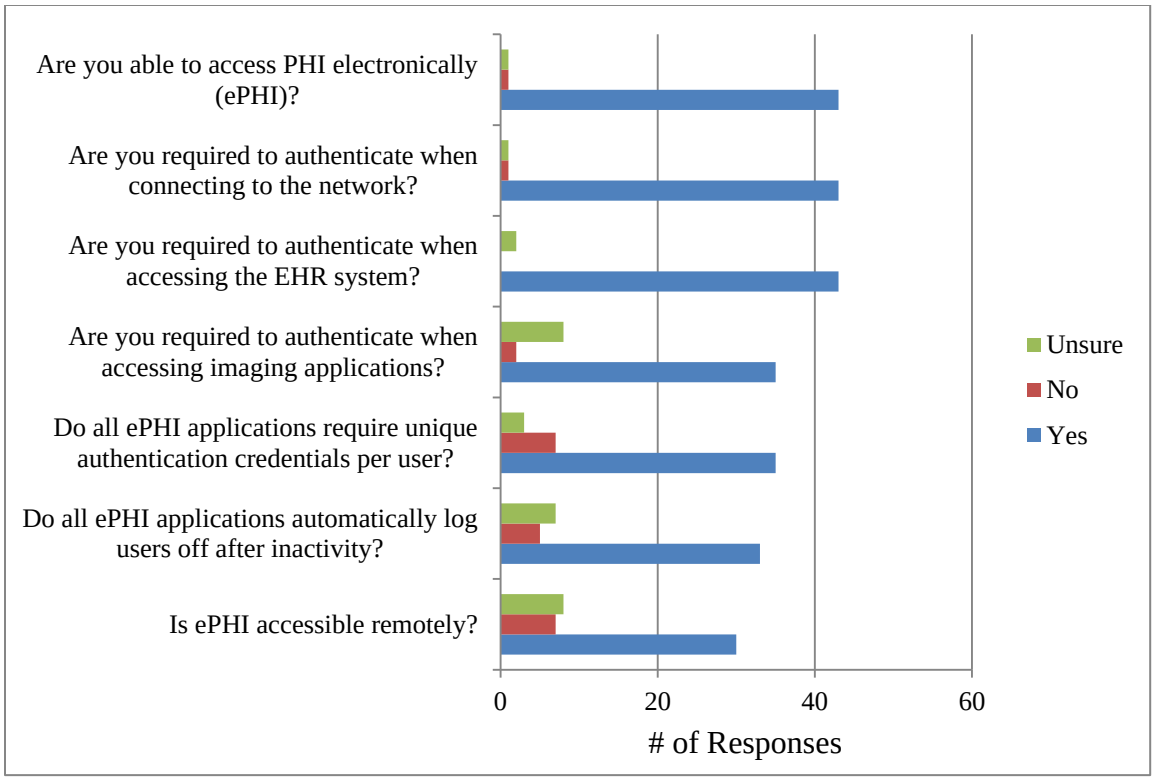

Figure 22. HPS - ePHI Access Results from Pennsylvania Hospital Use Case

The first 7 questions of the HPS were all relevant to the HIPAA Security Rule. The purpose of these questions was to provide a set of baseline questions to ensure the respondents did indeed work with ePHI and had a basic familiarity the hospital's computing environment. Over 95% confirmed this familiarity in questions 1-3 and this only dipped as low as 70% as the complexity of the questions increased about general accessibility of ePHI at the healthcare provider. It is significant that almost 20% of the respondents were unsure whether authentication was needed for imaging applications. Federal regulations require authentication for all access to any application that holds ePHI. The responses of this question suggest that the organization was meeting this requirement satisfactorily and a significant part of the population was unfamiliar and potentially uninvolved with imaging applications. It was also noteworthy that 16% of the

survey responses stated that shared accounts were in use to some degree for ePHI-relevant applications. Federal regulations mandate user accounts for ePHI applications be unique per individual for auditing and non-repudiation. The responses suggest that the majority of ePHI applications were using unique user accounts but not all. It is critical for the healthcare provider to review the authentication model for each ePHI application and implement user-specific accounts for any application that doesn't already employ that scheme. Similarly around 12% of the responses stated automatic log offs did not occur for all ePHI applications. HIPAA regulations clearly require all applications that interact with ePHI to automatically log users off after a period of inactivity. According to the responses, a comprehensive review of all ePHI relevant applications was needed to ensure each application had this capability enabled. There was a specific comment that some applications within the hospital kept the original user logged in indefinitely.

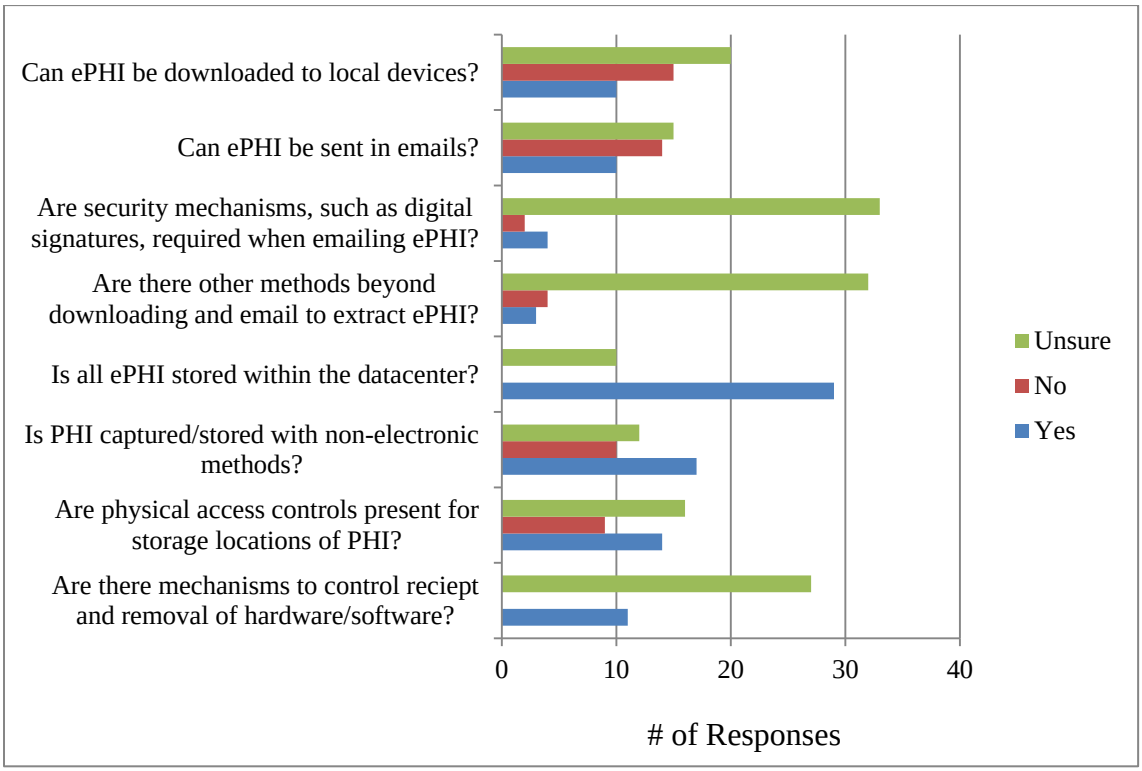

Figure 23. HPS - ePHI Data Control Results from Pennsylvania Hospital Use Case

The next group of questions had to do with how ePHI is controlled, including how it can be replicated, where it can reside, and security around its transmission. Based on the range of responses, it was not universally clear whether ePHI data could be saved on mobile and/or personal devices or included in emails. The responses were somewhat split across the board as to the perceived or actual capability of taking ePHI data outside of the organization's data center or including it in email messages. While the capacity to perform either activity is allowable within the HIPAA regulations, it becomes increasingly more challenging to maintain and demonstrate control of that data. Furthermore, if the organization does allow ePHI data to be included in and/or attached to emails, it is recommended that measures be taken to ensure its integrity. Digital signatures, encryption, and Data Loss Prevention systems are possible mechanisms that can be used for increasing the security of ePHI data included in email. As to the location of ePHI storage, about 74% of the respondents stated all ePHI data was stored within the organization's data center and none of the other responses contradicted the assertion. Control of all ePHI data is required to satisfy HIPAA regulations and having a common, centralized location to store all data makes the control of that data manageable. Similarly, the range of responses about how ePHI is captured suggests that there is not a clear, organizational understanding of all methods for capturing and storing ePHI data. HIPAA regulations mandate that ePHI be stored in electronic format for interoperability with other healthcare providers and payers. 26% of the responses indicated that there were non-electronic methods being used and a number of additional comments expanded upon this assertion noting that there was considerable data storage using paper. One comment described the environment as half paper and half 'scanned' paper, which may in

of itself not have been a completely accurate portrayal of the entire organization but it did suggest improvements may have been necessary to achieve the electronic storage requirements. Furthermore the responses indicated that many locations that store ePHI data were secured physically but not all locations had been adequately addressed. With almost 23% of the respondents stating that physical controls were not present in all ePHI relevant locations that indicated some areas either had no or insufficient controls for ingress/egress. HIPAA regulations require physical access be secure and monitored. Any areas that did not have these controls in place had to be corrected.

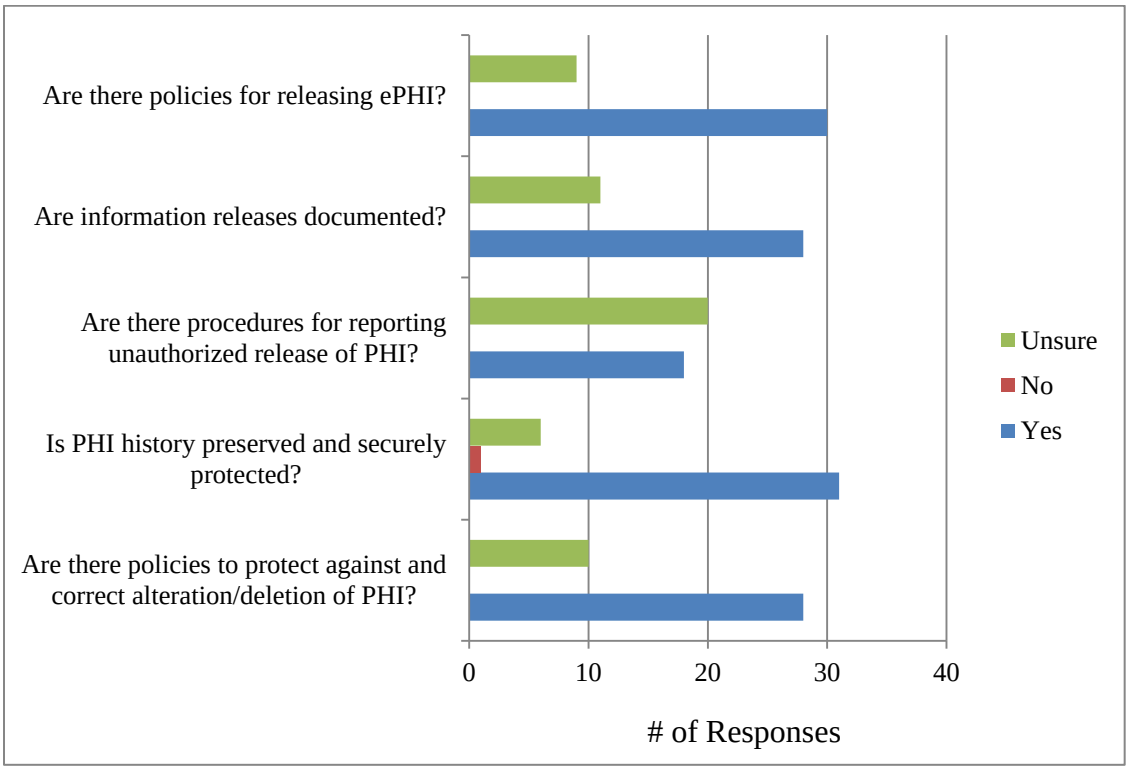

Figure 24. HPS – ePHI Integrity and Privacy Results from Pennsylvania Hospital Use Case

Following the questions related the security of how ePHI was controlled, there were a section of questions related to the healthcare provider's privacy practices and policies. Almost 77% of the respondents stated policies and procedures were in place for

each of the proposed situations related to ePHI data releases and none of the other responses contradicted the assertion. Additionally 72% of the respondents stated ePHI data releases were documented and securely recorded and none of the other responses contradicted the assertion. HIPAA regulations clearly require such policies and procedures to exist and require ePHI data releases to be documented and securely stored. Based on the responses the indication was the organization was satisfactorily meeting this requirement. Similarly, about 82% of the respondents stated ePHI data history was preserved and protected and there was only 1 response contrary to the assertion. Nearly 74% of the respondents stated policies and procedures existed to address ePHI data being changed or deleted and there were no responses that contradicted the assertion. HIPAA regulations require history to be securely stored for all ePHI data and safeguards be in place to ensure the integrity of ePHI data to include any changes or deletions. Based on the responses the indication was the organization was satisfactorily meeting that requirement. Finally, just less than half of the responses stated that procedures existed 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. HIPAA regulations 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 created an implied deficiency.

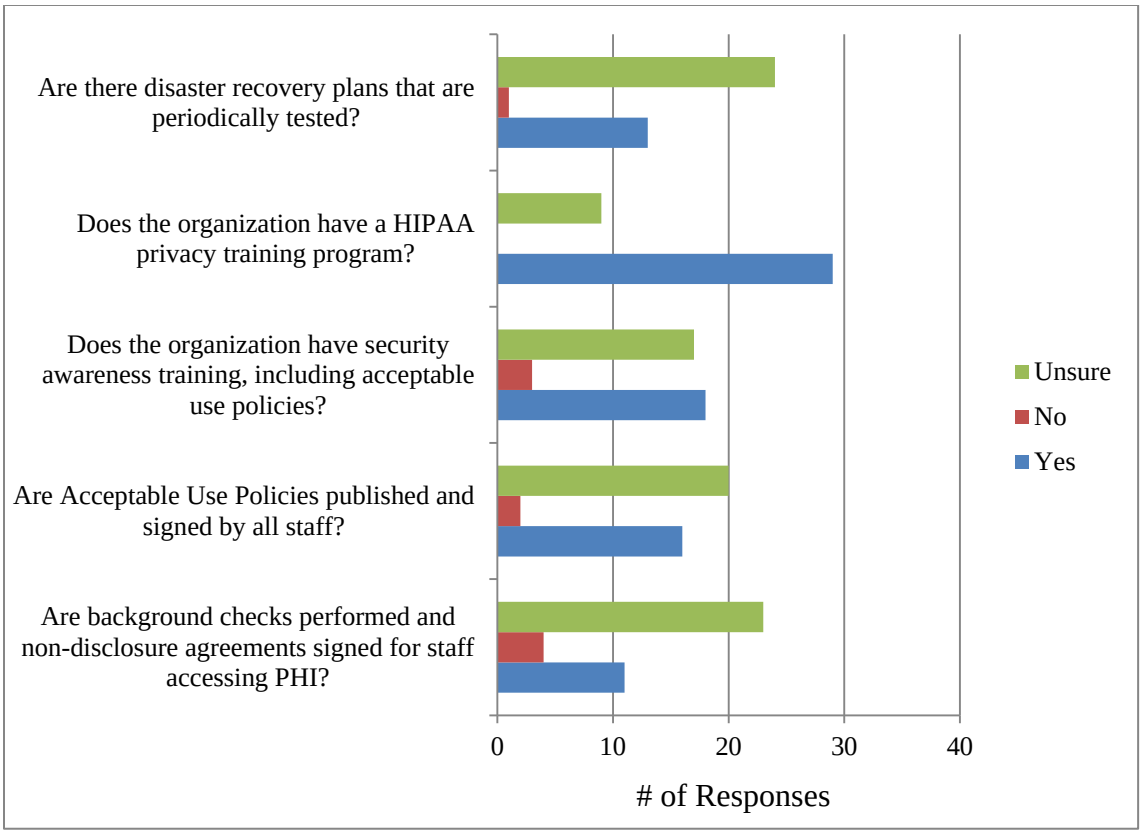

Figure 25. HPS – Policies Results from Pennsylvania Hospital Use Case

The last group of questions related to the organization's policies and their staff's knowledge and awareness of those policies. Only a third of the respondents definitively stated that disaster recovery and emergency plans existed and were periodically tested. The majority, 63%, of the responses indicated that it was unclear whether plans existed or were tested. Business continuity is a HIPAA regulation of which disaster recovery and emergency plans are a critical component. Almost 78% of the respondents stated a HIPAA privacy training program existed and none of the other responses contradicted the assertion. Privacy training is a requirement of the HIPAA regulations and based on the responses the indication was the organization was satisfactorily meeting that requirement. Just under half of the respondents stated security awareness training was provided on a regular basis although almost as many responses indicated they were unsure if such

training existed. Likewise, about 42% of the respondents stated acceptable use policies were published and signed by all users with access to ePHI data. However, almost 53% of the responses indicated they were unsure if such policies existed or were signed by ePHI relevant users. HIPAA regulations clearly require routine security awareness training and acceptable use policies be created, users agree to them, and this agreement must be documented prior to accessing ePHI data. Based on the responses the indication was while privacy training and acceptable use policies existed within a portion of the organization, they were not pervasive through all units. Roughly 29% of the respondents stated background checks and non-disclosure agreements were signed prior to access being granted to ePHI data. About 11% indicated those practices were not present within the organization and 60%, the majority of responses, were unsure. HIPAA regulations require all personnel, business associates, and contractors to be adequately screened prior to gaining access to ePHI data. Based on the responses, the indication was that some units were performing the necessary screening and some were not.

