A Study of U.S. Battlefield Medical Treatment/Evacuation Compliance with HIPAA Requirements

John Chessman
Captain, United States Air Force

Alan R. Heminger, Ph.D.
Air Force Institute of Technology
alan.heminger@afit.edu

The views expressed in this paper are those of the authors and do not reflect the official policy or position of the United States Air Force, Department of Defense, or the United States Government

Abstract

The Health Insurance Portability and Accountability Act (HIPAA, 1996) requires secure and private treatment of medical information. Congress included the U.S. military healthcare system under HIPAA's umbrella. However, a combat environment can place unusual constraints on the provision of medical services. This paper develops a model of battlefield medical treatment and evacuation, and then uses the knowledge of experts in a Delphi group to assess the completeness and accuracy of that model, and to recommend improvements to the process.

The Delphi group agreed that partial compliance is provided for HIPAA at the beginning of treatment and evacuation, and full compliance is followed later in the process. Recommendations for improving this model were largely administrative, (written guidance, training, and use of cover sheets.) Authorities may want to revisit the issue of the partial compliance to bring law and policy into agreement with practice learned in the crucible of the battlefield.

1. Introduction

The Health Insurance Portability and Accountability Act (HIPAA) of 1996, Public Law 104-191, was enacted on August 21, 1996, and went into effect on April 14, 2003. HIPAA was intended to protect the health insurance coverage for working families when they changed or lost their jobs, guard against fraud, waste, and abuse, and establish specific requirements for security, privacy, and administrative simplification in the exchange of electronic health data among employers, insurers, and providers [1]. The Military Health System is considered a health plan under HIPAA law and is obligated to comply with all HIPAA regulations [3]. The battlefield is a uniquely military environment in which time is of the essence, and the extra burdens imposed by HIPAA compliance could impact the survival of military wounded.

The purpose of this study is to examine the implementation of HIPAA during battlefield medical treatment to determine how HIPAA is being interpreted by those providing battlefield medicine and to determine where it may make sense for battlefield medical teams to comply with HIPAA regulations when treating military wounded.

HIPAA has three main parts: (1) Insurance Portability, (2) Preventing Health Care Fraud and Abuse, and (3) Administrative Simplification, focusing on privacy and security [14]. This study will address only the Administrative Simplification section of HIPAA. Administrative Simplification is intended to protect access to patient protected health information (PHI) and improve the efficiency and effectiveness of the health care system by standardizing electronic data exchange. HIPAA requires appropriate technical, administrative and physical safeguards to protect the privacy of health information. HIPAA is designed to standardize the handling of PHI and to promote data standards for the electronic exchange of medical information [14].

HIPAA Administration Simplification implementation is guided by two formal rules: the Security Rule and the Privacy Rule. The Security Rule describes the standards for the security of electronic PHI in any electronic medium [9]. The Privacy Rule protects all individually identifiable health information records held or transmitted by a covered entity and specifies who can access the patient information [12, 13]. The Privacy Act of 1974 and HIPAA Privacy Rule have very similar requirements. The Security and Privacy rules are the basis for handling and transmitting protected health information in all media [18].

The active duty Military Health System is specifically mentioned in the HIPAA law. All
Military Treatment Facilities must comply with the HIPAA regulations. The Department of Defense (DoD) position is that HIPAA also applies to battlefield medical treatment [2]. The law does permit exceptions to support unique military requirements such as information crucial to force health readiness. HIPAA places additional administrative burdens on deploying medical forces [3]. Additional administrative personnel are required to process the extra requirements and properly protect the information. The forms, paper, and processing equipment required take up precious pallet space on military airlift. For these reasons alone, the Air Force medical community has requested waivers to HIPAA compliance [2, 7].

