USAWC STRATEGY RESEARCH PROJECT

INTEROPERABILITY IN COMMAND, CONTROL, COMMUNICATIONS, AND COMPUTER SYSTEMS (C4) IN SUPPORT OF JOINT MEDICAL OPERATIONS

by

Colonel Robert F. Rhodes
United States Army

Colonel Dallas Hack
Project Adviser

This SRP is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
15 MAR 2006		**00-00-2005 to 00-00-2006**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Interoperability in Command, Control, Communications, and Computer Systems (C4) In Support of Joint Medical Operations	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
Robert Rhodes	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
U.S. Army War College,Carlisle Barracks,Carlisle,PA,17013-5050	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

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

13. SUPPLEMENTARY NOTES

14. ABSTRACT
See attached.

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**		**26**	

ABSTRACT

AUTHOR: Colonel Robert F. Rhodes

TITLE: Interoperability in Command, Control, Communications, and Computer Systems (C4) In Support of Joint Medical Operations

FORMAT: Strategy Research Project

DATE: 13 March 2006 WORD COUNT: 7101 PAGES: 25

KEY TERMS: (Military Health System, BRAC, Net Centric)

CLASSIFICATION: Unclassified

The Department of Defenses (DOD) Health Affairs (HA) Directorate and its corresponding service component counterparts constitute a variety of highly complex and unique organizations, providing health support for the full spectrum of military operations and sustaining health services. Yet, as Command, Control, Communications, and Computer (C4) systems develop within the joint military environment at an accelerated rate; a clear vision toward joint medical communications has not been forthcoming. Who is responsible for the medical IT environment and how is it managed? What are the strategic implications that characterize the requirement for a holistic joint medical infrastructure in DOD? Research suggests that with reductions in resources, the Military Health System (MHS) will focus on integrating the communications infrastructure across the service components.

This research paper studies the implications of infrastructure changes under the Base Realignment and Closure (BRAC) initiative, technology proliferation and business system integration, data network security, and structure of the MHS. After critical examination, findings suggest that transformational issues, such as greater emphasis on policy development, joint medical operations and greater DoD C4 integration are necessary to garner greater synchronization in enterprise services and data exploitation in a net-centric environment.

INTEROPERABILITY IN COMMAND, CONTROL, COMMUNICATIONS, AND COMPUTER SYSTEMS (C4) IN SUPPORT OF JOINT MEDICAL OPERATIONS

The Department of Defense (DOD) Health Affairs (HA) Directorate and its corresponding service components: Army, Navy, and Air Force Medical Departments, constitute a variety of highly complex and unique organizations, providing health support for the full spectrum of military operations and sustaining health services. As the Military Health System (MHS) continues to develop telecommunications strategies and business system applications portfolios, a growing expectation exists for increased transparency of medical data available to providers, their beneficiaries and private sector partners. Service roles, relationships, and mission are increasingly driving business processes toward a net-centric environment within DOD, but strategies supporting convergence of medical Information Management and Technology services is problematic. This research paper studies the implications of the impending infrastructure changes under the Base Realignment and Closure (BRAC) initiative, healthcare technology proliferation and business system integration, data security concerns, and the possible formation of a Joint Medical Command. The concept of net-centricity and net-centric warfare also plays a role in the development of joint communications efforts within the DOD. A net-centric environment is a construct which demands improved business models for providing information and technology to DOD organizations and ubiquitous access to reliable, decision-quality information through a net-based services infrastructure and applications to bridge real-time and near-real-time Communities of Interest (COI).[1]

In concert with other sweeping changes under transformation initiatives, the Department of Defense established the Military Health System Office of Transformation in September, 2005. This tri-service organization has been chartered as the architect of the future military health system, capitalizing on the new technologies resulting from a constantly changing American health system.[2] To create change, it is necessary to gain perspective on information technology services and business systems integration. Also, a clear understanding of organizational relationships within the Department of Defense's Military Health Services (MHS) is necessary. Identifying relationships in the community provides greater comprehension on formal relationships in the MHS and how organizations are structured to manage information technology portfolios and the current enterprise environment.

Department of Defense (Health Affairs)

Hierarchal, the Health Affairs Directorate, a subordinate of the Undersecretary of Defense for Personnel and Readiness, is composed of the Assistant Secretary of Defense for Health

Affairs (ASD (HA)) with eight subordinate directors. In addition, these directors also serve in a dual capacity in the TRICARE Management Activity (TMA). TMA is a field activity of the Undersecretary of Defense for Personnel and Readiness and manages the TRICARE health care program for active duty members and their families and others entitled to DOD medical care.[3] Both organizations include a single Chief Information Officer (CIO) who is responsible for leading and orchestrating the information management and information technology portfolios representing these staff proponents. Within the Chief Information Officer's directorate, there are several key organizations that significantly contribute to the overall joint information management and information technology mission, including: Joint Medical Information Systems Office, Enterprise Architecture Integration and Communications Office, Technology Management Integration and Standards Office, and Network Operations. Health Affairs and the TRICARE Management Activity provide service components information management and information technology policy, enterprise architecture and standards, software and hardware development and system integration, and sustainment.