4.1.1.4. Overall Phase 1 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 HISQ is provided in Appendix 8. Additional human-technology interaction results were derived from the submitted responses to the Healthcare Practitioner Survey shown in Appendix 6.

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.

4.1.1.4.1. Phase 1 Critical Findings

The three assessments in Phase 1 yielded a significant number of critical findings within the organization's environment. Considering the partner healthcare system is a HIMSS Analytics Stage 6 Hospital, 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.

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 those 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. Redundancy within the network can be achieved using a variety of hardware and/or software solutions that was detailed in the COAR.

2) *Disaster recovery (DR) and emergency plans* – Only a third of the Healthcare Practitioner Survey respondents definitively stated that disaster recovery and emergency plans existed and were periodically tested. The majority, 63%, of the responses indicated that it was unclear whether plans existed or were 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 – §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 were not configured such that web services, application services, and database services were segregated from one another. In many cases all these services resided on the same physical machine and were directly accessible by internal and external hosts. The final COAR recommended that all ePHI data that would 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 have been 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 did not have an adequate demilitarized zone (DMZ) configuration that contained all publically accessible web servers. Many of the application's web servers resided in the same network subnets where the application and database servers were 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-tier 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 – §164.308(a) (4).
5) *Use of shared accounts* – 16% of the Healthcare Practitioner Survey respondents stated that shared accounts were in use to some degree for ePHI-relevant applications. HIPAA regulations – §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 were using unique user accounts but not all. It was critical to review the authentication model for each ePHI application and implement user-specific accounts for any application that didn't already employ that scheme.

6) *Automatic logoff* – About 12% of the survey responses stated automatic log offs did NOT occur for all ePHI applications. HIPAA regulations – §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 was needed to ensure each application had this capability enabled. There was a specific comment that some applications within the hospital kept the original user logged in indefinitely, which precluded compliance.

7) *Security awareness training* – Just under half of the survey respondents stated security awareness training was provided on a regular basis although almost as many responses indicated they were unsure if such training existed. The HIPAA regulations – §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 needed to be established and implemented across the organization.

8) *Acceptable use policies* – Almost 53% of the Healthcare Practitioner Survey responses indicated they were unsure if such policies existed or were signed by ePHI relevant users. HIPAA regulations – §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 was while acceptable use policies existed within a portion of the organization, they were 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 existed 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 – §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 created 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 Practitioner Survey respondents stated that physical controls were not present in all ePHI relevant locations. That indicated some areas either had no or insufficient controls for ingress/egress. The HIPAA regulations – §164.310(a) (1) – require physical access be secure and monitored. Any areas that did not have these controls in place had to be corrected.

4.1.2. HISCF - Phase 2

Phase 2 of the framework included an intensive technical review and assessment of the organization's IT environment. This phase measured and analyzed the actual performance of the systems and practices both against the theoretical goal presented in the HISG and the reported state of the organization provided in the assessment stage of Phase 1. It was critical for the success of this phase to identify the key IT staff within the hospital that could facilitate the exhaustive testing performed as part of the penetration and vulnerability testing. Once this staff was pinpointed, initial interviews were arranged to walk through the testing process and obtain contextual information about the environment to ensure the testing was indeed thorough but wouldn't interrupt normal business operations. It was also very important that we were able to engage directly with the manager of the EHR system to complete the EHR security and privacy assessment - Appendix 8. Since the assessment covers a range of areas – policy, functional, and technical – it is impractical for one individual or even one group in a department to adequately respond to all questions. As such, the manager of the EHR system was able to facilitate the completion of this assessment survey. It is important to note that all systems in the organization that were hosted offsite, were considered out of scope for this phase. The technical implementation and likewise testing of those systems was implicitly regarded as meeting all compliance standards by obtaining certification from the hosting entity that their systems are compliant with the appropriate federal regulations, such as HIPAA. This is consistent with the federal government's treatment of hosted systems for audit purposes. This phase's assessments included technical interviews and inspections, penetration and vulnerability testing, and a comprehensive evaluation of security and

privacy related to their EHR system. By the conclusion of Phase 2, the organization's complete IT environment had been methodically examined, tested, and documented.

4.1.2.1. Penetration and Vulnerability Testing Results

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 [91]. 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. The survey portion of the security testing discovered the presence of 5,967 unique systems on the organization's production network. These hosts were running a variety of services, amongst which were SMTP, SNMP, SSL, and HTTP, which are protocols that are commonly compromised or exploited. While many of these services may serve an operational purpose, it is important to verify there are no extraneous or unexpected services operating on these ports. The partner hospital's information technology staff did examine these results and confirmed that all hosts discovered were known and the services each hosts was running, was intentional.

An intensive battery of penetration tests and vulnerability scans were performed on the Pennsylvania hospital's production computing environment. Initially the organization's primary server subnet, subnet A, was examined exhaustively and 98 unique 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. After the expanded testing was completed a total of 1,012 unique systems had been identified across the organization and 13,037 total issues of critical, high, medium, or low risk. Based on the high number of critical and high risk issues exposed in subnets A through I, the organization decided that a full examination of all their subnets, including those throughout the main campus that only contained workstations, would be beneficial. Following this last round of testing, 5,967 unique systems had been scanned cumulatively between all three testing exercises. In total, there were 14,448 issues found, 5,846 of which posed either a critical or high risk to the organization. The summary of the findings from all the security testing exercises can be seen in Table 7.

	Subnet	Unique Hosts	Unique Hosts with an Issue	Critical	High	Medium	Low	Totals
Data Center (Hospital)	A	100	98	66	234	406	93	**799**
Servers and Workstations (Hospital)	B	175	171	1583	2155	1611	415	**5,764**
	C	15	11	97	15	95	36	**243**
	D	205	179	24	43	1025	195	**1,287**
	E	205	192	0	10	1114	187	**1,311**
	F	209	198	15	15	1146	196	**1,372**
	G	183	87	126	291	603	92	**1,112**
	H	143	26	359	436	219	50	**1,064**
	I	123	50	0	54	13	18	**85**
	J	252	20	0	6	146	41	**193**
	K	40	35	38	89	253	107	**487**
Workstations (including Partner Practices)	L	254	18	6	33	105	30	**174**
	M	254	6	3	19	27	6	**55**
	N	254	1	0	2	7	1	**10**
	O	254	5	0	0	25	6	**31**
	P	254	3	0	0	16	3	**19**
	Q	254	2	0	0	12	3	**15**
	R	254	0	0	0	0	0	**0**
	S	254	0	0	0	0	0	**0**

	Subnet	Unique Hosts	Unique Hosts with an Issue	Critical	High	Medium	Low	Totals
	T	254	9	0	6	18	8	**32**
	U	254	11	0	2	51	7	**60**
	V	254	13	8	5	38	8	**59**
	W	254	0	0	0	0	0	**0**
	X	254	10	0	3	27	4	**34**
	Y	254	8	38	49	42	4	**133**
	Z	254	13	0	16	59	10	**85**
	AA	253	0	0	0	0	0	**0**
	BB	254	6	0	0	20	4	**24**
	Totals	**5,967**	**1,172**	**2,363**	**3,483**	**7,078**	**1,524**	**14,448**

Table 7: Security Issues per Severity from Pennsylvania Hospital Use Case

4.1.3. HISCF - Phase 3

The final phase of the compliance framework, depicted in Figure 6, 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. Using the findings revealed in the assessments in Phases 1 and 2, the final COAR report was created that detailed these findings and all other assessment results to the partner hospital. The IT staff reviewed the findings and results for accuracy and ultimately confirmed their validity.

Also part of the final COAR report was a remediation plan, leveraging implementation recommendations set forth in the HISG. This plan of recommended changes was reviewed with the Pennsylvania Hospital's IT staff and leadership. Following the review, the changes were discussed and then implemented to mitigate all findings from Phase 1 and 2. In particular, the Phase 2 findings served as a catalyst to get leadership buy-in for the implementation of a periodic security assessment program. Similarly, another key development was the creation of formal risk management policies and procedures that were drawn directly from the recommendations laid out in the HISG.

Once the entirety of the remediation plan had been implemented by the Pennsylvania hospital, they contracted with an external auditing company to perform a comprehensive audit. The results of that audit were resoundingly positive as no significant findings were cited. Having gone through the HISCF implementation prior to the external audit, the hospital's staff was able to present all necessary documentation of the organization's policies and procedures - something that was severely lacking prior to the HISCF implementation. By the end of Phase 3 and confirmed by the external audit, the Pennsylvania hospital had achieved 100% compliance for both the Security and Privacy Rules of HIPAA.

4.2. Case Study of the Healthcare Federated Identity Framework

While healthcare providers must address information security compliance in their computing environment, they are being faced with having to provide their patients electronic access to their health information. The Meaningful Use guidelines dictate that healthcare providers accomplish this feat within 36 hours of providing care to all their patients. As part of the same federal grant that created the Healthcare Information Security Compliance Framework, the Pennsylvania hospital was also keenly interested in achieving Meaningful Use Stage 1. Similarly, another large private national hospital in Maryland (specific identity of the hospital has been suppressed due to non-disclosure agreement), was similarly interested in solving this patient access dilemma for Meaningful Use attestation.

4.2.1. HFIF - Federated Identity Pilots

Similar to the HISCF, it was important to demonstrate whether the Healthcare Federated Identity Framework was realistic and practical in a real-world healthcare

environment. As such, arrangements were made with two national hospitals to evaluate use cases and implement pilots as appropriate. Each of these hospitals interacts with a significant number of patients each year, and both are faced with the daunting and costly challenge of providing these patients access to their EHRs in a timely fashion. The Maryland hospital has more than 800 licensed beds and more than 350,000 combined inpatient and outpatient admissions every year, while the Pennsylvania hospital has more than 500 beds and more than 400,000 patient admissions each year. With hundreds of thousands of patients each year, the effort required to provide patients with electronic access to their health records is significant. In fact, the large PA hospital has not provided any patient access to date because the necessary resources have been deemed so high. The Maryland hospital, which is providing patient access, reported that the information technology (IT) help desk fielded almost 37,000 calls in 2012, related specifically to patient authentication issues. Authentication issues included questions about a patient's username, password, and secret question and answer or PIN for resetting a forgotten password, as well as other general inquiries. The breakdown of helpdesk tickets for each particular authentication issue is illustrated in Figure 26.

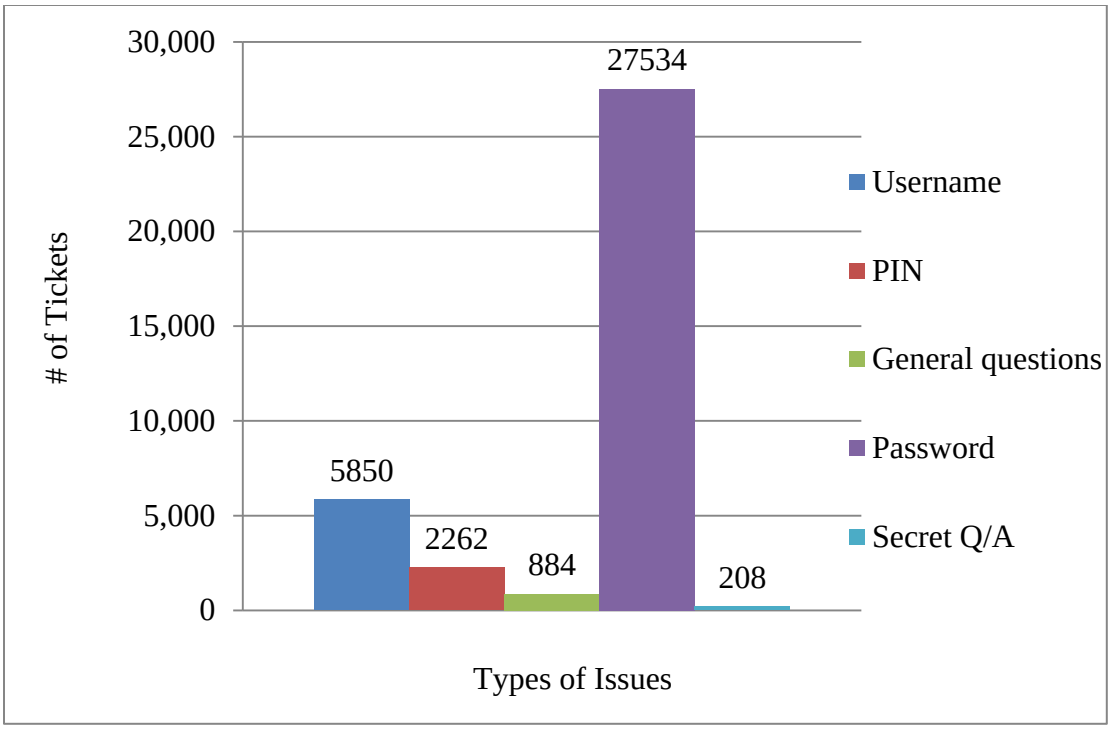

Figure 26. 2012 Helpdesk Tickets Related to Authentication at Maryland Hospital Use Case

Each of the partner hospitals was looking to leverage existing, robust technologies to solve their patient access issues. Using the proposed framework, a series of pilots and concept projects were established with the Maryland hospital. The goal of the pilot was to determine whether the accessibility and corresponding support requirements of applications that patients accessed electronically on a regular basis could be improved.

4.2.1.1. Application Selection Process

The first step was to identify which applications of the existing 26 patient-accessed applications would be good candidates to pilot the Federated Identity framework. It was important that the applications chosen have regular electronic patient access and this access be repetitive such that the same patient would be accessing the applications multiple times to judge whether usability had been improved or not. Ultimately it was decided that diagnostic and scheduling applications would be a good fit

while also not creating potential undue ePHI exposure for the hospital. The applications were also evaluated by whether the software was already designed to work with some type of external authentication system such as a single sign-on technology or the Lightweight Directory Access Protocol (LDAP). It is an important point to recognize that a software's ability to integrate with an external authentication system is critical to being able to apply the HFIF. Fortunately, all commercial EHR systems natively have the ability to integrate with an external authentication system as this concept has become prevalent in most commercial applications even beyond the healthcare industry. In the case of the pilot project, none of the applications considered were EHR systems, although they all interacted with ePHI to some degree. The 4 selected applications for the pilot project are listed in

Table 8.

Vendor	Product	Functional Use
Tempus	Encompass	Patient Appointment Scheduling
Sensor Medics	Somnosar (Sleep System)	Diagnostic
Natus Medical	Ceegraph	Diagnostic
LifeLine Software	RadCalc	Diagnostic

Table 8. Applications Selected for HFIF Pilot at Maryland Hospital Use Case

4.2.1.2. HFIF Implementation Process

Once the applications had been selected for the Maryland hospital's pilot project, the next step was to plan the implementation of the HFIF. The implementation had 4 major parts: the technical integration of the OpenID standard with each application; developing a common patient-Cloud Identity mapping site; providing communication with patients about how the change for authentication for the pilot applications; and

determining a support model for assisting patients as well as generating metrics to measure the pilot's success.

The first and decidedly the easiest of the 4 main tasks was the technical integration of the OpenID standard with the 4 applications selected for the pilot project. As part of the selection criteria for participation, applications that could natively work with external authentication systems were targeted. Specifically for these 4 applications, the .NET library built for OpenID was used to facilitate the integration [121]. OpenID has freely available libraries for nearly all programming languages including but not limited to .NET, Java, Perl, PHP, Python, and Ruby. The integration part itself went very quickly as there is an abundance of documentation on how to integrate OpenID at a very basic level with an application – it has been done over 50,000 times to date.

