THE UNITED STATES ARMY MEDICAL DEPARTMENT

JOURNAL

ETHICS, CONTRACTS, PROCUREMENT, AND MORE FOR HEALTHCARE PROFESSIONALS: THE LEGAL CHALLENGES, RISKS, AND SOLUTIONS

January – March 2012

THE UNITED STATES ARMY MEDICAL DEPARTMENT

A Professional Publication of the AMEDD Community

JOURNAL

Online issues of the *AMEDD Journal* are available at http://www.cs.amedd.army.mil/amedd_journal.aspx

January – March 2012 | The Army Medical Department Center & School | PB 8-12-1/2/3

© George Lamson and Studio E, printed with permission. The *AMEDD Journal* is proud to present his artwork specially created for this issue.

By Order of the Secretary of the Army:
Official:

JOYCE E. MORROW
Administrative Assistant to the Secretary of the Army

RAYMOND T. ODIERNO
General, United States Army
Chief of Staff

DISTRIBUTION: Special

1128505

The Army Medical Department Journal [ISSN 1524-0436] is published quarterly for The Surgeon General by the US Army Medical Dept Center & School, Journal Office, AHS CDD Bldg 4011, 2377 Greeley RD STE T, Fort Sam Houston, TX 78234-7584.

Articles published in *The Army Medical Department Journal* are listed and indexed in MEDLINE, the National Library of Medicine's premier bibliographic database of life sciences and biomedical information. As such, the *Journal*'s articles are readily accessible to researchers and scholars throughout the global scientific and academic communities.

CORRESPONDENCE: Manuscripts, photographs, official unit requests to receive copies, and unit address changes or deletions should be sent to the *Journal* at the above address. Telephone: (210) 221-6301, DSN 471-6301

DISCLAIMER: The *AMEDD Journal* presents clinical and nonclinical professional information to expand knowledge of domestic & international military medical issues and technological advances; promote collaborative partnerships among Services, components, Corps, and specialties; convey clinical and health service support information; and provide a peer-reviewed, high quality, print medium to encourage dialogue concerning healthcare initiatives.

Appearance or use of a commercial product name in an article published in the *AMEDD Journal* does not imply endorsement by the US Government.

Views expressed are those of the author(s) and do not necessarily reflect official US Army or US Army Medical Department positions, nor does the content change or supersede information in other Army Publications. The *AMEDD Journal* reserves the right to edit all material submitted for publication (see inside back cover).

OFFICIAL DISTRIBUTION: This publication is targeted to US Army Medical Department units and organizations, and other members of the medical community worldwide.

Perspectives

Commander's Introduction

MG David A. Rubenstein

Two years ago, the January-March 2010 issue of the *AMEDD Journal* highlighted important legal considerations across a number of areas of military medicine. The articles in that issue were provided by the legal professionals of the Army Judge Advocate General's Corps who specialize in supporting the Army Medical Department. Those articles undoubtedly reacquainted many Army medical professionals with the enormous legal complexities that surround the practice of medicine, whether military or civilian, and reminded us of the valuable support provided by the Army JAG Corps. These legal specialists, including attorneys, paralegals, and administrators, provide the counsel, assistance, guidance, and yes, sometimes intervention, that make it possible for those of us in the practice of military medicine to do what we should do best, care for the health and well-being of our Soldiers, their Families, and military retirees.

The articles in that issue focused primarily on legal considerations directly related to the practice of medicine, such as consent to treatment, risk management, human subject research, and off-duty employment. It was so well received that the Army Medical Command Staff Judge Advocate was asked for more published discussions of the legal aspects of military medicine. In response, MAJ Joseph Topinka, the Deputy Staff Judge Advocate, has assembled another excellent collection of articles addressing additional vitally important areas of military healthcare delivery, including ethics, contracting, fiscal law, and agreements with civilian agencies and institutions. While, on the surface, some of those topics may appear to clinical practitioners to be someone else's problems, the articles in this *AMEDD Journal* illustrate the absolute folly of that idea. Every single day Army medical professionals have interactions involving contractors, funding, and procurement, just to name a few of the areas that may not seem to be of great concern in their daily activities. Unfortunately, an uninformed decision, a misguided involvement, or an incorrectly framed agreement can have serious ramifications, not only to an individual, but sometimes to an organization or to the mission of healthcare delivery itself.

Clearly, the practice of medicine is an intense, extremely complex responsibility, requiring years of education, training, and experience to achieve the necessary levels of competence and skills. Sadly, medical professionals must also cope with an extraordinarily complicated, exhaustively regulated, and highly litigious societal environment which affects virtually every aspect of their vocation. Fortunately for those of us in Army medicine, our partners in the MEDCOM Staff Judge Advocate are there to specifically help navigate that byzantine world of laws, regulations, rules, protocols, and restrictions as advisers, advocates, and sometimes defenders. Those legal professionals have also committed themselves to years of education, training, and experience to achieve their positions in the practice of law. They represent an invaluable resource that is absolutely necessary for AMEDD's primary mission to maintain a healthy, sustainable, combat-ready fighting force. Simply stated, we could not do it without them.

Editors' Perspective

The foundation for any successful free society which is based on the rule of law is the ethical conduct of its members, and, more significantly, its leaders. A free society cannot be long maintained when individuals and groups disregard the communal standards of fairness and morality, placing their own benefit above all else. Unfortunately, in human society, that type of conduct is expected, and laws, rules, and regulations are implemented in an effort to establish an artificial conscience among those so inclined. Ethical conduct has been the subject of discussions and writings since humans began living together in structured societies, and great philosophers and ethicists have endlessly pondered its successes and failures. In their article, COL Jonathan Kent and MAJ Joseph Topinka explain the concept of expected ethical conduct among those in government service using 14 common sense principles. These clearly defined and explained principles appear to be obvious, not requiring an understanding of anything more than simple decency and respect for others in the society in which we live. However, the reader will quickly recognize how many of these principles are constantly violated, or "bent" to the benefit of the violator. The article cites the various laws and military regulations that attempt to institutionalize expected behavior at the risk of penalty, but, as arrests and convictions all too regularly demonstrate, even the

prospect of such penalty does not deter certain individuals in government service from unethical, illegal activity. This article is an easily understood, comprehensive outline of what is expected, and ultimately demanded, of those holding the public trust, and should be required reading at regular intervals throughout a government career.

In the course of the normally very demanding work days, leaders in supervisory positions in military medical facilities are very happy to have a capable, functioning team to perform the functions and/or provide the services for which they are responsible. However, those same leaders, especially the less experienced, may also not completely understand the significant difference of their relationship with contractor personnel as opposed to that with military personnel and civilian government employees. After all, throughout a military career, leaders receive extensive training focusing on the unit/team perspective, a military unit must be cohesive and uniform, especially in the treatment of its members. A leader may therefore unwittingly—perhaps reflexively—deal with contractor employees as though they are no different from anyone else, which could be problematic, perhaps significantly so. Kim Judd and Kathleen Post have contributed two articles that clearly explain the basics in the contractor employee status from a contractual (legal) perspective. While contractor employees usually function seamlessly as fully integrated members of the team in the performance of their duties, that is where the similarity ends. Mr Judd's article focuses on the mechanism of the contracting process, and how that establishes the legal structure within which the contractor employees perform their functions. His explanation is key to understanding why and how their status is different and requires a different approach to both working and management interactions. Ms Post's article deals with the specifics of that relationship within the work environment, a concise, clearly presented discussion of the necessary perspective that government employees must maintain in their dealings with contractor personnel.

Lt Col (Ret) Eugene Smith's article addresses another surprisingly common problem involving MEDCOM contracts. Unauthorized commitments for goods or services by military personnel or government employees would seem to be an obvious and avoidable occurrence, but such is apparently not the case. As clearly explained in the article, unauthorized commitments occur for a number of reasons, under a variety of circumstances. Further, from a legal perspective, it is a complicated problem because all of the situations, circumstances, participants, and other conditions must be defined so that each occurrence can be evaluated within the framework of the contract and those legal definitions. This is necessary because the contractor/vendor wants to be paid for the product or service provided, and the government must determine if it, or someone else, is legally obligated to make that payment. Lt Col (Ret) Smith carefully develops different aspects of the problem with understandable explanations and illustrative scenarios, carefully and thoroughly referencing key points as the legal bases for his discussion. This is an excellent look at an important problem which is not understood well enough by military and government personnel. Hopefully this article will become standard reading for all AMEDD personnel, especially those in leadership and supervisory positions involving contact (by them and/or their subordinates) with contractors and vendors.

Obviously, operating the federal government costs money, and that money must be obtained, distributed to those who will use it, and spent to keep the government "open." CPT Juan Lozada-Leoni and his coauthors capture the distribution and use aspect of that function quite succinctly in the opening paragraph of their article in a single sentence: "Fiscal law is the body of law that governs the availability and use of federal funds." That is a concise definition of a very complex structure of laws, rules, regulations, procedures, and responsibilities that govern the entire process of deciding how much money will be spent, and specifying how that happens. Their article is a comprehensive look at the US federal appropriation process, providing insight into the evolving foundational legal requirements which have driven the development of fiscal law as the complexity of operating the government has dramatically increased. CPT Lozada-Leoni et al have successfully distilled this abstruse process into a well-organized, easy-to-understand primer that allows the reader to grasp both its scope and necessity. While it may not relieve the confusion and frustration that we often experience as we work with the finances of making AMEDD operate, this article puts the complexity and requirements into context, and, at the least, provides understanding of the reasons for the existence of the procedures and protocols that we must use.

It may come as a surprise to lean that not all of the financial responsibilities of operating military healthcare involve expenditure of funds. As Jackey Nichols describes in his informative and interesting article, the DoD has the authority to bill insurance companies who provide healthcare coverage to nonactive-duty beneficiaries who receive care in a military medical facility. That is the good news. The not-so-good news is that over the 20 years that the collection authority has existed, the billing process has fallen woefully behind the industry norm,

including little to no automated capabilities to generate and follow invoices, responses, and payments. Mr Nichols does, however, project improvements in this area, with the attendant reduction in redundancy, time, and cost in obtaining payments for services rendered from obligated insurance carriers, just as civilian treatment facilities do every single day.

