Running Head: The Privacy Officer: A critical success factor for Health Insurance Portability and Accountability Act (HIPAA) in Department of Defense Medical Treatment Facilities (MTFs)

# The Privacy Officer: A critical success factor in the implementation and maintenance of HIPAA legislation in DoD Medical Treatment Facilities

Graduate Management Project
U.S. Army-Baylor Graduate Program in Health Care Administration

MAJ Joseph A. Ponce

21 May 2002

# Report Documentation Page

*Form Approved*
*OMB No. 0704-0188*



| 1. REPORT DATE | 2. REPORT TYPE | 3. DATES COVERED |
|---|---|---|
| **21 MAY 2002** | **Final** | **Jul 2001 - Jul 2002** |

4. TITLE AND SUBTITLE
**The Privacy Officer: A critical success factor in the implementation and maintenance of HIPAA Legislation in DoD Medical Treatment Facilities**

5a. CONTRACT NUMBER
5b. GRANT NUMBER
5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
**MAJ Joseph A. Ponce, USA**

5d. PROJECT NUMBER
5e. TASK NUMBER
5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
**Brooke Army Medical Center Fort Sam Houston, TX**

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
**US Army Medical Department Center and School Bldg 2841 MCCS-HRA (US Army-Baylor Program in HCA) 3151 Scott Road, Suite 1412 Fort Sam Houston, TX 78234-6135**

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
**3-02**

12. DISTRIBUTION/AVAILABILITY STATEMENT
**Approved for public release, distribution unlimited**

13. SUPPLEMENTARY NOTES

14. ABSTRACT
**This study examines the issue of privacy and security in the Military Treatment Facility(MTF) in light of the Health Insurance Portability and Accountability Act (HIPAA). It analyzes the actions of players within the healthcare industry with regard to preparation for these regulations and seeks to draw a parallel for success in the Department of Defense (DoD), specifically, the Armed Services environment. The role of the privacy officer is examined in detail including job specifications and potential placement within the organization. The study conducts a survey of MTFs with regard to preparation on a questionnaire basis. This is correlated with whether or not the organization has a dedicated a privacy officer or privacy team. The study shows a strong correlation exists between those MTFs that have recognized the need for and dedicated a privacy officer or team and perceived success in preparation. Civilian institutions are examined thoroughly for their mechanisms in planning and training in the areas of privacy and security. The study attempts to raise the awareness of the criticality of HIPAA regulations and the need for adequate and prepared personnel to deal with the approaching changes. Finally, a road map is offered for commanders and DCAs to achieve compliance with HIPAA regulations within the required time frame.**

15. SUBJECT TERMS

| 16. SECURITY CLASSIFICATION OF: | | | 17. LIMITATION OF ABSTRACT | 18. NUMBER OF PAGES | 19a. NAME OF RESPONSIBLE PERSON |
|---|---|---|---|---|---|
| a. REPORT | b. ABSTRACT | c. THIS PAGE | | | |
| **unclassified** | **unclassified** | **unclassified** | **UU** | **58** | |

## Acknowledgments

I would like to sincerely thank COL Martin Fisher, previous Deputy Commander for Administration (DCA), Brooke Army Medical Center, COL Stephen Markelz current Deputy Commander for Administration, Brooke Army Medical Center (preceptor), and Mr. William D. Rasco, COL, USAF (Ret), President and CEO of the Greater San Antonio Hospital Council for their leadership, guidance, and assistance with this project. My residency in Healthcare Administration through the U.S. Army Baylor program has been thoroughly enhanced by the mentorship of these individuals. I would also like to thank the great number of DCAs and other fine officers who responded so graciously to my survey request. Perhaps soon, we as Armed Services can offer some needed assistance in the preparation of MTFs to meet these coming challenges.

## Abstract

This study examines the issue of privacy and security in the Military Treatment Facility (MTF) in light of the Health Insurance Portability and Accountability Act (HIPAA). It analyzes the actions of players within the healthcare industry with regard to preparation for these regulations and seeks to draw a parallel for success in the Department of Defense (DoD), specifically, the Armed Services environment. The role of the privacy officer is examined in detail including job specifications and potential placement within the organization. The study conducts a survey of MTFs with regard to preparation on a questionnaire basis. This is correlated with whether or not the organization has a dedicated a privacy officer or privacy team. The study shows a strong correlation exists between those MTFs that have recognized the need for and dedicated a privacy officer or team and perceived success in preparation. Civilian institutions are examined thoroughly for their mechanisms in planning and training in the areas of privacy and security. The study attempts to raise the awareness of the criticality of HIPAA regulations and the need for adequate and prepared personnel to deal with the approaching changes. Finally, a roadmap is offered for commanders and DCAs to achieve compliance with HIPAA regulations within the required time frame.

Table of Contents

# List of Tables

List of Figures

## 1. INTRODUCTION:

It is no secret that privacy legislation regarding patients and records in medical facilities is a very real and serious concern from the legislative and public opinion standpoints. Recent laws such as the Health Insurance Portability and Accountability Act (HIPAA) are poised to have a dramatic impact on the day-to-day operations of many of the United States' Army's Medical Treatment Facilities (MTFs). These laws were designed to improve the availability of health insurance to working families and their children, and establish specific requirements for administrative simplification in the exchange of electronic health data among employers, insurers, and providers. These regulations will require major changes in how health care organizations manage all facets of information, including reimbursement, coding, security, and patient records (Blair, 1996). The Health Privacy Project sponsored by Georgetown University publishes updates on individual state privacy laws. A summary of the project's most recent report illustrates how governing access to medical records is accomplished and this summary may be found in Appendix 2.

Over the last 10 years, the federal government has attempted to address the patchwork nature of state laws regarding patient privacy but has largely failed to complete this task. In an effort to ensure that all citizens have a minimum standard level of protection, the Department of Health and Human Services has promulgated regulation, under the authority of HIPAA, to provide a universal floor of protection. The responsibility of compliance with these new regulations falls squarely on the backs of all healthcare providers and facilities. This is a significant and costly added burden to an industry often struggling to maintain fiscal solvency. The timeline for implementation is also relatively short adding further details to the complex

issue of patient care. The healthcare industry as a whole is very concerned with meeting these new requirements (Marks, et. al., 2001).

Because of the scope of these responsibilities, many civilian organizations have taken steps to create relatively new positions to manage and advise senior leaders on patient privacy concerns. Since many areas of an organization are affected by the recent legislation, these 'privacy officers' or 'privacy teams' serve as central points of contact concerning these issues (Kelly, 2001). Privacy legislation impacts obvious areas such as medical records and insurance data. However, areas such as information systems, legal departments, and provider personal habits are often less considered. As such, it is important to assess, study, and determine if the creation of a privacy officer or team may be helpful in effectively implementing this legislation within Department of Defense (DoD) medical treatment facilities.

Privacy legislation is serious business. Healthcare is a service industry that relies on information for every facet of its delivery. Health information has value to the patient it describes, the provider it serves, and the organization it supports. In addition, this information is a vital component of society as it helps to direct local, state, and national objectives in establishing policy to ensure the health of the population. In its primary form as the medical record of a unique individual, it must be protected as a valuable asset and safeguarded.

The proposed regulations and safeguards are a significant source of consternation among healthcare professionals that are familiar with what these requirements entail. For those that are not as familiar, the tendency may exist to ignore or delay the planning and preparation required. In the case of privacy legislation, this practice may be hazardous to the very existence of the healthcare organization. Compliance with these laws and regulations is mandatory by a certain

date and potential penalties for violation include serious fines and potential prison time for willful misconduct (American Hospital Association, 2002).

Privacy concerns have grown as technology has increased access to health information. Mental health, substance abuse, sexually transmitted disease, and now genetic information create a heightened awareness of the need for privacy. Documented cases of the use of health information to make decisions about hiring, firing, loan approval, and to develop consumer marketing have sensitized the public to the risks of sharing information with many organizations including healthcare providers (Briggs, 2001).

As a result of this heightened awareness, many organizations throughout the country have created privacy officers or teams to help manage these concerns. According to the American Health Information Management Association (AHIMA), (2001), many medically-related organizations are beginning to recognize the increasing complexity of patients' privacy and the need for dedicated individuals or teams to assist in their protection. This change must be progressive in that organizations must advance in information capability while managing the access to, and the release of information, about patients and other healthcare consumers. Finding individuals to assist in the management of this new information paradigm requires a benchmark to measure qualifications. AHIMA maintains that because of their credentialing of health information management (HIM) professionals, they provide individuals that are uniquely capable of assuming positions as designated privacy officials as required by HIPAA. While certification is certainly important in a privacy officer, academic preparation, work experience, commitment to patient advocacy, and a professional code of ethics are a must with regard to these individuals' capabilities.

The role of the privacy officer may be quite unique depending upon his or her location throughout the country. For years, states have written laws and regulations to protect their citizens' privacy by limiting the release of information based upon the requestor, the type of information, and the use of that information. Due to the complexity of the issue, the number of concerned parties, and the variety of health information, no two states have the same laws. As Appendix 2 illustrates, access to medical records varies widely not only between states, but also between the different types of medical entities within these states (Georgetown University, 2002).