However, after each application was set up to work with OpenID in the most basic sense, the application had to have a way to consume the OpenID identities it was presented and translate them into an identity it was aware of that corresponded to a patient. This task relates to the concept of mapping a healthcare provider's patient identities to Cloud identities presented in §3.2.3.6. In fact, the solution to this problem was built directly from the identity mapping prototype designed as part of the HFIF. A website was designed similar to the one shown in Figure 9 through Figure 17. It asked patients to enter personally identifiable information – first name, last name, date of birth, and last 4 digits of their social security number – and used this information to determine the which patient they were, if at all, at the Maryland hospital. Once they website knew who they were internal to the hospital, it then asked them to authenticate with an OpenID provider of their choice to link the Cloud identity to the internal identity. This one

registration website was used by all 4 applications and once you had used the site once for any of the applications, there was no need to do it for the other applications. In this Maryland hospital's case, the internal identities of all 4 applications were already co-aware as there was a common 'patient number' that most applications within the hospital used to represent the same individuals across those systems.

After completing the mapping site, the technical portions of the integration was essentially complete. The next task was to communicate with the patients to alert them of the new way to log into these 4 applications. This was done through a series of methods including announcement postings on websites, information on the application websites themselves, and user-targeted emails to the existing users of those applications. The hospital's helpdesk was also engaged to help promote use of these pilot applications.

The hospital's helpdesk was more importantly involved in developing self-help documentation as well as basic troubleshooting information that the staff of the helpdesk could use when helping patients by phone and email. It was also critical that the helpdesk incorporate a method of recording the specific support tickets they serviced related to the pilot applications. Having a way to measure how many times users required assistance with the pilot applications was essential to determine whether the HFIF model was viable in practice.

4.2.1.3. Pilot Project Results

Once each of the steps of the implementation process had been completed, the hospital ran the pilot project for approximately 4 months or 120 days. At the end of that period, an examination was done of how many support tickets had been fielded for these applications compared to the other patient-accessed applications as well as historically

for the pilot applications in the first 120 days of 2012. The results of that examination can be seen in Figure 27.

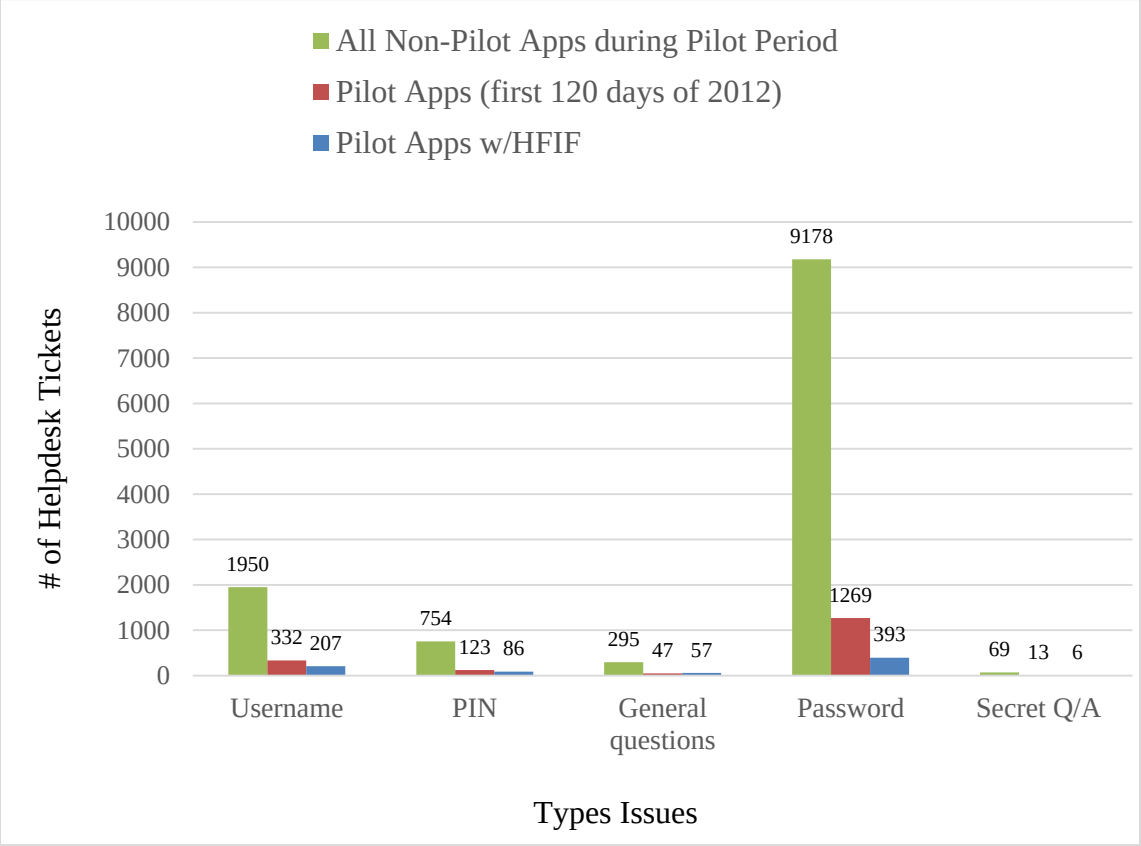

Figure 27. HFIF Pilot Support Results at Maryland Hospital Use Case

It is interesting to note that username and password related tickets reduced from 332 and 1269 in the first 120 days of 2012 to 207 and 393 respectively during the 120 day pilot at the Maryland hospital. The number of general inquiries actually rose slightly for the pilot applications during the pilot compared to the similar timeframe in 2012 – up from 47 to 57 tickets. This was attributed to the fact a change was implemented for how these applications were accessed. It is somewhat expected that while an initial spike of support may occur from confusion and curiosity about the change, over an extended period of time, the reduction in support requirements around general questions would

mirror the other areas. Overall combining all 5 support categories, the 4 pilot applications saw nearly a 60% reduction in support over the initial 120 days of the project compared to the first 120 days of 2012 dropping from 1784 to 749 tickets respectively. This was a significant outcome for the pilot project and has compelled the Maryland hospital to consider other expanded pilots.

4.2.1.4. HFIF Adaptation

While working with the Maryland hospital to implement the HFIF pilot for enabling electronic patient access from the Cloud, another use-case was identified by the hospital IT staff for how to apply the proposed federated identity solution. Many of the hospital's practitioners accessed numerous external medical resources maintained by the federal government or other entities. The hospital was interested in how a similar federated identity relationship could be set up with these resources but basically turning the tables 180 degrees. Instead of using an external credential to access an internal system as proposed by the HFIF and likewise the goal of the pilot project, the hospital was looking to use an internal credential to access an external resource. In essence, the HFIF could still be applied in almost the exact same way but swapping in the hospital's credential store for the OpenID Cloud Providers. In this scenario, the hospital had to conform its credentialing practices to the identity assurance profiles laid out in the HFIF. Once this was done and leveraging pre-existing trust agreements and vetting processes established by Federal Identity, Credential, and Access Management (FICAM), the Maryland hospital was able to successfully use their credential repository to federate with a number of National Institutes of Health (NIH) resources including PubMed, the Clinical Translational Sciences Award (CTSA) Management System, and the database of

Genotypes and Phenotypes (dbGaP). By having the identity assurance profiles from the HFIF that satisfy the National Institute for Standards and Technology (NIST) and FICAM requirements for e-Authentication, the hospital had all the necessary procedures in place and was able to easily produce the required documentation to establish the trust agreements. This was a noteworthy implementation of the HFIF, albeit a slight adaptation.

The implementation of the proposed solutions with the 2 national healthcare providers was a crucial exercise that allowed the instruments designed by this research to be tested with real-world data in real-world environments. In the case of the Healthcare Information Security Compliance Framework, the results of applying the various assessment tools identified key issues that required the partner hospital's attention. Furthermore, once the results had been responded to the hospital was then able to successfully pass an external audit and validate the HISCF had a positive impact on that computing environment. The pilot implementation of the Healthcare Federated Identity Framework at the Maryland hospital demonstrated the potential for improving electronic accessibility for patients to ePHI applications while also possibly providing considerable cost savings to the healthcare provider by lowering support requirements. Chapter 5 will expand the discussion of the results presented in Chapter 4 and suggest what inferences can be made for the partner hospitals and potentially other healthcare providers.

Chapter 5. Discussion and Implications

The core goal of this research was to develop potential solutions for improving accessibility, efficiency, and integrity in healthcare delivery. While this research proposes standardized approaches for evaluating and ensuring Health Insurance Portability and Accountability Act (HIPAA) compliance and for providing electronic patient access to EHR systems, these solutions needed to be tested and legitimized through actual application in a real-world environment. Chapter 4 detailed the case studies of the framework implementations with 2 national healthcare providers and the results borne out of those efforts. While the initial review of those results seem very positive, this chapter aims to delve deeper into what the results actually mean and what possible wider implications they may have for other hospitals.

5.1. Healthcare Information Security Compliance Framework

The HISCF was applied with the Pennsylvania hospital, a 500-bed HIMSS 6 national hospital that admits over 400,000 patients per year. Phase 1 of the HISCF did a systematic review of the organization's policies and procedures. This phase also analyzed the hospital's technical architecture and surveyed healthcare practitioners to get a perspective on how technology was actually being used in day-to-day practice. Phase 2 of the HISCF did a thorough battery of security testing on every aspect of the Pennsylvania hospital's computing environment. Even though considered in the upper tier of hospitals in the United States with regard to information security, there were significant findings that indicated areas where Health Insurance Portability and Accountability Act (HIPAA) compliance was not being met.

5.1.1. Phase 1 Inferences

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 was on par with the industry averages. The industry averages, derived from HIMSS sponsored research [6], indicated 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 was relatively close to compliance but not at the federally mandated 100% compliance.

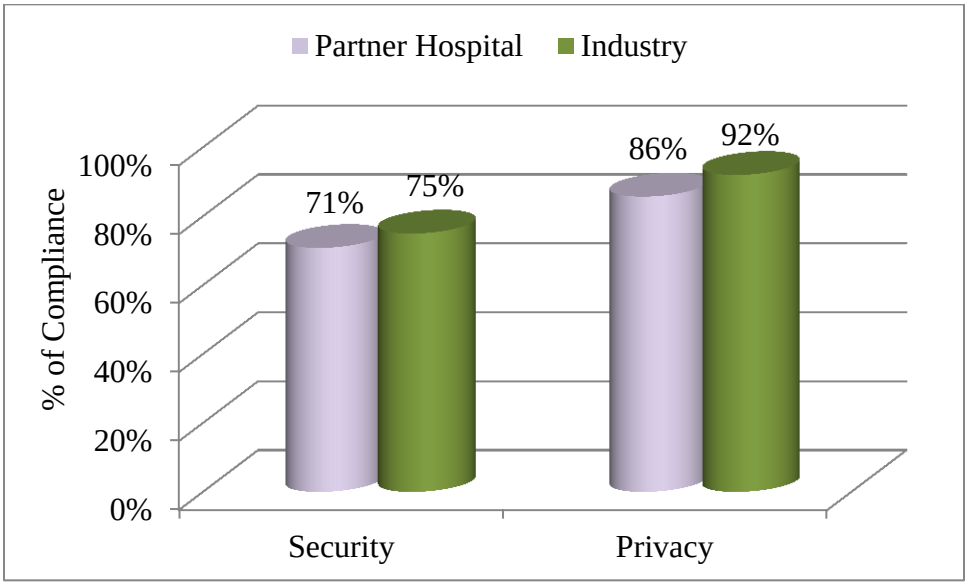

Figure 28. Overall Compliance Performance

The functional area that required the most improvement by the organization was policy and procedures. This deficiency is fairly common throughout all industry with respect to IT and Kwon and Johnson suggest it is also one of the hardest areas to correct [63]. 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.

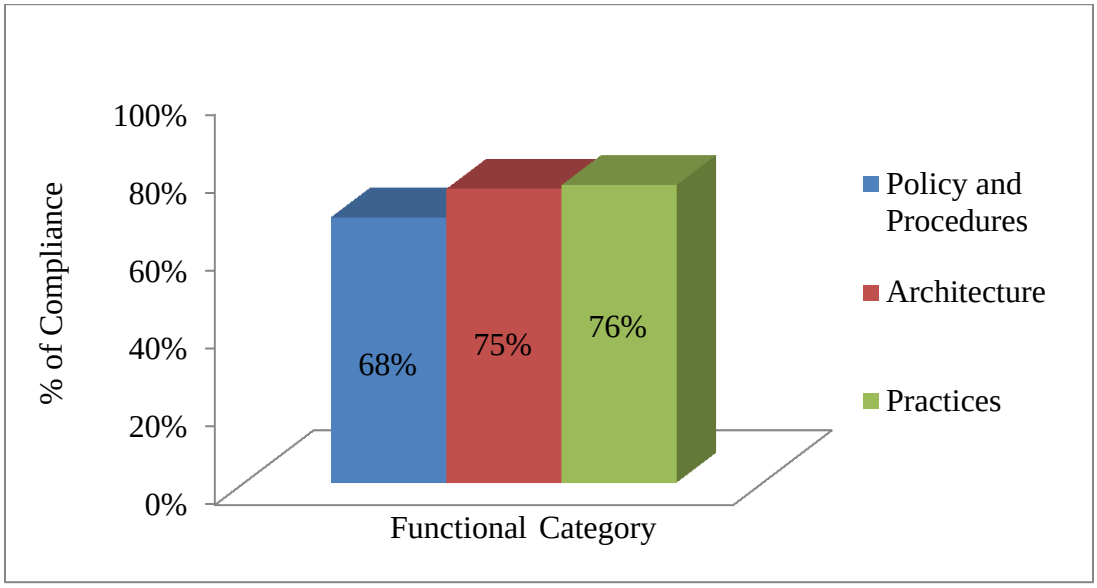

Figure 29. Compliance per Functional Category

Similarly, the organization had the most compliance issues with regard to the human-technology interaction element of IT compared to the four solely technical areas, as depicted in Figure 30. This was actually a good indicator for the organization that their workforce had an increasing propensity for compliance beliefs. Cannoy at al [122] contend that in larger healthcare providers, over 300 beds, a high proclivity for compliance is typically indicative of a high level of intervention by management through training, meetings, policy implementation, and enforcement. Having leadership buy-in and involvement in compliance efforts is a critical factor for an organization's compliance programs to be successful [70].

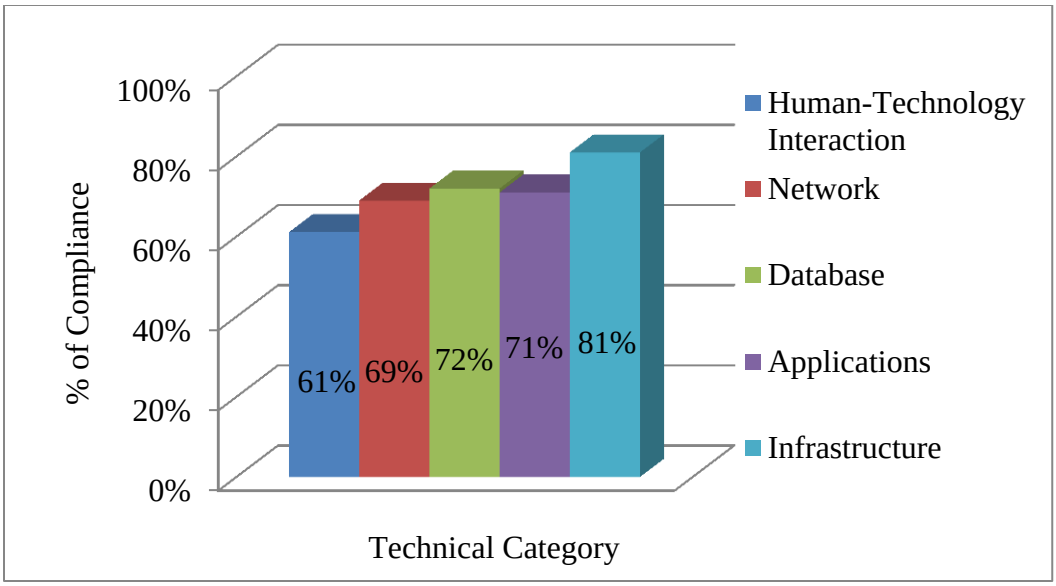

Figure 30. Compliance per Technical Category

Even though Phase 1 yielded significant gaps in functional and technical areas that spanned the Pennsylvania hospital's computing environment, none were unsurmountable to remediate. Arguably the hardest step in compliance is simply the recognition of a requirement and corresponding discrepancy in meeting it. Ignorance through a lack of understanding and awareness is oft times the main reason for organizations be out of compliance [22]. Once the issue has been identified, many times remediating the technical problem is not that difficult and can very done very quickly. This was demonstrated by the hospital's ability to respond to the majority of all of Phase 1's findings within a matter of weeks of when they were brought to their attention. Additionally, as the HISG could be leveraged for implementation level guidance, the Pennsylvania hospital's IT staff did not have to go searching for remediation solutions as they were readily available. The fact that the application of the HISCF was directly responsible the realization of the gaps in compliance and facilitated the remediation efforts suggests that the HISCF is an effective tool and was more comprehensive than the

compliance program previously instituted at the Pennsylvania hospital. This claim was offered by the organization themselves after having gone through the assessment exercises laid out in Phase 1.