Army medicine strongly encourages its professionals to explore their interests and engage in research and development projects in the course of their career progression. However, most projects of significant scope usually cannot be prosecuted using the resources available at a single facility, even a major medical treatment facility. So, in order to avail themselves of other resources, participants will pursue collaborative relationships with professionals at other locations, often in other agencies of the government or in the civilian world, who can provide the needed expertise and resources for the project to continue. This is where the legal aspects of such collaborations become important. In his well-developed and clearly presented article, Robert Charles explains the various types of agreements that are necessary to allow the transfer of technology between entities, whether within the Army, DoD, other US government agencies, or even to civilian, including commercial, activities. Such agreements are absolutely necessary to ensure that the government's rights to the property involved in the project, both physical and intellectual, are protected. Such agreements can specify the sharing of technology with commercial activities to allow them to further pursue its development, to both their benefit and that of the government. This article is an overview of a dynamic, complex area of military medicine within which leadership by the legal professionals is absolutely critical.

Social media is an ubiquitous fact of modern life. The potential problems of irresponsible use by individual military personnel and civilian government employees have long been recognized and are continually addressed. However, there is another side of social media within the government that can be valuable in a number of ways, but presents its own set of concerns. CPT Adam Jonasz has contributed an article that discusses the use of social media by Army commands at literally all levels, detailing the many setup, management, and maintenance considerations; the regulations; and the procedures that must be addressed prior to implementing an official organizational presence among the social media sources. He carefully details the regulatory structure that governs use of the media, and describes the types of sites, the advantages and disadvantages, and the specific legal considerations that must be included in the decision process before and after the decision is made to establish a presence. This article is contains very important, timely information that is highly relevant for today's AMEDD and MEDCOM leaders at all levels. It should be the among the first documents read when the pros and cons of establishing a social media presence are discussed.

Professional education programs available to Army healthcare providers are a very important component in the development of well-rounded, highly competent, experienced practitioners. Among the most productive of these programs are those in which civilian and military medical facilities allow each other's providers to train at the respective facilities. This training expands the skills of those providers, as well as those with whom they work, as they bring different experiences, skills, and perspectives to the practice of medicine, which fosters confidence and enthusiasm. However, notwithstanding the benefits of this process of "provider exchange tours," it has historically presented a serious legal concern for the Army: liability coverage for the provider working in the nonmilitary facility. In his very important and timely article, Maurice Deaver carefully lays out the parameters of that problem, and chronicles the evolution of DoD's efforts to sufficiently address the legal exposure to the provider trainee. He clearly explains the conditions and criteria for placing a military provider in a given civilian medical facility, and, most important, the necessary language in the medical training agreement that must be in place before any provider may work in that facility. The government's specific, virtually inflexible conditions regarding liability protection must be accepted by the civilian institution, or the agreement never happens. Those conditions are contained in two forms which were developed by MEDCOM and approved by the Department of Justice. Mr Deaver details those forms, their respective contents and applicability to the situation that the agreement must address. This article provides an easily understood ready reference for leaders in military medical facilities who are exploring training arrangements with civilian institutions.

David Claypool's article examines another type of nongovernment, noncontractor worker that is sometimes present in military healthcare facilities, the "student volunteer." These are students at accredited educational institutions who are working at a military medical facility as part of their medical education. Similar to the medical training agreements discussed in Mr Deaver's article, the placement of students in our facilities has strict criteria and conditions which must be met, and a carefully designed memorandum of agreement (which institutes the affiliation agreement) between the Army and the student's educational facility must be executed.

Mr Claypool clearly and succinctly describes the parameters of such arrangements, how they can be initiated, and the regulatory limitations the government places on use of student volunteers. As with other articles in this *AMEDD Journal*, this article is an excellent primer on how to establish such arrangements, which, among other things, can be a valuable way to stimulate interest in Army medicine among aspiring, future medical professionals.

Natural and (unfortunately) man-made disasters are all too common occurrences throughout the world, and of course the United States is by no means exempt. We are familiar with the news reports chronicling the occurrence of the disaster, and the initiation of the relief efforts from many sources, including the federal government, frequently including the use of the military, especially military medical resources. Often it may seem that the response "just happens," but as MAJ Joseph Topinka and Ida Agamy explain in their illuminating, very informative article, the commitment and use of federal resources in response to such emergencies are very closely governed and specifically structured by federal laws and implementing policies. The article details the Secretary of Health and Human Services public health declaration that initiates the federal medical response to the medical needs of a disaster, the liability considerations of responding healthcare workers, and the more serious aspects of such situations, such as isolation and quarantine. The military's participation in relief efforts is governed by DoD regulations, and is designed to initially provide support as needed by other agencies, unless the scope of the disaster and/or the security situation exceeds the capability of other agencies to organize and control. The article addresses the significant considerations surrounding US military involvement in overseas disasters, which is exponentially more complex than domestic responses. This is another excellent, important article that should be a handy reference for US military medical commanders and leaders who may be called upon to respond to such emergencies.

MSG Christopher Chouinard closes this issue of the *AMEDD Journal* with an article that gives long overdue recognition to a vital, yet largely unknown resource within the Army Medical Command. The Staff Judge Advocate's office is obviously populated with talented, capable lawyers who provide the counsel, advice, and guidance we need it to perform our jobs (whether we know it or not), but the SJA also has a number of energetic, dedicated, highly skilled paralegals and paralegal specialists who do much of the detailed, "dirty" work in support of the attorneys. However, they can also provide direct assistance to those requiring research, documentation, correct forms, and referrals to other resources that can provide further assistance. As MSG Chouinard writes, perhaps your first step in addressing a legal matter should be "call your paralegal." You may find the answer you need more quickly and easily than you imagined.

14 Principles of Ethical Conduct in Practice

COL Jonathan A. Kent, JAG, USA
MAJ Joseph B. Topinka, JAG, USA

Introduction

This article was prepared as a tool for readers to remember the Standards of Ethical Conduct through the use of the 14 Principles of Ethical Conduct set forth in 1989 by Executive Order 12674[1] (shown on the following page). In our experience, if you adhere to these basic principles, you will always be on solid ground when it comes to the *Joint Ethics Regulation*.[2] Of course, you should contact your local ethics counselor if you have any questions.

Do Not Use Public Office for Private Gain

Your service to the government takes priority over your own private interest. You can never use your government job to benefit your private interests. As military personnel and Department of Defense (DoD) employees, we work to further the best interests of the military, not ourselves.

For example, a program director for a government agency cannot use his or her position at a military installation to award payments from the government to himself or herself or his or her family. According to the *Encyclopedia of Ethical Failure*[3] published by the DoD Office of General Counsel's Standards of Conduct Office, a program administrator participated in such a practice:

> by awarding projects to two contractors who in turn hired the employee's personal business enterprise and his daughter as subcontractors. Over the course of 3 years, they received over $800,000 in fees from the government; the only catch, neither the employee's personal business nor his daughter actually performed any services for the government at all. Aside from the obvious fraud to which the former employee, his wife, and his daughter pled guilty, federal law also prohibits federal employees from making decisions concerning matters in which they or their family members have a personal financial interest. Even if the former GSA [General Services Administration] employee and his daughter had actually rendered the services that they billed for, the former employee would still have been in violation of federal law by awarding the projects to the contractors in the first place because his own financial interests were involved. The former GSA employee and his family were ordered to pay over $800,000 in restitution, and they each received prison sentences ranging from 12 to 46 months.[3(p38)]

Public Service is a Public Trust. Put Loyalty to the Constitution, the Laws, and Ethical Principles Above Private Gain

This principle really goes to what taxpayers expect of their government employees. We are all taxpayers and should ask ourselves what we would think of our conduct if looking at ourselves as taxpayers from the outside. Remember that perception is often a reality for those that see our conduct as government employees from outside federal service. You need to ask yourself whether your conduct on any given action fulfills the trust given to you by your fellow citizen taxpayers who expect you to adhere to the standards under the law and regulations.