To ensure the necessary leadership for compliance with these various laws, the Standards for Privacy of Individually Identifiable Health Information released in December 2000 a series of requests. The December release request asked that each health plan, healthcare clearinghouse, and certain healthcare providers designate a privacy official who is responsible for the development and implementation of the organization's policies and procedures relative to privacy (Standards for Privacy of Individually Identifiable Health Information, 45 CFR Parts 160 and 164, 2000). According to the standards, the job of the privacy officer in a medical setting is to maintain the privacy, confidentiality, and security of health information. As illustrated in Appendix 3, these individuals must assume a leadership role in compliance with state and federal laws, develop appropriate organizational initiatives, and exercise ethical decision making (Wilcox, 2000).

Given the complexity of these privacy regulations and the unique nature of the United States Army's mission, this study will ultimately seek to discover ways to ease the burden of compliance with respect to privacy legislation on the operations of MTFs. Medical treatment facilities will be surveyed to assess current knowledge and plans to deal with the perceived

impact of privacy legislation. The study will compile these findings, perform a statistical analysis on the data, and offer a recommendation whether or not the creation of a privacy officer would be beneficial in the DoD MTF. A secondary function will be to provide MTF commanders with a general roadmap to success in the implementation of the current and future HIPAA requirements.

**HIPAA Overview**

The Health Insurance Portability and Accountability Act (HIPAA) (Public Law 104-191) of 1996 was signed into law by President Clinton on August 21, 1996. The legislation was enacted as part of a broad Congressional attempt at incremental healthcare reform. The intent of HIPAA is to improve the efficiency and effectiveness of the healthcare system by encouraging the development of health information systems that utilize Electronic Data Interchange (EDI) for the administrative and financial transactions specified (Leahy, 1997). The "Administrative Simplification" aspect of that law requires the United States Department of Health and Human Services (DHHS) to develop standards and requirements for maintenance and transmission of health information that identifies individual patients (Manning, 1997). In addition, HIPAA seeks to establish the required use of national standards when performing these business transactions between organizations electronically. It further requires that all parties using these transactions for healthcare follow the guidelines established by the national implementation guides.

HIPAA promotes two main goals with respect to privacy. Unfortunately, the goals lack the objective metrics by which to assess progress and measurement. It is a key point to understand that the ‘threat’ is constantly changing. Loopholes, cracks, and new ways to exploit information are being discovered on a daily basis. As such, HIPAA regulations are written in

broad and general terms that leave room for movement in the organization to be able to plan and react to new threats. While very general, the two main goals of HIPAA regulations are to:

1) Improve the efficiency and effectiveness of the healthcare system by standardizing the interchange of electronic data for specified administrative and financial transactions; and

2) Protect the security and confidentiality of electronic health information.

These requirements as outlined by the law and the regulations promulgated by DHHS are far reaching. All healthcare organizations that maintain or transmit electronic health information must comply. This includes health plans, health insurers, and healthcare providers, from large integrated delivery networks to individual physician offices. After the final standards are adopted, small health plans have 36 months to comply. Others, including healthcare providers, must comply within 24 months.

Despite the short time frame for implementation, the law provides for significant financial penalties to organizations and individuals who violate the intent of these regulations. There is a general penalty for failure to comply which may result in fines of up to $100 for each violation. The maximum penalty for identical violations may not exceed $25,000. The penalty for wrongful disclosure of individually identifiable health information can take two forms depending on the exact nature of the offense. They are as follows:

1) Wrongful disclosure offense: Consists of a fine of up to $50,000, imprisonment of not more than one year, or both.

2) Offense under false pretenses: Consists of a fine of up to $100,000, imprisonment of not more than 5 years, or both

3) Offense with intent to sell information: Consists of a fine of up to $250,000, imprisonment of not more than 10 years, or both

In addition to the potential punishment for information-related offenses, HIPAA will have a major impact on healthcare providers in other areas as well. Significant resources will be required in order to successfully assess and plan for the upcoming regulations. Varying degrees of Information Technology (IT) retooling will be required, as well as major operational and procedural changes in functions such as help desk operations, computer setup, and data storage systems. On a more positive note, electronic transactions will become more standardized among healthcare entities. While this may cause significant expense in the interim, the end result should show an eventual savings for electronic data interchange simply due to a reduction in claims processing times.

The implementation of transaction standards, code sets, and identifiers will be the most expensive for most healthcare organizations. Ongoing costs will be involved in obtaining and implementing updates to the standards. The cost and the burden to the organization will vary directly with the scope and frequency of these updates. The security and privacy regulations will be the most difficult and costly to implement and maintain because they are broad in scope, less definitive, and require constant vigilance for ongoing compliance.

HIPAA is an enterprise-wide issue, not an information technology issue. There are legal, regulatory, processes, security, and technology aspects to each proposed rule that must be carefully evaluated before an organization can begin its implementation plan (Rutherford, 2001). HIPAA is rapidly becoming a major issue in healthcare because of a number of issues: 1) Implementation time frames are short—organizations must be in compliance 24 months after the regulations become final. 2) Y2K efforts, coupled with new and destructive computer

viruses have kept organizations from focusing on HIPAA. 3) Senior executives are clearly responsible for the security and confidentiality of patient health information, yet many know little of the scope of the requirements that must be accomplished in most organizations to protect this information. 4) There are significant criminal and civil penalties for non-compliance as well as serious liability risks for unauthorized disclosure.

There are no quick fixes or easy solutions to meet the HIPAA requirements and issues listed previously. Because of this, it becomes exceedingly difficult to assess the costs and benefits of HIPAA compliance due to these sweeping changes. Estimated costs of implementation vary widely but will certainly be in the billions of dollars (Kelly, 2001). The government estimated the five year "conservative" cost of the privacy regulation alone to be $3.8 billion (Staggers et. al., 2000).

HIPAA puts extensive requirements on every area within healthcare. Regulations will govern the transmission, maintenance, security and privacy of electronic health information transmitted by health care providers, payers and others. While HIPAA legislation should ultimately lead to administrative simplification and significant cost savings, the implementation of HIPAA is anything but routine. It will require changes in the health information systems and procedures at the core level to be successful. The philosophy and operational requirements of HIPAA must be integrated into the overall strategic initiatives of the military treatment facility (Staggers et al, 2000). The designation of a privacy or compliance team may be one of the necessary keys to success along with a significant commitment in organizational time to reach required compliance levels.

**Conditions which prompted the study:**

Three HIPAA conferences were conducted in Washington D.C over the past 12 months with DoD employees as the primary attendees. Representatives included members of the Army, Navy, Air Force, Marine, Coast Guard and other Government entities. The conferences offered numerous opportunities for networking among their participants and have illustrated an interesting phenomenon concerning current and forthcoming privacy legislation. Discussions with the attendees indicated that the backgrounds and positions of the individuals varied widely. Attendees included physicians, nurses, administrators, IM/IT professionals, medical records officers, and TRICARE and regional support personnel. This diversity of backgrounds leads one to ask the key management question - who should be the center point of leadership with respect to privacy legislation?

In addition to the question of leadership, concerns and questions with cost of compliance in terms of money and manpower were also raised. Many asked if the Department of Defense had requested additional money to cover these unfunded mandates. The answers to these questions by the panel of speakers indicated that no formal request for additional funding had been made at that time. According to the lecturers, the conferences were convened to discuss patient privacy and to offer tools, tips, and techniques to help personnel to assess their compliance with rapidly approaching HIPAA deadlines. Many individuals were dissatisfied with the lack of specificity, direction, and focus. The subject of a privacy officer was broached several times during these lectures although no one speaker postulated a proposed individual or specific area within the MTF. The ensuing network sessions offered a much more valuable forum for the initial assessments of such a position, as individuals were able to discuss the meaning of these lectures among themselves. From a compliance standpoint, there seemed to be

no concrete opinion that success in preparing for and maintaining privacy legislation requirements should be designated to one individual, a team, or just left to each individual department or service. Rather than specify organizational structuring, the conferences focused more on the mechanism of assessment and how to best accomplish the HIPAA objectives. Several frustrated individuals commented to the speakers that they needed more concrete suggestions and data as to the location and composition of the privacy individual or team.

It is not surprising that the speakers and hosts of these conferences were unwilling to suggest a structure for a privacy program. Some variations exist in DoD medical facilities among different services and there may be no best single answer. Also, the Department of Defense, because of its size, might be less willing to react rapidly and prefer to wait for further clarification of the legislation. Even as these conferences were taking place, companies and service industries were reacting swiftly and decisively. One company in particular that deals with the military was rapidly changing its privacy infrastructure. In a TRICARE press release in March, 2001, Sierra Military Health Services, which has the TRICARE Northeast contract, created and filled a very senior Chief Privacy Officer position. Sierra stated that with the advent of a comprehensive pharmacy benefit and increasing Internet-based information exchange, the company must ensure its covered population is comfortable with its security efforts in these areas.