1.1. Need for Solution

When HIPAA was written, Congress made it clear that HIPAA applies to the DoD. However, it did not foresee all of the potential impacts of the HIPAA regulations on military operations. For example, any information about battlefield casualties which could lead to the identification of a specific member is prohibited from public release. This has implications for family members’ ability to get a status update and even state governors and members of congress ability to obtain casualty information for their districts. Senator Ted Kennedy, one of the sponsors of the HIPAA bill, has publicly said it was not his intent to block battlefield casualty information from being released when HIPAA was written. Yet this is one of the unintended consequences of the HIPAA law [17]. Thus, it appears not to make sense for HIPAA to completely apply to battlefield wounded at all stages of the treatment process, yet the intention of Congress was to apply it to the U. S. military. This has led to confusion as to where it should take effect. At some point between being wounded and arriving back in the United States for treatment the HIPAA requirements take effect.

1.2 Problem to be researched

This study will explore how the Administrative Simplification, security and privacy provisions of HIPAA are currently being implemented in the provision of U.S. Military battlefield medicine, as well as seeking to elicit recommendations for improvements from those involved in the process.

1.3. Scope

Of the three main parts of HIPAA, (1) Insurance Portability, (2) Preventing Health Care Fraud, and (3) the security and privacy rules of Administrative Simplification, the security and privacy issues appear to have particular relevance to how medical treatment is provided on the battlefield. Therefore, the study was limited to HIPAA compliance with the security and privacy aspects of the HIPAA law during the battlefield medical treatment/evacuation process. Further, much of the emphasis was on the Air Force evacuation steps, because the Air Force is the primary service to carry out the evacuation of battlefield wounded.

2. Literature Review

Public Law 104-191, The Health Insurance Portability and Accountability Act (HIPAA) was signed into law by President Clinton on August 21, 1996. HIPAA protects individuals from losing their health coverage when changing jobs (Portability) and it increases the federal government’s authority over medical fraud and abuse (Accountability) [8]. The HIPAA law lists the Military Health System as a Health Plan, which is a covered entity under HIPAA and subject to the HIPAA regulations [3]. Covered entities are health care providers, health plans, and health care clearinghouses. They are required to protect individually identifiable health information. Protected health information (PHI) is individually identifiable health information relating to an individual's past, present, or future physical or mental health condition, provision of health care, or payment for the provision of health care [1].

To improve the efficiency and effectiveness of the health care system, Congress included Administrative Simplification provisions into HIPAA [14]. Sections 261 through 264 require the Secretary of the Department of Health and Human Services (HHS) to publish national standards for the electronic exchange, privacy and security of electronic health care information transactions between covered entities and these together are known as the Administrative Simplification provisions [14]. Congress recognized that the pace of electronic technology advances would endanger the security and privacy of health information. [12]. To meet this need, Congress included provisions in HIPAA that mandated federal privacy protections for individually identifiable health information [3]. Another goal of HIPAA was the development of the electronic health record, or the electronic medical record as it is commonly referred
to. Electronic medical records help reduce the administrative costs of updating, storing, and protecting health records. The HIPAA Administrative Simplification provisions are guided by two rules: the Security Rule and the Privacy Rule [14].

While we found no research that directly addressed HIPAA compliance on the battlefield, situated learning [11] suggests that we may find that the actual practice of battlefield medicine with respect to HIPAA compliance with security and privacy may not map directly to the explicit expectations of the law. Situated learning suggests that learning occurs as a function of the activity, the context in which it takes place, and the culture of the participants. In other words, learning to do something as a member of a community of practice is affected not only by the abstract knowledge that can be delivered in a sterile or academic environment; it is also affected by the context in which the activity occurs, and the culture of those involved. Thus, in a war zone, we could expect that a medical team would learn to carry out its tasks in the context of an active battlefield and the culture of those operating in that environment.

Thus, we might expect that the actual practice of providing battlefield medicine may not look exactly like it would be presented in an abstract classroom far removed from the chaos, fear, and confusion of a life-threatening environment.

### 2.1. Security Rule

The Administrative Simplification provisions of HIPAA required the Department of Health and Human Services to establish national standards for the security of electronic health care information. The Health Insurance Reform: Security Standards, better known as the Security Rule, describes the standards for the security of electronic protected health information (E PHI), The Security Rule was published in the Federal Register on February 20, 2003, and final compliance took effect on April 21, 2006. The Security Rule has three subsections: Administrative, Physical, and Technical. Administrative safeguards are policies and procedures to clearly demonstrate how the entity will comply with HIPAA, and include written privacy policies and the designation of a Privacy Officer. Physical safeguards control physical access to protected health information to avoid unauthorized access to protected data. Technical safeguards control access to computer systems and protect PHI transmitted over open networks from being intercepted [9].

