17801 – Privacy Policy, Law and Technology
Carnegie Mellon University
Fall 2005 – 12.09.05

Cost of Privacy: A HIPAA perspective

Richa Arora
richaa@andrew.cmu.edu

Mark Pimentel
mpimente@andrew.cmu.edu

Abstract

For many organizations, HIPAA compliance is a considerable and organization-wide effort. The process requires a great deal of planning, expertise, and manpower, all of which can be extremely expensive. It is therefore very important for affected organizations to evaluate implementation decisions with a careful eye on their financial capabilities. By thoroughly analyzing the costs of hospitals that have gone through the compliance process, we hope to analyze key financial decisions and educate future compliance efforts.

Introduction

The Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191 was introduced in 1996 to improve the overall state of health insurance and health care. It included the Administrative Simplification provisions, which mandates a number of changes in the way that health care organizations handle patient health information (PHI).

HIPAA has stimulated considerable attention and controversy within the health care industry. The general goals of HIPAA are to improve portability and continuity of health insurance coverage and delivery. A portion of it, known as Subtitle F, has developed into HIPAA's privacy, security, and transaction and code sets rules. These privacy regulations, which became effective on April 14, 2001 and were required to be implemented by April 14, 2003, govern the use and release of personally identifiable medical information.

For affected organizations, HIPAA compliance can be a costly, Herculean task. In fact, many of these efforts have been compared with Y2K preparations in terms of their impact and costs. Surveys project upgrade costs to vary from $10,000 for a small private practice to $14 million for a larger organization (Nunn, McGuire, 2005). The average cost of $3.1 million from surveyed firms is considerably more expensive than the projected average estimate of $450,000 that was done prior to implementation.

Given these cost variances, it is paramount to understand the costs of implementing HIPAA and the benefits arising from these investments. This paper examines the cost of HIPAA compliance for hospitals. We analyze a variety of expenses, from the costs of policy and organizational changes, to information system purchases. We also estimate future costs of compliance resulting from changes that are made possible by HIPAA, such as revisions in health care operations, policy, or technology.

Outline

We begin our analysis by carefully examining and classifying related HIPAA compliance costs in the *Framework for Analyzing Costs of HIPAA Compliance* section. This allows us to establish a shared and comprehensive set of expenses that will be referenced and explored in later sections.

In *A Study of Pittsburgh Hospitals*, we examine costs at the state level by analyzing surveys done at the University of Pittsburgh. These results, from a sampling of 250 hospitals, give us an adequate set of aggregate information in which to compare later and more specific facts to.

Industry Experience presents material from interviews conducted with HIPAA Privacy Directors from hospitals in the Pittsburgh, PA area.

All of the information we've gathered is studied and explored in *Analysis & Discussion*. In this section, we again reference our framework to make sure that we discuss all of the relevant costs that we've previously identified.

Framework for Analyzing Costs of HIPAA Compliance

HIPAA compliance costs cover a bewildering array of expenses, from training and hiring processes, to the purchasing of new information systems. For an unseasoned health information manager, managing these costs can be daunting and frightening. We attempt to alleviate these problems by carefully classifying and dissecting the most common expenses. They will be analyzed in further detail in a later section.

From speaking with industry professionals and conducting research on the field, we have classified costs into three broad categories:

- **Administrative costs** cover organizational process changes, reevaluations, and the creation of policies. It includes follow-up gap analyses to ensure that compliance efforts are successful, and the maintenance of business continuity plans like backup and recovery facilities. Additionally, it covers personnel-related expenses like hiring and training costs.

- **Technical security costs** are concerned with the technology and systems necessary to safeguard health information systems from intrusion, attack, and other privacy violations. It includes the purchasing costs of secure systems and software, as well as the ongoing maintenance costs of the facility's information technology systems.

- **Physical security costs** are concerned with the costs of creating physical privacy safeguards of patient data. This includes surveillance equipment to monitor data accesses and retrievals, as well as locks and other intrusion-prevention devices. Additionally, with the rise of next-generation authorization equipment, like biometric sensors, many hospitals are incurring costs for these technologies as well.