Creating a sense of comfort may not be possible given the ease with which information is available today. This fact is beginning to cause some public concern. A recent example in New York illustrates this. Voter registration records have always been available at the county record department. Interestingly, much of this information was available before the advent of the Internet and many online search engines. If an individual was determined enough or had

adequate resources, they could easily access this information by collecting it themselves or purchasing it through an information source provider. When the department transitioned to online access, public awareness changed. According to the article,

> "The material on the site that created the hue and cry isn't exactly private information: Anybody can walk into the city's Board of Elections, plunk down some cash to cover administrative costs and leave with as much voter-registration information as they can cart out. People don't mind having such records available for public viewing in the dank basement of a city hall building, observers have noted, because it takes time and effort to locate those records, let alone to sift through them for particular bits of information. The fact that a small percentage of the population is actually willing to expend that time cloaks those records in an aura of unavailability. Putting once-obscure material on easily searchable Web sites changes the equation" (Peterson, 2001).

The above example indicates how the 'perception' of how information is handled can often have a broad impact on a customer or patient population. Many companies have been quite vocal about their appointment of Chief Privacy Officers through press releases and links on their websites. While procedurally, few changes may have been made in the way many of these organizations handle information, the perception among customers is recognized as a critical component in the business process. The military MTF is beginning to realize this also as issues of privacy and security become more intertwined in light of recent terrorist activities. With guards at the gates and entrances to our MTFs, we hope to deter threats and create a feeling of safety for ourselves and our customers. This same approach should be taken to the privacy of

patient information. The creation of a privacy officer team in the military MTF might very well enhance the solid reputation for security. Perhaps these sentiments are summed up best by one of IBM's executives,

> "Appoint a Chief Privacy Officer: The battle for trust among customers in the emerging digital economy is just getting started. The commitment of executive attention to the matter of trust in your enterprise is a signal of a trust to your customers as well" (Howard, 2001).

The HIPAA and privacy regulations required to gain the trust of consumers are inherently complex due to the lack of a well-defined structure and standards. There are a variety of concerns among DoD personnel as to the impact of this current legislation on operations at their facilities. There is widespread concern that the requirements of privacy regulations will seriously impact the ability of the Department of Defense to deliver quality health care and control costs (Staggers et al, 2000). Issues such as adequate guidance from the senior DoD levels along with funding challenges and personnel shortages are all woven into these concerns. Our civilian counterparts share these concerns as well. Regardless of the size of the treatment facility or number of personnel employed, HIPAA and privacy requirements must be followed. This applies from the largest of hospital systems to the individual practitioner. The cost of compliance can be significant and organizations including civilian treatment facilities are concerned (Streveler, 2001).

Without question, the issue of privacy is an on-going compliance issue. It is, and will continue to be, a serious effort that commands a significant amount of job hours and funding to accomplish properly. Seeking ways to effectively streamline the process of ensuring compliance

and reduce the overall impact on continuous operations is an effort worthy of focus. The study was prompted by one overriding question.

**Statement of the Problem:**

Is the task of implementing, educating, and monitoring the various aspects of privacy legislation of HIPAA so broad and time consuming as to warrant the designation of a privacy officer or team within the DoD MTF?

**Literature Review:**

The problem statement above regarding privacy should be predicated upon two important factors: the scope of the hospital or treatment facility and the overall size of the institution. The reason for the second factor is that many hospitals today have satellite facilities. As we examine these issues, much of the literature with respect to HIPAA privacy and security will deal with civilian institutions. With a few minor exceptions addressed in this section, the legislation and literature concerning HIPAA is generally similar between civilian and military hospitals (Joseph, 1997).

Like many civilian hospitals, Military Treatment Facilities offer specific guidance to providers and staff in the form of regulations and directives concerning the handling of privacy and patient records. What these regulations often lack is the specificity as to which individual or team should have responsibility for these actions concerning privacy and security of patient information. In many instances, these directives are standards of care promulgated by an institution or a collective body such as the Joint Commission for the Accreditation of Healthcare Organizations (JCAHO) (Staggers et al, 2000). While the Joint Commission may issue a finding for failure to keep patient information secure, they are less likely to suggest a detailed privacy structure be put in place for the purpose of HIPAA compliance.

A related question that is frequently raised in the MTF is how HIPAA will affect the flow of information in a JCAHO accreditation. The Joint Commission is technically defined as a "business associate" of the organization where the organization being surveyed gives access to identified health information for a particular purpose. In the case of the Joint Commission, that purpose is quality review. Because of this relationship, JCAHO is developing a contract between itself and the accredited organization that will outline its use and protection of the information that is shared during a survey. (Tirone, 2001).

Due to the interdisciplinary nature of these standards, as a healthcare facility prepares for a known JCAHO inspection, the organization will often appoint a team. These may be the heads of certain departments or staff members working with one key leader. For the most part, MTFs do not have privacy officers, or privacy management teams defined by position structure. Most have an information security officer under the Information Management Department, but this role is not comprehensive.

While JCAHO accreditation is a concern, some leaders are simply not aware of the planning required to be in compliance with the approaching privacy legislation. Commanders must be vigilant and stay abreast of the changing regulations. Those with a decentralized style of leadership may possibly rely too heavily on each department or service in order to ensure compliance with privacy legislation. Other commanders may run the risk of waiting too long for expected concrete guidance from higher headquarters that mandate DoD-wide changes.

Commanders obviously have the ultimate responsibility when it comes to privacy but responsibility also rests with everyone else in the organization who deals with patients and information about them. More concerns are being expressed over privacy in DoD facilities than ever and this trend seems to be continuing (Gostin et al, 1996). Since military dependants,

retirees, and civilians are also treated in many of these facilities, the differences between military and civilian institutions are less well-defined. As a result, governmental agencies have expressed an increased interest in patient privacy in military facilities. (Auston et. al, 1996). This interest can be seen in the number of Department of Defense representatives that have been called to testify before governmental entities such as the National Committee on Vital and Health Statistics. Questions such as when privacy related data may be released were of particular concern to the committee members. It is recognized that the military often has some unique requirements with respect to the health of its members which may impact privacy of medical records. These situations have been explained by senior DoD officials in recorded testimony (Leahy, 1997).

It is unfortunate that much of the HIPAA legislation being enacted is a result of cases dealing with or surrounding certain abuses of information in the past. Much of these abuses have been driven by a profit motive due to the highly competitive marketplace. It is interesting to note that the cost of compliance varies inversely with the time remaining before mandated compliance dates. Those organizations who seek to improve their financial positions have a strong incentive to act early and build a privacy process into their business model. Time is of the essence in moving toward compliance. According to Joseph Pokorney, principal, Phoenix Health Systems, Inc.,

> "Waiting to meet the deadline in the last six months could increase costs by as much as 100 percent because healthcare providers that begin working on HIPAA immediately can actually comply with much of HIPAA using their own resources."

In many cases, organizations are not completely certain how the result of HIPAA legislation with affect their costs and day to day operations. Therefore, the idea or concept of having a privacy expert or team has risen in importance in the eyes of many CEOs throughout the country. According to Mendels, 2000, the visibility of this position has risen in response to the number of vendors offering services to help healthcare organizations develop the tools to survive the coming requirements. At a recent Texas Hospital Association meeting, 21 companies offering some form of HIPAA preparation service were present in an exhibition hall of approximately 150 vendors. Leaders are asking their advisors what it takes to achieve compliance. They are asking if their organizations have the expertise internally to achieve compliance and wondering if outsourcing may be the most cost effective option. The answers these leaders receive in return may not produce feelings of comfort that the organization is steady and on-course toward compliance (MacMillan, 2001).

Perhaps the reason for this feeling of insecurity is that HIPAA is a complex mix of legal, safety, privacy, and customer service issues. Organizations are finding it takes an individual with specific skills and experience in multiple areas to accomplish this role effectively (Schlesinger, 2001). Finding qualified individuals is often not easy. The nature of the privacy position can often put the individual in charge at odds with the direction of the organization particularly in areas such as marketing. The person or team addressing compliance must have the ability to say no to some of the internal proposals of an organization. This person or team must not fear retribution for this action. To say yes to an illegal use of information would be a lose-lose situation for the organization and the privacy officer or team. Probably one of the most important characteristics of this position is the ability to decide whether or not the use of certain information in marketing methods violates the spirit of the law. This will be just one of the

many ways privacy officers will have to curtail efforts to use information in ways that do not agree with corporate policies (USA Today, 2000).

Because of the use of some unethical policies in the past, privacy concerns have leaped to the front of the agenda for corporations, business groups, state and federal legislators, consumer organizations and privacy advocates alike. As the Internet and other advanced technologies have grown, privacy concerns have increased, too, both online and offline. Many businesses have recognized the growing urgency of this issue and have appropriately responded to their customer's concerns. This can be seen in the increasing number of statements made concerning security of information. The phrase, "we never disclose any of our customers' names and addresses" appears with greater frequency every day.