5.1.2. Phase 2 Inferences

While Phase 1 performed a passive examination of the organization's computing environment and practices, Phase 2 did an active evaluation through a series of targeted tests and inspections. Phase 2 identified 5,846 critical and high risk issues. Undoubtedly the presence of this many elements of increased risk throughout the environment was unfortunate and disappointing to the organization. On the other hand it was fortunate for the organization that these issues were found so they could be mitigated before the risks turned into compromises. 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 5,846 critical and high risk issues found, they are made up only 483 unique vulnerabilities.

This finding demonstrated the product of the organization not having a formal security assessment program that performed periodic testing. At a minimum it was recommended that an enterprise wide patching process and schedule be established. Additionally, it was recommended that a standardized deployment configuration for servers and workstations be developed. These fairly simple steps could mitigate many of these issues very quickly and reliably. Furthermore, the routine testing would bring to light any poor implementation choices or mistakes that were made when a new system or application is brought online. The Pennsylvania hospital's technical staff was able to

validate these findings and corresponding mitigation steps to resolve nearly 90% of the findings in about 1 month.

Following this analysis, the results were then examined to determine how many issues each individual host had to see if there were any trends or high concentration areas of increased risk. The complete breakdown of the number of issues per host is depicted in Figure 31.

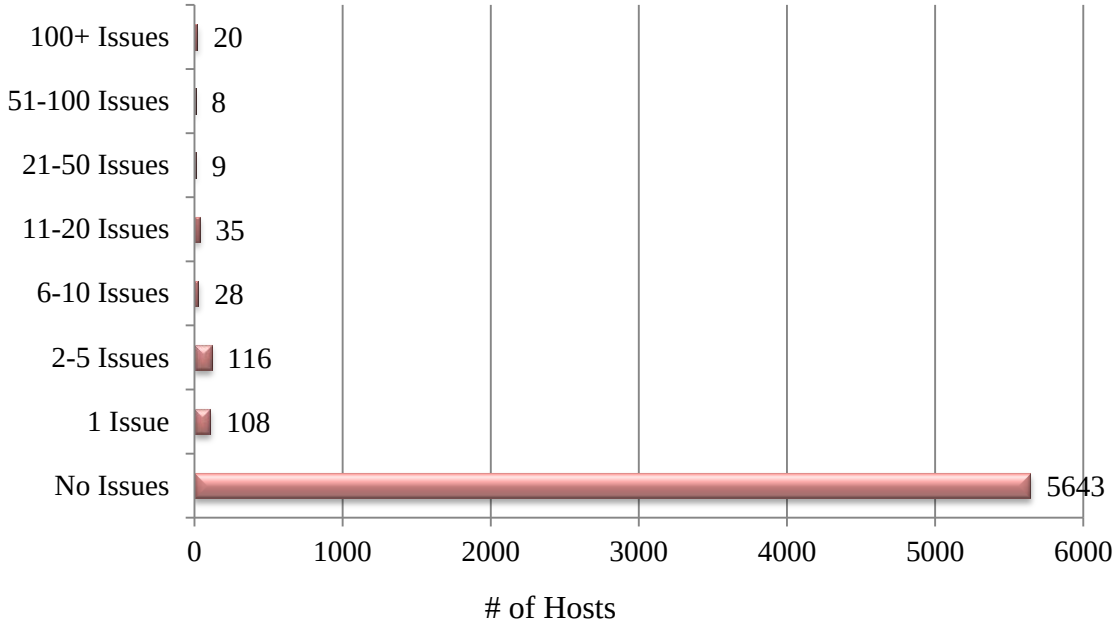

Figure 31: Number of Security Issues per Host

Of the 5,967 hosts present in the healthcare provider's production environment, 324 of these systems had at least 1 issue of critical or high risk. In contrast, 5,643 of the 5,967 hosts, about 95%, had no critical or high risk issues at all. When looking only at the 1,012 machines at the hospital's main campus - subnets A through K, 725 of these machines, 72%, had no critical or high risk issues at all. This percentage is notably similar to the organization's approximate 71% overall compliance with the HIPAA Security Rule measured in Phase 1. This similarity in results using different testing

methods provides a measure of validation for the evaluation process itself as it produced comparable results between both Phases. It is significant to note that there were 20 systems that had 100 or more unique elevated risk concerns. In fact, these 20 machines account for 4,153 of the 5,523 total critical or high risk issues present at the main hospital campus. Which is to say just fewer than 2% of the organization's computing environment represented about 75% of its increased risk exposure. This is a common condition in most organizations as it is typical for the majority of an organization's computing environment is operating at an adequate security level and there is just a small fraction of the systems that are not [123].

It is concerning however that the data center, subnet A, which housed only servers (production, testing, and development), exhibited 300 critical and high risk issues. Furthermore, only 16 of the 100 systems in this vital area of the organization and where all the storage of ePHI resided did not have at least 1 issue of critical or high risk. This means 84% of all the systems in effectively sensitive area of the environment had an elevated level of risk. The crux of the organization's condition was a lack of true patch management program and periodic security assessment program within their computing department. As such a complete periodic security assessment program was proposed for the Pennsylvania hospital that included recommendations for all critical and high risk issues to be measured and addressed within 30 days. It is industry-recognized that a patch management and vulnerability assessment process is a key element to mitigating risk [124]. This was a significant realization that came out of the testing that provided an impetus for the organization's leadership to move swiftly and decisively to correct these issues.

Similarly to Phase 1, the fact that the Pennsylvania hospital going through Phase 2 of the HISCF generated the volume and significance of results that it did, coupled with the healthcare provider's size and reputation in the industry, seems to support the claim of the effectiveness and usefulness of the HISCF.

5.1.3. Overall Implications of HISCF's Validity and Future Recommendations

The outcomes of applying the HISCF at the Pennsylvania hospital are very compelling and seem to suggest the framework is comprehensive and effective, at least within the scope of that hospital. Prior to applying the HISCF, the Pennsylvania hospital had failed an external audit, being cited for numerous violations related to HIPAA. Following the HISCF implementation, the hospital was audited again and no significant findings were reported. This suggests the HISCF was instrumental in the organization's improvement. This research recommends that further application of the HISCF is needed to strengthen the premise that it can be an effective tool for other hospitals as well. While the simple number of times the framework is applied needs to be increased, so does the variety in hospital sizes. The HISCF may not be a 'silver bullet' solution for every type of healthcare entity but the results from the case study with the Pennsylvania hospital seem indicate the potential that it could benefit other organizations.

5.2. Healthcare Federated Identity Framework

A pilot project was established with a Maryland hospital to test the HFIF. The Maryland hospital is an 800-bed hospital that admits over 350,000 patients per year. The pilot project's goal was to evaluate the technical and functional feasibility of leveraging the Cloud as an external authentication source for applications patients regularly accessed electronically. The key questions the pilot was purposed to answer were:

1. Was it technically possible to integrate an application at the Maryland hospital to use Cloud Identity Providers for authentication?
2. Once an application leveraged the Cloud for authentication, would support requirements change?
3. Could the Cloud be used to assist with updating common contact information to hopefully improve the hospital's ability to communicate with its patients?

5.2.1. Inferences

The results of the HFIF pilot project presented in Chapter 4 seem to indicate success on all fronts for the Maryland hospital. With respect to question 1, the technical integration of the Cloud with the selected applications proved very straightforward. The key question for the pilots was really question 2 related to support requirements; would the Cloud integration make electronic access easier for patients thereby reducing the amount of support needed? The results seemed to indicate this resoundingly was the case. Based on the number of helpdesk tickets generated over the initial 120 days of the pilot implementation, there was a 60% reduction in the support requirements for these 4 applications. Within the scope of that hospital and that period of time, the HFIF model markedly improved patient accessibility. Working on the assumption that this trend would continue at least for that hospital, extrapolated across all 26 applications that patients access at the Maryland hospital, this would be a reduction of 22,000 tickets annually. This suggests a significant costs savings for the healthcare provider. This research suggests that additional pilots of the HFIF with higher numbers of applications over longer periods of time is needed to have a better indication what the actual long-term implications are for support requirements at the Maryland hospital from applying

the federated identity model. Furthermore, similar to the HISCF, testing of the HFIF is needed at other hospitals of a diverse size. As the HFIF interacts with patients directly, the healthcare provider's geographical location and types of services rendered may have an impact on the demographic makeup of that provider's patient population. Further research is needed to determine whether demographic characteristics such as gender, ethnicity, age, creed, or income have any bearing on the patient population's reaction to the HFIF's Cloud-integrated model.

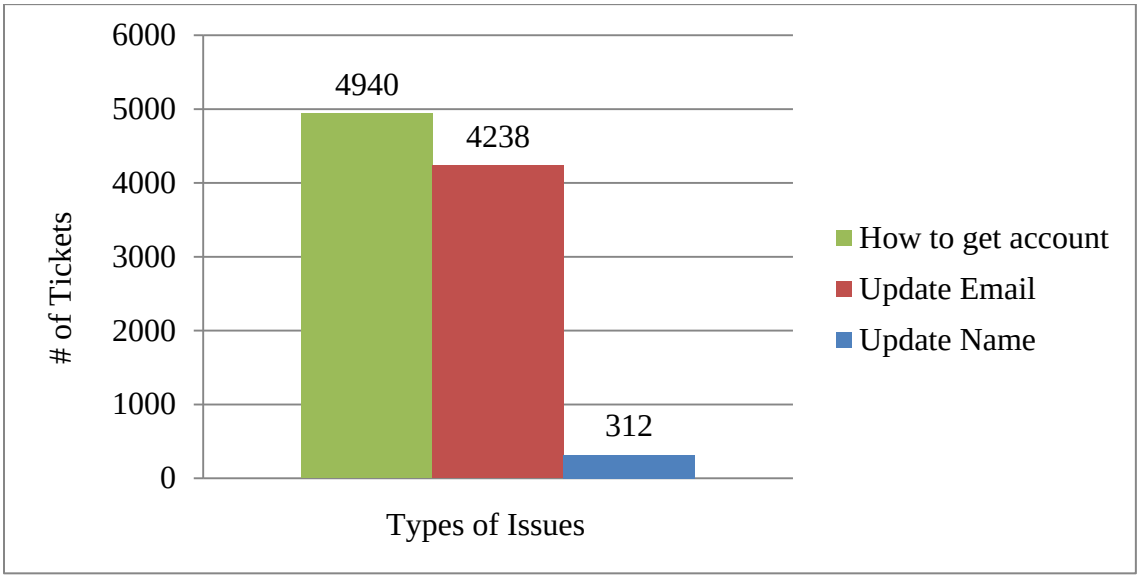

Figure 32. 2012 Helpdesk Tickets Related to Contact Information at Maryland Hospital Use Case

Beyond authentication issues, each hospital's IT helpdesk were fielding thousands of calls related to how to establish their account with the hospital or the need to update their email address in the system, shown in Figure 32. Cloud IdPs have a vested interest in keeping contact information such as name and email up to date. With this research's proposed integration, healthcare providers could potentially extract this information from the Cloud periodically for all the patients that have registered their Cloud identities with

the healthcare provider. The OpenID standard makes the consumption of this information by integrated systems very straightforward. The hospital did not opt to leverage this feature of OpenID therefore Question 3 of the pilot project's purpose ultimately went unanswered. Indications from data presented by OpenID [119] suggest that thousands of applications are doing this successfully every day and the Maryland hospital and any other integrated entity should prove no different.

5.2.2. Overall Implications of HFIF's Validity and Future Recommendations

The results of applying the HFIF at the Maryland hospital in a limited pilot are encouraging. For those 4 applications over the course of a 4 month window, there was a 60% reduction of support requirements. This suggests patients were able to access these applications with less assistance from the hospital and ultimately have an improved access experience. This outcome further suggests that more testing is warranted to determine if the HFIF will have similar successes on a larger scale and in different environments.

There are some technical implications of implementing the HFIF on a larger scale. The identity assurance profiles detailed in the HFIF are at this stage only a proposal and have not had formal certification by the Federal Identity, Credential, and Access Management (FICAM) agency nor the OpenID standard itself. There currently is a LOA1 profile that OpenID has adopted and FICAM certified, but the Department of Health & Human Services (HHS) has determined that a LOA2 profile is needed to access one's own PHI and an LOA3 profile to access someone else's. The first recommendation is for the OpenID organization to adopt this research's proposed LOA2 profile at a minimum. After adopting the LOA2 profile, the Identity Provider participants of OpenID

such as Google and Yahoo would need to establish procedures for implementing the profile within their current infrastructures. The OpenID standard would then need to be expanded to include a LOA distinction per identity so that Service Providers, such as hospitals and other healthcare providers, could consume that LOA classification and determine whether the identity was trusted 'enough' to be used so as not to introduce security and privacy risk and thereby compliance discrepancies.

Once the LOA2 profile was incorporated into the OpenID standard, the next step would be to apply for FICAM certification of that profile. FICAM is responsible for vetting and approving all standards related to identity, credential, and access management that can then be endorsed or condoned by other federal agencies. Furthermore, HHS, which stipulates e-Authentication practices and standards that are Health Insurance Portability and Accountability Act (HIPAA) compliant, has already made its ruling in this respect. Having a formal certification by FICAM provides healthcare providers indemnity for any issues related to a Cloud Identity Provider's practices. The certification also eliminates the need for each healthcare provider having to do its own individual vetting of each Cloud Identity Provider before integrating their systems with OpenID.

In the case of the HFIF pilots, a simulated LOA2 profile had to be established. All the responsibility for conformance with that LOA2 profile actually fell to the Maryland hospital since the current OpenID standard has no way to assert anything higher than a LOA1 profile. Therefore the tasks of identity vetting, authentication entropy, and all the other aspects of the LOA2 profile needed to be accounted for through other means. While there was the capacity to accomplish those tasks, it was an arduous

process that wouldn't need to be done if the OpenID standard supported an LOA2 profile natively.

5.3. Limitations of the Case Studies

While examining the results and attempting to draw inferences from them, it is an important step to revisit the limitations of this research and frame them specifically in the contexts of the two associated cases studies that were performed. The limitation to the sample size used to model the research design as well evaluate the proposed solutions is a very critical limitation to recognize. Both the HISCF and HFIF were only implemented in single environments respectively albeit both hospitals were national providers and assumed to be good representations of typical medium-to-large hospitals in the United States. Certainly multiple implementations of both frameworks will provide a more diverse sample set and enable stronger and more meaningful inferences to be drawn from the cumulative results. However, the results from applying this research are not trivial and within the contexts of the partner hospitals, had very tangible outcomes.

Additionally, while both proposed frameworks employ industry standards and federal government sanctioned recommendations, only a comparative review of the existing methodologies was performed. An exhaustive systematic review of all possible IT standards and frameworks is theoretically desirable but challenging to be practically feasible. This research suggests that in fact there are often multiple different methods that can produce the same end result. It is suggested that the key is finding an easily repeatable method that can be proven to be successful while also being flexible and agile enough to adapt to different environments. The results from applying both frameworks

demonstrated success for those specific hospitals and hold promise for being beneficial to many others as well.

For the HISCF specifically, not having the open availability of similar frameworks such as HITRUST's CSF to compare and contrast the proposed solution was a limiting factor. Ultimately this is likely to become a necessary step to truly validate this research's potential benefit on a much larger scale than the hospitals involved in the case study.

Another limitation for this framework was some of the methods used to conduct Phase 1 of the HISCF. With regard to the HISQ, it was essentially a survey of 1 that was completed through a single point of contact at the hospital. That individual took responsibility for coordinating with the appropriate internal staff and departments to collect the needed responses. The quality of those responses was directly related to that individual's cooperation, honesty, and competency to provide that coordination. In that particular instance, the point of contact was a senior security engineer in the hospital's IT department and the assumption was made that person could and would adequately be able to serve in that role. There was also routine interaction with the CIO of the organization that provided an element of oversight to the interactions and data being presented by the point of contact.