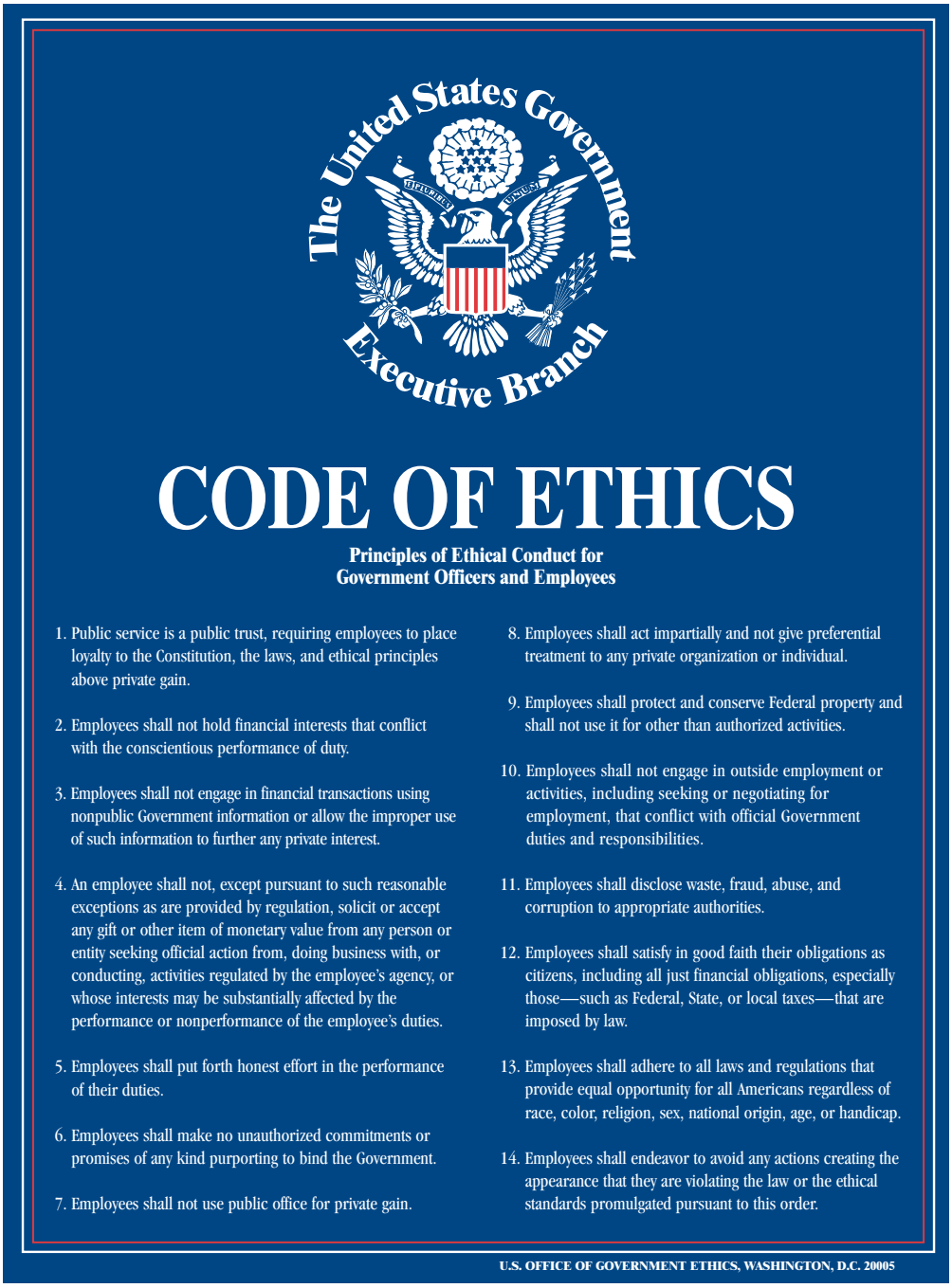
Do Not Hold Financial Interests That Conflict With the Honest Performance of Your Duty

A government employee's personal financial interests should never create a conflict of interest for the employee in regard to what that employee does in his or her official capacity. That is not to say a government employee cannot invest or even have a small business on the side. However, any personal financial interest cannot be in conflict with the employee's daily duties.

As a result of potential conflicts of interest, the federal government has a financial reporting process. Each year many employees find themselves completing an Executive Branch Confidential Financial Disclosure Report (Office of Government Ethics (OGE) Form 450: http://www.ogc.doc.gov/pdfs/OGE_Form_450.pdf). General officers and senior executive service (SES) employees must fill out a similar form designated the OGE 278 (http://www.usge.gov/Forms-Library/OGE-Form-278--Public-Financial-Disclosure-Report/). The process of completing these forms ensures the integrity of the system.

Do Not Use or Allow the Use of Government Information Not Released to the Public to Further Any Private Interest

Information is very powerful in today's world of information sharing. Proprietary information that is controlled by the government is very valuable to outside parties who may want to get an edge over other organizations for procurement, or influence, or inappropriate



The United States Government
Executive Branch

CODE OF ETHICS

Principles of Ethical Conduct for Government Officers and Employees

1. Public service is a public trust, requiring employees to place loyalty to the Constitution, the laws, and ethical principles above private gain.
2. Employees shall not hold financial interests that conflict with the conscientious performance of duty.
3. Employees shall not engage in financial transactions using nonpublic Government information or allow the improper use of such information to further any private interest.
4. An employee shall not, except pursuant to such reasonable exceptions as are provided by regulation, solicit or accept any gift or other item of monetary value from any person or entity seeking official action from, doing business with, or conducting, activities regulated by the employee's agency, or whose interests may be substantially affected by the performance or nonperformance of the employee's duties.
5. Employees shall put forth honest effort in the performance of their duties.
6. Employees shall make no unauthorized commitments or promises of any kind purporting to bind the Government.
7. Employees shall not use public office for private gain.
8. Employees shall act impartially and not give preferential treatment to any private organization or individual.
9. Employees shall protect and conserve Federal property and shall not use it for other than authorized activities.
10. Employees shall not engage in outside employment or activities, including seeking or negotiating for employment, that conflict with official Government duties and responsibilities.
11. Employees shall disclose waste, fraud, abuse, and corruption to appropriate authorities.
12. Employees shall satisfy in good faith their obligations as citizens, including all just financial obligations, especially those—such as Federal, State, or local taxes—that are imposed by law.
13. Employees shall adhere to all laws and regulations that provide equal opportunity for all Americans regardless of race, color, religion, sex, national origin, age, or handicap.
14. Employees shall endeavor to avoid any actions creating the appearance that they are violating the law or the ethical standards promulgated pursuant to this order.

U.S. OFFICE OF GOVERNMENT ETHICS, WASHINGTON, D.C. 20005

involvement in government operations. A government employee is expected to safeguard that information.

This rule is very significant for the federal procurement process. Protected information can give an invaluable edge to one potential contractor over another during the bidding process for a government contract. In addition, with the workforce consisting of more and more contractors, the US Army Medical Command (MEDCOM) has gone to great lengths to ensure that there is "arm's length" between government employees and contractor employees through the implementation of *MEDCOM Regulation 715-3*.[4] This regulation specifically entrusts MEDCOM employees to protect procurement-sensitive information from unauthorized disclosure or compromise. Such information includes but is not limited to budget matters, strategic planning, short term and mid-term plans, other contractor's proprietary information, and any other information that could be used to gain a competitive advantage.

DO NOT SOLICIT OR ACCEPT ANYTHING OF MONETARY VALUE FROM ANYONE SEEKING OFFICIAL ACTION FROM DOING BUSINESS WITH, OR CONDUCTING ACTIVITIES REGULATED BY YOUR AGENCY, OR WHOSE INTERESTS MAY BE AFFECTED BY THE PERFORMANCE, OR NONPERFORMANCE OF YOUR DUTIES

You may never solicit anything in your official position. If organizations offer you items of value you should consult with your servicing ethics counselor. Government ethics regulations contain specific guidelines for gift-giving to avoid situations of bribery or the appearance of bribery. When in doubt about whether to accept something or not, consult with your ethics counselor immediately. For MEDCOM employees, ethics advice can be obtained from your supporting legal office, whether within the medical facility or command, or through supporting, installation-based legal offices throughout the Army.

PUT HONEST EFFORT INTO THE PERFORMANCE OF YOUR DUTIES

The government expects its employees to come to work, work hard, work the appropriate hours of the duty day, and meet the standards established for employee conduct. The federal government does not hide anything and presents its expectations up front when an employee is hired.

PROTECT AND CONSERVE FEDERAL PROPERTY, USE IT ONLY FOR AUTHORIZED ACTIVITIES

The taxpaying citizens of this country expect government employees to be good stewards of the equipment, services, and property that the government provides for their use to fulfill their official duties. These resources should be used properly for official purposes and should not be wasted or stolen.

ACT IMPARTIALLY AND DO NOT GIVE PREFERENTIAL TREATMENT TO ANY PRIVATE ORGANIZATION OR INDIVIDUAL

There are literally hundreds of organizations in the country that support Soldiers, their Families, and members of the US military. These organizations often do great things for us. However, these organizations are nonfederal entities and we must be always vigilant in our dealings with them. We cannot give one an unfair advantage over another.

For example, in one incident, 7 senior military officers, including 4 general officers, were found to have misused their positions, improperly implying DoD endorsement or support of a nonfederal entity while appearing in a promotional video for a private organization. Two SES government employees who appeared in the video without title and whose comments did not create the appearance of DoD sanction were found to have properly participated in their personal capacity. The military officers, however, were found to have violated the *Joint Ethics Regulation*[2] in that they were in uniform and displaying their rank as they discussed their private affiliation.

In the Army Medical Command, our dealings take on significant importance as many organizations and individuals wish to donate gifts to Soldiers and Army medicine. We must always be careful about accepting gifts from outside sources even if the gifts on their face appear to be needed, and the gesture is kind and thoughtful. The MEDCOM published *MEDCOM Regulation 1-4*[6] which applies to gift acceptance from outside sources. In accepting gifts, members of this command must ensure that we do so properly and do not give the impression that, by the acceptance of a gift, we give some special status or endorsement to the organization of the individual making the donation.

DO NOT ENGAGE IN OUTSIDE EMPLOYMENT OR ACTIVITIES, INCLUDING SEEKING OR NEGOTIATION FOR EMPLOYMENT, THAT CONFLICT WITH OFFICIAL GOVERNMENT DUTIES AND RESPONSIBILITIES

This principle does not prevent a government employee from having an outside job, but it does prevent the employee from working in an outside job that conflicts with his or her official government duties. The two cannot cross or create a conflict. When such a conflict exists, the employee must remove the conflict by either ending the outside employment or ending federal service.

Postgovernment employment, negotiating with future employers, and off-duty employment are significant issues facing government employees, especially during times prior to transition from government service to civilian employment. Employees should be mindful of conflicts of interest. They also must be cautious about the parameters of their authorization to work in a nonfederal capacity. Due to the fact that the Army Medical Command has a significant population of medical clinicians that often seek off-duty employment, the command developed a regulation specifically addressing off-duty employment, primarily for active duty and government civilian employee healthcare practitioners: *Medical Command Regulation 600-3*.[7]

Do Not Make a Commitment or Promise of Any Kind That Could Bind the Government if You Don't Have Authority to Do So

Not everyone is legally authorized to enter into agreements or bind the government to a contract, or to spend the government's money on products and services. Sometimes government employees think, as a byproduct of their status, that they are, but that is not always automatic. Employees must think very seriously about what they say or do with regard to nonfederal parties when it involves obligating the US Government.