### 2.2. Privacy Rule

HIPAA required the Secretary of HHS to issue privacy regulations covering PHI within three years of passing if Congress did not enact Privacy Legislation. In 1999, Health and Human Services (HHS) published the Standards for Privacy of Individually Identifiable Health Information, or the Privacy Rule, and it went into effect on April 14, 2003. The Privacy Rule protects all individually identifiable health information held or transmitted by a covered entity. Unlike the Security Rule, the Privacy Rule is not limited to PHI in electronic format. It covers all PHI information in any format to include: electronic, written, or oral form. The Privacy Rule applies to health plans, health care clearinghouses, and to any health care provider who transmits health information in electronic form [13].

The Privacy Rule gives patients more control over their medical records. Patients have the right to see their records, the right to request corrections to the record, and the right to restrict its use for certain purposes. The privacy rule also requires that covered entities provide their privacy policies to their patients on their first visit. The HHS Office for Civil Rights is charged with enforcing the Privacy Rule [13].

### 2.3. HIPAA Impact

The Floyd D. Spence National Defense Authorization Act for Fiscal Year 2001 required the DoD to develop regulations to improve the privacy protections of DoD medical records. The Act required a comprehensive plan be submitted to Congress to improve medical record privacy protection. The Act also required the plan to be consistent with the soon-to-be-implemented HIPAA requirements [18]. The Act passed during the interim period after HIPAA was in effect on 14 April 2003. The Authorization Act shows Congress’s determination to protect the privacy of all Health information regardless of the entity.

The Military Health System is considered a health plan under HIPAA and must comply with the requirements of HIPAA as if it were a civilian healthcare plan [3]. HIPAA does make certain limited exceptions to meet unique military requirements, such as the transfer of medical information about active duty force health readiness [3]. Compliance to the HIPAA provisions has required and will continue to require considerable resources from the DoD. Full compliance with all sections of HIPAA is expected to cost over $100 million [17].

Under the HIPAA privacy rules, individually identifiable health information is not allowed to be
publicly reported without the express permission of the patient or next of kin. It is possible that if a service member has not authorized the release of his or her PHI, then not even family members are authorized to receive medical updates [17]. HIPAA regulations make tracking casualty information difficult even for state governors and members of congress [2, 17].

Literature relating directly to HIPAA on the battlefield is almost non-existent. Most information relating to active duty health is focused on the Military Treatment Centers in the United States and established bases overseas, where the normal HIPAA requirements are identical to those of civilian facilities. There are indications that the HIPAA requirements put an enormous burden on deployed medical teams. A 2004 position paper by Maj Greentree AF/SGMA suggested the HIPAA requirements detract from the primary medical mission of treating and evacuating patients. HIPAA would require that extra administrative personnel and supplies be transported on already crowded airlift assets. The position paper recommended excluding Air Force Medical Service deployed units and operating forces from HIPAA compliance while in theater [7].

The literature is clear that the military is required by law to comply with HIPAA regulations under normal day to day operations. Congress included the Military Health System in the language of the HIPAA law to ensure it was covered. Given the demands of the myriad of privacy regulations the military must adhere to and the exemptions allowed under HIPAA, it is not clear when real world enforcement makes sense in a combat theater of operations. If the question is asked of the military medical community, the quick answer will likely be, “It applies everywhere.” The reality of enforcement in a theater of active combat operations may be quite different.

3. Methodology

This study used the Delphi Method to address the research problem. Delphi Studies were developed by the RAND Corporation for the US Air Force as a method of forecasting solutions to strategic military problems. It is a method for utilizing the expertise of a group of experts while minimizing the negative aspects of group interactions by eliminating the need for physical interaction among the group members. It is intended to “obtain the most reliable consensus of opinion of a group of experts” [5]. It uses a series of questionnaires and controlled opinion feedback [6, 15].