Similar in function, each branch of service has a corresponding medical organization complementing Health Affairs and the TRICARE Management Agency (TMA). The structure of these organizations though is quite different, uniquely adapted to support service centric missions and roles with medical IM/IT services. Under the umbrella of TMA, joint medical business systems are fully integrated through IM/IT policy and network and systems architectures, achieving greater economies of scale through an emerging net-centric environment which is centrally funded through the Defense Health Program (DHP). The DHP is a single appropriation consisting of operation and maintenance and other procurement funds designed to finance the non-military personnel requirements of the MHS.[4] "Currently, DHP funding flows from TMA through the services according to submissions through the Program Objective Memorandum (POM). The TMA Director, resource manager is responsible for all the programming, budgeting, and budget execution oversight functions for private sector healthcare, the DHP Central IM/IT programs, other TMA central programs, and TMA operations."[5]

TRICARE Management Activity

Information transparency to health care organizations is critical to effectively command and control medical health services across the armed services. Information technology creates the physical environment by which information transparency is attained, especially in a technologically complex environment such as modern medicine. In support of the TRICARE Management Activity (TMA) and the services' medical components, federations of IT

organizations have developed to support expanding medical business system requirements for clinicians and their beneficiaries. As IT enablers, these organizations provide for the planning, integration, protection, and sustainment of business systems and C4 infrastructure. Within DOD, TMA and each of the services approach these tasks in part with a joint effort and others in a service centric environment creating a complex infrastructure to manage and sustain.

Under the TMA umbrella, the MHS Joint Medical Information Systems (JMIS) Office and a subordinate element, the Tri-Service Infrastructure Management Program Office (TIMPO) are responsible for the planning, programming, implementation and sustainment of IT infrastructure to include the associated end-user hardware support for nineteen centrally managed MHS health information systems.[6] TIMPO typically uses the Defense Information Systems Agency (DISA), another DOD organization, for IT services execution. Conversely, TIMPO does not support service specific systems or services unless it is fiscally and technically advantageous to both TMA and the service component. In summary, implementation and operation of medical information systems is a mixture of centralized systems provided by JMISO/TIMPO and decentralized by the Service components. TIMPO is geographically separated into two elements, the headquarters residing in Washington, D.C. and the remainder of the office in San Antonio, Texas. Additionally, as a joint program office, TIMPO does not have a joint manning document supporting its personnel structure, but rather a "collection of service manning documents which are sometimes prey to service availability or other service priorities and constraints."[7]

Military Health System (MHS)

The complexity of service-oriented medical missions over time and the rapid proliferation of information technology in recent years have driven some changes in IT organizational structure and implementation throughout DOD, but not to the extent where the responsibilities of Health Affairs and the services are blurred. Service-centric approaches to IT implementation and sustainment to medical business requirements have resulted in a network of complex organizations, competing for similar resources. These organizations competed for an estimated $862M in the 2005 DHP IM/IT budget, but does not reflect service related expenditure requirements.[8] It is noted that DOD recognized in the mid-1990s that consolidating medical IT infrastructure and shared business systems could lead to greater efficiencies and economies, resulting in the creation of the Joint Medical Information Systems (JMIS) Program Executive Office (PEO) under the TRICARE Management Activity (TMA) in 1998.

Understanding the complex relationships and resources of each service contributing to the MHS assists in defining shared responsibilities on IM/IT policy and business systems development, deployment and integration. Each service's diverse IT infrastructure and distinct mission requirements have constrained their capability to support greater information transparency in concert with DOD vision of a net-centric environment. "The DOD Net-Centric vision demands improved business models for providing information and technology across the Department. Net Centric Enterprise Services (NCES) is a powerful transformational construct that will revolutionize the way we conduct warfighting and business operations throughout the DOD."[9]

Army Medical Department Information Management

The Army Medical Department's (AMEDD) Information Management Directorate (IMD) is organized under the "One Staff" concept; this blends the Army surgeon general's staff, located in the Washington, D.C., area, and the MEDCOM commander's staff at Fort Sam Houston, Texas, into a single staff for both three-star functions.[10] The Army Medical Department CIO serves in a dual capacity, managing the IMD staff supporting the Army Surgeon General and his mission and an additional staff managing information management and information technologies for the Army Medical Command (MEDCOM). The Chief Information Officer "One Staff" is comprised of three supporting deputies and two additional functional support elements, these include:

- Deputy CIO, Plans, Policy, Security, and Resources
- Deputy CIO, Medical Health Systems (MHS) Integration
- Deputy CIO, Army Integration

The CIO subdivides functional proponency for IM/IT strategy, IT infrastructure, and knowledge strategy and management. Other key organizations that influence planning, integration and sustainment of IM/IT infrastructure in the Army Medical Department include the U.S. Army Medical Information Technology Center (USAMITC) and its higher headquarters, the U.S. Army Medical Research & Materiel Command (MRMC). MRMC serves as the AMEDD's Information and Technology materiel developer, with USAMITC as the lead organization for IM/IT development initiatives where those initiatives cut across organizational boundaries.[11]

In conjunction with the Army Medical Department (AMEDD) who is responsible for both the sustaining base and deployed medical environment, the Medical Command (MEDCOM) provides the planning and operational information technology requirements. These requirements are met through several organizations, including: MRMC, USAMITC, and the

Network Enterprise Technology Command (NETCOM). Distinct duties and responsibilities have been apportioned among these organizations to fulfill IT systems and services requirements, with the majority of services being provided through the MRMC/USAMITC. "As core competencies, the USAMITC is responsible for the deployment and sustainment of IM/IT systems supporting the AMEDD as well as tri-Service organizations around the world. It is responsible for the AMEDD electronic mail system, electronic forms system, and the video teleconferencing center, as well as full life-cycle management of over 85 IT applications and administration of computer systems security worldwide.[12] In partnership with the AMEDD and the MEDCOM, NETCOM provides network security monitoring, data network capabilities for non-medical business systems and telephony.