Recognizing the importance of building consumer trust levels, more than 75 Chief Privacy Officers have been appointed in the last year among the Fortune 1000 companies (Privacy Leadership Initiative, 2001). In fact, a growing number of privacy officers are being appointed or hired to lead senior management in creating a privacy-sensitive culture among the company's various stakeholders. The result is the development of new professional associations and conferences dealing solely with privacy to meet the rising demand by organizations who are concerned about HIPAA legislation. Regardless of the title used: privacy officer, privacy manager, or privacy team, the perceived need is very real for leadership in this area and CEOs are beginning to take action. (Privacy Leadership Initiative, 2001).

To create a sprit of cooperation and help further define this new position, a conference entitled "The Online Privacy Conference: Integrating Security and Privacy for Data Protection" was held in Chicago in July 2001. The event focused specifically on the needs, problems and demands that information security personnel, privacy officers, and audit professionals face in

today's market. A large portion of the conference was focused on HIPAA and its impact on corporate operations. The keynote address was delivered by two individuals from Microsoft Corporation. The address was significant because the titles of the two positions revealed how one of the country's largest companies views two critical issues. Microsoft sent their Chief Privacy Officer and Chief Security Officer to illustrate that security and privacy issues are quite different. The title of the presentation was "Privacy and Security: Oil and Water?" These two executives revealed how they have learned to respect one another's differing perspectives and plan mutual goals they both believe in - goals that enhance both the security and privacy of their organization. Both individuals agree that good communication and planning are key ingredients for success in meeting HIPAA requirements. (Guardent Press Release, 2001). Perhaps this notion is best summarized by Joseph Pokorney, principal, Phoenix Health Systems, Inc.,

> "Unlike Y2K, HIPAA is an organization-wide issue requiring cultural as well as technological change. Compliance is 80 percent policy and planning related and only 20 percent technology related."

The transition to a more privacy conscious environment does not necessarily have to be painful. Computer users are all familiar with the standard security message that appears when they log onto a secure system. However, as with many burdensome delays, it is questionable as to how many individuals have ever read this information or realized the impact of what they were reading (Landro, 2001). Leaders must ensure the appropriate training takes place on the use of these systems. The future will likely expand this security definition to explain the meaning of privacy in greater depth with respect to patient information. (Kibbe, 1997).

For the military MTF, the issue of privacy and planning has yet to be universally and formally assigned to any specific area. It is tempting to place the issue of privacy under the

MTF's Information Systems Security Officers (ISSO) position usually located in the Information Management Divisions (IMD). As the conference speakers pointed out, some of the country's most knowledgeable organizations have chosen to separate these two roles. In the MTF, the ISSO position is generally concerned with the security of the systems he or she monitors within the facility. The authorization to use certain systems and password maintenance more appropriately describes the ISSO position as opposed to the much broader sharing of privacy information concerns. Even so, some installations have designated this person as their HIPAA senior technical advisor due to their inherent knowledge of the IT structure of the facility. Unfortunately, the security officer's position may be too narrowly focused and so this individual my not have exactly the right skill set to accomplish both missions. Of course, the size of the installation will certainly be a factor and so adding privacy as an additional duty may or may not be possible. Traditionally, ISSOs have a multitude of responsibilities especially in a large facility with many different specialties and unique computer systems to support them. Conversely, a small facility may not be able to hire or dedicate a full-time privacy individual. It may have to outsource or rely on a team approach. Privacy requirements are not necessarily the same due to mission differences and the approach one takes toward the management of information will differ based upon these criteria. (Guardent Press Release, 2001).

Despite the fact that enacting a privacy structure to ensure compliance with HIPAA rules and regulations are likely to be burdensome, there are some distinct benefits from this legislation particularly in the area of Electronic Data Interchange (EDI). The Transaction and Code Set Standards Regulation is the first to become law under HIPAA. It is quite likely that these regulations could yield the most actual dollar savings by reducing administrative costs and processes. Throughout the country, providers and payers currently use a number of different

formats to handle transactions. These transactions often have varying data requirements to submit electronic claim forms. Certain healthcare providers process as many as 140 formats (Lanser, 2001).

In addition to the benefit to healthcare providers who will collect and submit electronic health information in a common format, the Transaction and Code Set Standards Regulation's common format will allow providers to check the status of claims electronically and verify eligibility in real time. It will also reduce or eliminate many of the paper-based activities that currently take place in many facilities. From a claims perspective it should enhance and accelerate the receipt of payment for claims and shorten the overall payment cycle. It should also reduce the significant number of claim errors that occur due to differing formats and reduce write-offs. On average paper claims take about 60 days to process until receipt of payment occurs. Each of these claims cost approximately $5. In contrast, processing a clean electronic claim takes only 14 days with a cost of only $.25-.30 per claim. The Department of Health and Human Services predicts that over the next 10 years the savings could be as high at $29.9 billion (Lanser, 2001).

The source of this predicted savings occurred when President Bush recently, signed into law H.R. 3323, the Administrative Simplification Compliance Act (now known as Public Law 107-105), on December 27th 2001. The Act requires that, by October 16, 2002, hospitals and other covered entities must either be: 1) In compliance with the electronic transactions and code sets standards as described under the Health Insurance Portability and Accountability Act (HIPAA), or 2) Submit a summary plan to the Secretary of Health and Human Services (HHS) describing how the entity will come into full compliance with the standards by October 16, 2003. No HHS approval of the summary plan is required however.

The new law requires that the Secretary develop and issue by March 31, 2002 a model form that may be used in drafting this required summary compliance plan. It is critical to understand that in order to receive the one-year extension, hospitals and other covered entities must by October 16, 2002 submit to the Secretary of HHS this summary plan for coming into full compliance by October 2003. Such plans may be submitted electronically (American Hospital Association, 2002).

The plan must contain the following specific provisions which will likely be contained in the summary compliance plan to be released on March 31, 2002. It must address the extent of noncompliance and the reasons why the organization is not in compliance. It must lay out a budget, timeline, strategy and work plan for achieving compliance. It must establish a timeframe for testing, which must start no later than April 16, 2003, and also indicate whether or not the organization plans to use a contractor or other vendor to help achieve compliance (Marks, et. al., 2001).

In general, most military individuals understand the importance of the process of planning and security within the first few weeks after joining the ranks. Security is defense and the military understands defense. Medical privacy is a bit different than simply making systems secure. It involves a multitude of issues on various levels of communication including telephone, personal conversations, and record keeping. These privacy issues will impact areas of healthcare in ways that are somewhat new to the Department of Defense.

Privacy or secrecy is already practiced when dealing with confidential, secret, or top-secret information (Staggers et. al., 2000). As a result, the privacy mindset already exists among some users of DoD information systems but not all. Providers who leave patient information available on the screens of their computer in view of others are only one example. There are

paper charting, conversations, and other communications that will have to be examined. With HIPAA, many of these same protections that we have applied to secret operational plans will now apply to patient medical records and as a result, the transition may be somewhat less painful for the organizations that are familiar with these procedures.

**Purpose Statement of Study:**

The purpose of this study is to determine if there is a correlation between the success of an organization with respect to preparing for HIPAA requirements and the designation of a privacy officer. The study will assess the overall level of HIPAA preparedness among a number of Medical Treatment Facilities within the Department of Defense. It will examine a portion of the legislative requirements of these new laws and examine the data for a correlation with those organizations that have designated a privacy officer or team. It is believed that organizations that designate a specific person for the task of privacy issues are more likely to have attained a greater level of compliance with the requirements of HIPAA and current privacy practices. As such, designation of a privacy officer can be a predictor of success in these organizations.

**Variables**: The variables used in the study consist of the following:

**Dependant Variable (Y) Preparedness:** The level of success an organization has attained in preparing for and meeting HIPAA requirements. This variable is calculated as the average of preparedness level questions on a scale from 1-10. The result is converted to a percentage to three decimal places.

**Independent Variables (X) Privacy Officer**: A binary variable indicating the specific designation or lack of designation of a privacy officer in the organization.

**Working Hypothesis:**

Ho--Designation of a privacy officer has no bearing on the preparedness of the MTF with respect to HIPAA regulations and requirements.

Ha--MTFs that have designated a specific privacy officer are significantly more prepared to deal with HIPAA and privacy regulations than those who have not.

## 2. METHOD AND PROCEDURES

In order to obtain data, all Army MTFs throughout the country were contacted and asked to participate in a short nine-question survey (See Appendix 1). Those clinics and smaller facilities that were subordinate to another facility were not used. A total of 23 Army MTFs met this criteria and were sent surveys electronically in January 2002. Responses were received from 17 for a total response percentage of 74%. All surveys were sent directly to the email account of the Deputy Commander for Administration (DCA). In a few cases he or she passed these questions along to the most knowledgeable person in the organization to answer them. The responses to the questions came from users with varying degrees of knowledge of privacy and HIPAA requirements. Points of contact/responders came from several areas of the medical facility including: Administration, Medical Records, Patient Administration, and Information Management. This survey assessed the perceptions of the MTFs level of privacy awareness, training, current compliance, and projected compliance. The names of the participating facilities were not recorded to help ensure complete anonymity and honesty without inflation of variables.

Response rates via email were expected to be fairly low. The 74% response rate, which was surprisingly high, indicates a significant interest in the subject of privacy and HIPAA preparedness among our MTF senior leaders. A few telephone contacts were made to clarify

certain questions. These conversations were very revealing regarding the significance many facilities are placing on these future privacy requirements. A data set of findings is illustrated in Table 1 followed by the statistical methods and charts used to examine and explain the data and results.