The Delphi panel for this study was comprised of HIPAA and Privacy officers, a civilian HIPAA expert from a major university, emergency room personnel, and medical readiness specialists. Because of the proximity of the researchers to a major U.S. Air Force base, it was possible to find people in each of these knowledge areas who had extensive experience and knowledge of their part of the overall issues. The panel members were selected from among the available people based on both the researchers’ informal assessment of their particular expertise, and their reputation among their peers in the local area. The Delphi study questionnaire was developed from the results of the literature review and initial interviews of medical personnel.

There is no clear consensus concerning the appropriate number of participants for a Delphi study [15], but the number seems to fluctuate somewhere between 7 [5] and 15 [16]. If the Delphi participants all come from the same discipline (e.g. computer programmers) the general rule of thumb is 15-30 participants, whereas a more heterogeneous population (expertise in the same area, but pulled from different social/professional levels) would only require 5-10 participants [4]. Since the participants for this study came from different disciplines, it was determined that somewhere between 5 and 10 participants would be sufficient.

3.1. Initial Model

A conceptual model of the battlefield treatment/evacuation process was developed from information gleaned from unstructured interviews with 3 recently deployed military personnel. They had all recently served in the medical field in the Iraq theatre. This model provided the beginning point for the Delphi group’s efforts to reach agreement on the as-is model of battlefield treatment and evacuation. The initial model consisted of the following six steps.

<table>
<thead>
<tr>
<th>Table 1 Initial Battlefield Treatment/ Evacuation Model</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 – Battlefield treatment/evacuation</td>
</tr>
<tr>
<td>Step 2 – Battalion Aid Station</td>
</tr>
<tr>
<td>HIPAA Issues Unit inquiries</td>
</tr>
<tr>
<td>Step 3 - Medical Company</td>
</tr>
<tr>
<td>HIPAA Issues Unit inquiries</td>
</tr>
<tr>
<td>Step 4 – Combat Support Hospital (CSH)</td>
</tr>
<tr>
<td>HIPAA Issues Unit inquiries</td>
</tr>
<tr>
<td>Step 5 – Air Force Theater Hospitals</td>
</tr>
<tr>
<td>HIPAA Issues Covered charts</td>
</tr>
<tr>
<td>50 person bays</td>
</tr>
<tr>
<td>Step 6 – Army Medical Center</td>
</tr>
</tbody>
</table>
3.2. Delphi Group

The Delphi group members were Active Duty and Civilian Air Force medical personnel, an Active Duty Army surgeon, and a civilian university professor. Subjects were selected based on two factors: HIPAA knowledge and deployed medical experience in a combat arena. The criterion for deployment was at least one deployment to a combat theater of operations in the last three years in a medical capacity. For selection based on HIPAA knowledge the criteria was extensive knowledge of HIPAA in a military medical environment. Two civilian HIPAA experts were on the panel, one of whom is a university professor who served on a HIPAA advisory committee to congress when the law was drafted. The military members were emergency room and deployment readiness experts who have extensive medical experience in a deployed, combat environment. These are personnel who each have multiple deployments to medical facilities in the Iraq and Afghanistan Theaters of operations and have been involved with HIPAA compliance while deployed.

The following protocol was developed to guide the Delphi study: Building on the initial as-is battlefield treatment/evacuation model, flesh out and validate the model based on input from the Delphi group. Then, based on the improved as-is model, ask the Delphi group to recommend a to-be model of HIPAA compliance. Before Round One, the model and questions were pilot tested on 2 individuals and they were found to be clear after a few minor changes were made.

4. Results of the study

Round one of the Delphi study included the initial model, plus a questionnaire, asking the Delphi group members to express their level of agreement with the model and to suggest any changes needed to make it more accurate.