Navy Bureau of Medicine and Surgery CIO

Under the auspices of the Navy Bureau of Medicine and Surgery (BUMED), the headquarters command for Navy Medicine, the Chief Information Officer leads the Navy and Marine Corp's effort in managing medical information systems and their overarching governance. The CIO is responsible for the overall strategy, governance, IM/IT portfolio management, and liaison with Navy organizations to include the Department of the Navy CIO, the Navy Medical Information Management Center (NMIMC) and TMA. Areas of specific mission interest include the development of the Military Health System (MHS) Enterprise Architecture, policy development, configuration management, information assurance and other communications services.[13] Organizationally, the CIO's office is simple in structure and consists primarily of two subordinates, one for policy and plans, and the other for program management and integration. While the CIO focuses on strategic planning and policy, the operational IT environment is managed by the NMIMC.

The NMIMC's contribution to the MHS is to articulate the unique requirements of the Navy and Marine Corps and insure its implementation throughout the Navy part of the MHS infrastructure. The mission also includes the technical oversight of information assurance, but relies on the local information management teams to manage the network layer and its security. This network is centrally funded through the DHP and is separate and distinct from the Navy Marine Corps Intranet (NMCI). The current direction of BUMED suggests that the two networks, NMCI and the Medical Community of Interest (MCOI), will remain segregated; performing different functions but both adhering to DOD technical standards, with the common tenants of redundancy, reliability, centralization and consolidation. This is significant as transformation

efforts are rapidly moving the medical mission towards a unified medical command organization that would require an MCOI to support the mission.

Air Force Medicine

In support of the Air Force Surgeon General, the Chief Information Officer (CIO) serves both as the Director of Information Management and as the Assistant Surgeon General for Modernization. The dual mission of the CIO and his office was recognized as a critical step forward in defining the future capabilities of information management and technological advances within the Air Forces' medical service. The realignment of mission and organizational structure took place in November, 2005. In these key roles, the CIO provides planning and oversight on the development and integration of medical information systems into the Air Force's contribution to the DOD's Global Information Grid (GIG) called the ConstellationNet.

> The ConstellationNet is a communications network air, space, and terrestrial that allows a free flow of information so that it is rapidly accessible and presented to warfighters at the right time and right place to create the commander's desired effects. GIG transport layer components delivered under this effort are included in various USAF programs. The USAF portion of GIG-BE (GIG Bandwidth Expansion) provides expanded terrestrial service at key USAF bases globally. [14]

Realigned, the CIO's organization is subdivided into functional elements which specifically focus on the Air Force's medical IT portfolio, these include;

- Requirements
- Program Management Support
- Research and Development
- Test, Evaluation & Transition
- Healthcare Informatics
- Compliance

A key component of health care delivery is the Air Force's ability to create a seamless, net-centric environment through its communications infrastructure. Significantly different in its execution from the other armed services, the Air Force maintains its communications infrastructure holistically. Data networks operations are not tethered to different organizational entities as found in the other services, but subscribes to a "One Air Force, one network" concept and ultimately falls to the Air Force Communications Agency (AFCA) for implementation and management. The new concept embodies a family of policies, procedures, standards and technologies founded on five primary tenants including: information transport, information computing, information assurance, information management, and enterprise architecture.[15]

Base Realignment and Closure (BRAC)

Transformational forces including the 2005 Base Realignment and Closure (BRAC) initiative may have set in motion forces that will move the MHS toward an increasingly joint medical C4 environment, well beyond what currently exists today. Beginning in 2002, the Department of Defense began the arduous task of planning and coordinating actions that would eventually lead to the submission and Congressional approval of the 2005 BRAC Commission's recommendations.

> The Base Realignment and Closure Commission's recommendations for reshaping the Defense Department's infrastructure and force structure officially took effect at 12:01 a.m. today after Congress allowed them to pass into law at the mandated Nov. 8 deadline. BRAC 2005 is being called an important milestone in restructuring DoD's domestic base structure to improve efficiency and operational capabilities. Many of the transformational recommendations in the report, particularly those to establish joint operations, will present significant challenges as they are implemented, officials acknowledged.[16]

Since organizational structure relies heavily on mission requirements, geographic location and other factors, the services have philosophically advanced their IT portfolios differently for service unique business processes. These organizational differences have led to limitations on the execution of non-joint medical business systems and IT services implementation. The outgrowth of this situation has led the services to diversify IT service support structure in which no service provides the same type of IT function in the same manner. As indicated in a Rand Corporation testimony to the Senate Committee on Armed Services, Subcommittee on Personnel on 21 April 2005, Susan Hosek pointed out that change to the organizational structure of the MHS was one of two areas that could have the greatest impact on cost saving in the execution of the medical mission. Additionally, the testimony references a dozen other reports over the past six decades that indicate that consolidation of management and organizational structure would benefit the military health care community. [17]

Organizational structure changes will also be closely related to the results of BRAC and the consolidation of medical health care facilities in the Continental United States (CONUS). In an effort to consolidate resources in the MHS, the development of joint medical facilities under the BRAC is becoming a reality. [18] The challenges of merging service component medical operations into joint medical operations pose a significant change in structure and how IT services are provided. Under BRAC, multiple organizations are anticipated to close or realign under several joint medical centers or activities. The ensuing infrastructure and organizational shift is illustrated by two BRAC initiatives in the MHS. The first initiative is the closure of Walter Reed Army Medical Center and moving of its mission to the new Walter Reed National Medical

Center in nearby Bethesda, Md., current site of the National Naval Medical Center.[19] The second initiative is the San Antonio, Texas based merger of Brook Army Medical Center (BAMC) and Wilford Hall Medical Center. The joint recommendation establishes the San Antonio Regional Medical Center. This effort moves the inpatient function at Wilford Hall Medical Center to BAMC, Fort Sam Houston. Wilford Hall Medical Center converts into an ambulatory care center.[20] These joint operations constitute two unique IT future integration efforts involving all three services with fundamental differences in their approaches to IT services execution.