## 3. THE RESULTS

The results below indicate the responses from 17 different Army MTFs throughout the country.

Table 1—Data for MTFs

Privacy Officer (X) & Preparedness Level (Y)

| Variable | X | Y |
|---|---|---|
| **MTF** | **PrivOff** | **PrepLvl** |
| A | 0 | 63.750 |
| B | 1 | 75.625 |
| C | 0 | 41.250 |
| D | 0 | 46.250 |
| E | 1 | 60.000 |
| F | 0 | 48.750 |
| G | 0 | 52.500 |
| H | 0 | 61.250 |
| I | 1 | 61.250 |
| J | 1 | 62.500 |
| K | 1 | 50.000 |
| L | 0 | 40.000 |
| M | 1 | 58.750 |
| N | 1 | 50.000 |
| O | 1 | 72.500 |
| P | 0 | 20.000 |
| Q | 1 | 53.750 |

The number of treatment facilities surveyed is listed under the MTF by variable. The independent variable (X) is the presence or absence of a designated privacy officer at the facility (Presence=1 Absence=0). The dependant variable (Y) indicates the average score of the final eight survey questions and is a score between 0 and 100 when multiplied by 10. For each facility, the results of the individual questions are averaged. The higher the total score the greater level of the facility's preparedness.

**Alpha probability level used:** The alpha probability used is .05.

Results from the data are analyzed to detect significance in preparedness level. An analysis of variance (ANOVA) is conduced along with an independent T-Test. The results for the data set are illustrated below:

Figure 1: Descriptive Statistics

**Descriptives**

PREPLVL

| | N | Mean | Std. Deviation | Std. Error | 95% Confidence Interval for Mean | | Minimum | Maximum |
|---|---|---|---|---|---|---|---|---|
| | | | | | Lower Bound | Upper Bound | | |
| 0 | 8 | 46.71875 | 13.773316 | 4.869603 | 35.20397 | 58.23353 | 20.000 | 63.750 |
| 1 | 9 | 60.48611 | 8.990977 | 2.996992 | 53.57503 | 67.39719 | 50.000 | 75.625 |
| Total | 17 | 54.00735 | 13.175236 | 3.195464 | 47.23327 | 60.78143 | 20.000 | 75.625 |

Figure 2: ANOVA

**ANOVA**

PREPLVL

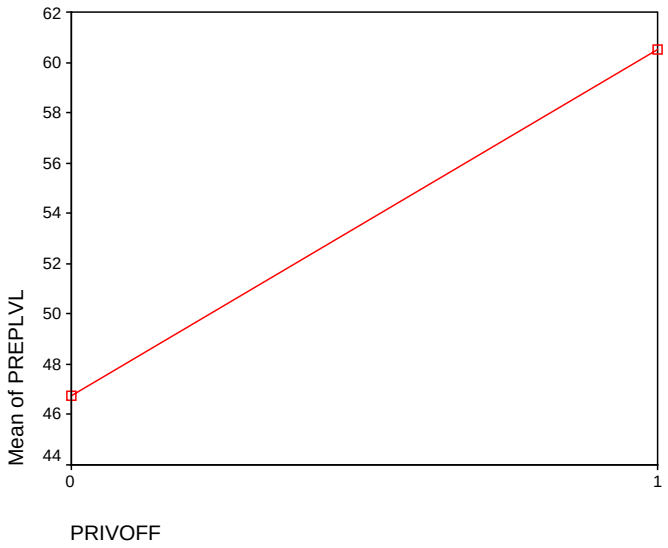
| | Sum of Squares | df | Mean Square | F | Sig. |
|---|---|---|---|---|---|
| Between Groups | 802.759 | 1 | 802.759 | 6.098 | .026 |
| Within Groups | 1974.631 | 15 | 131.642 | | |
| Total | 2777.390 | 16 | | | |

Figure 3: Independent Samples T-Test

**Independent Samples Test**

| | | Levene's Test for Equality of Variances | | t-test for Equality of Means | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | 95% Confidence Interval of the Difference | |
| | | F | Sig. | t | df | Sig. (2-tailed) | Mean Difference | Std. Error Difference | Lower | Upper |
| PREPLVL | Equal variances assumed | .808 | .383 | -2.469 | 15 | .026 | -13.76736 | 5.575137 | -25.6505 | -1.884237 |
| | Equal variances not assumed | | | -2.408 | 11.823 | .033 | -13.76736 | 5.717954 | -26.2464 | -1.288288 |

Figure 4: Graph




**Reliability and Validity:**

The question of reliability and validity of the data must be addressed at some point and what factors might affect these measures. By definition, reliability is the consistency of the measurement, or the degree to which the survey measures the same way each time it is used under the same conditions with the same subjects. In short, it is considered the repeatability of

the measurement used. In this study, the author attempts to measure the perceived level of preparation within each MTF. Since the DCA was the point of contact, one can assume that he or she has a substantial level of knowledge as to the preparedness of the facility. If the DCA was new to the position, they were given the option to direct the survey to the most knowledgeable person in the organization to assist in answering these questions. This ensures high reliability as we assume there is no change in the underlying conditions of our measurements. Interestingly, most answers (over 80%) were answered directly by the DCA. Only a few surveys were directed to others to answer.

In order to ensure content validity, a thorough examination of the survey questions was conducted. A number of current HIPAA preparedness surveys were reviewed and the central themes extracted for use in this study (See Appendices 3-4), (Cassidy, 2000). To help ensure construct validity, 10 surveys were examined for similarities in questions and ideas. The format along with a portion of the questions came from the OCTAVE assessment system which contains approximately 15 manuals designed to lead the DoD MTF on the road to compliance. By focusing on major points and cross referencing those with what was considered critical in civilian surveys, the magnitude of the error of the measurement was reduced and a nine question instrument was developed. In the initial survey instructions, all respondents were assured that their individual responses would be confidential. As the surveys were returned to the author, the top portion (or header) containing identifying information was removed. When all the responses were returned, they were shuffled and assigned an alphabetical letter. Responses to the final eight questions were then averaged (See Appendices 3-4).

As mentioned previously, training, knowledge, systems surveyed, and expected overall compliance were the central themes in developing the construct to assess preparedness. The

author attempted to ensure the persons selected to do the survey exhibited extensive knowledge on the subject of HIPAA and privacy. The comments received back helped to further clarify the understanding of the requirements among the survey participants. The survey was useful in measuring the perceived level of education of different groups within the treatment facilities. Persons who completed the survey generally indicated that they had been with the organization for greater than six months.

## 4. DISCUSSION

The analysis of the survey responses reveals a strong correlation exists between those organizations that have designated a privacy officer or team and the measure of success as determined by the survey. This correlation is illustrated in the F-score of 6.098 at a .026 level of significance. The results may also be seen in Figure 4 which clearly illustrates that organizations that designate privacy officers are more likely to achieve a higher level of preparedness in privacy-related requirements. The T-test confirms these results with a 2.469 score at the .026 level of significance.

The usefulness of this study is readily apparent. The appointment of a privacy officer has a direct bearing on the success of the MTFs level of preparedness. Commanders may use the findings to help make a decision whether to appoint a full time or part time privacy officer. This decision will likely depend upon the size of the facility along with the skill and number of available personnel. Larger facilities with more complexity and more information systems may require the full time work of a privacy officer. Smaller facilities may be able to designate privacy duties as an additional duty. The Department of Defense is not unique in many of the problems is faces with HIPAA compliance (Staggers et. al., 2000).

Among civilian organizations, the expectation of healthcare facilities throughout the country is not particularly positive with respect to meeting the HIPAA deadlines. According to the American Hospital Association (AHA), a survey of 481 hospitals shows that 43% of the respondents do not expect to meet the transaction and code sets compliance date. Similar results were noted in the comment sections of the surveys sent to the DoD medical facilities. As a result, many organizations such as the American Hospital Association, National Governors Association, and the Workgroup for Electronic Data Interchange are in favor of the additional delays and have lobbied hard to achieve them (Briggs, 2001).

A recent survey by the Health Care Compliance Association conducted at the end of 2001 in New York, indicates where many civilian hospitals and healthcare providers currently stand on the issues of HIPAA preparedness and privacy. The survey indicates that many healthcare providers are beginning to take the steps necessary to become compliant, but still have a long way to go. The survey received 237 responses of which 107 were from hospitals. The majority (93%) of the respondents indicated that they have established a HIPAA task force and 77% stated that they have designated a privacy officer (Marks et. al., 2001).

While many organizations may have designated these positions, the actual work or progress made in the direction of compliance with currently known requirements is often substantially less. For example, only 31 percent of participants have developed a notice of privacy practices for participants in the patient care environment. As part of a litigation prevention strategy, 12 percent have developed loss reduction programs aimed at reducing costly legal battles and potential ensuing judgments (Health Privacy, 2002).