Eight surveys were sent out and seven were returned over a three week period. All seven members of the Delphi group responded to all questions. All seven members of the panel agreed with the model in general. However, five of the seven members pointed out missing steps that could be included to make the model more accurate. The changes and additional steps were incorporated into the new models for round two. The responses about compliance with HIPAA were divided between full compliance and partial compliance at various steps. When those in the group said that the treatment/evacuation model used partial compliance, they were specifically referring to partial compliance in two areas. First, partial compliance occurred when medical treatment took precedence over administrative tasks, and when letting a wounded soldier’s buddies know his/her condition at or near the battlefield. This division spawned two models for round two reflecting the split in responses. The differences were between partial and full compliance with the HIPAA requirements.

Table 2: Round one Battlefield Treatment/Evacuation Model 2A

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>HIPAA Issues</th>
<th>HIPAA Compliance</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Battlefield treatment/evacuation</td>
<td>Unit inquiries</td>
<td>Full</td>
</tr>
<tr>
<td>2</td>
<td>Battalion Aid Station</td>
<td>Unit inquiries</td>
<td>Full</td>
</tr>
<tr>
<td>3</td>
<td>Medical Company</td>
<td>Unit inquiries</td>
<td>Full</td>
</tr>
<tr>
<td>4</td>
<td>Combat Support Hospital (CSH)</td>
<td>Unit inquiries</td>
<td>Full</td>
</tr>
<tr>
<td>5</td>
<td>AF Contingency Aeromedical Staging Facility (AFCASF)</td>
<td>Unit Inquiries</td>
<td>Full</td>
</tr>
<tr>
<td>6</td>
<td>Air Force Theater Hospitals</td>
<td>Unit Inquiries</td>
<td>Full</td>
</tr>
<tr>
<td>7</td>
<td>AF Contingency Aeromedical Staging Facility (AFCASF)</td>
<td>Unit Inquiries</td>
<td>Full</td>
</tr>
<tr>
<td>8</td>
<td>Army or AF Medical Center</td>
<td>Unit Inquiries</td>
<td>Full</td>
</tr>
<tr>
<td>9</td>
<td>Return to U.S.</td>
<td>Unit Inquiries</td>
<td>Full</td>
</tr>
</tbody>
</table>

Table 3: Round one Battlefield Treatment/Evacuation Model 2b

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>HIPAA Issues</th>
<th>HIPAA Compliance</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Battlefield treatment/evacuation</td>
<td>Unit inquiries</td>
<td>Partial</td>
</tr>
<tr>
<td>2</td>
<td>Battalion Aid Station</td>
<td>Unit inquiries</td>
<td>Partial</td>
</tr>
<tr>
<td>3</td>
<td>Medical Company</td>
<td>Unit inquiries</td>
<td>Partial</td>
</tr>
</tbody>
</table>
A panel member who had served in the Afghanistan area of operations responded to the question, ‘In general, do you agree with the model?’, that the model did not allow for the differences between Iraq and Afghanistan. But in general, it represented the ‘general scheme of things’ and that operational situations may dictate changes to the flow of the model. On the next question, ‘Do you have any changes to make to the model?’ he stated that the Afghanistan treatment/evacuation process is very compressed compared to the Iraq model. In Afghanistan, the Forward Surgical Teams (FST) are split in half and are co-located with Battalion Aid Stations on small forward bases along the Pakistan border. The combat support hospital (CSH) in Afghanistan is also the Theater Hospital and the Contingency Aeromedical Staging Facility (CASF), and the patients are evacuated straight to the OCONUS step of the treatment/evacuation model. This was a surprise finding due to the fact that up to this point in the study, all research suggested that the Iraq and Afghanistan theaters of operations were the same from a treatment/evacuation perspective. Most of the panel members had only been deployed to the Iraq or Kuwait theater of operations and apparently were unaware of the differences between these areas and the Afghanistan theater of operations. These findings prompted the creation of a separate model to reflect the Afghanistan battlefield medical treatment/evacuation procedures (See Table 4 below). In response to the question “How does HIPAA apply at each stage?”, the panel member with Afghanistan experience reported that, in Afghanistan, the patient documentation relating to care and evacuation for the CSH is entered and stored in a secured clinical database which makes it easier to be tracked by all authorized parties. On the ground, the commanders are made aware of all pertinent medical information that affects the mission capabilities of his/her soldiers and unit. The system has both security and privacy built in. This helps meet HIPAA requirements, but according to the panel member the system is focused primarily on operational security.