Substantive planning and agreements within the MHS and the armed services are critical to the direction taken in IT support to members of differing services working in joint medical operations. Currently, there is no consensus on how to efficiently and effectively support these future organizations with such diverse IT infrastructure support arrangements. The potential exists for de-synchronizing the greater effort in BRAC by approaching IT support functions differently through service parochialism and may manifest itself in regional solutions, rather than holistic solutions across the DOD. To illustrate this point, the simplest of information systems, email provides an example of the challenges that the services must come to consensus in developing strategies that support the DOD net-centric environment. E-mail services are likened to other utilities; they are reliable, ever present and a necessity of everyday business. By whom, and how, will email services be provided to these future joint medical complexes? It is clear that IT strategy must change to accommodate the shift in overall organizational structure.

The future San Antonio Regional Medical Center illustrates the complex and often dynamic environment in which IT services are provided. Focusing on the complex IT environment in the San Antonio area, the Air Force's Wilford Hall Medical Center at Lackland AFB receives its e-mail services through the base communications squadron and in parallel, Brook Army Medical Center's e-mail services are provided by Medical Command's Western Message Center located at Ft Sam Houston. This center provides centralized email for all Army Medical units west of the Mississippi River and the Office of the Surgeon General (OTSG). This enterprise system is operated by USAMITC, also located at Fort Sam Houston. Lastly, the Directorate of Information Management (DOIM) at Fort Sam is the primary provider of enterprise services for that particular installation. While the services' MHS currently approach e-mail systems implementation differently, a regional approach to the challenge is likely without a coherent approach to enterprise services across the DOD in emerging joint facilities.

MHS Information Systems Proliferation and Integration

The prolific growth of health care technology in the MHS has placed considerable pressure on information managers and their corresponding infrastructure to meet the needs of their community. The seemingly limitless flood in medical information systems development and network requirements have stretched limited resources valued in time, human capital, financial capacities, and technological upgrades. This was evident in an article espousing the criticality of information technology collaboration, foresight, and integration.

> Information technology offers tremendous opportunity as well as growing challenges for the health care industry. Great potential exists to apply information systems beyond administrative functions, with particular emphasis on clinical applications. And, due to the exponential growth and capabilities of information systems, health care leaders and practitioners must take a strategic and longitudinal view to invest, prepare for, and shape the future.[21]

The TRICARE Management Activity realized that to control the growth of information systems and their underlying data infrastructure, good governance was necessary to establish conditions that support development and integration of hardware and software unique to the MHS. For this purpose, the TRICARE Management Activity sponsors 56 named committees, working groups and charters. Ironically though, few committees include representation from those who manage the DOD networks and rely on representation from within the MHS to bridge the gap between those who develop or acquire medical information systems and those who manage the network transport layer. This may not always be the case, but with so many disparate organizations managing DOD networks, collaboration, integration and consistency is difficult to obtain. The rise of Telehealth initiatives in the MHS provides an excellent example in the strategic development and proliferation of medical information systems and the overall effect on DOD networks.

> Telehealth focuses on the transfer of basic patient information over networks and the diagnosis, treatment, monitoring, and education of patients using systems that allow access to expert advice and patient information. A technical definition of Telehealth technology would include those devices and software that enable healthcare providers and educators to diagnose, consult with, monitor, treat and educate patients and consumers remotely. [22]

Typically, the services have pursued advanced technology supporting Telehealth in parallel resulting in a variety of dissimilar systems, governing policies and network integration solutions. Of particular concern with respect to information management are transport (bandwidth) requirements over existing networks, life cycle costs, and the increasing demand for technical support personnel. “The problems associated with interoperability are due in large part to the fragmented nature of Telehealth – many participants each having different

requirements or solutions and each applying different technical standards."[23] Continued efforts in managing Telehealth portfolios have achieved success in moving forward Telehealth clinical collaboration, systems development, and deployment under less than ideal conditions.

> I think there are at least two major parts to the lack of a centralized consolidation. First has been the delay in the deployment of an enterprise electronic health record (EHR) (CHCSII). The delays and the disconnected systems (CHCS II T) have made it difficult for the Telehealth community to plan for integration of telemedicine into the way we do business (teleconsults and consults should really be one in the same). Secondly, the lack of a consistent and predictable communication infrastructure/bandwidth for the medical assets in theatre has made it difficult to plan or implement a centralized, integrated approach.[24]

Increased pressure on IT specialists to sustain an increasingly complex environment of interim and legacy systems, applications, projects, and initiatives within the MHS is illustrated by the advancing numbers of medical information systems. Though current estimates by the Business Management Modernization Program (BMMP) places the number of unique medical systems at 55, the database is incomplete and will be updated over the course of fiscal year 2006.[25] The Secretary of Defense established the BMMP to provide policy, strategic planning, oversight, and guidance for the Department's BMMP transformation efforts and complies with the FY05 National Defense Authorization Act (FY05 NDAA). [26]

MHS and Service Information Systems Integration

In 1998, the DOD Health Affairs consolidated systems management functions and personnel into a single organization, called the Joint Medical Information Systems (JMIS) Program Executive Office (PEO). This organization under TMA is responsible for procurement, development, implementation, deployment, maintenance, and operations of joint medical information systems.[27] Under the PEO, functional representation supports lifecycle management of a variety of automated information systems including clinical, financial, human resources and medical logistics. Also developed and integrated are service unique automated information systems, which are not developed and deployed centrally under TMA, nor do they necessarily have relational databases.