A Study of Pittsburgh Hospitals

In our efforts to study overall HIPAA costs, we found it useful to first examine HIPAA implementation at a smaller scale by contacting hospitals in the Pittsburgh area, talking with their privacy officers, and learning about their specific needs and challenges. Pittsburgh is a great sample city for this study, as it offers a mix of world-class hospitals, like the renowned University of Pittsburgh Medical Center (UPMC), and much smaller facilities like the Western Pennsylvania Hospital.

A good source of information for this cross-section is a questionnaire administered in early 2003 by Patricia Firouzan, MSIA, RHIA at the University of Pittsburgh, and James McKinnon of the Children's Hospital of Pittsburgh. They sent a 20-question survey to over 250 Pennsylvania hospitals' health information managers (HIMs), addressing various topics from privacy training, HIPAA effectiveness, and additional staffing requirements (Firouzan, 2004).

The overwhelming trend in the responses is that HIPAA costs are substantial, but manageable. Many surveyed hospitals worked hard to implement the necessary changes in the late winter of 2003 (the deadline was April of that year), and most reported that they were compliant with between a fourth to half of all requirements. Many of the changes made were related to training procedures and administrative processes. Staffing levels, on the other hand, did not fluctuate very much; only 29 percent of respondents saw the need to add new staff, and most HIPAA privacy obligations were given as additional responsibilities to existing personnel. (Firouzan, 2004)

Training costs are likely significant. Though the survey does not ask for any detailed figures, most HIMs report classes, pamphlets, and informal training procedures. Most facilities report training sessions which last from one to four hours. Though we do not have data on who teaches these classes, when they occur, or how many employees are taught at once, it is likely that there are significant costs in gathering willing students and a capable instructor together. (Firouzan interview, 2005)

Another obvious cost is in the hiring of external consultants. Many surveyed hospitals did not have the resources or expertise to deal with HIPAA implementations; in fact, 44 percent of respondents reported hiring help. One interesting fact to note is that 45% of mid-to-small hospitals used consultants, while only 33% of larger ones did. This compounds the idea that smaller entities, with less experience, have more significant costs to overcome than their larger counterparts. (Firouzan, 2004)

Most HIPAA privacy responsibilities were given to existing resources, rather than new ones. In 41 percent of facilities, privacy obligations were given to the existing HIM director. 25 percent of respondents appointed the existing corporate compliance officer as the privacy officer. Though many of these arrangements were likely done as a cost savings, it is not clear how they will affect existing obligations and tasks. Stretching personnel too thinly will likely create problems in other areas, and reduce the overall quality of security and privacy compliance. (Firouzan, 2004)

In our discussions with Ms. Firouzan, she highlighted the fact that most organizations would use existing personnel to absorb additional HIPAA-related duties. Additionally, she emphasized that training costs would be a significant repeating cost. The trend on training seems to be retraining exercises after every two years. (Firouzan interview, 2005)

Industry Experience

Introduction

We contacted a handful of local Pittsburgh hospitals to gain first-hand knowledge on HIPAA implementation costs and expenses. Aside from phone calls and e-mails, we also sent out a questionnaire to certain institutions with a few basic questions regarding their HIPAA expenses. This survey is attached as Appendix A.

Our first goal in this experience was to meet with real privacy officers to understand their concerns and experiences. We wanted to learn about their budgets, get input on their feelings towards these expenses, and gauge how effectively money was being spent towards HIPAA implementation. We felt that only by meeting with privacy officers, who were on the front lines of HIPAA compliance, could we measure the true successes and failures of these practices.

Children's Hospital of Pittsburgh

The Children's Hospital of Pittsburgh (CHP) is the only independent hospital in Western Pennsylvania that is dedicated to the care of children and infants. It is consistently considered one of the top 10 pediatric case centers in the United States, and is a subsidiary of the University of Pittsburgh Medical Center (UPMC) Health System.