With respect to security levels for employees, medical staff, and business associates, 27 percent have established a system of determining and controlling access to critical areas of the

healthcare facility. The Health Care Compliance Association survey also found that most organizations have already held 1-2 hours of training on HIPAA privacy regulations for physicians, staff, executives, and board members and that 40 percent had developed organizational structures that delineate responsibilities for privacy and security requirements (Marks et. al., 2001).

Cost estimates for privacy, security, and transactions requirements have been developed by 33 percent and policies related to discipline for breach of privacy principles and breaches of security and have been developed by 49 percent. As part of the policy that works hand in hand with loss/litigation prevention practices, 41 percent of organizations have developed a grievance policy to address complaints and breaches of confidentiality (Marks et. al., 2001).

Policies related to patient access to records have been developed by 53 percent of the organizations surveyed although 78 percent indicate they have not developed access to "minimum necessary" information policies. This implies that while many organizations have policies in place to deal with access to patient records, some still have a way to go to reach the minimum standard. Even so, 80 percent of the organizations indicated they have yet to develop policies addressing the potential exposure of protected health information (PHI) through viewing, paging, or other operational activities within the facility. This seems to be in line with the 78 percent above who claim to have to reach a minimum level of security. This also seems to indicate that potential breaches of security may be less related to digital attack than they are to simply poor operational practices. Examples of this might be computer monitors or printouts viewable by unauthorized individuals (Health Privacy, 2002).

Verbal discussion as related to protected health information appear to need clarification or improvement as 73 percent of survey respondents indicated that they have not developed

policies related to discussion of PHI by authorized persons. As we explore the percentages indicated by this unique survey, it becomes apparent that the human element is often lacking in the preparation for security guidelines. Many organizations seem to suspect a greater digital threat to privacy and security from cyber attacks than from accidental or intentional violations from human interactions.

External to the organization, 59 percent of respondents have identified all transactions standards and code sets that will be used in conducting business. It is interesting to note though that only 32 percent have determined preparedness of trading partners with respect to the transfer of this information. Finally, only 28% have systems in place for the ongoing maintenance of standards with respect to transaction and code sets while 47 percent have identified all electronic data and interchange partners. The survey percentages mentioned by (Marks et. al., 2001) offer perhaps the clearest picture of where the healthcare industry stands with regard to privacy and security of patient information. While not a DoD specific survey, the results indicate that many hospitals and healthcare providers have a long way to go to achieve full compliance. On a more positive note, it is quite apparent that HIPAA regulations are making a solid impact on the behavior and planning of our civilian counterparts as many are actively making strides toward compliance. This insight into the progress of civilian institutions offers a useful comparison tool to those in military treatment facilities.

As the nature of the survey indicates, we live in an age where the power of information continues to grow. As a result, privacy is a necessary part of our concern for the welfare of our patients. In the right hands, this information can save lives. In the wrong hands it can damage and destroy peoples' lives. On whose shoulders do we delegate the responsibility of the congressional mandates of privacy legislation in our MTFs? These regulations are as worrisome

in their complexity and breadth as they are in their lack of specificity. Deciphering, dividing, and delegating the many facets of these requirements upon the departments they touch requires a well coordinated plan on the part of the MTF. In the following section, we will explore some of the different ways to handle these evolving requirements in an effort to achieve maximum advantage with minimal invested personnel resources.

## CONCLUSION AND RECOMMENDATIONS

As the survey indicates, a consistent effort by a qualified person or team should be created and staffed in MTFs to handle these challenges. The appointment of a privacy officer in the MTF correlates strongly with the success an organization is experiencing in preparation for HIPAA and privacy regulation. The bottom-line recommendation is to appoint a privacy officer or team as soon as possible and begin the planning process. The complexity begins when one looks at the specifics and diversity of the MTF environment. A few important questions must be answered including: 1) Who should the privacy officer be? Should the position be held by a military officer, government service worker, or should the position be contract worker? 2) Should the position fall under patient administration/records, information management, or should he or she report directly to the commander? 3) What should the duties of the privacy officer be? Should it be an additional duty or a full-time responsibility? We discuss these questions and recommendations further in this section.

As mentioned earlier, the size of a healthcare organization will have a direct impact on its ability to appoint a full-time privacy officer. Smaller facilities may have to designate the work of this position as an additional duty. Ideally, this individual should head a group that is representative of the individual treatment facility's sections. At a an absolute minimum, the privacy team should have representation from Patient Administration, Nursing Services,

Information Management, Legal Services, Administration, and the major services such as the Departments of Surgery and Medicine in the larger MTFs.

The privacy officer must be able to coordinate this diverse group of specialists and draw on the specific knowledge of these individuals to interpret state and federal laws that apply to the use of health information. The group should also actively research and understand the military applicability under these laws. The officer or the team should understand the decision-making processes throughout healthcare facility and ancillary entities that rely on information in order to care for their patient population. The official must be able to direct the flow of information within healthcare organizations and throughout higher headquarters in compliance with the intent of the rulings and the evolving standards.

Commanders should engage early in the planning process and monitor the HIPAA team to assess strengths and vulnerabilities. Members from IT, Patient Administration/Records, Administration, Finance, and Legal areas should be considered part of the core group and be present for all meetings. Not all members need to be a part of the core group as defined but others should be available for consultation on an ad hoc basis. All personnel involved should understand that the need exists to formally document the group's actions and progress to better comply with both HIPAA and JCAHO performance improvement documentation requirements. The privacy rule of HIPAA requires that healthcare organizations inform patients of their privacy rights and what privacy policies and procedures their facility has in place. As mentioned earlier, JCAHO is likely to become quite alert to these issues in future surveys. Planning for a standardized process to accomplish these objectives is initially likely to consume a significant amount of time. Finally, the privacy officer and advisory group must develop these policies and procedures and be prepared to receive and act on privacy complaints. These final two duties

point directly to a series of mandated duties for the creation of such a position under the current HIPAA privacy rule.

Individuals or teams designated to be privacy officers must possess a number of different skills not the least of which is to be able assess, recognize and establish best practices in the management of privacy of health information. This is particularly critical and leads to skills in networking which allow collaboration with other healthcare professionals to ensure appropriate security measures are in place. The privacy officer must be an advocate for the patient, relative to health information confidentiality and must work tirelessly to appropriately manage the release of historically sensitive information. The privacy officer must continue to strive at all times to live by a professional code of ethics specific to maintenance of patient privacy.

From a health information management perspective, these duties and principles should apply to all healthcare information in all its forms within the MTF. The privacy officer and team should have a thorough understanding of the content of health information in its clinical, research, and business contexts. New technologies should be applied as costs and other considerations allow for more efficiently collecting, accessing, storing, transmitting, and successfully using this information in all its forms.

Ideally the privacy officer should have just the right mix of legal, administrative, and technical background. Certainly much discussion exists as to what the optimum mix of skills and experience should be for this role in the healthcare facility. Ideally the privacy officer should be accessible since he or she must be able to answer questions and receive complaints. The privacy officer in the MTF might be an informatics or information management professional, working in patient administration/records, with a strong understanding of the medical information systems in the facility, and the legal issues surrounding HIPAA and privacy.

While that might seem like a tall order to fill, many Commanders and DCAs may be surprised at the level and scope of information technology and legal education among the current workforce. Some individuals have advanced degrees or additional training in these areas that are not currently working in this field. Even without such individuals, it is possible that a current worker with the correct aptitude and desire could be trained to fill a privacy officer position.

It is certainly possible that some DCAs in the MTFs are not aware of the potential impact a qualified privacy officer or team can have on the organization. HIPAA has traditionally been associated as a function of the Information Management Department or under the direction of the Chief Information Officer (CIO). However as quoted earlier, HIPAA is 80 percent planning and only 20 percent technology. The privacy rule, however, incorporates much more internal business practices than it does technologies. Based upon the potential for conflict in approaching information from a security-only perspective, caution should be exercised in this regard. As discussed previously regarding the Microsoft presentation entitled “Oil and Water”, it may be best to ensure that the privacy officer position resides elsewhere in the facility rather than under the direction of the Information Management Division.

A proper roadmap for the MTF to follow in preparing for HIPAA and privacy is to use the OCTAVE system for planning. Once again, 80% of the effort should be dedicated to this area. Commanders should seek to use as many existing tools as possible to prepare for HIPAA. The privacy officer should use the OCTAVE Assessment program developed by Carnegie Mellon University. This is the DoD supported program for planning for privacy implementation. The program is a series of checklists and questions designed to assess preparedness within the facility. The problem with the OCTAVE assessment is that it does not currently exist in any electronic form as of this writing. This means that there is no database structure from which to

generate reports or briefings. Also, it does not allow for the trending of data to help measure performance improvement. From an IT perspective, using this system makes it difficult to track and assess one's progress in preparing to meet these requirements. An excellent model of a program to use in the preparation endeavor is the JCAHO Score 100 program. The program allows individual input and is flexible enough to allow policies specific to the organization to be entered. It can calculate an overall score and give commanders valuable feedback on areas that are doing well and those that need improvement. The final program should contain a briefing module or a way to quickly compile and present the data in meaningful form such as charts and graphs. While such a program is currently in development, for now, assessments should be made with paper and pencil using the checklists.