Similarly, the HPS had another set of limitations that are noteworthy. While this survey was sent out to roughly 400 practitioners of the hospital and partner clinical practices, the hospital acted as the distribution point. This meant that the results and corresponding response rate of the human-technology survey were directly dependent on the hospital's capacity and competency to send the survey out to the proper population,

using a reliable method, and in a timely manner. The resultant 10% response rate is high enough such that meaningful inferences can be drawn from them, but certainly the higher the response rate was the less amount of deviation needs to be considered when reviewing the results and their implications as a reflection of the entire organization. Lastly, as the hospital controlled the distribution and the survey submission were anonymous, there is a limitation on whether the survey submission's authenticity can be verified. The survey did require an access code to be used to submit the survey but this wouldn't prevent a practitioner with knowledge of the code from submitting multiple times or distributing the required information to individuals not qualified to participate. This identity verification restraint was deemed necessary as the opportunity of anonymity improving honesty in the responses outweighed the potential negative impact of the limitation.

For both the HISQ and HPS, neither of these instruments were vetted by external source for completeness and appropriateness. The project director of the grant for which this research worked in conjunction with served as the quality control agent for the survey instruments produced and implemented. This is limitation as there may have been biases introduced into that quality control process by nature of familiarity with the project itself and parties involved. While cost and opportunity prevented the external validated of these instruments, this exercise would bring additional legitimacy to the results produced and implications of broader application.

Another limitation of the HISCF evaluation was that it was only applied over the course of a 3 year period. Over a longer period of time, the HISCF's claim of effectiveness and comprehensiveness could be more substantiated once the established

compliance assessment program goes through a number of cycles and demonstrates it can be used successfully repeatedly.

The HFIF evaluation had its own set of unique limitations that could have potential ramifications on the validity of the results and corresponding inferences. The HFIF pilot project was limited to only 4 applications of the 26 total patient-accessed applications that could have possibly been selected for inclusion. The inclusion of those specific 4 applications, the exclusion of the other 22, the number of applications chosen, and which specific applications selected could have directly impacted the results. There is a potential that not all applications will have the same results related to user acceptance and the corresponding support requirements. Different applications certainly have different functionality and different patient demographics and the combination chosen for the pilot project may have unknowingly altered the results. Furthermore, the period of time over which the results have been presented are a limitation. This research acknowledges that data related to support requirements over a longer period is need to substantiate the true impact to the hospital. Lastly, it is important to make the distinction that the pilot project included patient-accessed applications that interact with ePHI but none of the four were commercial EHR systems. The case study infers an EHR system would have the same experience related to a reduction in support requirements but that needs to be demonstrated specifically to legitimize the claim.

The evaluation of the HISCF was performed with a collaborative partnership with a Pennsylvania hospital that has achieved HIMSS Stage 6 certification – only 248 hospitals/systems have achieved the certification in the United States. The healthcare system was provided the benefit of a comprehensive assessment of their entire

environment, including specific, actionable tasks to remedy any deficiencies uncovered related to compliance. Moreover, the application of this research at the Pennsylvania hospital allowed the proposed framework to continue to evolve based on results from real-world use. Similarly, through the collaboration with the Maryland hospital, the Healthcare Federated Identity Framework was able to be implemented and tested in a limited fashion. This Maryland hospital realized quantifiable benefits through the pilot project and now better positioned to map a path forward for expanding patient access for other ePHI-related applications and services, including their patient EHRs, with the adoption of the proposed identity assurance profiles laid out in the HFIF by the OpenID standard and subsequent certification by the Federal Identity, Credential, and Access Management (FICAM) agency. This research has proposed potentially significant solutions that appear to have the capacity to offer other healthcare providers similar successes to those the improvements the Pennsylvania and Maryland hospital were afforded.

Chapter 6. Conclusions

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. The Health Insurance Portability and Accountability Act (HIPAA) and EHR systems lay the foundation for satisfying these concerns. Unfortunately, these endeavors has proved challenging to accomplish with the absence of standardized, freely available, implementation plans. Each HIPAA covered entity has been forced to approach these tasks from their localized, individual perspective and hence the figurative wheels are being reinvented again and again. Further, each one of these entities is 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 offer promise for assisting healthcare providers with the initial implementation of these initiatives as well as better equip organizations to maintain their ongoing compliance.

6.1. Outcomes

The opportunity to apply this research at the two national healthcare providers proved to be an excellent exercise. The Pennsylvania hospital was struggling with getting their computing environment to 100% compliance with the Health Insurance Portability and Accountability Act (HIPAA). 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, the Pennsylvania hospital was eager to satisfy the Meaningful Use objectives and complete the attestation to qualify for the more than $2 million annual incentive payment. They had an EHR implemented to some extent for 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 complete the MU program.

This research was able to close the gap for the Pennsylvania hospital 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 systems in their data center and 5,846 critical and high risk issues across the entire organization. Only 16% of the organization's servers did not have at least 1 issue that required attention. This was a concerning discovery as this meant 84% of the hospital's server infrastructure was exposed to some degree to unnecessary risk. While finding issues in an environment can oft times not be well received, the Pennsylvania hospital’s IT 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.

The federated identity pilots seem to have been significantly beneficial for the Maryland hospital and its patients alike. The Cloud access model requires very little user support overhead compared to the hospital supporting a system that issues, maintains, and

revokes credentials for all their patients. The healthcare provider's IT helpdesk has estimated almost a 60% reduction in the number of tickets related to authentication issues for the pilot applications in the initial 120 days of the OpenID integration. Based on this trend and if OpenID and the federated identity framework was integrated across all 26 systems that patient access electronically, the healthcare provider could potentially see a reduction of upwards of 22,000 tickets annually. The man-hours associated to this reduction in helpdesk tickets are quite significant and therefore a very compelling reason to consider moving forward. In fact, due to the tremendous success of these pilots, other integrations are already being considered by the Maryland hospital to include nearly all scheduling applications (physician practices, diagnostic, imaging), patient reminders for preventive/follow-up care, and patient discharge instructions dissemination. While not as far along as the Maryland partner hospital, the Pennsylvania hospital is actively performing use-case analyses to determine how best to integrate this research into their environment. Building upon the early successes with this research's framework, the Maryland hospital is positioned to continue to grow their Cloud integration to the point of truly achieving patient access for all health information electronically.

6.2. Future Research

Beyond the frameworks presented by this research, there is still considerable work to be done in both the compliance and federated identity arenas. The regulations for ensuring data integrity change continuously and all industries struggle to stay up with the new rules and standards. The healthcare industry is constantly bombarded with new guidelines and requirements to follow from federal and state levels. The Federal Information Security Management Act (FISMA) of 2002 has been acting as yet another

catalyst to enact new, improved standards for how sensitive data, including ePHI, is managed. FISMA actually encompasses not only the Health Insurance Portability and Accountability Act (HIPAA) regulations but all other federal regulations set forth in any way related to information security. Like HIPAA, FISMA compliance has now become an auditable requirement and obligation of all healthcare providers. Similar to what was presented in this research, healthcare providers will need standardized approaches and frameworks to follow to institute policies and practices that guarantee integrity as well as have a reliable way to test those controls. Even as it relates to HIPAA and the compliance framework laid out in this dissertation, further research is important to address how this framework is updated to include new regulations, testing, auditing, and/or attestation requirements as they are enacted. Furthermore, more research is needed to either expand this research's compliance framework to include other regulations beyond HIPAA or create a way for multiple compliance frameworks to work together to prevent duplication of efforts by the implementers. Hiring consulting firms and paying for proprietary guides should not be the only answer. The regulations are public and so should the solutions. As such, there will be a continual need to provide healthcare providers implementation specific guidelines in order to make the achievement of compliance of these regulations a possibility.

While compliance and data integrity is an area that the healthcare industry has been working in for decades, the concept of a portable, digital identity is quite a bit more recent. Ubiquitous access is rapidly becoming both a reality and expectation of our connected society. The Meaningful Use programs are just a piece of this larger evolution and are forcing healthcare providers to enable patients greater and easier access to their

health information. The Meaningful Use objectives related to patient access to their EHR are very focused on a single healthcare provider scenario. The concept and scope of pervasive patient access to multiple EHR systems is still quite organic as there are a number of possible paths forward. This area needs considerable more analysis and research as a non-scalable solution in information technology almost always proves to be the wrong solution. At a basic level, there are only 2 basic choices when considering how to access patient data from multiple providers - aggregate or federate.

There are multiple other mature technologies and protocols that allow for a federated authentication model similar to OpenID. Security Assertion Markup Language (SAML), perhaps OpenID's most prevalent alternative, is used heavily within the higher education community and throughout many federal government agencies. Many organizations have other Single Sign-on (SSO) technologies such as Jasig's Central Authentication Service (CAS) [125] and Microsoft's Active Directory Federation Services (ADFS) [126] that effectively accomplish the same basic federated approach. As many organizations adopt one solution or the other, considerable work is being done to establish bridges between the technologies to expand the possibilities of interoperability even farther. Social-to-SAML is one such project that allows OpenID identities to access resources that are configured to use SAML [127]. Likewise, there are initiatives for almost all the major SSO solutions to interoperate in all conceivable directions. Therefore it is not as critical which specific technological solution an industry or entity embraces as it is that they move quickly and surely to make the necessary organizational and technical choices to position themselves to participate.

The alternative to federated access to multiple EHR systems is to provide access to a single, aggregated system. Health Information Exchanges (HIEs) approach the issue of accessing multiple EHR's data at the data store layer instead of the authentication layer. The focus of HIEs is primarily targeted on the practitioners and the sharing of the medical data between providers. The data sharing within HIEs is typically accomplished by creating master sets of all participating EHR systems' data with data warehousing or some form of longitudinal data replication. This research is specifically focused at how access is being granted to the EHR systems and how EHR systems can grant access to phi using non-traditional methods for users to validate their identity. As such, the products of this research can potentially complement existing HIEs or provide similar benefits for those providers that do not participate in an HIE. The goal of simplifying and enhancing ePHI data access is consistent across both approaches. The HIE model enables participating EHR systems to exchange all their information such that every EHR now has the cumulative data of all EHRs. This research submits that there are some inherent unnecessary efforts being expended in this model as well as complexities to data security and privacy that a federated access model would eliminate. HIEs introduce significant challenges potentially including: duplication of data records across all providers requiring extra storage requirements at each and every healthcare provider; providers having to store an abundance of phi that may or may not be relevant and potentially for individuals that have never been or ever will be patients at their organization; the relinquishing of control of a provider's ePHI to other providers or a data warehouse for better or worse with respect to financial and legal responsibility; and the need to establish

expensive, high bandwidth connections between providers or a central data warehouse to move large quantities of data regularly.

Another consideration for federated access is for access to individuals for ePHI belonging to someone else. This could be for practitioners to gain access to their patients' data in another EHR system or for a patient to delegate access of their ePHI data to a loved one. The Centers for Medicare & Medicaid Services (CMS) has mandated that access to any ePHI by anyone beyond that individual requires a LOA 3 credential. A key requirement of LOA 3 is the introduction of multi-factor authentication. This is where the proposed OpenID solution needs further development. The OpenID credential provides only a single factor and would need to be combined with some form of token (soft or hard) or a biometric credential to meet the LOA 3 requirements. The need of this second factor will revisit the issue of making tokens or biometrics a more cost-effective, scalable solution for wide spread adoption.

There are many perspectives on how to address this distributed patient access issue. However, it is clear all of these areas are moving in the same direction with all industries and technologies converging to form a larger interoperable community. Even with the early success being realized by the adoption of this initial research, there is much work left to complete to further broaden its application. The next stage of this research involves examining how the different federating technologies and standards can work together. The next permutation of the proposed access model is to become technology-agnostic in order to expand the horizon of possible integrations even further. Healthcare providers will not be afforded the choice of whether to participate in this developing

identity ecosystem, so further development of the solutions raised in this research is needed to provide the maximum amount of flexibility.

6.3. Research Contributions

Specifically, this research's goals were to lessen the challenges of achieving integrity, by way of compliance, and enabling pervasive access to EHR systems for patients. Underpinning both of the proposed solutions for these challenges is the focus on ensuring that the frameworks are streamlined and easily adaptable, thus improving the overall efficiency of the healthcare provider. The measure of whether this research's goals were accomplished is the appraisal of whether the original key questions related to integrity, efficiency, and accessibility in healthcare information technology where answered.

1. *How do organizations verify that their security measures are functioning adequately and comprehensively address the requirements for federal compliance?*

This research purports the only accurate way that organizations can verify their security controls are operating as expected is to perform routine testing of those controls and configurations. Furthermore, it is imperative that the periodic testing is carried out in a uniform way each time to ensure results can be reasonably measured and compared to prior testing cycles [123]. This research has generated a framework potentially for organizations to easily and consistently perform testing using a standardized plan. Using the Healthcare Information Security Guideline (HISG), created by this research, as its basis, the compliance framework attempts to ensure all testing and assessments comprehensively evaluates the organization's compliance with the Health Insurance

Portability and Accountability Act (HIPAA) and many other federal regulations. The Pennsylvania hospital's implementation of the Healthcare Information Security Compliance Framework (HISCF) and the subsequent findings and resulting improvements are significant. As this hospital is a national HIMSS Stage 6 healthcare provider, it bears testament to the effectiveness of the framework to generate such a significant net advancement of the organization's security and privacy.

2. *How do organizations provide documentation that the measures have been tested and work as intended whether for audit or attestation purposes?*

Building upon the proposed HISCF, this research presents a straightforward solution to documentation of compliance to be used for auditing or attestation requirements such as Meaningful Use. The assessment and testing tools all have clear, comprehensible output along with methods of measuring security and privacy effectiveness and adequacy. The Pennsylvania hospital has validated this claim by successfully completing Meaningful Use Stage 1 attestation using the products of this research.

3. *How can healthcare providers enable easy access to their EHR systems for patients while preserving security and privacy but also be financially viable?*

Providing easy, secure, and private patient access inexpensively to EHR systems is a critical need faced by tens of thousands of healthcare providers today. As discussed in Chapter 2, many experts agree that generically the Cloud is the natural solution to this issue. The Cloud quickly solves the 'easy' and 'inexpensive' challenges but there are still security and privacy requirements to consider. The National Institute for Standards and Technology (NIST) offered in 2011 that public Clouds are typically much more scalable

and reliable and possess superior infrastructure homogeneity [128]. Further, NIST purports that many of the public Cloud computing environments already are compliant with key federal regulations, including HIPAA. This research embraces these strengths and offers the Healthcare Federated Identity Framework (HFIF) to allow healthcare providers to integrate their respective EHR systems into the public Cloud. Therefore the proposed solution allows patients to use credentials they are intimately familiar with from other Cloud interactions with little to no cost to the healthcare provider. Once the Cloud providers can certify themselves against the Identity Assurance profiles laid out in the HFIF, that are built off of the federal guidelines for federated identity, the healthcare provider and patient alike can be confident that security and privacy have been adequately protected.

4. *How can patients access their medical information for all healthcare providers in a similar fashion, without needing provider-specific credentials?*

The HFIF proposes that it can easily scale from a relationship of one Cloud identity to one healthcare provider up to a many to many relationship as depicted in Figure 8. By leveraging the HFIF model for mapping Cloud credentials to EHR identities at a healthcare provider, there should be no limit to how many healthcare providers or Cloud identity providers could participate in the federation. NIST aptly points out in their Guidelines on Security and Privacy in Public Cloud Computing that one of the key advantages of public Clouds is the ability for other entities to easily integrate the Cloud's mature identity and access management systems [128]. The HFIF builds on this premise by proposing healthcare providers leverage federated authentication to their EHR systems using the Cloud-prevalent OpenID standard. Once

healthcare providers and Cloud identity providers are participating in a common federation, all participants can easily interoperate and thus patients could access multiple EHR systems using a single, familiar credential. The federated identity pilots underway at the Maryland hospital lay bare how the technology can work in real-world applications. Furthermore, the pilots show how healthcare providers can realize tangible benefits from the HFIF by significantly lowering their support costs related to patient access issues.