According to Jodi Innocent, former Chief Privacy Officer at the Children's Hospital of Pittsburgh, HIPAA compliance costs are generally budgeted with other compliance costs. In total, she estimates that the Children's Hospital of Pittsburgh has spent approximately $88,000 to develop and implement HIPAA compliance. $43,500 of this was for a software program that would track disclosures.

In fact, the Children's Hospital of Pittsburgh is spending a great deal of money on technology. At its new $500 million hospital, technologies like electronic signature and single sign-on are being implemented to create a more modern facility. The new environment is expected to be a paper-less environment, which will drastically reduce the chance of information being left unprotected.

One significant cost incurred at the Children's Hospital of Pittsburgh has been related to HIPAA promotion and education. Privacy practice notices have been reproduced and plastered all over the walls at the CHP to remind everyone about new administrative procedures and a continuing dedication to patient privacy. Events like the annual "HIPAA Awareness Week" also promote HIPAA. This particular event takes yearly during the week of April 14 (the original HIPAA compliance deadline) and involves training sessions, games on the web page, and additional notices in the hospital newsletter. These particular items were budgeted as $5000 last year.

The Children's Hospital of Pittsburgh is extremely aware that HIPAA compliance is an ongoing process. When asked about their progress, Ms. Innocent stated, "Like all things in health care, I never—and don't think that anyone else—anticipated that we'd be all done with HIPAA on April 14. We will always have to revise policies, procedures, practices, and systems to keep up with the ever-changing technology and environment."

Magee Women's Hospital

Magee Women's Hospital is dedicated to providing excellent health care to women. It is one of only five women's non-profit hospitals in the United States, and is a leading institution in obstetrics, gynecology, and neonatology. They are also a member of the University of Pittsburgh Medical Center (UPMC) Health System.

We spoke with Ann Mathias, Chief Privacy Officer of this institution. She says that so far, the costs for the privacy part of HIPAA have not been significant. However, there have been considerable expenses budgeted for HIPAA security, since that aspect necessitates software maintenance costs.

At Magee, HIPAA is not even a line item on the budget any more. In previous years, there had been a cost center for HIPAA, but after the initial changes, the budgets have been coming down and it is not needed to budget specifically for this cost center.

We could not get the exact figures of the expense on compliance efforts at Magee, but learned that Magee completed the compliance steps without the help of an external consultant. This is an expense that many other hospitals did not have the ability to avoid.

Mercy Hospital

At Mercy Hospital of the Pittsburgh Mercy Health System, the HIM director doubles up as Privacy Officer. We spoke to Frances Ciamacco, Privacy Officer at Mercy, who informed us that recruiting a Privacy officer would have cost Mercy at least $75,000 per year.

Mercy hospital is still in the process of implementing all the standards prescribed in HIPAA. Their first priority was to deal with items that are extremely client-facing, such as the education and training of medical staff. Mercy is still working on establishing audit trails as required by the Privacy Rule.

Ms. Ciamacco could not provide the exact amount that was spent on compliance or is being spent because the budget for HIPAA at Mercy is decided under the Corporate Compliance Office. The compliance budget for HIPAA would include items like training of employees (manuals, videos), privacy notices etc. There is no budgeting done for "non-compliance costs" like penalties, as it is difficult to put a dollar figure on such cases in advance.

Direct benefits from HIPAA compliance are obvious at Mercy. From her interactions with patients, Ms. Ciamacco firmly believes that patients have a higher level of confidence in the hospital after instituting HIPAA-related privacy measures. The number of complaints has also fallen. The privacy office at Mercy aims to have a complaint rate of less than 0.05% from the approximately 700 patients that are treated at Mercy Hospital every week. This goal has not yet been realized, but is becoming more possible with every passing week.

Most employees have been overwhelmed with the additional work that is now required of them. Added duties include handing out privacy notices to patients, and informing them about their available opt-out choices. Ongoing support and education for employees are therefore very important in order to alleviate these worries.