Table 4: Battlefield Treatment/Evacuation Model for Afghanistan

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Battlefield treatment/evacuation</th>
</tr>
</thead>
<tbody>
<tr>
<td>HIPAA Compliance</td>
<td>Partial</td>
</tr>
<tr>
<td>HIPAA Issues</td>
<td>Unit inquiries</td>
</tr>
<tr>
<td>HIPAA Compliance</td>
<td>Full</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Battalion Aid Station</th>
</tr>
</thead>
<tbody>
<tr>
<td>HIPAA Compliance</td>
<td>Partial</td>
</tr>
<tr>
<td>HIPAA Compliance</td>
<td>Full</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 3</th>
<th>Army or Air Force Medical Center</th>
</tr>
</thead>
<tbody>
<tr>
<td>HIPAA Compliance</td>
<td>Full</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 4</th>
<th>Contingency Aeromedical Staging Facility (CASF)</th>
</tr>
</thead>
<tbody>
<tr>
<td>HIPAA Issues</td>
<td>Unit inquiries</td>
</tr>
<tr>
<td>HIPAA Compliance</td>
<td>Full</td>
</tr>
</tbody>
</table>

For Round Two, models 2A, 2B and the Afghanistan model were presented, and the panel members were asked to respond the models that fit their area of deployment. For those representing the Iraq/Kuwait area, the Delphi members were asked to reflect on models 2A and 2B and select the one that they believed was a better fit. The two models differed in that some reported in the first round that there was full compliance at every step in the medical treatment/evacuation process, while others reported only partial compliance in the early stages of the process.

The participants were then asked if they had any additional changes to the model they chose. Finally, each participant was asked what could be done to better implement HIPAA at each step of the model. Eight sets of questions were sent out and five were returned over a two week period. Some of the Delphi group members had redeployed to the war zone during the time of the study, so they were not all able to respond to all rounds of the study.
For the model of how the HIPAA requirements for security and privacy were implemented, all members of the panel with Iraq experience selected Model 2b, which had partial compliance in steps 1 thru 6 and full compliance in steps 7 thru 9, indicating that unit inquiries were answered up through the time that the wounded left the theater of war and were evacuated to medical centers. The single panel member with Afghanistan experience made no changes to that model for round 2. Although the Afghanistan model was more compressed than the Iraq model, unit inquiries were also honored while the wounded were still in the theater of war. Once the wounded left the theater, some unit requests were still received, but by this time full compliance was the norm.

The Delphi group was also asked for recommendations to better implement HIPAA at each stage of the model. In general, the group suggested that model 2B was a good model for the future implementation of HIPAA requirements. Several members did offer suggestions for further improvement that were mainly centered on administrative fixes such as “Clear written guidance”, “Cover letters”, and “Education to field medics.” One of the panel members noted that full compliance with HIPAA is probably somewhat budget constrained as full compliance would require additional resources of people and equipment.

5. Summary

The responses to the Delphi Rounds suggest that there is a common perception among the Delphi Panel members that HIPAA compliance is largely in place throughout the treatment/evacuation process, with partial compliance at or very near the time and place of battlefield injuries. At that point, variances from full compliance reflect a focus on medical treatment over administrative procedures, and telling buddies of the wounded soldier his/her condition. The panel recommendations for improvements in the model are entirely administrative in nature, leaving these two areas of deviation from HIPAA requirements in place. The initial model of HIPAA compliance with battlefield medicine appeared to match closely with the learning of how “it is supposed to be”, even though the model was created by people who had served in that battlefield environment. Interestingly, when, in round one of the Delphi study, several of the participants pointed out that what actually happens isn’t quite what the abstract-learning model would indicate, everyone agreed on a modified model in which several deviations from prescriptive behavior take place. It appears that the learning that takes place in the actual battlefield environment takes into account factors such as saving lives first, administrative tasks second, and keeping soldiers advised of their buddies conditions, even though that isn’t prescribed behavior for HIPAA compliance. This appears to support what might be predicted by situated learning [11].