This dissertation's research was singularly focused on creating tangible solutions for applying technology more easily and more effectively to ultimately generate a better net outcome for patient and healthcare provider alike. As with so many theories, the proof is in the figurative pudding and as such this research has attempted to demonstrate its usefulness to the healthcare industry at two distinct healthcare providers. The collaboration with the partner hospitals suggests a degree of legitimacy and value of this research's contributions with documented improvements to security and privacy for these national healthcare providers. Additionally, this research provided the impetus to help one of those organizations complete the Meaningful Use Stage 1 objectives and generate significant financial compensation for the hospital. The key contributions of this research are as follows:

- The creation of the overarching Healthcare Information Security Compliance Framework (HISCF) that offers direction for organizations to plan and execute their overall HIPAA compliance efforts including Meaningful Use attestation,

- The creation of the Healthcare Information Security Guide (HISG) that provides comprehensive implementation level guidance that are directly mapped to HIPAA regulations and requirements,
- The creation of a set of assessment questionnaires and surveys, based off the guidelines set forth in the HISG, that comprehensively evaluate an organization's information technology architecture as well as policies and practices,
- The creation of the Healthcare Information Security Testing Directive (HISTD) and open source security testing toolkit for organizations to actively test their environment then mitigate any findings,
- The creation of the Healthcare Federated Identity Framework (HFIF) that assist healthcare providers to enable distributed electronic access to patient data and potentially realize significant reduction in related support, and
- The creation of a set of identity assurance profiles for Cloud Identity Providers to follow to ensure their practices conform to industry standards and meet HIPAA guidelines;
- Enhanced security and privacy for a national healthcare provider that enabled certification for Meaningful Use Stage 1.

There are many factors that contribute to the quality of healthcare delivery for patients. Accessibility, efficiency, and integrity are but some of those ingredients and while addressing these issues does not alone dictate success, ignoring or under valuing them will surely guarantee failure. The examination of the proposed Healthcare Information Security Compliance Framework and the Healthcare Federated Identity Framework through this case study suggest the solutions have the potential to improve

these areas of information security dramatically and raise the bar for healthcare delivery standards.

Appendices

Appendix 1. Summary of HIPAA Security Rules

Note: The descriptions below have been largely quoted and paraphrased from NIST Special Publication 800-66 (rev 1).

164.308(a)(1) – Security Management - *Implement policies and procedures to prevent, detect, contain, and correct security violations.*

164.308(a)(2) – Security Responsibilities - *Identify the security official who is responsible for the development and implementation of the security policies and procedures required for the entity.*

164.308(a)(3) - Workforce Security - *Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information and to prevent those workforce members who should not have access from obtaining access to ePHI.*

164.308(a)(4) – Access Management - *Implement policies and procedures for authorizing access to ePHI.*

164.308(a)(5) – Security Awareness and Training - *Implement a security awareness and training program for all members of its workforce (including management).*

164.308(a)(6) – Incident Response- *Implement policies and procedures to address security incidents.*

164.308(a)(7) – Contingency Plan - *Establish policies and procedures for responding to an emergency or disaster that damages systems that contain ePHI.*

164.308(a)(8) – Organizational Evaluation - *Perform a periodic technical and nontechnical evaluation of environmental or operational conditions that affect the security of ePHI.*

164.308(b)(1) – Business Associate Contracts or Other Arrangements - *Establish policies and procedures for allowing a business associate to create, receive, maintain, or transmit ePHI on the covered entity's behalf while appropriately safeguarding the information.*

164.310(a)(1) – Facility Access Controls - *Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.*

164.310(b) – Workstation Use - *Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access ePHI.*

164.310(c) – Workstation Security - *Implement physical safeguards for all workstations that access ePHI, to restrict access to authorized users.*

164.310(d)(1) – Device and Media Controls - *Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain ePHI into and out of a facility, and the movement of these items within the facility.*

164.312(a)(1) – Access Controls - *Implement technical policies and procedures for electronic information systems that maintain ePHI to allow access only to those persons or software programs that have been granted access rights.*

164.312(b) – Audit Controls - *Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI.*

164.312(c)(1) – Data Integrity - *Implement policies and procedures to protect ePHI from improper alteration or destruction.*

164.312(d) – Person or Entity Authentication - *Implement procedures to verify that a person or entity seeking access to ePHI is the one claimed.*

164.312(e)(1) – Transmission Security - *Implement technical security measures to guard against unauthorized access to ePHI that is being transmitted over an electronic communications network.*

Appendix 2. Proposed Cross Reference of Meaningful Use Objectives and HIPAA Security Rules

Stage 1	Stage 2	Relevant HIPAA Security Rule(s)																	
		164.308(a)(1)	164.308(a)(2)	164.308(a)(3)	164.308(a)(4)	164.308(a)(5)	164.308(a)(6)	164.308(a)(7)	164.308(a)(8)	164.308(b)(1)	164.310(a)(1)	164.310(b)	164.310(c)	164.310(d)(1)	164.312(a)(1)	164.312(b)	164.312(c)(1)	164.312(d)	164.312(e)(1)
Core Objectives																			
Computerized Provider Order Entry (CPOE)		■		■	■	■	■					■	■		■	■	■	■	■
E-Prescribing (eRx) (EPs ONLY)		■		■	■	■	■					■	■		■	■	■	■	■
Report ambulatory clinical quality measures to CMS/States	***Has been combined into another objective***	■														■	■		■
Implement one clinical decision support rule	Use clinical decision support to improve performance on high-priority health conditions																		
Provide patients with an electronic copy of their health information, upon request	Provide patients the ability to view online, download and transmit their health information (4 business days - EPs 36 hours - Hospitals)	■	■		■		■	■	■	■					■	■	■	■	■
Provide patients with an electronic copy of their discharge instructions at time of discharge, upon request (Hospitals ONLY)	***Objective removed in 2014 from Stage 1, combined into another objective for Stage 2***	■	■		■		■	■	■	■					■	■	■	■	■
Provide clinical summaries for patients for each office visit (EPs ONLY)		■	■	■	■	■	■		■			■	■		■	■	■	■	
Drug-drug and drug-allergy interaction checks	***Has been combined into another objective***																		
Record demographics		■	■	■	■	■	■		■	■		■	■	■	■	■	■	■	
Maintain an up-to-date problem list of current and active diagnoses	***Has been combined into another objective***																		
Maintain active	***Has been***																		

Stage 1	Stage 2	Relevant HIPAA Security Rule(s)																
		164.308(a)(1)	164.308(a)(2)	164.308(a)(3)	164.308(a)(4)	164.308(a)(5)	164.308(a)(6)	164.308(a)(7)	164.308(a)(8)	164.308(b)(1)	164.310(a)(1)	164.310(b)	164.310(c)	164.310(d)(1)	164.312(a)(1)	164.312(b)	164.312(c)(1)	164.312(d)	164.312(e)(1)
medication list	***combined into another objective***																		
Maintain active medication allergy list	***Has been combined into another objective***																		
Record and chart changes in vital signs		■	■	■	■	■	■		■	■		■	■	■	■	■	■	■	
Record smoking status for patients 13 years or older		■	■	■	■	■	■		■	■		■	■	■	■	■	■	■	
Capability to exchange key clinical information among providers of care	***Objective removed in 2013 from Stage 1, immediately from Stage 2***	■														■	■		■
Protect electronic health information		■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Drug-formulary checks	***Has been combined into another objective***																		
Incorporate clinical lab test results as structured data		■														■	■		■
Generate lists of patients by specific conditions		■		■	■	■	■								■	■	■	■	■
Send reminders to patients per patient preference for preventive/follow up care	Use certified EHR technology to identify and send reminders to patients per patient preference for preventive/follow up care	■		■	■	■	■								■	■	■	■	■
Provide patients with timely electronic access to their health information	***Objective removed in 2014 from Stage 1, immediately from Stage 2***	■		■	■	■	■								■	■	■	■	■
Use certified EHR technology to identify patient-specific education resources and provide to patient, if appropriate		■		■	■	■	■								■	■	■	■	■
Medication reconciliation																			
Summary of care record for each transition of care/referrals		■		■	■	■	■								■	■	■	■	■
Capability to submit electronic data to immunization registries/systems		■														■	■		■
NEW	Use secure electronic messaging to communicate with patients on	■		■	■	■	■								■	■	■	■	■

Stage 1	Stage 2	Relevant HIPAA Security Rule(s)																
		164.308(a)(1)	164.308(a)(2)	164.308(a)(3)	164.308(a)(4)	164.308(a)(5)	164.308(a)(6)	164.308(a)(7)	164.308(a)(8)	164.308(b)(1)	164.310(a)(1)	164.310(b)	164.310(c)	164.310(d)(1)	164.312(a)(1)	164.312(b)	164.312(c)(1)	164.312(d)	164.312(e)(1)
	relevant health information																		
Menu Objectives																			
Capability to provide electronic syndromic surveillance data to public health agencies		■														■	■		■
NEW	Record electronic notes in patient records	■		■	■	■	■				■	■	■	■	■	■	■	■	■
NEW	Imaging results consisting of the image itself and any explanation or other accompanying information are accessible through CEHRT	■		■	■	■	■				■	■	■	■	■	■	■	■	■
NEW	Record patient family health history as structured data	■		■	■	■	■				■	■	■	■	■	■	■	■	■
NEW	Capability to identify and report cancer cases to a State cancer registry, except where prohibited, and in accordance with applicable law and practice	■														■	■		■
NEW	Capability to identify and report specific cases to a specialized registry (other than a cancer registry), except where prohibited, and in accordance with applicable law and practice	■														■	■		■

Appendix 3. Healthcare Information Security Guideline (HISG)

http://bscoats.wordpress.com/dissertation-material/

Appendix 4. Healthcare Information Security Questionnaire (HISQ)

http://bscoats.wordpress.com/dissertation-material/

Appendix 5. Information Technology Architecture Review (ITAR)

http://bscoats.wordpress.com/dissertation-material/

Appendix 6. Healthcare Practitioner Survey - Questions & Responses

http://bscoats.wordpress.com/dissertation-material/

Appendix 7. Healthcare Information Security Testing Directive (HISTD)

http://bscoats.wordpress.com/dissertation-material/

Appendix 8. EHR Security and Privacy Assessment

http://bscoats.wordpress.com/dissertation-material/

Appendix 9. Identity Assurance Profiles for Identity Providers

http://bscoats.wordpress.com/dissertation-material/

Appendix 10. Complete Organizational Assessment Results

http://bscoats.wordpress.com/dissertation-material/

Bibliography

[1] United States. White House, "Health Reform in Action," 2010. [Online]. Available: http://www.whitehouse.gov/healthreform/healthcare-overview. [Accessed May 2012].

[2] United States. Department of Health and Human Services. Office of Civil Rights, "HIPAA Administrative Simplification," 2006. [Online]. Available: http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/adminsimpregtext.pdf. [Accessed 2011 November].

[3] United States. Department of Health and Human Services. Center for Medicare and Medicaid Services, "CMS EHR Meaningful Use Overview," 2012. [Online]. Available: https://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Meaningful_Use.html. [Accessed June 2012].

[4] United States. Department of Commerce. National Institute of Standards and Technology, "About NSTIC," 2012. [Online]. Available: http://www.nist.gov/nstic/about-nstic.html. [Accessed November 2012].

[5] United States. National Archives and Records Administration, "Title 45 – Public Welfare, Subtitle A – Department of Health and Human Services, Part 164 – Security and Privacy," 1996. [Online]. Available: http://www.access.gpo.gov/nara/cfr/waisidx_07/45cfr164_07.html. [Accessed April 2012].

[6] A. Appari, D. L. Anthony and M. E. Johnson, "HIPAA Compliance: An Examination of Institutional and Market Forces," Healthcare Information Management Systems Society, 2009.

[7] United States. Department of Health and Human Services. Center for Medicare and Medicaid Services, "Enforcement Results per Year," 2010. [Online]. Available: http://www.hhs.gov/ocr/privacy/hipaa/enforcement/data/historicalnumbers.html.

[Accessed November 2011].

[8] United States. Department of Health and Human Services. Center for Medicare and Medicaid Services, "Regulations and Guidance," 2004. [Online]. Available: https://www.cms.gov/home/regsguidance.asp. [Accessed November 2011].

[9] 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. [Online]. Available: http://csrc.nist.gov/publications/nistpubs/800-66-Rev1/SP-800-66-Revision1.pdf. [Accessed July 2011].

[10] HIMSS Analytics, "EMR Adoption Trends," 2014. [Online]. Available: http://www.himssanalytics.org/stagesGraph.asp. [Accessed May 2014].

[11] D. Blumenthal and M. Tavenner, "The “Meaningful Use” Regulation for Electronic Health Records," *New England Journal of Medicine,* vol. 363, pp. 501-504, 2010.

[12] United States. Department of HHS. The Office of the National Coordinator for Health Information Technology, "EHR Incentive Programs," 2012. [Online]. Available: http://www.healthit.gov/providers-professionals/ehr-incentive-programs. [Accessed February 2013].

[13] United States. Department of Health and Human Services. Center for Medicare and Medicaid Services, "Data and Reports," 2012. [Online]. Available: http://www.webcitation.org/6EMwIm36I. [Accessed July 2012].

[14] M. M. Helms, R. Moore and M. Ahmadi, "Information Technology (IT) and the Healthcare Industry: A SWOT Analysis," *International Journal of Healthcare Information Systems and Informatics,* vol. 3, no. 1, pp. 75-92, 2008.

[15] G. Annas, "HIPAA Regulations - A New Era of Medical-Record Privacy?," *New England Journal of Medicine,* vol. 348, pp. 1486-1490, 2003.

[16] Blue Cross Blue Shield Association, "HIPAA Return On Investment," National Committee on Vital Health Statistics, Subcommittee on Standards and Security, 2005.

[17] United States. Department of Health and Human Services, "45 CFR parts 160 and 164: Modifications to the HIPAA Privacy, Security, Enforcement and Breach Notification Rules Under the HITECH Act and the Genetic Information

Nondiscrimination Act: Other Modifications to the HIPAA Rules: Final Rule," 2013. [Online]. Available: http://gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf. [Accessed July 2013].

[18] R. D. Hirsch, "Final HIPAA Omnibus Rule brings sweeping changes to health care privacy law: HIPAA privacy and security obligations extended to business associates and subcontractors," *Bloomberg Bureau of National Affairs Heath Law Reporter,* vol. 415, pp. 1-11, 2013.

[19] United States. Department of Health and Human Services. Center for Medicare and Medicaid Services, "HIPAA Compliance Review Analysis and Summary of Results," 2008. [Online]. Available: http://www.hhs.gov/ocr/privacy/hipaa/enforcement/cmscompliancerev08.pdf. [Accessed October 2013].

[20] D. Solove, "HIPAA Turns 10: Analyzing the Past, Present, and Future Impact," *Journal of American Health Information Management Association,* vol. 84, no. 4, pp. 22-28, 2013.

[21] R. Fichman, R. Kohli and R. Krishnan, "The Role of Information Systems in Healthcare: Current Research and Future Trends," *Information Systems Research,* vol. 22, no. 3, pp. 419-428, 2011.

[22] J. Kwon and M. E. Johnson, "Healthcare Security Strategies for Regulatory Compliance and Data Security," in *Proceedings of the 46th Hawaii International Conference on System Sciences,* 2013.

[23] United States. Department of Health and Human Services. Office for Civil Rights, "Breach Notification Rule," 2009. [Online]. Available: http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html. [Accessed September 2013].

[24] T. Kayworth and D. Whitten, "Effective Information Security Requires a Balance of Social and Technology Factors," *MIS Quarterly Executive,* vol. 9, no. 3, pp. 163-175, 2010.

[25] S. Bharadwaj, A. Bharadwaj and E. Bendoly, "The Performance Effects of Complementarities Between Information Systems, Marketing, Manufacturing, and Supply Chain Processes," *Information Systems Research,* vol. 18, no. 4, pp. 437-453, 2007.

[26] Z. Xia and M. E. Johnson, "Access Governance: Flexibility with Escalation and Audit," in *Proceedings of the 43rd Hawaii International Conference on System Sciences*, 2010.

[27] M. E. Johnson, E. Goetz and S. L. Pfleeger, "Security through Information Risk Management," *IEEE Security & Privacy,* vol. 7, no. 3, pp. 45-52, 2009.

[28] S. Aral and P. Weill, "IT assets, organizational capabilities, and firm performance: How resource allocations and organizational differences explain performance variation," *Organization Science,* vol. 18, no. 5, pp. 763-780, 2007.

[29] HIMSS Analytics, "EMR Stage 7 Hospitals," 2011. [Online]. Available: http://www.himssanalytics.org/hc_providers/stage7Hospitals.asp. [Accessed October 2012].

[30] C. Clark, "Top 10 Healthcare Quality Issues for 2011," HealthLeaders Media, 2011. [Online]. Available: http://www.webcitation.org/6A1XB4Hc3. [Accessed June 2012].