Current mission guidance by the PEO clearly distinguishes between joint medical information systems and service unique systems through mission requirements, policy, and funding sources. These factors have contributed to the evolution of disparate service centric systems, diminishing the concept of an integrated, transparent and unambiguous system of systems to manage health care activities across the DOD. The Theater Medical Information Program (TMIP), an MHS program with the participation from DOD Health Affairs, the armed

services, the United States Transportation Command, United States Joint Forces Command, and the Joint Staff illustrates this point.[28]

TMIP integrates the DOD's "peacetime" medical software and tailors it to run on a combination of hand-held devices, stand-alone laptops, and client-server computers in the field.[29] The system is jointly developed, but allows the addition of service unique software resulting in the delivery of a dissimilar technical architecture, additional distinctive software and hardware.

> The practice of maintaining disparate information systems across multiple departments and multiple facilities came first out of necessity, then out of habit. As the functionality of specialized systems became more complex, the task of connecting applications through electronic interfaces became exponentially cumbersome, to the point where a simple change in one application can now have costly ripple effects throughout the IT configuration.[30]

A further example of parallel system development in the MHS is found in the reporting and tracking mechanisms for immunizations. In the DOD, five systems currently report and track immunizations for service members. In the MHS, the Armed Forces Health Longitudinal Technology Application (AHLTA), Medical Protection System (MEDPROS), Shipboard Automated Medical System (SAMS), Medical Readiness Reporting System (MRRS), and Air Force Complete Immunization Tracking Application (AFCITA) represent TMA and service efforts to manage this data. It is apparent that the immunization information systems grew out of necessity by the services, but only in parallel. Regrettably, these systems have limited collaborative ability across service domains.

Analyzing the approach to development and integration of automated information systems in the MHS has revealed the propensity to develop independent systems based on unique service requirements, service preferences and general parochialism. In an interview with the deputy director of TIMPO, this scenario was demonstrated while beginning its deployment of the Armed Forces Health Longitudinal Technology Application (AHLTA) and resistance to change from one product line of hardware to another as dictated by the systems architecture requirements.[31] This resistance to change in brand name loyalty led to an integration failure in the upgrade of a LAN at a regional medical facility, disrupting health care operations.[32] Ultimately, TIMPO redirected efforts toward the approved systems architecture, overcoming the technical difficulties in establishing a seamless data network.

Further complicating the development and integration of medical information systems are a combination of Congressional Acts and DOD policies directing greater governance in the use of DOD resources toward the development, implementation and sustainment of all IM/IT

systems, including medically related systems. The Defense Business Systems Management Committee (DBSMC) under the auspices of the Business Management Modernization Program (BMMP) resides as the approval authority for the spending of funds for the development of systems in excess of $1M.[33] Though, this program has significantly improved the governance aspects of IM/IT systems development, modernization and enhancement, it has also increased the level of bureaucracy in the process. To this end, IM/IT governance at all levels has the potential to slow the advancement of medical information systems with material solutions adding months to existing processes.

Information Assurance

A high degree of information assurance is required in today's uncertain threat environment. An obvious theme in the MHS's business management portfolio is the integration of these systems onto the Global Information Grid (GIG) with elements encompassing information assurance. Key elements of this environment include transmission and storage integrity, availability, confidentiality, non-repudiation and authentication.[34] As indicated in an article by the Carnegie Mellon Software Engineering Institute, security management is a key enabler to mission success.

> Managing security across an enterprise is one of the many business problems that organizations must solve in order to accomplish their missions. Regardless of what organizational assets are to be secured—information or technical assets, physical plant, or personnel—the organization must have a security strategy that can be implemented, measured, and revised as the business climate and operational environment change. In the long run, the effectiveness of the security strategy depends on how well it is aligned with and supports the organization's business drivers: mission, business strategy, and critical success factors.[35]

Enterprise security management encompasses a variety of strategies and programs in the DOD, one being the Defense in Depth strategy. The strategy is considered by the Defense Information Systems Agency (DISA) as a practical strategy to achieving information assurance.

> Defense in Depth is practical strategy for achieving Information Assurance in today's highly networked environments. It is a "best practices" strategy in that it relies on the intelligent application of techniques and technologies that exist today. The strategy recommends a balance between the protection capability and cost, performance, and operational considerations.[36]

The corollaries of Protection, Detection, and Reaction provide the fundamental construct for information assurance activities.[37] The services and the MHS have adopted this model and collaborate on activities that include the integration of human capital, technology and operational policy to achieve protection.[38] The challenges throughout the MHS are similar to

other aspects of managing IM/IT, consistency and conformity. Since the development and implementation of Enterprise and systems architectures are managed in a collaborative manner between TMA and the Services' medical departments, standardization is achieved through collaboration and consensus. This remains true for all centrally managed medical information systems today. The technical architecture though, is influenced not only by the MHS, but also by those who develop network security policies and the Designated Approving Authority's (DAA) implementation of those policies at each site with a tailored technical architecture which, although compliant with the original policies, may also level additional stringency. The division of labor though has its shortcomings when not approached holistically across the Enterprise. This condition has led to a number of diverse policies and technical solution sets at the installation level. These two approaches to architecture implementation have led to greater uniformity across the COI, but struggle to gain consistency at the installation network layer. This situation was recently illustrated by challenges in the deployment and integration of AHLTA at medical treatment facilities in the Continental United States (CONUS).

Concurrently with the introduction of AHLTA in the MHS, the Air Force launched an initiative to increase network security at its installations with the deployment of Sidewinder, a network security gateway otherwise commonly known as a firewall. This allows an organization to connect to the Internet while protecting the systems on its internal network from unauthorized users and network attackers. In the ensuing months, Sidewinder configurations at various installations disrupted AHLTA's ability to perform data transactions across the medical domain. While the gateway performed well, the configuration varied from installation to installation based on unique network security requirements demanded at the local level. Information assurance by definition fails when data is not available.