6. Discussion

In the first round of the study all participants were in agreement except for how much HIPAA is being implemented. The third question asked each participant “How does HIPAA apply at each step?” The basic breakdown of responses was that several of the participants felt that HIPAA was partially implemented at each step and a few others said that HIPAA was fully implemented in each step. As noted earlier, this difference prompted the creation of two models for Round Two. For those who said compliance was partial, all were referring to a focus on patient care and keeping units and buddies informed about medical status to the extent that some administrative steps were not always carried out in full, and information about a wounded persons condition was shared with his/her buddies. In all cases the responses said that patient care took the precedence over administrative requirements. Situated learning may explain why what takes place on the battlefield doesn’t fit with what was contemplated in the abstract creation of the HIPAA law. Those in a position to do so may want to revisit the legal and policy positions with regard to HIPAA compliance with security and privacy to take these situated learning behaviors into account.

When asked to provide suggestions for improvements in how HIPAA requirements could be implemented the panel gave a range of administrative responses. The three most frequent responses were: clear written guidance, training on the guidance and clearly marked cover sheets.

One of the issues mentioned by two members of the panel during the study was unauthorized requests for patient information from unit members and high ranking military members. The study suggests that when these requests occur, the lack of written guidance puts an extra burden on the medical personnel because they don’t have clear written operating instructions to fall back on. It is not inconceivable that low ranking military members could be approached for patient PHI by a high ranking military member or even a member of congress. The pressure felt to release the requested information would likely be immense. Without clear written
guidance to reference, the members would have to rely upon the support of their chain of command to ensure they didn’t release patient PHI to unauthorized individuals. If they were to release the requested PHI to an unauthorized person, they would have violated HIPAA and could conceivably find themselves facing legal and financial penalties.

Another and more frequent source of unauthorized requests for patient PHI was reported to come from the members of the patient’s unit. When a member of a unit is wounded in the course of a mission, it is only natural his or her buddies will likely want to know the status of their team mate. Under current HIPAA policy, these unit members are not one of the authorized categories authorized to receive this information without the patient’s permission. The responses from the panel suggest the morale of the remaining members of the wounded individual’s unit should be taken into account, and that the current practice, especially at the initial steps of the model, is to provide at least minimal information to the unit members. In many cases, the bonds between unit members in combat are as strong as if they were family members. The morale of a unit could be affected by the denial of status information for the fallen team mate and could affect performance in coming missions.

HIPAA policy allows commanders and their designees to ask for information regarding the status of personnel under them, but is limited to PHI in the interests of fitness for duty and to perform a mission. There are other individuals who may have an interest in PHI in a combat situation, other than the commander, and who may not be a “designee” and probably do not have access. In addition to morale factors, the health information could, in combat, be critical to squad leaders, platoon leaders, flight leaders, or anyone else who might not fit the definition of “commander”. They would certainly be concerned about the person, but would also need to know “information” for replacement of a skill set, to protect others, or to assess readiness. They may need to know the person’s status to know if the person will return or if they will need to request a replacement. A unit missing critical skills sets could be at a disadvantage when operating in the field. This issue could impact the mission readiness of combat units and may need to be addressed in the future. The Delphi group responses suggest that policy may need to be modified to allow for some information on patient condition to be legally given to unit members on the basis of morale concerns and unit readiness as this may impact readiness of combat units.

The issues raised by the Delphi panel suggest that the DoD policy formation may not have completely considered HIPAA implications in a combat zone. There are provisions in the policy for fitness for duty, fitness for a particular mission and casualty reporting, but beyond that it seems like DoD may have extended the HIPAA policy without thinking it through. It may be that DoD wanted to avoid any possibility of a lawsuit or other legal issue and may have extended HIPAA compliance too far down.

All members of the Delphi Panel chose a model of partial compliance in the combat theater of operations not one of full compliance. Current practice suggests that having freedom of motion in complying with HIPAA during combat seems to be working well according to the Delphi panel. While current interpretation of HIPAA policy does not appear to be full compliance on the battlefield itself, it does appear that full compliance kicks in soon after the wounded person is evacuated and medical treatment is begun, and tends to be in place by the time the wounded soldier leaves the theater of operations. It may be worth looking at how the policy can be written to fit how things are actually done.