We will now attempt to answer the three questions posed earlier. 1) Who should fill the role of the privacy officer in the MTF? Due to the rotation of military personnel and the required continuity of the position, it may be best to designate or hire an individual who will have some longevity with the organization. The privacy position is highly paid in the civilian sector with salaries for major companies in the $140-$180 thousand range. While smaller companies pay certainly less, commanders should seek to adequately compensate the position to draw the required skill set. A senior Government Service (GS) position would not be unreasonable for a medium sized facility given the complexity and breadth of compliance requirements.

2) Where in the organization should the privacy officer be located? This question is somewhat more difficult to answer as it may well depend on the design of the facility. Two factors should be considered when selecting a location: 1) Proximity to the base of patient information, and 2) Direct access to the patient population to handle questions and concerns.

3) What should the duties of the privacy officer be? As far as the duties of the privacy officer we have to look at the size and resource available to the organization before making a decision on weather a full-time individual is appointed or hired versus an additional duty to an existing position. For larger medical centers, it is advisable to have a full time position. Smaller treatment facilities and satellite clinics can most likely function with an individual who has been assigned this additional duty. If possible, this individual should seek to reserve a full-time seat on the core group of the parent treatment facility.

As the deadlines begin to approach, commanders must begin to take seriously the appointment of privacy officers. Almost 50% of those surveyed indicated that they had not yet appointed a privacy officer or team. Commanders have a number of civilian medical facilities to reference as models for guidance on some of the requirements sought in these individuals. The hospital commander should seriously consider these requirements when seeking to fill the position of the privacy officer in the MTF (See Appendix 3 for more details on a general example of the position requirements of a privacy officer in the civilian sector).

Privacy and HIPAA are closely intertwined within the working of the medical facility and the complexity further increases when dealing with specific military issues. The tools available to the MTF such as the OCTAVE assessment program are not perfect, but they are a start in the right direction. The sooner we as a service make the transition to understanding how broadly and deeply these regulations will affect us, the sooner we will act to provide the proper planning, leadership, and guidance to be successful in providing the highest quality of care in this rapidly changing environment.

Appendix 1

**Survey of MTFs** **Organization Name**: _____

Reporting Official: _____

1. Has your MTF designated a privacy officer to address HIPAA compliance concerns?

1 = Yes 2 = No

**The following questions are rated on a scale of 1-10 with 10 being the highest.**

2. How many hours of training will you dedicate (per user) on HIPAA compliance?

1 2 3 4 5 6 7 8 9 10+

3. How far along is your organization in planning for privacy and HIPAA compliance?

1 2 3 4 5 6 7 8 9 10

4. What is the level of knowledge of privacy requirements among your IT personnel?

1 2 3 4 5 6 7 8 9 10

5. What is the level of knowledge of privacy requirements among your admin personnel?

1 2 3 4 5 6 7 8 9 10

6. What is the level of knowledge of privacy requirements among healthcare providers?

1 2 3 4 5 6 7 8 9 10

7. Percentage of systems surveyed for HIPAA compliance.

1 2 3 4 5 6 7 8 9 10

8. How compliant do you expect to be by the implementation deadlines in 2002?

1 2 3 4 5 6 7 8 9 10

9. How compliant do you believe you are now with current HIPAA requirements?

1 2 3 4 5 6 7 8 9 10

**Notes and Other Observations: Other Concerns with Privacy Compliance**

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

Conducted By: _____ Date: _____

Appendix 2

| Entity | States that Provide Access | Total |
|---|---|---|
| State Provides Some Access | AL*, AK, AZ, CA, CO, CT, DC*, DE, FL, GA, HI, ID*, IL, IN, KY, LA, MA, ME, MD, MI, MN, MS, MO, MT, NC, NH, NJ, NM,* NY, NV, OH, OK, OR, PA, RI, SC, SD, TN, TX, VA, WA, WI, WV, WY<br>* The state only explicitly grants patients access to mental health Records (4 total). | 44 |
| Hospitals and Health Care Facilities | AK, AZ, CA, CT, CO, GA, HI, IL, IN, KY, LA, MA, ME, MI, MN, MO, MS, NJ, NH, NY, NV, OH, OK, PA, SC, SD, TN, TX, VA, WA, WI, WV, WY | 33 |
| Health Care Parishioners, Providers, or Physicians | AK, AZ, CA, CT, CO, FL, GA, HI, IL, IN, LA, MA, MD, ME, MN, MO, MT,NH, NY, NV, PA, SC, SD, TN, TX, VA, WA, WI, WV | 29 |
| HMO:s | CA, CT, GA, HI, IL, MA, MN, MT, NC, NJ, NY, PA, VA | 13 |
| Insurers | AZ, CA, CT, HI, IL, MA, MD, ME, MN, MT, NC, OH, NJ, OR, RI, VA, WI | 17 |
| Optometrists | CO, SD, WI | 3 |
| Pharmacists or Pharmacies | AK, AZ, CO, CT, HI, IN, LA, NV, SD, VA, WI | 11 |
| Mental Health Records (Explicit Access Granted) | AL, AZ. CT, DC, DE, FL, GA, ID, IL, IN, MI, MO, MS, NC, NM, NV, OH, SC, SD, TX, VA, WI | 22 |
| Additional Access: | AK, CO, FL, MN, NY, SC, WI | 7 |
| No access provided | AR, *IA, KS, ND, NE **, VT, UT*** | 7 |

for in statute.

* The state only provides access in conjunction with an anticipated or on-going legal proceeding.

** The state only provides access in connection with proceedings for commitment to a mental health facility.

*** The state only provides limited access to an attorney or to government records.

The State of Health Privacy: An Uneven Terrain, (A Comprehensive Survey of State Health Privacy Statutes), (Georgetown University, 2002).

Appendix 3

A typical job description for the privacy officer was published recently by AHIMA, 2001.

**Position Title:** (Chief) Privacy Officer[1]

**Immediate Supervisor:** Chief Executive Officer, Senior Executive, or Health Information Management (HIM) Department Head[2]

**General Purpose:** The privacy officer oversees all ongoing activities related to the development, implementation, maintenance of, and adherence to the organization's policies and procedures covering the privacy of, and access to, patient health information in compliance with federal and state laws and the healthcare organization's information privacy practices.

**Responsibilities:**

- Provides development guidance and assists in the identification, implementation, and maintenance of organization information privacy policies and procedures in coordination with organization management and administration, the Privacy Oversight Committee,[3] and legal counsel.
- Works with organization senior management and corporate compliance officer to establish an organization-wide Privacy Oversight Committee.
- Serves in a leadership role for the Privacy Oversight Committee's activities.
- Performs initial and periodic information privacy risk assessments and conducts related ongoing compliance monitoring activities in coordination with the entity's other compliance and operational assessment functions.
- Works with legal counsel and management, key departments, and committees to ensure the organization has and maintains appropriate privacy and confidentiality consent, authorization forms, and information notices and materials reflecting current organization and legal practices and requirements.
- Oversees, directs, delivers, or ensures delivery of initial and privacy training and orientation to all employees, volunteers, medical and professional staff, contractors, alliances, business associates, and other appropriate third parties.
- Participates in the development, implementation, and ongoing compliance monitoring of all trading partner and business associate agreements, to ensure all privacy concerns, requirements, and responsibilities are addressed.

- Establishes with management and operations a mechanism to track access to protected health information, within the purview of the organization and as required by law and to allow qualified individuals to review or receive a report on such activity.
- Works cooperatively with the HIM Director and other applicable organization units in overseeing patient rights to inspect, amend, and restrict access to protected health information when appropriate.
- Establishes and administers a process for receiving, documenting, tracking, investigating, and taking action on all complaints concerning the organization's privacy policies and procedures in coordination and collaboration with other similar functions and, when necessary, legal counsel.
- Ensures compliance with privacy practices and consistent application of sanctions for failure to comply with privacy policies for all individuals in the organization's workforce, extended workforce, and for all business associates, in cooperation with Human Resources, the information security officer, administration, and legal counsel as applicable.
- Initiates, facilitates and promotes activities to foster information privacy awareness within the organization and related entities.
- Serves as a member of, or liaison to, the organization's IRB or Privacy Committee,[4] should one exist. Also serves as the information privacy liaison for users of clinical and administrative systems.
- Reviews all system-related information security plans throughout the organization's network to ensure alignment between security and privacy practices, and acts as a liaison to the information systems department.
- Works with all organization personnel involved with any aspect of release of protected health information, to ensure full coordination and cooperation under the organization's policies and procedures and legal requirements
- Maintains current knowledge of applicable federal and state privacy laws and accreditation standards, and monitors advancements in information privacy technologies to ensure organizational adaptation and compliance.
- Serves as information privacy consultant to the organization for all departments and appropriate entities.
- Cooperates with the Office of Civil Rights, other legal entities, and organization officers in any compliance reviews or investigations.
- Works with organization administration, legal counsel, and other related parties to represent the organization's information privacy interests with external parties (state or local government bodies) who undertake to adopt or amend privacy legislation, regulation, or standard.