[31] P. Chang, "Modeling the Management of Electronic Health Records in Healthcare Information Systems," in *Proceedings of the International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery*, 2011.

[32] W. Hersh, "Improving Health Care Through Information," *Journal of the American Medical Association,* vol. 288, no. 16, pp. 1955-1958, 2002.

[33] A. Appari and M. E. Johnson, "Information Security and Privacy in Healthcare: Current State of Research," *International Journal of Internet and Enterprise Management,* vol. 6, no. 4, pp. 279-314, 2010.

[34] D. Bates, M. Ebell, E. Gotlieb, J. Zapp and H. C. Mullins, "A Proposal for Electronic Medical Records in U.S. Primary Care," *Journal for American Medical Informatics Association,* vol. 10, pp. 1-10, 2003.

[35] J. Saleem, A. Russ, C. Justice, H. Hagg, P. Ebright, P. Woodbridge and B. Doebbeling, "Exploring the Persistence of Paper with the Electronic Health Record," *International Journal of Medical Informatics,* vol. 78, no. 9, pp. 618-628, 2009.

[36] D. Baumer, J. Earp and F. Payton, "Privacy of medical records: IT Implications of HIPAA," *ACM SIGCAS Computers and Society*, vol. 30, no. 4, pp. 40-47, 2000.

[37] W. Yina, "Application of EHR in Health Care," in *Proceedings of 2nd International Conference on Multimedia and Information Technology*, 2010.

[38] L. Røstad, Ø. Nytrø, I. Tøndel and P. Meland, "Access Control and Integration of Health Care Systems: An Experience Report and Future Challenges," in *Proceedings of the 2nd International Conference on Availability, Reliability and Security*, 2007.

[39] PricewaterhouseCoopers Health Research Institute, "Top Health Industry Issues of 2013," 2013. [Online]. Available: http://pwchealth.com/cgi-local/hregister.cgi/reg/pwc-hri-top-health-industry-issues-2013.pdf. [Accessed February 2013].

[40] F. Ueckert, M. Goerz, M. Ataian, S. Tessman and H. Prokosch, "Empowerment of patients and communication with health care professionals through an electronic health record," *International Journal of Medical Informatics,* vol. 70, pp. 99-108, 2003.

[41] T. T. May, "Medical information security: the evolving challenge," in *Proceedings of the 32nd Annual International Carnahan Conference on Security Technology*, 1998.

[42] United States. Department of Health and Human Services, "42 CFR parts 412, 412, and 495: Medicare and Medicaid Programs; EHR Incentive Program Stage 2; Standards, Implementation Specifications, and Certification Criteria for EHR Technology, 2014 Edition; Final Rules," 2013. [Online]. Available: http://www.gpo.gov/fdsys/pkg/FR-2012-09-04/pdf/2012-21050.pdf. [Accessed October 2013].

[43] V. S. Cheng, "Towards an integrated privacy framework for HIPAA-compliant Web services," in *Proceedings of 7th IEEE International Conference on E-Commerce Technology*, 2005.

[44] R. Jones, "Making health information accessible to patients," *Aslib Proceedings,* vol. 55, no. 5-6, pp. 334-338, 2003.

[45] M. Staroselsky, L. A. Volk, R. Tsurikova, L. Pizziferri, M. Lippincott, J. Wald and D. W. Bates, "Improving electronic health record (EHR) accuracy and increasing compliance with health maintenance clinical guidelines through patient access and input," *International Journal of Medical Informatics,* vol. 75, pp. 693-700, 2006.

[46] D. T. Gunter and P. N. Terry, "The Emergence of National Electronic Health Record Architectures in the United States and Australia: Models, Costs, and Questions," *Journal of Medical Internet Research,* vol. 7, no. 1, p. e3, 2005.

[47] Triple Space Communication, "Netherlands: Assessment of existing national e-health infrastructures," 2009. [Online]. Available: http://www.tripcom.org/docs/del/D8B.3.pdf. [Accessed October 2013].

[48] Örebro University Hospital, "National Patient Summary," 2012. [Online]. Available: http://www.flexlab.com/labdays/Ia%20Jansson%20NP%C3%96%20Malm%C3%B6%20090918.pdf. [Accessed October 2013].

[49] J. Weber-Jahnke and M. Price, "Engineering Medical Information Systems: Architecture, Data and Usability & Security," in *Proceedings of the 29th International Conference on Software Engineering*, 2007.

[50] H. Linden, D. Kalra, A. Hasman and J. Talmon, "Inter-organization future proof EHR systems-A review of the security and privacy related issues," *International Journal of Medical Informatics,* vol. 78, pp. 141-160, 2009.

[51] S. Sherlock and W. Chismar, "What Airline Reservation Systems Tell Us about the Future of EHRs," in *Proceedings of the 39th Hawaii International Conference on System Sciences*, 2006.

[52] R. Zhang and L. Liu, "Security Models and Requirements for Healthcare Application Clouds," in *Proceedings of the IEEE 3rd International Conference on Cloud Computing*, 2010.

[53] L. Beard, R. Schein, D. Morra, K. Wilson and J. Keelan, "The Challenges in Making Electronic Health Records Accessible to Patients," *Journal of American Medical Informatics Association,* vol. 19, pp. 116-120, 2012.

[54] D. B. Baker and D. R. Masys, "PCASSO: a design for secure communication of personal health information via the internet," *International Journal of Medical Informatics,* vol. 54, pp. 97-104, 1999.

[55] X. Li, Y. Xue and B. Malin, "Towards Understanding the Usage Pattern of Web-Based Electronic Medical Record Systems," in *Proceedings of the 2011 IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks*, 2011.

[56] A. Hassol, J. Walker, D. Kidder, K. Rokita, D. Young, S. Pierdon, D. Deitz, S. Kuck and E. Ortiz, "Patient Experiences and Attitudes about Access to a Patient Electronic Health Care Record and Linked Web Messaging," *Journal of American Medical Informatics Association,* vol. 11, pp. 505-513, 2004.

[57] W. Pratt, K. Unruih, A. Civan and M. Skeels, "Personal Health Information Management," *Communications of the ACM,* vol. 49, no. 1, pp. 51-55, 2006.

[58] United States. Department of Health and Human Services. Center for Medicare and Medicaid Services, "HIPAA Security Series – Security Standards: Technical Safeguards," 2007. [Online]. Available: http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/techsafeguards.pdf. [Accessed September 2011].

[59] C. J. Wang and D. J. Huang, "The HIPAA Conundrum in the Era of Mobile Health and Communications," *Journal of American Medical Association,* vol. 310, no. 11, pp. 1121-1122, 2013.

[60] B. Middleton, W. Hammond, P. Brennan and G. Cooper, "Accelerating U.S. EHR Adoption: How to Get There From Here," *Journal of American Medical Informatics Association,* vol. 12, pp. 13-19, 2005.

[61] A. Massey, P. Otto and A. Anton, "Aligning Requirements with HIPAA in the iTrust System," in *Proceedings of the 16th IEEE International Requirements Engineering Conference,* 2008.

[62] C. Lambrinoudakis, "Evaluating and enriching information and communication technologies compliance frameworks with regard to privacy," *Information Management and Computer Security,* vol. 21, no. 3, pp. 177-190, 2013.

[63] J. Kwon and M. E. Johnson, "Health-Care Security Strategies for Data Protection and Regulatory Compliance," *Journal of Management Information Systems,* vol. 30, no. 2, pp. 41-66, 2013.

[64] Kroll, "HIPAA Self Risk Assessment," 2013. [Online]. Available: http://www.krollcybersecurity.com/hipaa-risk-assessment/. [Accessed November 2013].

[65] Clearwater Compliance, "Achieve HIPAA HITECH Compliance," 2013. [Online]. Available: https://www.hipaasecurityassessment.com/. [Accessed November 2013].

[66] Health Information Trust Alliance, "Understanding and Leveraging the CSF," 2014. [Online]. Available: http://www.hitrustalliance.net/csf/. [Accessed March 2014].

[67] M. Delgado, "The Evolution of Health Care IT: Are Current U.S. Privacy Policies Ready for the Clouds?," in *Proceedings of the 2011 IEEE World Congress on Services*, 2011.

[68] United States. Department of Commerce. National Institute of Standards and Technology, "Risk Management Framework (RMF) Overview," 2013. [Online]. Available: http://csrc.nist.gov/groups/SMA/fisma/framework.html. [Accessed February 2014].

[69] Banking Industry Technology Secretariat, "BITS Publications," 2013. [Online]. Available: http://www.bits.org/publications/index.php. [Accessed March 2014].

[70] C. Harle and M. Dewar, "Factors in Physician Expectations of a Forthcoming Electronic Health Record Implementation," in *Proceedings of the 45th Hawaii International Conference on System Sciences*, 2012.

[71] United States. National Archives and Records Administration, "Federal Register, Vol. 78, No. 17, Part II – 45 CFR Parts 160 and 164," 1996. [Online]. Available: http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf. [Accessed October 2013].

[72] A. J. Bianchi, "An Overview of the Impact of the American Recovery and Reinvestment Act of 2009 on the HIPAA Medical Privacy and Security Rules," *Tax Management Compensation Planning Journal*, vol. 37, no. 9, pp. 227-236, 2009.

[73] R. Agrawal and C. Johnson, "Securing electronic health records without impeding the flow of information," *International Journal of Medical Informatics*, vol. 76, pp. 471-479, 2007.

[74] P. Tang, J. Ash, D. Bates, J. Overhage and D. Sands, "Personal health records: definitions, benefits, and strategies for overcoming barriers to adoption," *Journal of American Medical Informatics Association*, vol. 13, pp. 121-126, 2006.

[75] United States. Department of Commerce. National Institute of Standards and Technology, "Making Online Transactions Safer, Faster, and More Private," 2012. [Online]. Available: http://www.nist.gov/nstic. [Accessed October 2012].

[76] A. Mohan and D. M. Blough, "An Attribute-Based Authorization Policy Framework with Dynamic Conflict Resolution," in *Proceedings of the 9th Symposium on Identity and Trust on the Internet*, 2010.

[77] Internet2. InCommon, "What is the Assurance Program?," 2012. [Online]. Available: http://www.incommon.org/assurance/. [Accessed November 2012].

[78] United States. General Services Administration. Office of Government-wide Policy, "OpenID 2.0 Profile," 2009. [Online]. Available: http://www.idmanagement.gov/documents/ICAM_OpenID20Profile.pdf. [Accessed November 2012].

[79] Open Identity Exchange, "About Open Identity Exchange," 2012. [Online]. Available: http://openidentityexchange.org/about. [Accessed November 2012].

[80] EMR, EHR & HIT News, "Verizon Gives Health Care Identity Services a Booster Shot," 2011. [Online]. Available: http://www.emrandehrnews.com/tag/verizon-cloud/. [Accessed 1 August 2013].

[81] N. Dagdee and R. Vijaywargiya, "Credential based hybrid access control methodology for shared Electronic Health Records," in *Proceedings of the 2009 International Conference on Information Management and Engineering*, 2009.

[82] G. D. Katehakis, S. Sfakianakis, M. Tsiknakis and C. S. Orphanoudakis, "An Infrastructure for Integrated Electronic Health Record Services: The Role of XML (Extensible Markup Language)," *Journal of Medical Internet Research,* vol. 3, p. e7, 2001.

[83] W. B. Lee and C. D. Lee, "A cryptographic key management solution for HIPAA privacy/security regulations," *IEEE Transactions on Information Technology in Biomedicine,* vol. 12, no. 1, pp. 34-41, 2008.

[84] A. Wright and D. Sittig, "Encryption Characteristics of Two USB-based Personal Health Record Devices," *Journal of American Medical Informatics Association,* vol. 14, pp. 397-399, 2007.

[85] J. Hu, H. H. Chen and T. W. Hou, "A hybrid public key infrastructure (HPKI) solution for HIPAA privacy/security regulations," *Computer Standards and Interfaces,* vol. 32, no. 5-6, pp. 274-280, 2010.

[86] S. Tanimoto, M. Yokoi, H. Sato and A. Kanai, "Quantifying Cost Structure of Campus PKI," in *Proceedings of the 2011 IEEE/IPSJ International Symposium on*

Applications and the Internet, 2011.

[87] R. Bhatti, A. Samuel, M. Eltabakh, H. Amjad and A. Ghafoor, "Engineering a Policy-Based System for Federated Healthcare Databases," *IEEE Transactions on Knowledge and Data Engineering,* vol. 19, no. 9, pp. 1288-1304, 2007.

[88] G. Gardarin, S. Gannouni and B. Finance, "A Distributed System Federating Object and Relational Databases," in *Object-Oriented Multi-Database System: A Solution for Advanced Applications*, Prentice Hall, 1995.

[89] D. Daglish and N. Archer, "Electronic Personal Health Record Systems: A Brief Review of Privacy, Security, and Architectural Issues," in *Proceedings of the 2009 World Congress on Privacy, Security, Trust, and the Management of e-Business*, 2009.

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

[91] United States. Department of Commerce. National Institute of Standards and Technology, "Technical Guide to Information Security Testing and Assessment," 2008. [Online]. Available: http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf. [Accessed June 2012].

[92] United States. Department of Commerce. National Institute of Standards and Technology, "Guide for Assessing the Security Controls in Federal Information Systems and Organizations (rev 1)," 2010. [Online]. Available: http://csrc.nist.gov/publications/nistpubs/800-53A-rev1/sp800-53A-rev1-final.pdf. [Accessed July 2011].

[93] Canonical Ltd, "Ubuntu Desktop," 2014. [Online]. Available: http://www.ubuntu.com/download/ubuntu/download. [Accessed 9 June 2014].

[94] Tenable, "Nessus," 2014. [Online]. Available: http://www.tenable.com/products/nessus. [Accessed 9 June 2014].

[95] BackTrack Linux, "BackTrack 5," 2013. [Online]. Available: http://www.BackTrack-linux.org/downloads/. [Accessed 9 June 2014].

[96] NMAP.org, "NMAP," 2013. [Online]. Available: http://nmap.org/. [Accessed 9 June 2014].

[97] The Hackers Choice, "THC-AMAP," April 2011. [Online]. Available: http://www.thc.org/thc-amap/. [Accessed 9 June 2014].

[98] Portcullis Labs, "enum4linux," 16 September 2008. [Online]. Available: http://labs.portcullis.co.uk/application/enum4linux/. [Accessed 9 June 2014].

[99] J. Jetmore, "Swaks - Swiss Army Knife for SMTP," 9 February 2013. [Online]. Available: http://www.jetmore.org/john/code/swaks/. [Accessed 9 June 2014].

[100] Sourceforge, "SSLScan - Fast SSL Scanner," 24 April 2013. [Online]. Available: http://sourceforge.net/projects/sslscan/. [Accessed 9 June 2014].

[101] Bluediving, "Bluediving," 27 December 2007. [Online]. Available: http://bluediving.sourceforge.net/. [Accessed 9 June 2014].

[102] Aircrack-NG, "Aircrack-NG," 2013. [Online]. Available: http://www.aircrack-ng.org/. [Accessed 9 June 2014].

[103] BackTrack Linux, "Pentesting VOIP," 12 June 2011. [Online]. Available: http://www.BackTrack-linux.org/wiki/index.php/Pentesting_VOIP#SMAP. [Accessed 9 June 2014].

[104] A. Sotirov, "Security Research," 2011. [Online]. Available: http://www.phreedom.org/software/onesixtyone/. [Accessed 9 June 2014].

[105] SQLMAP.org, "sqlmap," 2014. [Online]. Available: http://sqlmap.org/. [Accessed 9 June 2014].

[106] Strategic Cyber LLC, "Armitage," 2014. [Online]. Available: http://www.fastandeasyhacking.com. [Accessed 9 June 2014].

[107] The Hackers Choice, "THC-Hydra," 12 May 2014. [Online]. Available: http://www.thc.org/thc-hydra/. [Accessed 9 June 2014].

[108] w3af.org, "w3af," 2013. [Online]. Available: http://w3af.sourceforge.net/. [Accessed 9 June 2014].

[109] Sourceforge, "Uniscan," 18 August 2012. [Online]. Available: http://sourceforge.net/projects/uniscan/. [Accessed 9 June 2014].

[110] C. Sullo and D. Lodge, "Nikto2," 2014. [Online]. Available: http://cirt.net/nikto2. [Accessed 9 June 2014].

[111] PortSwigger Ltd, "Burp Suite," 2014. [Online]. Available: http://portswigger.net/burp/. [Accessed 9 June 2014].