At Mercy, the HIPAA Security Rule likely causes more significant costs than the Privacy Rule. This is because it is the Security Rule which requires the encryption of electronic information and the implementation of technologies like electronic signatures.

Analysis & Discussion

Overall Costs & Cost Variances

HIPAA expenses are significant, but extremely manageable for most organizations. Drastic organizational changes can be avoided by assigning additional privacy responsibilities to existing personnel who already do similar work, or by hiring temporary consultants to come in for a short period of time.

There are considerable sources of variance for HIPAA compliance. For example, Ms. Innocent from the Children's Hospital of Pittsburgh stated that HIPAA was drafted for adult patients in mind. Even as a hospital that caters to children, the Children's Hospital of Pittsburgh was forced to engage in expensive privacy compliance efforts that would be more of an adult concern (Innocent interview, 2005).

In certain areas, laws may already exist which duplicate HIPAA functionality. At Magee Women's Hospital, the view was that privacy protection already existed through existing laws (Mathias, 2005). For areas like this, the HIPAA compliance effort may not be as significant as in others.

According to a 2003 survey by Dr. Kilbridge, more than 70% of hospitals with less than 400 beds budget less than $100,000 per year for HIPAA compliance. As the number of beds increases, this expense rises as well: nearly half of hospitals with more than 400 beds, for example, spend from $100,000 to $500,000.

Appointing a Privacy Officer

HIPAA asks organizations to appoint specific individuals to deal with both privacy and security. In many smaller organizations, these positions are tasked to existing personnel, but many larger covered entities (CEs) need to appoint dedicated officers.

The Practical Guide to Privacy and Security Compliance (Beaver 2005) estimates costs for these positions: The HIPAA Privacy Officer, for example, is estimated to have a salary range of $80,000 to $140,000. For the HIPAA Security Officer, an individual tasked with ensuring compliance to security procedure requirements, large covered entities should expect to pay $30,000 to $300,000 and up for this role. To keep this cost in perspective, the authors add that security officers in the financial services are paid from $125,000 to $400,000, which is certainly a significant expense.

In the two hospitals we examined, Magee and the Children's Hospital of Pittsburgh, neither facility hired additional resources to deal specifically with HIPAA. Both assigned compliance duties, including the position of HIPAA Privacy Officer, as additional responsibilities for existing personnel, and dealt with all HIPAA challenges internally.

Training Costs

Training is a significant aspect of the HIPAA implementation procedure, and is the source of a large part of HIPAA budgets and expenses. All employees must be trained in the protection of patients' privacy, and it is required that this training is documented. A study commissioned by the American Hospital Association in 2000 estimates the average cost of training at $16 per employee. (Kilbridge 2003). This could easily be one of the most significant expenses for a revamping hospital.

One difficult area of compliance involves the implementation of behavioral changes. Physicians and nurses will be required to exercise additional restraint and caution in how they talk about patients' diagnostic and care related information in public areas. Hospitals will also need to pay increased attention to logistical details, such as the relative placements of reception and administrative areas, and the location of faxes and computers throughout the ward (Kilbridge 2003).

To check if HIPAA guidelines were firm in the mind of its staff, the Children's Hospital of Pittsburgh conducted a "Compliance Effectiveness" survey last year that contained HIPAA elements. This survey asked employees general questions regarding compliance and HIPAA, and had a rather positive response. Ms. Innocent of the Children's Hospital of Pittsburgh did not release the results, but said that she was more than satisfied with the scores (Innocent interview, 2005).

At the Children's Hospital of Pittsburgh, there are also annual computer based training courses. These training courses record students' progress, and a 85/100 is considered a passing mark. Last year, the Children's Hospital of Pittsburgh had an approximate pass rate of 95% on HIPAA matters, which was thought of quite highly by privacy officials there. (Innocent interview, 2005)

Administrative Costs

There are also extensive administrative costs used for redesigning existing business processes and handling the additional paperwork caused by HIPAA regulations. These are difficult to quantify: recording additional items, for example, may be a relatively painless practice for a health care worker, but when this needs to be done several times a day for every patient, the process may become time-consuming (Kilbridge 2003).