In the Army Medical Command, there is a great concern for such conduct in the procurement environment, especially involving interactions with contractors, vendors, or other nongovernmental individuals who provide goods and services to the command. As a result, the MEDCOM has developed a publication to address these commitments, *MEDCOM Pamphlet 715-2*.[5] The MEDCOM also has mandatory training for all employees, especially those involved in procurement on unauthorized commitments and how to avoid them.

Satisfy Your Obligation as a Citizen, Including All Just Financial Obligations, Especially Those That are Imposed by Law, Such as Federal, State and Local Taxes

Federal employees are citizens of the United States, and they have responsibilities as citizens to follow the law and pay their financial obligations. They should act appropriately in their personal capacity, just as they act appropriately in their official capacity as government employees. Their conduct in their personal capacity can actually impact their personal and official capacity.

Disclose Waste, Fraud, Mismanagement, and Corruption to Appropriate Authorities

This principle addresses the need for employee feedback in regard to the operation of our government. Leaders in the government must be open to the input of employees, and employees should have the freedom to communicate their feedback on potentially inappropriate activities that they observe in the operation of the government. Ideally, employees should be able to provide input or complain at the lowest level possible, but that is not always the case. Therefore, it is DoD policy that no person shall restrict a member of the armed forces from making lawful communications to a member of Congress or an inspector general.

Members of the armed forces shall be free from reprisal for making or preparing to make a protected communication which includes information that the member reasonably believes evidences a violation of law or regulation, including a law or regulation prohibiting sexual harassment or unlawful discrimination, gross mismanagement, a gross waste of funds or other resources, an abuse of authority, or a substantial and specific danger to public health or safety. Finally, paragraph 4.4 of *DoD Directive 7050.06*[8] specifies that:

> No person may take or threaten to take an unfavorable personnel action, or withhold or threaten to withhold a favorable personnel action, in reprisal against any member of the Armed Forces for making or preparing to make a protected communication.[8(p2)]

In other words, the government expects its employees to disclose waste, fraud, mismanagement, and corruption one way or another, and it offers appropriate protections to encourage such disclosure.

Follow All Laws and Regulations that Provide Equal Opportunity for All Americans Regardless of Race, Color, Religion, Sex, National Origin, or Handicap

Basically, this principle applies the ethic of reciprocity and focuses on DoD's leadership role in ensuring an equal opportunity, discrimination-free workforce. A key element of this rule is that persons attempting to live by this rule treat all people with consideration, not just members of their in-group. DoD policy is very clear in support of this principle. The defense of the nation requires a well-trained volunteer force, military and civilian, active and reserve. To provide such a force, DoD must ensure the attractiveness of a DoD career, providing opportunities for all DoD personnel to rise to as high a level of responsibility as their abilities allow. Therefore, programs or activities conducted by, or that receive financial assistance from DoD shall not unlawfully discriminate against individuals on the basis of race, color, national origin, sex, religion, age, or disability in accordance with guidance issued by the Departments of Justice, Health and Human Services, and Labor, as well as the Small Business Administration.

Avoid Any Actions Creating the Appearance That You are Violating a Law or Ethical Standards. Avoid the Appearance of Impropriety

The final principle is significant and one that we alluded to in the discussion of the second principle. Remember

that perception is often a reality for those that see our conduct as government employees from outside federal service. Even if you are not doing something wrong, there may be an appearance of wrong-doing or impropriety. Our experience has been that if you have doubts about some conduct, it may be questionable, or at least have a questionable appearance to someone looking from the outside. When considering that conduct, you must really look at the principles as a whole and, if you still have doubts, speak to someone else and get their perspective or, better yet, consult your ethics attorney. If you wish to go through with that conduct, appearance aside, you probably should get a written ethics opinion for your protection so that you understand the appropriate parameters of your conduct.

Remember that ethics advice is always available and encouraged. The advice does not create an attorney-client relationship, but it does help a person walk through an appropriate analysis of the ethical issues facing a government employee.

Conclusion

In the final analysis, public service is a public trust. To protect that trust, it is necessary that government employees uphold the highest ethical standards. DoD employees abide by the standards of ethical principles and set a personal example for fellow employees in performing official duties within the highest ethical standards. The Ethics in Government Act of 1978,[9] as amended, the Office of Government Ethics implementing regulations, and the *Joint Ethics Regulation*[2] are sources of standards of ethical conduct and ethics guidance, including direction in the areas of financial and employment disclosures and postgovernment-employment rules. Government employees fulfill the public's trust when following the ethical standards, and the 14 Principles always provide a solid ethical ground.

Acknowledgement

The authors thank Ms Margaret McCord for her vision in the preparation of this article.

References

1. Executive Order 12674: Principles of Ethical Conduct for Government Officers and Employees. Washington, DC: Office of the President of the United States; April 12, 1989 (modified by EO 12731, October 17, 1990). Available at: http://www.doi.gov/ethics/docs/eo12674.html. Accessed November 18, 2011.
2. *Department of Defense 5500.7-R: Joint Ethics Regulation*. Washington, DC: US Dept of Defense; 1993 w/change 6 March 23, 2006. Available at: http://www.defenselink.mil/dodgc/defense_ethics/ethics_regulation/. Accessed November 15, 2011.
3. *Encyclopedia of Ethical Failure*. Washington, DC: Office of General Counsel, US Dept of Defense; July 2010. Available at: www.dod.gov/dodgc/defense_ethics/dod_oge/EEF_complete_10.doc. Accessed November 15, 2011.
4. *Medical Command Regulation 715-3: Contractor/Contractor's Employees and MEDCOM Personnel Relationships.* Fort Sam Houston, Texas: US Army Medical Command; June 14, 1999. Available at http://www.samhouston.army.mil/sja/pdf_files/2007/715-3_Contractor_Employees_MEDCOM%20.pdf. Accessed November 15, 2011.
5. *Medical Command Pamphlet 715-2: US Army Medical Command Request for Approval of Unauthorized Commitment Processing Ratifications.* Fort Sam Houston, Texas: US Army Medical Command; March 10, 2005. Available at: http://hcaa.medcom.amedd.army.mil/assets/documents/pdf/MPam715-2.pdf. Accessed November 15, 2011.
6. *Medical Command Regulation 1-4: Gifts and Donations.* Fort Sam Houston, Texas: US Army Medical Command; September 30, 1999. Available at: https://www.us.army.mil/suite/doc/19473146. [note: restricted access] Accessed November 15, 2011.
7. *Medical Command Regulation 600-3: Off-Duty Employment.* Fort Sam Houston, Texas: US Army Medical Command; March 31, 2008. Available at: http://www.samhouston.army.mil/sja/pdf_files/2008/MEDCOM_600-3_Off-Duty_Employment.pdf. Accessed November 15, 2011.
8. *Department of Defense Directive 7050.06: Military Whistleblower Protection.* Washington, DC: US Dept of Defense; July 23, 2007. Available at: http://www.dtic.mil/whs/directives/corres/pdf/705006p.pdf. Accessed November 15, 2011.
9. Ethics in Government Act of 1978, Pub L No. 95-521, 92 Stat 1824.

Authors

COL Kent is the Staff Judge Advocate for the US Army Medical Command assigned to the Office of the Surgeon General, Falls Church, Virginia.

MAJ Topinka is Deputy Staff Judge Advocate, US Army Medical Command, Fort Sam Houston, Texas.

Legal Fundamentals of Contracting for Healthcare

Kim K. Judd, JD

Senior leaders, in fact leaders at all levels within the US Army Medical Command (MEDCOM), should understand basic principles of contracting for healthcare. Many practical and legal problems can be avoided if these principles are kept in mind as MEDCOM strives to provide healthcare to our Soldiers and other beneficiaries.

Scenario

Consider the following scenario which is based upon recent events at a major Army hospital. You are the Deputy Commander for Administration (DCA) at a hospital we will call The Medical Center. Your facility has previously awarded a contract for nurses to the company NursesRUS (NrUs) to address a critical shortage of nurses at The Medical Center. Under that contract, NrUs provides 47 nurses, all of whom work within the Department of Nursing. Most of the NrUs nurses are either former or retired Army Nurse Corps nurses or previous government civilian (GS) nurses, and many have previously worked at The Medical Center while on active duty/GS status. You have an open-door policy under which, once a month, you entertain complaints and allow anyone to come in and air their grievances. During one such open-door session, Nurse Johnson, an NrUs nurse, complains that she is not receiving her paycheck on a regular schedule. She also states that many NrUs nurses are not being paid on time, and further, more than a few of the other NrUs nurses are a month or more behind in receiving their paychecks. Nurse Johnson recently retired from the Army and worked for you before she retired.

What should you as the DCA do? What other parties should you involve? Should you have even entertained Nurse Johnson's complaint? As noted above, this particular scenario actually occurred, and is a textbook case of a good-intentioned DCA who failed to understand basic contracting principles. I will explain what happened at the end of the article.

First Fundamental

The first fundamental you must understand is that you, as a MEDCOM leader, do not have authority over contractor employees. While you are responsible and accountable to deliver healthcare to authorized beneficiaries, NrUs nurses are not your employees. They do not work for you, but rather are employed by a contractor, in this case, NrUs, which has a contract with an authorized MEDCOM agent empowered to enter into contracts which legally bind the Army. As a group, MEDCOM leaders are not empowered to enter into such contracts unless they are warranted contracting officers.

The only MEDCOM official who has authority over NrUs is the MEDCOM contracting officer that signed the contract with that company. That contracting officer almost always has a contracting officer's representative (COR), who helps the contracting officer monitor the performance of a company working under contract. The COR is usually nominated by the activity that needs contracting support. The contracting officer then appoints, in writing, the COR. The appointment letter specifies that the COR is only the eyes and ears of the contracting officer. In other words, the COR is to report contract performance issues to the appointing contracting officer so that the official with proper authority can attempt to resolve such issues.