In consultation with legal authorities DoD policy and HIPAA policy could be modified to accept current partial HIPAA compliance on the battlefield, thus supporting what was reported to be happening now. For example, we may want to consider unit members who may be giving medical aid at the front to be exempt from HIPAA until the wounded reaches the BAS. Once at the BAS, unit chain of command could be authorized get status and fitness for duty information, and they would then have authority to release information to unit members. Unit members may receive basic status information such as will they live and will the wounded members return. Once the wounded is at the CSH, status and fitness for duty information could be given to the unit commander’s and down to the squad leader level.

It was assumed there would be common way to handle battlefield casualties in the military medical system but the research suggests there may be differences in different areas of operations. Future research may need to tie down for sure if that is true in other cases as well, and if so, how this will have impact on how HIPAA is implemented.

7. Conclusions

There does seem to be fairly standard practice and implementation of HIPAA policy in combat areas and it is one in which the strict interpretation of HIPAA does not come into play until casualties reach a certain
stage of the treatment/evacuation process, generally when they leave the theater of war. *Situated learning* suggests that this may be based on learning that takes place in the context of actually providing battlefield medicine. The findings of the study suggest that the military may benefit from examining this learned behavior to see if it is to be preferred over current policy. If the current practice is preferable, the DoD could, in consultation with legal guidance, adjust DoD HIPAA compliance policy at every level of the battlefield medical process to clearly define who can have access to PHI at each stage and under what conditions that access is to be granted.

If DoD made these changes to the current policy it could go a long way toward clarifying the requirements placed on deployed medical personnel at all levels of the treatment/evacuation model. Clear written guidance and training would help ensure that the Privacy Rule of HIPAA was complied with and help avoid unnecessary and potentially costly violations of the law. The more the process can be clarified for the medical personnel all along the treatment/evacuation process the better the chance of full HIPAA compliance at all steps of the process.

### 8. Limitations of the study

An inherent limitation of all Delphi studies is that results depend on the knowledge of a small set of identified experts. To the extent that other experts might see things differently, the conclusions could be called into question. The panel consisted of Air Force medical personnel, with primarily Iraq and Kuwait deployment experience with one member having Afghanistan experience. A panel with more even distribution between the two theaters of operations might yield more refined insights into HIPAA compliance on the battlefield.

### 9. Recommendations for Future Research

Now that a basic model of the battlefield medical treatment/evacuation process, including HIPAA compliance at each step, has been identified, additional research could be done to validate the findings and look at areas beyond the scope of this study.

The panel consisted of Air Force medical personnel with primarily Iraq and Kuwait deployment experience. One member was knowledgeable about HIPAA issues in Afghanistan, due to past and current deployment experience. This study could be applied using members of services other than the Air Force to explore the possibility that medical personnel for the Army, Navy and Marines view the treatment/evacuation process differently.

*Situated learning* suggests that the modifications made to the rules for undertaking battlefield medicine may be at least partially the result of the chaotic, frightening environment within which such services are performed. However, even if this is the case, this research does not clarify whether this is the best way to implement HIPAA requirements; only that it happens. This research did not explore all the possible ramifications of working under the developed model versus a more rigidly enforced model of complying with HIPAA. Further research could explore whether this descriptive model should also be accepted as a prescriptive model.

This study assumed there would be a common way to handle battlefield causalities in the medical system, but there is evidence from the research to suggest there may be differences in different areas of operations. The study identified differences between Iraq and Afghanistan, and future research should explore the significance, if any, of this finding.

Many individuals within the military community, but outside the medical field must have access to patient PHI. A recommendation is made to conduct research on the many non-medical personnel who may have a need to have access to HIPAA information, such as unit members, squad leaders, and such. This could help to identify how these non-medical personnel can best be served while supporting the underlying concepts of HIPAA.

It would also be very important to explore the legal aspects of this issue, to ensure that solutions meet legal requirements.

### 10. References