HIPAA also mandates informing patients adequately of their privacy rights, and their signature must be taken to record that they have seen this policy. These costs—printing, bringing the form to the patient, classifying the record—can be significant for a firm of any size (Kilbridge 2003).

Additionally, HIPAA requires providers to reevaluate contracts with business associates in order for all parties to adhere to HIPAA privacy practices; this can be very costly as well (Kilbridge 2003).

Technical Security Costs

A major concern is technical security, including the networks, computers, and software systems needed to make sure that digitalized private information remains private.

The HIPAA security standards are a part of the Administrative Simplification provisions, just like the privacy standards. This rule enforces the security of electronic patient health information applicable to covered entities. Security and privacy are closely linked. The privacy protection of any information is heavily dependent on the steps taken for its security. The HIPAA security standards define the administrative, physical, and technical safeguards "to protect the confidentiality, integrity, and availability of electronic protected health information" (Centers for Medicare & Medicaid Services, 2003). The security standards require the covered entities to put in place basic safeguards necessary to protect electronic PHI from "unauthorized access, alteration, deletion, and transmission" (Centers for Medicare & Medicaid Services, 2003).

For many of our interviewed privacy officers, dealing with the HIPAA security rule has been more costly and troublesome than the privacy rule. Though we could not obtain much specific information on software implementations, packages from companies like Cerner or IBM can run to thousands of dollars.

The SANS Institute, a computer security training firm, insists that cost-effective solutions are possible to satisfy HIPAA's basic requirements, including an audit trail, message authentication, event reporting, and access control, using a combined Windows NT/UNIX environment (Romig, 2001). UNIX, for example, already includes many tools for creating event logs at no additional cost, including */var/run/wtmp* for logins and *syslog* for system messages. The *Event Viewer* tool in Windows allows an administrator to monitor abnormal activities. Though setups like this are simple, and may not be the best solution for large-scale implementations, it is important for hospitals to realize that it is possible to greatly reduce the cost of HIPAA compliance by utilizing tools built into existing technical resources.

Physical Security Costs

Aside from locks and cameras, which are bought by both hospitals and a wide range of other businesses, next-generation technologies are also being explored as an adequate HIPAA compliance solution. An article in the May 2001 edition of *Managed HealthCare Executive* (Brakeman 2001) suggests the use of biometric technologies for implementing single sign-on solutions. This technology is much more accurate than existing procedures in identifying individuals for privacy or security purposes. Single sign-on solutions would not only help providers and insurers meet the basic data security guidelines of HIPAA, but will aid them in building future customer confidence.

An increasing number of hospitals are looking into solutions like this to increase efficiency and reduce the probability of accidental information disclosure. In fact, one of the authors of this paper is working on a project with Mercy hospital to suggest feasible electronic signature technologies.

Measuring effectiveness

Hospitals adopt different approaches to measure the effectiveness of their HIPAA compliance efforts. Most of these revolve around the patient experience, and patient satisfaction before and after HIPAA compliance procedures.

At the Children's Hospital of Pittsburgh, effectiveness is measured by the number of HIPAA complaints after the first full HIPAA-compliant year (2004-2005). This measure was a high figure during the first year, which was likely due to the extensive awareness campaign that the Children's Hospital of Pittsburgh waged to patients and their families. However, the number of complaints has fallen since then, and continues to decrease as HIPAA compliance is improved.

On the other hand, at Magee, HIPAA did not have much impact on privacy protection, especially when looked at from the point of view of patients in Pennsylvania. Pre-HIPAA state law in Pennsylvania already incorporated many privacy rules of HIPAA, so HIPAA did not require significant changes for many Pennsylvania hospitals.

Overall, it is extremely difficult to measure the impact of HIPAA on hospital productivity and patient satisfaction. HIPAA implementations are so complex, and have so many consequences, that it isn't easy to narrow down changes as being the result of a HIPAA-related adjustment.