Analyzing the MHS Environment

In evaluating the current MHS information management and information technology environment, it is essential to understand and focus on the two primary missions of the medical community: TRICARE and service member readiness. TRICARE's advocacy resides with TMA under a joint umbrella, while more autonomy has been provided to the services on the readiness mission. Since the MHS's organizational structure relies heavily on mission requirements, the services have philosophically advanced their IT portfolios differently for service unique information systems through multiple staffs and IT organizations. These organizational differences have led to indifference among the services and TMA in the

development and deployment of non-joint medical information systems and IT services implementation.

In the near future, MHS efficiencies and economies will be closely linked to the performance of BRAC implementation and the resulting consolidation of medical health care facilities. In a genuine effort to conserve resources, the MHS is developing structures that operate like joint commands, even if not formally designated as such. Additionally, oversight coupled with the development of IM/IT governance has contributed to the convergence of IT infrastructure and information system development at the DOD level. With the prospects of creating two joint medical centers, one in the National Capital Region and the other in San Antonio, Texas, the question that must be answered quickly for the IT community is who will provide the C4 infrastructure and what unique service centric information systems will be integrated, virtually or physically? These are significant questions which will drive the future of medical operations throughout the MHS based on the totality of consolidation and systems integration across the services. In today's environment, consolidation of facilities offers the opportunity to commit to a long term strategy among the services and Health Affairs in IT resource consolidation and sharing.

The second way in which the MHS can move toward a more net-centric environment and improve its IT services resides with policy development and its implementation. Undoubtedly, the underpinning of DOD's current complex network environment is its IT policies and their implementation. Tied to organizational structure and emerging technology, most IT policies are complimentary, sometimes redundant, often difficult to implement and developed by multiple agencies. At present, many organizations contribute to the maze of policies developed and implemented within the IT community of interest, some of these include: the U.S. Congress, the White House, the Department of Defense, the National Security Agency, the Armed Services and commercial industry. At all levels, policies often build islands of information, denying the transparency that is envisioned by net-centricity. In the DOD, IT policy casts a wide net of activities consistent with commercial best practices, emphasizing seamless networks and systems security. These policies though are traditionally slower to evolve over time than information systems and services; this has a profound effect on the integration of new technologies in the medical community. An example of this situation presents itself in the slow advancement of software upgrades necessary to achieve greater integration and security.

The Defense Blood Standard System (DBSS), an automated information system regulated by the Food and Drug Administration (FDA) among others, is encumbered by regulations and the inability to achieve swift resolution on its upgrade or replacement. The

current Operating System (OS) for DBSS is New Technology (NT), an obsolete OS outside the lifecycle sustainment domain, with no support by its developer, Microsoft. This system experienced very limited deployment on tactical networks in Operation Enduring Freedom (OEF) or Operation Iraqi Freedom (OIF) since DOD mandated replacement of the OS by Windows 2000 or Windows XP. To date, DBSS has not achieved successful integration with an updated OS. This situation is not unique and derives its limitations from lack of consensus, regulatory inefficiencies, broad policies and short sightedness in long range systems lifecycle planning. This situation clearly illustrates the interconnected nature of the MHS in dealing with regulating and service agencies outside the DOD.[39]

Streamlining policy development and its implementation contributes to a holistic approach to the development of technical and systems architectures. These steps contribute to the integration and transparency of information sharing between diverse systems, especially across the GIG. Even though best business practices and in-depth technical standards are widely employed, governance and the ability to forecast technological advances must keep pace with industry to deliver systems that provide the best healthcare to patients.

Recommendations

To formulate actions that move the MHS toward a truly joint medical IT environment and progress toward DOD's net-centric vision, substantial changes are required throughout the MHS. These changes are manifested in two basic areas: the organizational structure of the MHS and policy development and its integration. These two areas constitute the means that will enable the MHS to achieve a joint medical environment through technology and attain the net-centric environment envisioned in the DOD.

First and foremost, the MHS has the opportunity during the great upheaval of Transformation to create lasting change and reshape its IT policies and their implementation today. This begins with a thorough review of IT policy development procedures at all levels throughout the MHS and those policies influencing the MHS from external sources, centralization is the key. Since there are a significant number of contributors to IT policy development and its implementation, broadening IT policy development and technical oversight must be a priority to Heath Affairs. The goal is to centralize, at the highest possible levels of command, those actions related to policies that require enterprise changes, thus relieving local commander's responsibility for much of the technical implementation of information security of their networks and direction of joint and service oriented automation programs. The effort would undoubtedly require a philosophical change in who is responsible for network security and drive

the MHS to oversee all automated systems programs development within the MHS. Additionally, a shift to centralized policy development and implementation would require changes to the authority and scope of local Designated Approval Authority (DAA). These recommendations would assist in limiting interpretation of IT policies, leading to greater synchronization of effort in building and maintaining automated medical information systems and their networks on the periphery the GIG.

Concurrently, consolidation of IT resources in the MHS and the services may well promote greater uniformity and provides the impetus to formulate a truly joint enterprise. The consolidation of IT resources rises above collaboration and fundamentally takes shape as a single entity to provide IT services. The argument that is derived from this situation is the level to which integration and consolidation occurs and by whom. The risk of not pursuing further consolidation in the MHS, primarily under one authority will be the status-quo and a view far short of DOD's vision of a reliable, ever present network secure from intrusion.

> Department headquarters are hardly the only scenes of redundant bureaucracy. Health care is another. Each service branch has its own surgeon general and medical operation. At the department level, four different agencies claim some degree of control over the delivery of military health care. And all of them would likely be more efficiently delivered with fewer overlapping bureaucracies.[40]

Beyond IT policy reform, the consolidation of IT resources is remote unless organizational structure in the DOD is changed and responsibilities for IT implementation are realigned. To transform the MHS, organizations and missions must change to further evolve IT services necessary to support patient health care initiatives of tomorrow. To achieve world class health care, DOD must move toward the integration of all medical information systems across the MHS and lose service specific identities. To achieve greater interoperability, the MHS must also move to a centralized data network for all medical information systems, not just DHP funded systems or relinquish these responsibilities to the services' communications commands. Organized under OSD (HA), IT services could provide such a structure for the entire medical community, utilizing the GIG as its transport mechanism and provide universal connectivity for its systems and services.