To summarize this first principle, contractor employees are not government employees. Rather, they are employees of the company that hired them. Their employer is the holder of a contract with MEDCOM, and that contract is solely within the authority of the contracting officer who entered into that contract. Applying this principle to the described scenario, the DCA should not have heard complaints from someone who is not a government employee. Nurse Johnson is paid by NrUs, and the most that the DCA should have done was to tell Nurse Johnson that she should inform the COR that her employer, NrUs, was not paying its employees in a timely manner. It would then be the COR's duty to report the problem to the contracting officer.

Second Fundamental

The second fundamental is that government contracts are legal instruments between the government authorized buyer (the contracting officer) and the seller, NrUs. It is important that MEDCOM leaders clearly understand that there are 2 parties to a contract for sale of healthcare services. In our case, the buyer, as legal agent for the director of nursing at The Medical Center (the requiring activity with the need for contracted nurses) was

a warranted contracting officer assigned to support The Medical Center. Further, the seller of those services was NrUs, which had the obligation to supervise and compensate its own employees, in this case, Nurse Johnson. The responsibility to pay Nurse Johnson rested with NrUs, not the government.

Put another way, Nurse Johnson is not "your troop" or "your employee." In every government contract, just as in every contract you enter into in your private life, there is a buyer and seller. This fact is often lost in the day-to-day mission performance where contractor employees work alongside government employees, whether active duty military or civil service. Compounding the problem is the fact that often both the buyer's employees (active duty military or GS nurses) are performing the same healthcare functions as the seller's employees, in this case, Nurse Johnson and her fellow NrUs employees.

Third Fundamental

The third fundamental is that MEDCOM healthcare contracts, as with all federal government contracts, are bound by laws which are not applicable in the civilian world. Our contracts are funded with federal appropriated funds (mostly defense health appropriations). Because of this, federal laws and contracting rules, not state laws, apply.

The contracting rules are contained within the Federal Acquisition Regulation (FAR) (48 CFR chap 1). The federal rules generally require competition among healthcare sellers to win our contracts, and require that, for a MEDCOM contract to be legally binding, it can be entered into or changed only by a warranted contracting officer. As the US Supreme Court has stated (*Federal Crop Insurance Corp v Merrill*, 332 US 380), the fact that sellers

> …must turn square corners when they deal with the government"* does not reflect a callous outlook …it merely expresses the duty of all courts to observe the conditions defined by Congress for charging the public treasury.
>
> [**Rock Island, Arkansas & Louisiana R Co v United States*, 254 US 141, 254 US 143]

With regard to our Nurse Johnson situation, the FAR specifically states that it is illegal to treat Nurse Johnson as if she were a government employee, and it is illegal for anyone other than a warranted contracting officer to enter into or change a MEDCOM contract. Could the DCA legally have excused Nurse Johnson from coming to work? Hopefully the answer is painfully apparent to anyone who understands that Nurse Johnson is an employee of a recipient seller company, NrUs, which had been awarded a federal (FAR) contract for healthcare services.

Fourth Fundamental

The fourth fundamental is that acquiring healthcare services under the FAR is a 3-step process:

1. Acquisition Planning – Begins when the customer determines the agency's needs. The customer coordinates with the contracting officer. Often, the commanding officer/MEDCOM leader is in charge in this phase. The customer delivers an acquisition package to the contracting office.

2. Contract Solicitation and Award – Only the contracting officer has authority to enter into a contract. A contracting specialist delivers the acquisition package (from step 1) to the contracting officer, who solicits offers, evaluates offers, and awards the contract. The contracting officer is "the buyer" for the customer.

3. Contract Administration – Only the contracting officer has authority to administer, modify, or terminate a contract. The contracting officer appoints a contracting officer's representative (COR) to conduct contract surveillance and communicate, through the contracting specialist, to the contracting officer. The contracting officer administers the contract for the customer.

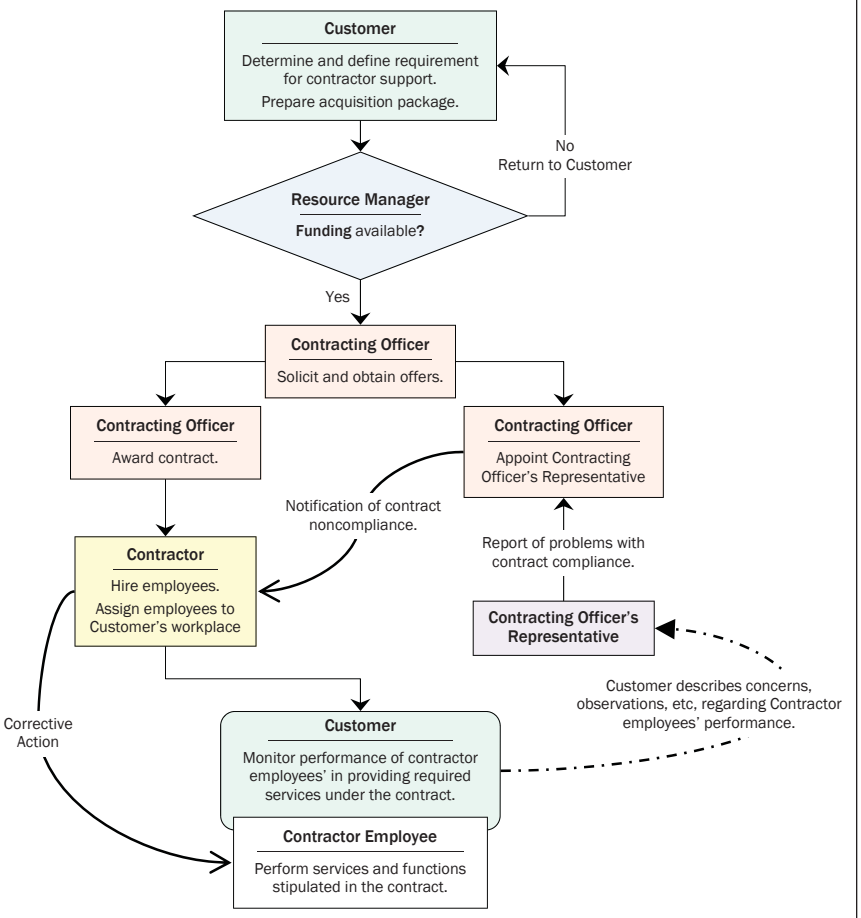
In the case of Nurse Johnson, the director of nursing at The Medical Center, let us call her COL Caring, determined that she needed 47 nurses more than she had in her active duty military/GS nursing staff. She determined what nursing specialties were needed and then went to her supporting resource management office with a statement of work to determine if The Medical Center had the appropriate funding to send the acquisition package to her supporting contracting officer. COL Caring also nominated someone for appointment by the contracting officer as the COR.

The supporting warranted contracting officer then proceeded to obtain competitive offers from companies interested in providing the required services/personnel. The contracting officer picked the winner of this competition based upon criteria provided by COL Caring. For instance, if COL Caring, as the head of the requiring activity needing the contract support, was willing (and capable) to pay more for a company with more experienced nurses, the solicitation for offers would include that criteria. Once the contracting officer picked the winner (NrUs in this case) the contracting officer signed the contract award, and the result is a legally binding FAR contract.

Finally, NrUs employees began performing under the contract, and the terms of employment between NrUs and Nurse Johnson is a matter solely between those 2

parties. If Nurse Johnson, or any other NrUs nurse, fails to get paid or fails to show up for work, that is an employment matter between NrUs and its employees. Failure to show up for work is a contract performance problem which should be noted by COL Caring and reported immediately to the COR. The COR should then immediately report the contractor's performance failure to the contracting officer.

The following is the actual sequence of events upon which the above NrUs scenario is based. After listening to her complaint in the open-door session, the DCA told "Nurse Johnson" that this was an intolerable situation and that the Army did not function in this manner. He asked her to come back in a week if the nonpayment problem persisted. A week later she came back with several other "NrUs" nurses and it became apparent that the problem was getting worse. The DCA stated that the Army does not "mess with the troops' pay," and should that occur, the troops would not come to work. He told the NrUs nurses he would look into the situation. He never informed "COL Caring," the COR, or the contracting officer, and then he became so busy that he never looked into the situation, although he intended to do so. The NrUs nurses started calling in sick which caused a severe problem for COL Caring. When she could no longer cover for the nurses with other staff, she finally called the supporting regional contracting officer, although she never informed the COR. The COR only found out about the problem when the regional contracting officer arrived at The Medical Center with a letter terminating NrUs for a FAR contract default. Fortunately, the contracting officer discovered the basic facts described herein, discovered a systems problem with payment of contractor invoices, and was able to resolve late payments by the Army to NrUs. Once NrUs began receiving timely payments for its services, the employees began to promptly receive their pay (we think). All the contracting officer and COL Caring knew was that the sickout situation resolved itself soon after the payment problem was addressed.



A simplified representation of a support contract origination and the process of dealing with contract noncompliance.

CONCLUSION

This is a very brief overview of contracting fundamentals, a simplistic representation of which is provided in the Figure. I encourage all readers to ask for additional training/seminars from their Office of the Staff Judge Advocate or their healthcare contracting activity if they wish more information on various subjects, such as hiring, interviewing, timesheets, commending, awarding, causing removal or just critiquing contracted performance, trying to resolve contractor employment problems, requiring work different than that which the government bought, and labor hour problems. The fundamentals of these issues should be familiar to all AMEDD leaders.

AUTHOR

Mr Judd is an Attorney Advisor in the Contract Law Section, Office of the Staff Judge Advocate, US Army Medical Command, Fort Sam Houston, TX.