Additionally, there are other complications related to measuring success. For example, there is no clear baseline data for comparison. How can we update patient satisfaction ratings on privacy when it was never measured before?

Non-compliance

With seemingly enormous HIPAA-related expenses, many hospitals considered non-compliance as a cost-savings option. However, costs for non-compliance are actually much more significant.

In an article from the Journal of Health Care Compliance, authors Bob Brown and Spence Wilcox examine the HIPAA privacy rule and find that it is often handled more leniently than it should be (Brown and Wilcox 2005). While HIPAA legislation spells out stiff civil and criminal penalties for violations of privacy rule provisions, to date there have been no civil money penalties imposed by the Office of Civil Rights, despite 13,000 privacy rule complaints lodged with the Office of Civil Rights. And the situation is not getting better: on April 18, 2005, the Department of Health & Human Services (HHS) proposed a rule on enforcement which eases the pressures of compliance efforts for many covered entities. Brown & Wilcox thoroughly believe that this approach is a mistake. HIPAA is not just about penalties or punishments, they attest, but is a measure for good clinical and business practices, and creating an improved and modern health care system. An approach which excuses non-compliance would not serve in furthering these goals.

One significant report by PriceWaterhouseCoopers (PriceWaterhouseCoopers 2001) argues that no health care organization can afford *not* to adopt HIPAA in the face of the changing health care environment. HIPAA calls for both civil and criminal penalties, which can be severe; PWC estimated that penalties would be at least $625,000 ($25,000 penalty per violation of a privacy rule standard).

There are other intangible costs as well. One crucial addition of HIPAA is a degree of standardization to health care information-handling procedures. An organization without the capability to make these transactions will endanger its relationships with customers, business associates, other partners, and the public at large. Additionally, as HIPAA takes hold, health care information systems and standards will move increasingly to a HIPAA-centric model. Organizations which choose to operate obsolete non-HIPAA compliant systems will face increasing maintenance costs. Failing to adhere to HIPAA will also jeopardize an organization's ability to associate with third parties such as licensing or accrediting bodies.

All of the health care entities we've spoken to have chosen to implement HIPAA, for many of the same reasons above.

Conclusion

HIPAA compliance costs range from process redesigns to employee training, and from securing a network infrastructure to safeguarding medical offices. By interviewing local privacy officers, analyzing state-wide surveys, and reading nationally-published research journals and papers, we've attempted to break down these costs and build new perspectives on how costly HIPAA compliance really has to be.

Though HIPAA compliance has been expensive, it has also been manageable. We have not found reports of hospitals closing down from staggering expenses, or budgets which have spiraled uncontrollably out of control. By and large, hospitals have been able to cope. Most of them have done this by avoiding drastic organizational redesigns: existing personnel are given additional privacy responsibilities, for example, or external consultants are brought in for a limited-time basis.

HIPAA compliance is an on-going process which will only continue to change as the environment adapts to medical advances, government regulations, and technological developments. Despite our focus on costs, we believe that it is paramount for privacy directors, health information managers, and other medical professionals to always keep in mind that HIPAA was drafted to better the privacy and care of patients. Health care is about saving and improving lives, oftentimes regardless of what the cost will be.

Acknowledgements:

Jodi K. Innocent, Esq.
General Counsel
Children's Hospital of Pittsburgh Foundation
1251 Waterfront Place
Floor 5
Pittsburgh, PA 15222.

Ann Mathias
Privacy Officer
Magee-Womens Hospital
300 Halket Street, Room 2308
Pittsburgh, PA 15213.

Frances Ciamacco, MS, RHIA
Director Health Information Management
PMHS Mercy Hospital of Pittsburgh
1400 Locust Street
Pittsburgh, PA 15219

Patricia Anania Firouzan MSIS, RHIA
School of Health and Rehabilitation Sciences
University of Pittsburgh
6051 Forbes Tower
Pittsburgh, PA 15260

Bibliography

Beaver, Kevin and Herold, Rebecca. "The Practical Guide to HIPAA Privacy and Security Compliance" SearchSecurity.com 19 October 2005 <http://searchsecurity.techtarget.com/tip/1,289483,sid14_gci941826,00.html>.