Net centric operations under Health Affairs would compliment medical C4 in the tactical environment through teleport communications sites, extending medical databases seamlessly to deployed forces worldwide. Ultimately, the potential for the consolidation of network functions could benefit the DOD through a reduction in human capital, centralized funding expenditures in the DHP, and moves the MHS toward a joint network that supports transparency of medical

information for practitioners and their beneficiaries. This direction has already been accomplished in the Air Force, where all network connectivity is provided by the AFCA.

BRAC provides the opportunity for the MHS to assess future IT concepts, integrating e-mail services across domains, ensuring single sign-on for service members and folding medical information systems into an integrated and interoperable system of systems. Two unique medical centers; the Walter Reed National Medical Center and the San Antonio Regional Medical Center have the opportunity to formulate a merged IT infrastructure from all three services and require an IT solution that embraces all service requirements under one IT provider. As an evolutionary step for these medical complexes, the MHS might consider establishing a joint medical domain under the Office of the Secretary of Defense (OSD) to facilitate a seamless environment to merge service members of the three services into one manageable IT environment.

A potential alternative to a drastic restructuring of the MHS as an interim step to further consolidation could potentially align itself to initiatives that are ongoing by the Army's MEDCOM. Rather than immediately attempting to transition to a completely centralized authority, the individual Services, where demonstrated capability/expertise exists, could be given the responsibility to become the provider of said service for all the components under a joint policy guideline and direction from the MHS. This is currently being demonstrated by MEDCOM's centralized approach to Active Directory implementation, e-mail services and network operating systems. By implementing a common IT infrastructure, especially at the BRAC sites, joint command and control could be achieved. This approach would sacrifice organizational structure for time, while gaining the ability to share data across common an infrastructure. This course of action would facilitate greater net centricity while the Services continue to consolidate and standardize disparate Service systems.

While restructuring or realigning of resources may further IM/IT integration and facilitate a renaissance in the MHS IT domain, medical information systems development looms in a continuing bureaucratic process involving many organizations with differing goals and objectives. It is incumbent upon health care professionals to transform their business processes to include good governance, while retaining flexibility and creativity at the lowest of levels for the development of medical information systems. To accomplish this Herculean task, the MHS must embrace knowledge management concepts and institutionalize governance processes to mitigate long lead times associated with the governance process.

Lastly, the MHS should consider greater collaboration with the services' IT providers, specifically focused on educating IT professionals outside the MHS. Education provides the

foundation for understanding and partnering on medical unique systems and services integration required for patient health care, especially in theaters of operations. This effort would manifest itself in the improvement of planning and integration across the GIG to deployed elements relying on service data networks.

Conclusion

The Department of Defense Health Affairs and the federation of medical IT providers all share a common vision of a seamless, integrated and ubiquitous network that supports the patient, provider and third party partners. For these organizations to achieve this vision a revolution rather than an evolution in IT services must take place - essential for an environment where change in technology is continuous, yet cold war attitudes still exist years later. Infrastructure changes under the Base Realignment and Closure (BRAC) initiative, healthcare technology proliferation and business system integration, data network and database security concerns pose a significant challenge to the DOD and can only be answered through greater collaboration and the realignment of IT systems and services within and outside the MHS.

Key IT interoperability issues can be realized if the DOD (HA) is willing to transform itself and the services transfer mission and responsibility to a centralized DOD authority. The proposed strategy in shifting IT responsibilities in the MHS is essential for making real change in C4 systems and services. This situation could potentially provide greater benefit in human capital reduction and consolidation, centralize funding expenditures under the DHP, and moves the MHS toward a joint network that supports transparency of information for practitioners and their beneficiaries. The risk of not pursuing the change in the MHS and the armed services will undoubtedly be the status-quo and a view far short of DOD's vision of a net centric environment and the DOD's vision of world class health care for service members.

Endnotes

[1] Defense Information Systems Agency, "Core Services - Net-Centric Enterprise Services," available from http://www.disa.mil/main/prodsol/cs_nces.html; Internet; accessed 11 November 2005.

[2] Samantha Quigley, "Transformation Office to Streamline Military Health System," 16 September 2005; available from http://www.defenselink.mil/news/Sep2005/ 20050916_2759.html; Internet; accessed 22 October 2005.

[3] MHS Committee, Workgroups & Charter, "TMA Charter," available from http://www. tricare.osd..mil/charters/chartermatrix.cfm ; Internet; accessed 24 October 2005.

[4] TRICARE Management Activity, “Enclosure 2 – Definitions”, available from http://www.tricare.osd.mil/charters/tmacharter.html; Internet; accessed 11 December 2005.

[5] TRICARE Home Page, “Resource Management,” available from http://tricare.osd.mil/rm/index.cfm?pageId=12, Internet; accessed 13 November 2005.

[6] Lynne Zetterholm, TRICARE Management Activity PEO, telephone interview by author, 12 December 2005.

[7] Mr. Joseph Martinez, Deputy Program Manager, Tri-Service Management Program Office, Video Teleconference interview by author, 1 November 2005.

[8] DOD Health Affairs Home Page, “Defense Health Program Budget Overview,” available from http://www.ha.osd.mil/budget; Internet; accessed 5 November 2005.

[9] Defense Information Systems Agency Home Page, “Net-Centric Enterprise Services (NCES) Program Management Office,” available from http://www.disa.mil/main/nces.html; Internet; accessed 7 November 2005.