Roadmap for Dealing with Contractor Employees

Kathleen Post, JD

For many persons doing business in today's integrated environment, the road to government contracting is as perilous and treacherous as Frodo Baggins' journey from Middle Earth to Mordor.[1] As it was for Frodo Baggins, vigilance is required—integration of contract employees into the workplace has added an additional layer of complexity which requires thoughtful oversight to ensure the working relationship between government and contractor is maintained in proper balance, and to enforce the prohibition on contractors performing inherently governmental functions.

A snapshot of a typical day at a medical treatment facility or one of its satellite clinics would show civilian employees and military personnel working alongside a cadre of contractor employees, all performing medically-related mission essential functions. Working behind this scene to ensure that uninterrupted health care is provided to our Soldiers serving on 2 war fronts is the Army's acquisition force who, on a daily basis, contract for a variety of medical services, ranging from physicians and nurses to imaging maintenance, as well as laboratory and hospital housekeeping services. In 2010 alone, the contracting center of excellence and 6 regional contracting offices acquired over $1.67 billion ($10^9$) in specialized health care services and supplies (source: Army Contracting Business Intelligence System).

With the Army having moved toward achieving total Army integration by maximizing the contributions of the Army National Guard, the US Army Reserve, and the Active Army through a "one team, one fight" concept, the current operational tempo finds increasing numbers of contractors in both Iraq and Afghanistan. Recent statistics indicate there are over 224,000 DoD contractor personnel in the US Central Command area of operations, creating a 1:1 military to contractor ratio in both Iraq and Afghanistan.[2] There is no question that management of contractor activities by government employees is an integral part of doing business every day and is a critical link in US Army Medical Command's (MEDCOM) mission to Promote, Sustain and Enhance Soldier Health.

Whether as a civilian or armed services member, properly managing relationships with contractor employees is essential not only to the acquisition process but is the ethical obligation of every government employee. It rests on a rather simple but often misunderstood premise: contractor employees are not government employees and therefore cannot be managed in the same manner. The genesis of the relationship is found and subsequently defined by the contract, which forms the basis of the rights and obligations of the parties similar to the Uniform Code of Military Justice* or civil service rules and regulations. Adding complexity to this simple premise is the fact that, while contractors are not generally supervised by government employees, for personal health care services and medical malpractice purposes, there is generally language in the performance work statement that requires such supervision:

> This is a personal services contract and is intended to create an employer-employee relationship between the government and the individual contract health care providers (HCPs) only to the extent necessary for providing healthcare services required under this contract. The performance of the healthcare services by the individual HCPs under a personal services contract are subject to the day-to-day supervision, clinical oversight, and control by healthcare facility personnel comparable to that exercised over military and civil service HCPs engaged in comparable healthcare services.

Look or sound familiar? Wait a minute, did I not just say "contractor employees are not government employees and therefore cannot be managed in the same manner?" For medical malpractice reasons, healthcare providers in a personal services contract are generally supervised by civilian or military personnel. It is a unique exception to the general rule but one which exists within the MEDCOM with great regularity. However, this exception to the supervision requirement does not change the scope of the general guidelines on managing relationships with contract employees. It is essential that our medical force understand and employ the proper guidelines in effectively supporting the full spectrum of operations within the confines of the law.

Contracting with the United States rests on the basic premise that its rules are found in the laws and regulations which govern it. Because the acquisition process is

*The Uniform Code of Military Justice (UCMJ), a federal law (64 Stat. 109, 10 USC, chap 47) is the judicial code which pertains to members of the United States military. Under the UCMJ, military personnel can be charged, tried, and convicted of a range of crimes, including both common-law crimes (eg, arson) and military-specific crimes (eg, desertion).

structured and restricted, even the contracting officer has no authority to deviate from these laws or regulations. It is important to remember from the outset that any acquisition finds its genesis and guidance in the Federal Acquisition Regulation (48 CFR chap 1). Thus, any acquisition activity generally begins, continues, and ends under the guidance provided under this regulation. Understanding the basic legal framework for the relationship with exists between the government employee and the contractor employee will help frame how you analyze issues which will inevitably surface.

Just as the role of the government is governed by law, the role of the contractor is limited by law and provides a legal barrier which distinguishes the role of the contractor from that of the government employee in the federal workplace. For this reason, contractors cannot perform inherently governmental functions such as making management decisions on behalf of the government.[3] Inherently governmental functions also include activities that require the exercise of government authority to include monetary transactions and entitlements. Because of the strict prohibition against contractors performing inherently governmental functions, contractor employees must identify themselves as a contractor in phone, correspondence, and other communication.

It is important to remember that even in the context of medical services, it is a business relationship which exists between the government and the contractor. The contractor is furnishing supplies and services for a negotiated price. Performance requirements by the contractor and the obligations of the government are established solely by the terms of the contract. The only person with authority to change the terms of the contract, and thereby the requirements to be performed under the contract, is the contracting officer.

At this juncture, it is also important to note that the military chain of command can only exercise management control through the contract and does not exercise direct control over contractors and its employees. Commanders must manage whatever issues arise under the contract through either the contracting officer or the contracting officer's representative (COR). The COR is appointed by the contracting officer to be his or her eyes and ears on the ground to ensure the contractor is performing in accordance with the terms and conditions of the contract. While the COR is an important communication liaison between the commander and the contracting officer and an important player in contractor management and control, it must be understood that the COR does not exercise direct control over the contractor nor its employees. Only the contractor can directly supervise its employees (with the personal services exception noted above). While the COR can communicate the commander's needs to the contractor, any changes to the contract's requirements must be made by the contracting officer, the sole government official with authority to modify the contract.

Because the relationship between the government and the contractor is framed by the terms of the contract, the answers to issues are generally found there as well. Additional guidance can also be found in *MEDCOM Regulation 715-3.*[3]

General rules require, for instance, that government employees not direct the contractor to pay its employees a particular salary or to give performance bonuses. Contractor employees are also not authorized to participate in social events, training holidays, organizational day activities, or other similar events unless specified in the contract or an exception has been obtained. This is not because the Grinch stole Christmas,[4] but because any activity performed by the contractor's employees is governed by the terms of the contract and by the *Joint Ethics Regulation.*[5]

Spoiler: Just as Frodo Baggins successfully made the journey from Middle Earth to Mordor, every government employee can successfully navigate the labyrinth of business in today's integrated environment. Learning to manage expectations and understanding the contractual framework which governs the working relationship that exists between government and contract employees is the essential first step in keeping MEDCOM's mission to "Promote, Sustain and Enhance Soldier Health."

REFERENCES

1. Tolkien JRR. *The Lord of the Rings* [trilogy]. New York: HarperCollins Publishers LLC; 2007 [reissue].
2. *Contractor Support of US Operations in USCENTCO*M AOR, Iraq and Afghanistan [5A Paper]. Washington DC: Office of Deputy Assistant Secretary of Defense (Program Support); September 2010.
3. *MEDCOM Regulation 715-3: Contractor/Contractor's Employees and MEDCOM Personnel Relationships.* Fort Sam Houston, Texas: US Army Medical Command; June 14, 1999.
4. *Dr Seuss. How the Grinch Stole Christmas!*. New York: Random House; 1957.
5. *Department of Defense 5500.7-R: Joint Ethics Regulation*. Washington, DC: US Dept of Defense; 1993 w/ update 2006.

AUTHOR

Kathleen Post is a Contract Law Attorney Advisor with the Office of the Staff Judge Advocate, US Army Medical Command, Fort Sam Houston, Texas.

Have You Made an Unauthorized Commitment Lately?

Lt Col (Ret) Eugene J. Smith, JAG, USAF

Introduction

Have you made an unauthorized commitment lately? If you are a US Army Medical Command (MEDCOM) employee who interacts with contractors, vendors, or other nongovernmental individuals who provide goods or services to MEDCOM, the answer may be yes, and you may not yet know it. This article discusses what constitutes an unauthorized commitment, how it commonly occurs, at what point does it occur, why the occurrence date is significant, who is legally liable, why it is important to avoid causing it, why some of them cannot be corrected, and how to reduce the occurrence of unauthorized commitments within MEDCOM.

What Is An Unauthorized Commitment?

The Federal Acquisition Regulation (FAR) (48 CFR chap 1) contains the basic policies and procedures that federal government executive agencies must use to acquire goods and services. The FAR defines an unauthorized commitment as:

> an agreement that is not binding solely because the government representative who made it lacked the authority to enter into that agreement on behalf of the government.[1]

Although the Department of Defense has issued the Defense Federal Acquisition Regulation Supplement (DFARS)[2] and the Department of the Army has issued the Army Federal Acquisition Regulation Supplement (AFARS)[3] to implement the FAR, neither the DFARS nor the AFARS further defines, clarifies, or explains the phrase "unauthorized commitment." At first glance, the FAR's definition may seem straightforward since it specifies only 4 simple requirements for a communication or transaction to meet the definition of an unauthorized commitment:

1. There must be an agreement, commonly referred to in everyday language as a deal or an arrangement.

2. The agreement must have been made by a federal government representative.

3. The agreement must have been made on behalf of the United States.

4. The agreement must not be legally binding, also known as legally enforceable in court, solely because the government representative who made the agreement lacked the authority to act on behalf of the United States.

The regulatory definition in the FAR is not as simple or as comprehensive as it may initially appear. Upon closer examination, that definition leaves at least 3 major questions unanswered. First, the definition does not identify the status of the other party to the arrangement. Could an arrangement between 2 government representatives meet the definition of an unauthorized commitment? Second, the definition does not specify who qualifies as a "government representative." Could a government representative be the personnel of a government contractor? Third, the definition does not identify what authority is needed to properly act on behalf of the United States. Does a commanding general, subordinate commander, first sergeant, sergeant major, director, or department chief have enough rank or authority to make legally binding agreements on behalf of the United States? With help from the US Government Accountability Office (GAO), we know the answers to these questions will always be a clear and unambiguous, **NO**. One role of the GAO is to support congressional oversight by auditing agency operations to determine whether federal funds are being spent efficiently and effectively, and by investigating allegations of illegal and improper activities. In 1980, the GAO investigated alleged unauthorized commitments within a specific executive agency.[4] In the report, the GAO's working definition of an unauthorized commitment was

> …an informal agreement, between a contractor and a federal employee who does not have contracting officer authority, to begin work.[4(pvii)]

The GAO's definition clarifies that the government representative in the FAR's definition must be a federal employee (civil servants and military members are federal employees), the agreement must be with a contractor (a person not a federal employee), and the authority to make legally enforceable agreements on behalf of the United States is contracting officer authority, not military command authority.