Brakeman, Lynne. "Set your sights on exceeding the HIPAA requirements." Managed Healthcare Executive May 2001.

Brown, Bob, and Spence Wilcox. "HIPAA Privacy Rule Enforcement :All Bark and No Bite?" Journal of Health Care and Compliance Sept/Oct 2005

Centers for Medicare & Medicaid Services (CMS). "HIPAA Administrative Simplification - Security" Centers for Medicare & Medicaid Services, DHHS February 2003. 05 December 2005 <http://www.cms.hhs.gov/hipaa/hipaa2/regulations/security/03-3877.pdf>.

Ciamacco, Frances. Personal interview. 25 November 2005.

Firouzan, Patricia and McKinnon, James. "HIPAA Privacy Implementation Issues in Pennsylvania Healthcare Facilities." Perspectives in Health Information Management April 2004.

Firouzan, Patricia. Telephone interview. 16 November 2005.

Innocent, Jodi K. Personal interview. 2 November 2005.

Kilbridge, Peter. "The Cost of HIPAA Compliance." New England Journal of Medicine April 2003.

Mathias, Ann. Personal interview. 8 November 2005.

Nunn, Les and McGuire, Brian L. "The High Cost of HIPAA" Evansville Business Journal August 2005. 21 November 2005 <http://business.usi.edu/news/high_cost_of_hipaa.htm>.

Stephens, John M. "Assessment One: The Risks of Non-Compliance" PriceWaterhouseCoopers Healthcare Consulting Practice April 2001. 19 October 2005 <http://www.pwchealth.com/cgi-local/hcregister.cgi?link=pdf/hipaa_risk.pdf>.

Robbins, Christina. "A Single Solution: Cost Savings and Compliance." KM World Nov/Dec 2004.

Robert E. Nolan Company. "Analysis of HHS Cost Estimates for the Final HIPAA Privacy Regulation" HIPAAadvisory.com March 2001. 19 October 2005 <http://www.hipaadvisory.com/action/Compliance/BCBSPrivacy.pdf>.

Romig, Tautra. "SANS Institute White Paper: HIPAA Compliance-- Cost Effective Solutions for the Technical Security Regulations" SANS.org 2001. 9 December 2005 < http://www.sans.org/rr/whitepapers/legal/51.php>.

Walsh, Tom. "What Will HIPAA Cost? and HIPAA Privacy and Proposed Security Standards: A Tandem Approach to Compliance" Advance for Health Information Professionals 19 October 2005 <http://health-information.advanceweb.com/common/editorial/editorial.aspx?CC=858>.

Appendix A – HIPAA Compliance Survey

1. In general, how has implementing HIPAA increased costs? Please specify where the incremental costs are?

2. Have you done a study of HIPAA-related cost increases on a per capita basis? What the per-capita HIPAA-related expenses for training or technology?

3. Apart from development and implementation costs, what are some other tangential expenses? Could you quantify them? (For example, the time taken by employees to retrieve or access information)

4. How do you measure the effectiveness of your measures? HIPAA promised a great deal of savings from compliance efforts; do you see this materializing? If yes, where?

5. Did you perceive improved patient satisfaction as a result compliance, or was the effort largely a nuisance for them?

6. What measures did you take to encourage employees to be compliant? What has been the employee reaction?

7. Are there any ongoing compliance costs that are incurred periodically? How do you measure the benefits resulting from these investments?

8. How do you budget for HIPAA each year? What are the drivers? What % of the yearly budget is allocated for HIPAA compliance? What is the trend over the years? What are the reasons behind any significant changes?

9. Do you anticipate incurring any other costs in the future to increase the level of compliance? To upgrade the existing systems? Is the current level of compliance final, or is there still a long way to go beyond it?

10. Did you hire any external consultants to help with compliance efforts? If so, how expensive were they?