[10] Army Medical Department, “Introduction to the U.S. Army Medical Department,” available from http://www.armymedicine.army.mil/ about/introduction.html#structure; Internet; accessed 28 October 2005.

[11] U.S. Army Medical Research and Materiel Command Home Page, “U.S. Army Medical Information Technology Center (USAMITC),” available from https://mrmc.detrick.army.mil/mitindex.asp; Internet; accessed 29 October 2005.

[12]U.S. Army Medical Research and Materiel Command Home Page, “U.S. Army Medical Information Technology Center (USAMITC),” available from https://mrmc.detrick.army.mil/mitindex.asp; Internet; accessed 3 November 2005.

[13] Mr. Lon Thompson, Deputy Chief Information Officer, Bureau of Medicine and Surgery, telephone interview by author 14 December 2005.

[14] House Armed Services Community Home Page, “Regarding Department of Defense Information Systems Architecture: Are we on the Right Path to Achieving Net-Centricity and Ensuring Interoperability?,” available from http://armedservices.house.gov/openingstatements andpressreleases/108thcongress/04-02-11tillotson.html; Internet; accessed 3 December 2005.

[15] Greg Edwards, “One Air Force ... One Network”, August 17, 2001; available from http://www.dcmilitary.com/airforce/beam/6_33/commentary/9698-1.html; Internet; accessed 9 December 2005.

[16] Donna Miles, DefenseLink, “BRAC Deadline Expires; DoD to Begin Closures, Realignments, “ available from http://www.defenselink.mil/news/Nov2005/20051109_3280.html; Internet; assessed 29 November 2005.

[17] U.S. Congress, Senate, Committee on Armed Services, Subcommittee on Personnel on *Initiatives to Control Military Health Costs*, 109th Cong., 21 April, 2005, 6.

[18] The process DOD has previously used to reorganize its installation infrastructure to more efficiently and effectively support its forces, increase operational readiness and facilities new ways of doing business. DOD anticipates that BRAC 2005 will build upon processes used in previous BRAC efforts. See DefenseLink BRAC Home Page, "2005 Base Closure and Realignment Report," available from http://www.defenselink.mil/brac/pdf/VolX_Medical-o.pdf; Internet; accessed 14 November 2005.

[19] Ibid., 1.

[20] Air Force Link, "Base Realignment and Closure 2005, Texas," available from http://www.af.mil/brac/texas.asp#Anchor-Lackland-61711; Internet; accessed 10 December 2005.

[21] National Defense University, "Health Care," 24 April 2002; available from http://www.ndu.edu/ icaf/industry/IS2002 /IS2002WORD/2002% 20Health %20Care.doc; Internet; accessed 10 December 2005.

[22] Technology Administration, "Innovation, Demand and Investment in Telehealth - Feb 2004," available from http://www.technology.gov/reports/TechPolicy/Telehealth/2004Report.pdf; Internet; accessed 11 December 2005, 46.

[23] Ibid., 46.

[24] Col. Mark G. Janczewski, e-mail message to author, 13 November 2005.

[25] Lynne Zetterholm, TRICARE Management Activity PEO, interviewed 12 December 2005.

[26] AKO Files Home,"KC Christensen, BMMP," available from https://www.us.army.mil/ suite/portal/index.jsp; Internet; accessed 31 January 2006.

.

[27] TRICARE Management Activity, "Program Executive Office", http://www.tricare.osd.mil/ peo/peo/default.htm ; Internet; accessed 18 December 2005.

[28] Ibid., 1.

[29] TRICARE Management Activity, "TMIP," available from http://www.tricare.osd.mil /peo/tmip/default.htm; Internet; accessed 10 December 2005.

[30] Health Management Technology, "Patient Centric HIS," available from http://www. healthmgttech.com/; Internet; accessed 10 December 2005.

[31] The Composite Health Care System II has now been christened the Armed Forces Health Longitudinal Technology Application (AHLTA). The CHCS II is the military computer-based patient record that is accessed through a provider-developed graphical user interface. It facilitates outpatient management of health information requirements for the U.S. Armed Forces and provides MHS beneficiaries with a life-long medical record. See Pat Shannon, "CHCS II Name Change," *AMEDD Information Management News* , 8 November 2005 [newspaper on-line]; available from https://www.us.army.mil/suite/viewnotification.do?id=1053056&r=/ntf/ collabSentLink_pgRender.jsp#; Internet; accessed 13 November 2005.

[32] Mr. Joseph Martinez, Deputy Program Manager, Tri-Service Management Program Office, Video Teleconference interview by author, 1 November 2005.

[33] Sandy Parker, "AMEDD Overview Business Management Modernization Program (BMMP) and Legal Ramifications," email to author, 31 January 2006.

[34] Defense Technical Information Center," Department of Defense Instruction Number 8500.2, February 6, 2003," available from http://www.dtic.mil/whs/directives/corres/pdf/i85002_020603/i85002p.pdf; Internet; accessed 15 December 2005.

[35] Richard Caralli, "The Critical Success Factor Method: Establishing a Foundation for Enterprise Security Management," Carnegie Mellon Software Engineering Institute, July 2004, p.18.

[36] National Security Agency, "Defense in Depth", available from http://www.nsa.gov/snac/support/defenseindepth.pdf; Internet; accessed 17 December 2005.

[37] Ibid., 3.

[38] Ibid., 4.

[39] Mr. Duke Williams, e-mail message to author, 23 January 2006.

[40] DefenseLink, "DOD Acquisition and Logistics Excellence Week Kickoff—Bureaucracy to Battlefield," available from: http://www.defenselink.mil/speeches/2001/s20010910-secdef.html; Internet; accessed 13 November 2005.