The picture becomes much clearer when we view the FAR's definition in light of the GAO's clarifications. We see that an unauthorized commitment actually has the following 5, not 4, specific parts or requirements:

1. There must be an agreement.

2. The agreement must have been made by a federal government employee.

3. The agreement must have been made on behalf of the United States.

4. The agreement must not be legally binding solely because the federal government employee who made the agreement did not have contracting officer authority to act on behalf of (legally bind) the United States.

5. The agreement must have been made with a person who was not a United States government employee.

That 5-part definition is a more comprehensive, accurate, and usable definition to use when deciding whether an unauthorized commitment has occurred. Now that we have a clear, comprehensive, accurate, and usable definition of an unauthorized commitment, we can now explore how unauthorized commitments commonly occur within MEDCOM.

The Contracting Officer's Representative

It is physically impossible for a MEDCOM contracting officer to personally manage or administer every contract for which he or she is responsible, therefore, contracting officer's representatives (CORs) are designated to assist in managing and administering the contracts. The COR is a government employee who has received special training in contract administration issues,[5,6] and who has been appointed in writing by the contracting officer. The COR serves as the "eyes and ears" of the contracting officer in locations where the contract requires the contractor to actually perform the services or deliver goods. The job of the COR is to see that the contractor is performing all services as stated in the contract, and to promptly report all problems to the contracting officer. The role of the COR is so important to proper contract administration that the Department of Defense, the Department of the Army, and MEDCOM require the contracting officer to appoint an adequately trained COR for all service contracts prior to award of the service contract. Further, MEDCOM requires a general officer or member of the senior executive service to confirm in writing that the contracting officer has indeed appointed or will appoint an adequately trained COR for all MEDCOM service contracts valued over $100,000 prior to award.[7-9] The COR must be a military member or federal civil servant because COR duties are inherently governmental functions due to the amount of discretion and judgment necessary to perform these duties.[6,10]

How Do Unauthorized Commitments Commonly Occur Within MEDCOM?

There are 5 ways unauthorized commitments commonly occur. Four of those situations involve a federal employee who is not a contracting officer, who either:

(*a*) arranges for or permits MEDCOM to continue to receive goods or services after the lawful contract has expired, or

(*b*) arranges for or permits MEDCOM to receive goods or services when there was no lawful contract, or

(*c*) arranges for or permits MEDCOM to receive goods or services that are not included in the existing lawful contract, or

(*d*) directs or permits contractor personnel to deliver goods or perform services under terms and conditions contrary to those of the lawfully awarded contract.

All of the above situations commonly occur within MEDCOM. Although they usually occur at medical treatment facilities, each situation may occur just as easily at an administrative office. The fifth type of unauthorized commitment (Situation (*e*)) involves a contracting officer who purports to act on behalf of the United States, but the dollar amount of the agreement exceeds his or her designated contracting authority. This situation rarely occurred within MEDCOM during the last decade, perhaps because of the checks and balances in the contracting process.

Situation (*a*)

As previously described, the COR serves as the eyes and ears of the contracting officer. The general rule is that the COR has no authority to serve as the "mouth" of the contracting officer, and is limited to the authority granted by the contracting officer in the COR's appointment letter. Therefore, a COR or any other member of a department or MEDCOM office unintentionally makes an unauthorized commitment by ordering goods or services after the contract for those goods or services has expired. If the COR, department chief, office director, or anyone else other than a contracting officer tells or permits the vendor to deliver goods or perform services because he or she honestly but incorrectly believes a contract still exists, that person unintentionally makes an unauthorized commitment. The same is true if that

person honestly but incorrectly believes that a new contract to continue a particular contract service has already been awarded because the paperwork was submitted to the contracting office many weeks ago, but in fact the contract had not yet been awarded. Yes, a government employee may make an unauthorized commitment without intending to do so. Yes, a government employee may make an unauthorized commitment even if he or she orders goods or services that the government actually needed and the government actually received and used the goods or services to accomplish a critical part of the mission. These kinds of unauthorized commitments occur because the person incorrectly assumes that a prior contract is still in existence, or that the contracting office has already awarded a follow-on contract for the goods or services in question. The person's beliefs and intents are irrelevant for the purpose of determining if the person made an unauthorized commitment. The sole focus in determination as to whether an unauthorized commitment occurred is whether the government employee had authority to act on behalf of the government in arranging to obtain the goods or services from the vendor.

Situation (*b*)

The COR or other member of a MEDCOM organization makes an unauthorized commitment by arranging to receive goods or services when there is no contract for those goods or services. Since a government official can make an unauthorized commitment by acting under an honest but incorrect belief that there is an existing contract, it logically follows that the same action by an official in a situation where there never was an actual contract also creates an unauthorized commitment.

Unauthorized commitments occur in situations where the government official, being unfamiliar with the rules concerning who has authority to legally bind the government, purports to act on behalf of the government based on the official's military rank, civil service grade, and/or duty title. This situation is different from the earlier situations in which the government official incorrectly believed he or she was following proper procedures. In this situation, the government official is unaware of the proper procedures or elects to disregard the proper procedures. It takes time to process paperwork. Although time is valuable, a lack of planning or a failure to follow proper emergency procedures is irrelevant to the definition of an unauthorized commitment.[1] Even when time is of the essence and a MEDCOM medical facility or other MEDCOM organization needs goods or services that are not already under a contract, the only authorized method of getting them quickly is through the proper contracting process. Needing it now is not an exception or defense for creating an unauthorized commitment.

Situation (*c*)

An unauthorized commitment occurs when a government official who lacks proper authority orders particular goods or services that are not included on the existing contract. An example: there is an existing contract for goods or services X1 through X1001. That contract may have been in place for several years and the medical facility or other MEDCOM organization had never needed goods or services other than X1 through X1001 during the contract period. A new, bona fide need for goods or services X1002 may arise due to the arrival of a new provider, new person, or new patient; addition of new capabilities; or because of changes in other legitimate circumstances. An unauthorized commitment occurs if a government official other than a contracting officer orders goods or services X1002 on behalf of the government before the contracting officer modifies the contract to add these particular goods or services. This is true because goods or services X1002 is not among the goods or services the "noncontracting officer" government official is authorized to order under the terms of the existing contract. In a more specific example, let us suppose there is an existing contract for EEMMR Smith Knee Company to provide specified knee implant items to Best Army Medical Center. A new surgeon has been assigned, hired, or contracted to perform surgeries, including knee replacement surgeries, at Best Army Medical Center. The new surgeon has a legitimate reason to use knee implant items that are not listed on the contract with EEMMR Smith Knee Company, or on any other contract available to Best Army Medical Center. If a government official then arranges for any vendor to supply these different knee implant items, an unauthorized commitment is created because these items are not available under an existing contract. The same situation exists if the government official arranges for EEMMR Smith Knee Company to supply these knee implant items, because these items are not listed on their existing contract with the government.

Situation (*d*)

An unauthorized commitment occurs when a government official, who lacks proper authority, directs or permits contractor personnel to deliver goods or perform services under terms and conditions contrary to those of the lawfully awarded contract. If the contract requires the contractor to only perform services from Monday through Friday, any government official other than a contracting officer causes an unauthorized commitment by directing or permitting contractor personnel to perform services on a Saturday to help government employees eliminate a backlog, or help meet a need for services on that day. Changing the performance dates or increasing

the amount of contract services makes the government liable for an upward adjustment in the contract price. Only a contracting officer has authority to direct or permit changes in contract performance that may result in the government owing more money to the contractor, or receiving less goods or services. Likewise, if the contract requires the contractor to perform particular kinds of services, any government official other than a contracting officer causes an unauthorized commitment by directing or permitting contractor personnel to perform other kinds of services. For example, if the contract provides only for cleaning floors and carpets, directing or permitting contractor personnel to take out the trash is an unauthorized commitment. Since contractor personnel are authorized to be on government property solely for the purpose of performing the services specified in the government contract with their employer, they have no authority to provide free services on behalf of their employer. Even if contractor personnel have authority to provide free services on behalf of their employer or on behalf of themselves, such actions raise legal issues related to accepting gifts on behalf of the government. Gifts of goods or volunteer services must be processed in accordance with specific Department of Defense and Army rules.[11,12] These procedures are designed to protect the interest of the government and the gift-giver, but are not convenient for everyday use.

Situation (*e*)

The fifth type of unauthorized commitment occurs when a contracting officer purports to obligate the government in a contract that exceeds his or her warrant authority.[13-15] Just as a commander does not have unlimited authority to command, some contracting officers hold contracting warrants that limit their authority to contract on behalf of the government. If the contracting officer exceeds the dollar threshold or other limitation of his or her contracting warrant, such action causes an unauthorized commitment because the contracting officer is acting without contracting authority. This is the same situation that occurs when any other government official purports to contract on behalf of the government without having the required contracting authority. For example, an unauthorized commitment occurs if a contracting officer with a contracting warrant that is limited to awarding contracts up to $2 million awards a contract for $3 million. Similarly, an unauthorized commitment occurs if a COR or other government official exceeds his or her delegated authority to order goods or services under an existing contract vehicle. For example, suppose the contracting officer delegates authority to a government official to order up to $5,000 worth of goods or services in a single order under a specific blanket purchase agreement.[16,17] If that government official places an order for $6,000 in goods or services on the specified blanket purchase agreement, or places an order for $4,000 not using the specified blanket purchase agreement, an unauthorized commitment occurs. The government official exceeded his or her delegated authority to order goods or services on behalf of the government.