**Qualifications:**

- Certification as an RHIA or RHIT with education and experience relative to the size and scope of the organization.
- Knowledge and experience in information privacy laws, access, release of information, and release control technologies.
- Knowledge in and the ability to apply the principles of HIM, project management, and change management.
- Demonstrated organization, facilitation, communication, and presentation skills.

This description is intended to serve as a scalable framework for organizations in development of a position description for the privacy officer.

**Notes**

1. The title for this position will vary from organization to organization, and may not be the primary title of the individual serving in the position. "Chief" would most likely refer to very large integrated delivery systems. The term "privacy officer" is specifically mention in the HIPAA Privacy Regulation.
2. Again, the supervisor for this position will vary depending on the institution and its size. Since many of the functions are already inherent in the Health Information or Medical Records Department or function, many organizations may elect to keep this function in that department.
3. The "Privacy Oversight Committee" described here is a recommendation of AHIMA, and should not be considered the same as the "Privacy Committee" described in the HIPAA privacy regulation. A privacy oversight committee could include representation from the organization's senior administration, in addition to departments and individuals who can lend an organization-wide perspective to privacy implementation and compliance.
4. Not all organizations will have an Institutional Review Board (IRB) or Privacy Committee for oversight of research activities. However, should such bodies be present or require establishment under HIPAA or other federal or state requirements, the privacy officer will need to work with this group(s) to ensure authorizations and awareness are established where needed or required.

Appendix 4

Assessing Your HIPAA Readiness as an Organization

1. Does your organization have a group or individual responsible for HIPAA information and compliance planning?

2. Has your organization completed an internal high-level assessment for HIPAA compliance in these areas: privacy, security, data sets, and/or transaction standards?

3. Has your organization determined resources required to comply with HIPAA standards?

4. Has your organization created a "two-year action plan" as a result of conducting the high-level assessment?

5. Is your comprehensive two-year action plan consistent with information system and corporate strategic plans?

6. Have you created a step-by-step implementation work plan? Does someone "own" this?

7. Does your organization have a migration plan for electronic data interchange solutions?

8. Has your organization created a "vision of a future state"? Does the vision include best practices?

9. Does your organization have contractual obligations related to the implementation of government mandates?

Appendix 5

Assessing Your HIPAA Readiness Through Your Health Information Managers

1. Are you current on the regulations?

2. Have you established a Master Patient Index (MPI) cleanup plan (or have it completed)?

3. Are you active in working with your peers in improving the patient registration system?

4. Are ongoing data integrity checks in place?

5. Is the charge description master (CDM) kept up to date? Are health information managers playing a leadership role in the CDM updates?

6. Have you worked with your organization's information systems department to set up interfaces and cross-referencing?

7. Have you (or your team) conducted risk assessments on security?

8. Have you conducted a comprehensive analysis of current procedures in your health information department and throughout the revenue cycle?

9. Did you prepare work flows? Data modeling?

10. Have you encouraged your employees and peers to attend HIPAA continuing education programs?

## References

American Health Information Management Association. (2001). Sample (Chief) privacy officer job description. Retrieved February 6, 2002, from the World Wide Web: http://www.ahima.org/infocenter/models/PrivacyOfficer2001.htm

American Hospital Association. (2002). The one-year extension for complying with HIPAA's standards for electronic transactions: How does it affect you? Retrieved February 6, 2002, from the World Wide Web: http://www.aha.org/hipaa/resources/electransactextention.asp

Auston, I., Humprheys, B., Clayton, P., Kohane, I., Hoffman, L., & Geisslerova, Z., (1996). Confidentiality of electronic data: Methods for protecting personally identifiable information, US Department of Health and Human Services. Retrieved October 2, 2001, from the World Wide Web: http://aspe.hhs.gov/datacncl/privbibl.htm.

Blair, J. (1996). An overview of healthcare information standards. October 2, 2001, from the World Wide Web: http://cpri-host.org/resource.

Briggs, B. (2001). HIPAA rules demand changes. Health Data Management, August, Vol. 9, No. 9. 2001.

Guardant Press Release, (2001). Top business leaders assemble in Chicago to debate emerging security and privacy issues. Privacy and Security: Oil and Water?, Retrieved March 28, 2001, from the World Wide Web: http://www.guardent.com/pr2001-07-09-01-OnlinePrivacy.html

Gostin, L., Lazarini, Z., & Flaherty, K. (1996). Legislative survey of state confidentiality laws, with specific emphasis on HIV and immunization. U.S. Centers for Disease Control Prevention. Retrieved October 3, 2001, from the World Wide Web: http://www.epic.org/privacy/medical/cdc_survey.html.

Howard, P, (2001). Time to get serious about e-trust, ZDNet, May 10, 2001.

Joseph, S.C. (1997). Statement to Assistant Secretary of Defense for Health Affairs before the National Committee on Vital and Health Statistics.

Kelly, B. (2001). New officer prepare to protect privacy. Health Data Management, August, Vol. 9, No. 8.

Kelly, B. and Goedert, J. (2001) New legislation means HIPAA delays still on congressional plate. Health Data Management, August, Vol. 9, No. 7.

Kibbe, D., Bard, M. (1997). How safe are computerized medical records? American Academy of Family Physicians, 4(5), p. 21-30.

Landro, B. (2001). Health policy groups put data network on government agenda. Wall Street Journal, p. B1. March 16th, 2001.

Leahy, P. (1997). New bill offers medical privacy parameters for the information age. Privacy of Medical Records Committee on Labor and Human Resources, U.S. Senate. Retrieved October 2, 2001, from the World Wide Web: http://www.senate.gov/~leahy/press/199710/971028.html.

Lanser, E. G. (2001). Capitalizing on HIPAA Compliance. Healthcare Executive, Vol. 16, Number 3, May/June 2001).

MacMillan, R. (2001). Chief Privacy Officer: It's A Dirty Job But… Newsbytes. Retrieved October 2, 2001, from the World Wide Web: http://www.newsbytes.com/nes/01/162913.html

Manning, W. (1997). Privacy and confidentiality in clinical data management systems: Why you should guard the safe. The Health Law Resource. Retrieved October 2, 2001, from the World Wide Web: http://www.netreach.net/~wmanning/cdm.htm.

Marks, L. and Koshykar, W. (2001) Healthcare begins HIPAA preparations. HANYS News, Vol. 33, No. 50., 2001.

Marks, L. and Van Meter, S (2001). Bill would require hospitals to apply for HIPAA extension. HANYS News, Vol. 33, No. 50.

Mendels, P. (2000). The Rise of the Chief Privacy Officer. Business Week Online. Retrieved October 2, 2001, from the World Wide Web: http://www.businessweek.com/careers/content/dec2000/ca20001214_253.htm

Peterson, S. (2001). Unintended Consequences, Government Technology, February, 2002.

Privacy Leadership Initiative, 2001. Privacy Officer Associations. Retrieved March 28, 2002, from the World Wide Web: http://www.understandingprivacy.org/content/pmrc/officer.cfm

Rutherford, E. (2001). CIOs split over new health care regulations. CIO. Retrieved October 2, 2001, from the World Wide Web: http://www.cio.com/poll/052201.html

Schlesinger, L. (2001). Hire a chief privacy officer to keep sensitive material private. Zdnet Tech Update. Retrieved October 2, 2001, from the World Wide Web: http://www.zdnet.com/eweek/stories/general/0,11011,2716442,00.htm

The State of Health Privacy: An Uneven Terrain, (A Comprehensive Survey of State Health Privacy Statutes Retrieved May 1, 2002, from the World Wide Web: http://www.healthprivacy.org

Staggers, N., & Leaderman, A., (2000). The Vision for the Department of Defense's Computer-Based Patient Record. Military Medicine, 165, 180-181.

Standards for Privacy of Individually Identifiable Health Information, 45 CFR Parts 160 and 164, Retrieved March 2, 2002, from the World Wide Web: http://aspe.hhs.gov/admnsimp/final/pvcguide1.htm

Streveler, D. J. (2001). e-Health Care and Community Connectivity, Healthcare Landscape 2001. South Texas Joint Health Care Conference, San Antonio, TX.

Tirone, Anthony. (2001). How HIPAA affects JCAHO accreditation. Joint Commission Perspectives. Vol.21 No. 7., July 2001).

TRICARE Press Release, (Baltimore, March 12, 2001). Northeast Contractor Takes Proactive Steps toward Ensuring Patient Privacy and Implementing Senior Services, Retrieved March 28, 2002, from the World Wide Web: http://www.sierramilitary.com/press/PR_031201.htm)

U. S. Department of Veterans Affairs (1999). Computerized patient record system (CPRS) GUI reference materials. Office of Chief Information Officer, CIO National Training and Education Office.

USA Today, Tech Report, (2000). Meet the CPO: Chief Privacy Officer. Retrieved October 2, 2001, from the World Wide Web: http://www.usatoday.com/life/cyber/tech/cti212.htm

Wilcox, J. (2000). IBM appoints chief privacy officer. CNET News. Retrieved October 2, 2001, from the World Wide Web:

http://news.cnet.com/news/0-1003-200-3898890.html