[112] K. Houghton, "Vulnerabilities and Vulnerability Scanning," System Administration Networking, and Security (SANS) Reading Room, 2003. [Online]. Available: http://www.sans.org/reading_room/whitepapers/threats/vulnerabilities-vulnerability-scanning_1195. [Accessed January 2013].

[113] C. Brackin, "Vulnerability Management: Tools, Challenges and Best Practices," System Administration Networking, and Security (SANS) Reading Room, 2003. [Online]. Available: http://www.sans.org/reading_room/whitepapers/threats/vulnerability-management-tools-challengespractices_1267. [Accessed December 2012].

[114] M. Chan, I. Woon and A. Kankanhalli, "Perceptions of Information Security in the Workplace: Linking Information Security Climate to Compliant Behaviour," *Journal of Information Privacy & Security*, vol. 1, no. 3, pp. 18-41, 2005.

[115] United States. Department of Commerce. National Institute of Standards and Technology, "Electronic Authentication Guide (rev 1)," 2011. [Online]. Available: http://csrc.nist.gov/publications/nistpubs/800-63-1/SP-800-63-1.pdf. [Accessed December 2011].

[116] United States. Executive Office of the President. Office of Management and Budget, "M-04-04: E-Authentication Guidance for Federal Agencies," 2003. [Online]. Available: http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy04/m04-04.pdf. [Accessed March 2012].

[117] United States. General Services Administration. Office of Government-wide Policy, "Federal Identity, Credential, and Access Management," 2012. [Online]. Available: http://www.idmanagement.gov/pages.cfm/page/ICAM. [Accessed November 2012].

[118] United States. Department of Health and Human Services. Centers for Medicare & Medicaid Services, "CMS System Security and e-Authentication Assurance Levels by Information Type," 2011. [Online]. Available: http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Downloads/System-Security-Levels-by-

Information-Type.pdf. [Accessed November 2012].

[119] OpenID Foundation, "What is OpenID?," 2012. [Online]. Available: http://openid.net/get-an-openid/what-is-openid/. [Accessed November 2012].

[120] M. Gibbs and H. Quillen, "The Medical-Grade Network: Helping Transform Healthcare," CISCO, 2007. [Online]. Available: http://www.webcitation.org/6A1Wip07P. [Accessed August 2012].

[121] dotnetopenid, "DotNetOpenAuth," Google, 2014. [Online]. Available: https://code.google.com/p/dotnetopenid/. [Accessed April 2014].

[122] S. Cannoy and A. F. Salam, "A Framework for Health Care Information Assurance Policy and Compliance," *Communications of the ACM,* vol. 53, no. 3, pp. 126-131, 2010.

[123] United States. Department of Commerce. National Institute of Standards and Technology, "Guide for Conducting Risk Assessments," 2012. [Online]. Available: http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf. [Accessed December 2012].

[124] United States. Department of Commerce. National Institute of Standards and Technology, "Creating a Patch and Vulnerability Management Program," 2005. [Online]. Available: http://csrc.nist.gov/publications/nistpubs/800-40-Ver2/SP800-40v2.pdf. [Accessed October 2013].

[125] Jasig, "CAS," 2012. [Online]. Available: http://www.jasig.org/cas. [Accessed December 2012].

[126] Microsoft, "Windows Server: Active Directory Federation Services," 2012. [Online]. Available: http://technet.microsoft.com/en-us/windowsserver/dd448613. [Accessed December 2012].

[127] Internet2, "Social and Organizational Identities Discussion Space," 2012. [Online]. Available: https://spaces.internet2.edu/display/socialid/Home. [Accessed December 2012].

[128] United States. Department of Commerce. National Institute of Standards and Technology, "Guidelines for Security and Privacy in Public Cloud Computing," 2011. [Online]. Available: http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf. [Accessed December 2013].

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

[130] PricewaterhouseCoopers Health Research Institute, "Top Health Industry Issues of 2012," 2011. [Online]. Available: http://pwchealth.com/cgi-local/hregister.cgi/reg/top-health-industry-issues-of-2012.pdf. [Accessed May 2012].

Curriculum Vitae

BRIAN S. COATS

March 18, 2014

Business:
Director, Identity Mgmt & Sys Integration Planning
Center for Information Technology Services
University of Maryland, Baltimore
601 West Lombard Street, Suite 540
Baltimore, Maryland 21201
410.706.3070 (office)
bscoats@umaryland.edu

Home:

EDUCATION

- Master of Science, Information Technology, University of Maryland, University College, May 2005. Thesis: Analysis of an Enterprise Identity Management solution. Advisor: Dr. Carlo J. Broglio.

- Graduate Certificate, Information Technology, University of Maryland, University College, December 2004.

- Bachelor of Science, Aerospace Engineering, University of Maryland, College Park, May 2000.

PROFESSIONAL EXPERIENCE

Director, Identity Management and System Integration Planning

University of Maryland, Baltimore, 4/10 - Present

- Member of the senior leadership team of the institution-wide information technology (IT) department, providing leadership and direction for the following groups: Directory Services, Identity Management, Helpdesk, and Software Licensing.
- Coordinate with executive leadership and technical representatives throughout university community (7 schools, 2 divisions, and 8 corporate entities) to assess IT needs/requirements, ensure compatibility and integrity, and foster partnerships.
- Develop IT governance plans and protocols that advance the university's missions with significant attention on security/audit compliance.
- Identify, evaluate, and address opportunities for internal process improvement, mitigation of complex business and technology risks, and overall enhancement of institution's ability to collaborate internally and externally while addressing security and risk management.
- Active contributor to EDUCAUSE, Internet2, and NMI-EDIT middleware initiatives including Shibboleth, InCommon, and eduPerson/Org/Course LDAP standards. Significant fluency and experience working with federal regulations and standards related to privacy, security, and data integrity including FERPA, HIPAA, NIST SP800-63 eAuth, NIST SP800-53 Access Control, ICAM LOA guidelines, and ICAM IMI Profiles.

Senior Information Technology Architect

University of Maryland, Baltimore, 4/04 – 4/10

- Primary architect and project manager for team responsible for multi-institutional Directory Services and Identity and Access Management (IAM) initiatives for 48,000+ user community – current position (Director, IdM and Sys Integration Planning) is the result of an expansion of the group managed as Senior IT Architect (many similar duties/roles after promotion).
- Provide full life cycle project management for the following ongoing initiatives:
    - *Directory Services*, built on Novell's eDirectory, incorporates industry and Internet2 LDAP standards, used for central authentication source by more than 80 internal applications, 16 inter-institutional and federal government applications, leverages Shibboleth for WebSSO.
    - *Identity Management*, built with custom VBScript applications, receives feeds from 4 authoritative sources and has awareness of

21 independent applications, maintains 35,000+ active users' identity for each connected system. Custom integration was built specifically for the each application, of note include: Blackboard (OneCard, Learning System), PeopleSoft (HRMS, Financials and Grants, Enterprise Portal), Sunguard SCT Banner, COEUS, MAXIMUS, ImageNow, ARCHIBUS, e2Campus Alerts, iTunes University, MediaSite, Google Mail, Sympa ListServ, and Accellion Secure File Transfer.

- Planned, designed, and implemented a campus-wide Portal. Built on PeopleSoft's Enterprise Portal 8.8, utilizes the enterprise directory for authentication, provides SSO for PeopleSoft HRMS, PeopleSoft Financials and Grants, and a custom financial reporting application, serves as launching point for all enterprise applications that leverage Directory Services – around 100 applications.
- Active contributor in EDUCAUSE, Internet2, and NMI-EDIT, middleware initiatives including Shibboleth, InCommon, and eduPerson/Org/Course LDAP standards. Significant fluency and experience working with federal regulations and standards related to privacy, security, and data integrity including FERPA, HIPAA, NIST SP800-63 eAuth, NIST SP800-53 Access Control, ICAM LOA guidelines, and ICAM IMI Profiles.

Information Technology Coordinator

University of Maryland, College Park, 5/01 – 4/04

- Technical manager for IT group responsible for the Email/Calendaring system and Online Course delivery as well as provided support for Portal services, enterprise LAN of 30+ servers and 3500+ user community, and Technical Training/Orientation. Provided supervision and direct training for staff, including all typical personnel issues (hiring/terminating, budget, conflict resolution, and performance review).
- Performed full life cycle project management for information technology including:
    - *Network Architecture Design*, including capacity/scalability and performance, clustering (hardware and application) for load-balancing and fail-over, and wired/wireless network communication (TCP/IP, IPX, WAP).
    - *Security*, including intrusion detection, vulnerability assessment, encryption (PKI, DES, PGP, digital signatures/envelopes/certificates, WEP), firewalls, VPN, and virus protection.
    - *Systems Integration*, including integration of legacy systems/software, Single Sign-On, and directory architecture (LDAP migration/manipulation)

    - *Application Development*, including programming web services and software enhancements.
- Evaluated new technologies that related to the current computing environment, including infrastructure hardware, collaborative software, portal technologies/services, network security & auditing, and systems integration tools.
- Performed audit and assessment of current computing environment technologies (hardware/software) and business practices to ensure productivity, reliability, and future scalability. This included quality assurance/assessment, risk analysis, and documentation.
- Worked with faculty members to integrate technology into their curricula and classroom environment. This relationship included providing an on-line capability for course information, live on-line discussion groups, and live on-line lectures, as well as video conferencing (virtual classrooms). The span of this task covered more than 175 faculty/adjunct spread between the main campus and 3 remote distance learning locations (Washington DC, Baltimore, MD, and Shady Grove, MD).

Lotus Administrator

Robert H. Smith School of Business, 9/99 – 5/01

- Managed staff of 5, responsible for college-wide email/calendaring (Lotus Notes), on-line course system (Lotus Notes & Blackboard), network data storage, and LAN security/integrity.
- Administered 3000+ user network using Lotus Notes 4.5x, 4.6x, 5.0x, iNotes on Novell/NT network.
- Extensive development and programming experience: Lotus Domino, HTML, LotusScript, relational database enterprise-wide applications.
- Created, organized, and supervised the college-wide Technology Orientation program. Each target group (undergraduate, graduate, PhD, Faculty, Staff, and Adjunct) had a tailored orientation designed to provide useful information and training pertaining to their affiliation with the college. This program covered a range of technical, logistical, and personnel topics.

System Administrator/Technician

Robert H. Smith School of Business, 8/98 – 9/99

- Installed and managed LAN: servers, workstations, and audio/video equipment.
- Maintained 3000+ user network running on mixed network OS (Novell NDS/NT, Unix).

- Created and implemented software/hardware configurations (images) for 7 lab environments.
- Implemented upgrades for hardware/software, as well as user-level support.

Hardlines Manager

The Sports Authority, 9/96 – 11/98

- Led team of 20 at regional store for the largest and only national full-line sporting goods retailer at the time. This task included employee product education, customer service training and quality assurance, as well as all relevant personnel issues (hiring/terminating, budget, conflict resolution, and performance reviews).
- Responsible for sales, marketing, and inventory of over $15 million in merchandise.
- Ensured a high level of customer/employee satisfaction through corporate secret-shopper programs, personally devised sales incentive programs and product education incentive programs. Received highest customer satisfaction rating for 17-store district – awarded 5 months during a 14-month span.

PROFESSIONAL AFFILIATIONS AND ACTIVITIES

- National Strategy for Trusted Identities in Cyberspace (NSTIC) Identity Ecosystem Steering Group, Voting Member - 2012 to Present
- EDUCAUSE, Institutional Participating Member - 2004 to Present
- Internet2, Institutional Participating Member - 2004 to Present
- 47th Hawaii International Conference on System Sciences, Reviewer - 2013
- 46th Hawaii International Conference on System Sciences, Reviewer - 2012
- Institute for Electrical and Electronic Engineers (IEEE) Computer Society, Member - 2009 to Present
- Order of the Engineer – University of Maryland, College Park Link, Member - 2000 to Present
- American Institute of Aeronautics and Astronautics (AIAA), Member - 2000 to Present

HONORS

- Omicron Delta Kappa, National Leadership Honor Society, October 2013.
- College Park Scholars Citation – Science, Technology, and Society Discipline, September 1997.

TEACHING EXPERIENCE

Trainer
University of Maryland, College Park, 2/03 – 2/04
Instructed full-time and adjunct faculty members on the use of the Blackboard Learning System. This task included training the faculty on the features of the software as well as how best to incorporate an online presence into their curricula. This position included providing an on-line capability for course information, live on-line discussion groups, and live on-line lectures, as well as video conferencing (virtual classrooms). The span of this task covered more than 175 faculty/adjunct spread between the main campus and 3 remote distance learning locations (Washington DC, Baltimore, MD, and Shady Grove, MD).

Instructor, Certified
Robert H. Smith School of Business, 10/01 – 6/02
Provided technical training on the use of varying suites of IBM Lotus software. Format of instruction included lectures and hands-on sessions.

Trainer/Coordinator
Robert H. Smith School of Business, 1/00 – 9/02
Created curricula, organized, and ran the college-wide Technology Orientation program. The program was tailored for four target groups: undergraduate students; graduate students; PhD students; Faculty, Staff, and Adjuncts. The content covered a range of technical, logistical, and personnel topics pertaining to their affiliation with the college.

Director/Instructor
United States Air Force Auxiliary, Civil Air Patrol – Middle East Region Leadership Academy, 6/97 – 7/00
Created curricula, lectured, recruited other instructors (civilians, active military personnel, and military reservists), organized, and ran 80 hour leadership program for middle and high school students. This program taught effective speaking, effective writing, teamwork, and leadership through military principles.

PUBLICATIONS

S. Acharya, B. Coats, A. Saluja, and D. Fuller. (2014). "From Regulations to Practice: Achieving Information Security Compliance in Healthcare," *Proceedings of the 2014 Human Computer Interaction International Conference.* Creta Maris, Heraklion, Crete, Greece.

B. Coats and S. Acharya. (2014). " Leveraging the Cloud for Electronic Health Record Access," *Perspectives in Health Information Management (Winter 2014)*: 1-19.

B. Coats and S. Acharya. (2014). "Bridging Electronic Health Record Access to the Cloud," *Proceedings of the 47th Hawaii International Conference on System Sciences.* Waikoloa, Hawaii.

S. Acharya, B. Coats, A. Saluja, and D. Fuller. (2013). "A Roadmap for Information Security Assessment for Meaningful Use," *Proceedings of the 2013 IEEE/ACM International Symposium on Network Analysis and Mining for Health Informatics, Biomedicine and Bioinformatics.* Shanghai, China.

B. Coats and S. Acharya. (2013). "The Forecast for Electronic Health Record Access: Partly Cloudy," *Proceedings of the 2013 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining.* Niagara Falls, Canada.

B. Coats and S. Acharya. (2013). "Achieving Electronic Health Record Access from the Cloud," *Proceedings of the 2013 Human Computer Interaction International Conference.* Las Vegas, Nevada.

S. Acharya, B. Coats, A. Saluja, and D. Fuller. (2013). "Secure Electronic Health Record Exchange: Achieving the Meaningful Use Objectives," *Proceedings of the 46th Hawaii International Conference on System Sciences.* 46, 253-262. doi 10.1109/HICSS.2013.473.

B. Coats, S. Acharya, A. Saluja, and D. Fuller. (2012). "HIPAA Compliance: How Do We Get There? A Standardized Framework for Enabling Healthcare Information Security & Privacy," *Proceedings of the 16th Colloquium for Information Systems Security Education.* Orlando, Florida.

PRESENTATIONS

2013, August. *The Forecast for Electronic Health Record Access: Partly Cloudy*. 2013 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining, Niagara Falls, Canada.

2013, July. *Achieving Electronic Health Record Access from the Cloud.* 2013 Human Computer Interaction International Conference, Las Vegas, Nevada.

2013, January. *UM Community System: Expanding Identity Boundaries.* 2013 EDUCAUSE Mid-Atlantic Regional Meeting, Baltimore, Maryland.

2013, January. *Secure Electronic Health Record Exchange: Achieving the Meaningful Use Objectives*. 2013 46th Hawaii International Conference on System Sciences, Maui, Hawaii.

2012, June. *HIPAA Compliance: How Do We Get There? A Standardized Framework for Enabling Healthcare Information Security & Privacy*. Colloquium for Information Systems Security Education, Orlando, Florida.

2012, January. *Self-Service Identity: Join the Community*. 2012 EDUCAUSE Mid-Atlantic Regional Meeting, Baltimore, Maryland.

2006, June. *Portals and Identity Management: How Do They Fit Together?* Portal 2006, Gettysburg College, Pennsylvania.