Who Is Legally Responsible For Committing The Unauthorized Commitment?

The Vendor

Is the vendor legally responsible for committing the unauthorized commitment? After all, the vendors know (or should know) if they have contracts with the government, and know (or should know) the respective goods or services each contract requires the vendor to provide. While that may be true, vendors are not legally responsible for causing the unauthorized commitment. Remember, the government's definition of an unauthorized commitment looks at the actions of a government employee, not at the actions of the vendor's employees.[1] The definition is the same even if the same vendor repeatedly provides goods or services to the government with full knowledge that those goods or services are not covered by a lawful government contract. The vendor's financial risk, eagerness, or overeagerness to sell goods or services to the government has no role in the definition of an unauthorized commitment. However, the vendor does face a potential financial risk, which will be discussed later.

Commander or Supervisor

Is the commander or the supervisor legally responsible for committing the unauthorized commitment? After all, the commander and the supervisor are responsible for what happens in their organization. That may be true, but the commander and the supervisor are not legally responsible for creating the unauthorized commitment. Again, the government's definition of an unauthorized commitment looks at the actions of the government official who actually made the arrangements with the vendor on behalf of the government without having proper authority.[1]

The Responsible Government Official

Yes, the government official who made the arrangements with the vendor on behalf of the government is the person legally responsible for creating the unauthorized commitment. A government official may create an unauthorized commitment by words or actions that cause the vendor to deliver goods or services on behalf of the government. A clear example is when a government official calls the vendor and tells the vendor to deliver a specified amount of particular goods or services to a designated location by a certain date for use

by the government. The vendor does not know what the government needs until someone inside the government provides that specific information. If a government official provides this information to a vendor to obtain pricing information while conducting market research[18,19] or for any other reason, the burden is on that government official to make it clear to the vendor that their communication is not an order by the government for goods or services. Another clear example is a government official directing contractor personnel to perform services not included under the contract, or directing them to perform a greater quantity of services that the amount specified in the contract. Both situations cause the contractor to incur extra cost. Since goods or services are not free, the contractor naturally expects to be paid extra money for providing the extra goods or services.

A government official may also commit an unauthorized commitment by inaction or omission. For example, suppose the contract expires on Monday, but the contractor's personnel show up on Tuesday and continue to perform the same services, but the government official in charge of monitoring the contract services does nothing to stop that performance. If that government official knows (or reasonably should have known) about the contractor's continued performance and does nothing to stop it, that person commits an unauthorized commitment.

The bottom line; a government official may commit an unauthorized commitment by commission or by omission. The question is whether that person's actions or inactions with the vendor caused the vendor to deliver goods or perform services under the incorrect belief that this person had authority to act on behalf of the government.

At What Point Does an Unauthorized Commitment Occur?

The unauthorized commitment occurs at the moment the government official, without authority, completes the arrangements for the vendor to provide goods or services on behalf of the government. A government official may have several communications over many months with a vendor to discuss the needs of the government. Or, the government official may have only one communication—in person, by phone, by fax, or by email—with the vendor concerning the needs of the government. The amount of back and forth communications is not the key to determining the point at which the unauthorized commitment occurs. It occurs at the point when the government official and the vendor reach a general understanding or deal concerning what the vendor will do and how much the government will pay the vendor for doing it. The price need not be expressly stated. The facts may show the price was implied to be the amount the government paid the last time, derived from the vendor's catalog, or is simply what the parties incorrectly believe to be the contract price. By definition, the unauthorized commitment occurs at the time the government official, without authority, completes the arrangements for the vendor to provide goods or services on behalf of the government. The unauthorized commitment does not occur later when the vendor actually delivers the goods or performs the services.

In the case of an unauthorized commitment created by omission, the unauthorized commitment occurs at the time the government official knows, or should have reasonably known, of the vendor's continued performance without the benefit of a contract. The vendor will normally submit an invoice for payment at the same prices as in the expired contract.

What is the Significance of the Date on Which the Unauthorized Commitment Occurred?

It is critically important to determine the correct date on which the unauthorized commitment occurs because of fiscal law reasons. If the unauthorized commitment is later approved or ratified by a government official with authority to do so, the money must come from the fiscal year in which the unauthorized commitment was made.[20]

In some instances, the unauthorized commitment may have occurred 2 or more fiscal years ago, the vendor may have provided the goods or services one or more fiscal years ago, a government official may not have discovered and reported the situation until last fiscal year, and it may not be ratified or approved until this fiscal year. This is the case if the government official made the unauthorized deal with the vendor in August of fiscal year 2008, the vendor delivered the goods or services on time in November of fiscal year 2009, the vendor did not submit a proper invoice to the government until July of fiscal year 2010, and the transaction was not approved until December of fiscal year 2011. Using the wrong fiscal year money to pay the vendor is a Bona Fide Need Rule violation, a statutory violation.[21,22] That is why is it critically or criminally important to document in which fiscal year the unauthorized commitment occurred. That task becomes harder and harder the closer to the end of the fiscal year that the unauthorized commitment occurs, and government personnel with personal knowledge of communications between the vendor and the government official are no longer available to provide information. The absence of government officials with personal knowledge of the facts may mean having to rely on the "paper trail" to reconstruct what happened, and when it happened.

WHY IS IT IMPORTANT TO AVOID COMMITTING AN UNAUTHORIZED COMMITMENT?

One reason it is important to avoid committing unauthorized commitments is because committing them is a regulatory violation. The regulations say do not do it.[23,24] If you do not have a contracting officer's warrant that gives you authority to enter into contracts or make deals on behalf of the government, comply with the regulations and do not do it. Even in emergencies, there should be enough time to contact the COR, permit the COR to notify the contracting officer, and allow the contracting officer to make the necessary arrangements to avoid mission failure. The COR must be contacted so that an authorized government official may promptly take the proper contracting steps for mission success. If the COR is unavailable for any reason, the proper action is to contact the on-duty contracting officer that services your organization to quickly obtain the required goods and services.

Another reason it is important to avoid committing an unauthorized commitment is the harsh financial impact on the vendor. After the contracting officer has put a contract vehicle in place under which to make the payment, the vendor must still wait for the Defense Finance and Accounting Service to make the payment. Because of processing and paying times, it could take several months before the vendor actually receives payment, even if the unauthorized commitment is immediately discovered. As you might imagine, it is a severe financial hardship for small businesses to wait several months for payment from the government while those small businesses must meet weekly payroll and other operating costs.

Another reason it is important to avoid making an unauthorized commitment is the potential for personal financial disaster. Of course, a civil service official is subject to possible adverse personnel actions for failing to correctly perform his or her job since his or her job does not include making unauthorized commitments. Those adverse actions are stipulated in *Army Regulation 690-700*,[25] Chapter 751, Table 1-1, Offense 14, as shown in the Figure. A military official is subject to possible punishment under Article 134 of the Uniform Code of Military Justice.[26] The beginning of personal financial disaster for civil service officials and/or military members could also be the end of their government employment. Such is very unlikely to occur in MEDCOM, especially on a first offense and when the person was acting in good faith to get the mission accomplished. However, the other path to personal financial disaster could be a vendor suit for payment against the person who created the unauthorized commitment in his or her personal capacity, because the rules prohibited the government from ratifying the unauthorized commitment. If the vendor delivered goods and services as agreed, but the rules prohibit the government from paying the vendor for those goods and services, the vendor has a legal right to file a lawsuit against a government official in his or her personal capacity for full payment for those goods and services agreed to by that government official. Having to personally pay tens of thousands or hundreds of thousands of dollars for goods and services used by the government, plus interest, court costs, and attorney fees, would most likely be a personal financial disaster for most government employees.

Another reason it is important to avoid making an unauthorized commitment is the large amount of MEDCOM human resources required to process an unauthorized commitment action. The ratification process—the

Extract from Table 1-1, Chapter 751, *Army Regulation 690-700*.[25] Full table available at: http://www.apd.army.mil/cpol/ar690-700/ar690-700-751/penalty.html

Offense	Nature of Offense	First Offense	Second Offense	Third Offense	Remarks
14. Failure to observe written regulations, orders, rules, or procedures	a. Violation of administrative rules or regulations where safety to persons or property is not endangered.	Written reprimand to 1 day suspension	1-14 day suspension	5 day suspension to removal	
	b. Violation of administrative rules or regulations where safety to persons or property is endangered.	Written reprimand to removal	30 day suspension to removal	Removal	
	c. Violations of official security regulations. Action against National Security:				
	(1) Where restricted information is not compromised and breach is unintentional.	Written reprimand to 5 day suspension	1-14 day suspension	5 day suspension to removal	See *AR 380-67** and 5 USC §7532
	(2) Where restricted information is compromised and breach is unintentional.	Written reprimand to removal	30 day suspension to removal	Removal	
	(3) Deliberate violation.	30 day suspension to removal	Removal		

**Army Regulation 380-67: Personnel Security Program*, September 9, 1988

formal contracting procedures used to determine if the government can and should pay the vendor for the goods or services — is time-consuming.[1] Under current *MEDCOM Pamphlet 715-2*,[27] the vendor will almost always have to create and submit a special invoice. The vendor's usual invoice will almost never contain the special language required for the vendor to certify that the vendor delivered the goods or services to the government, and to certify that the vendor has not yet been paid for these goods or services. To avoid submitting a false claim,[28] the vendor must take the time to verify the facts, prepare the new special invoice, certify that invoice, and submit it to the government. In addition to obtaining a proper invoice, the person who made the unauthorized commitment must complete and sign a portion of MEDCOM Form 747-R to provide the facts as to what happened. The supervisor of the person must complete and sign another portion of that form to confirm the facts. The first colonel or civilian equivalent official in the person's supervisory chain must also complete and sign a portion of the MEDCOM Form 747-R. If the incident occurred at a military medical facility, the commanding officer of that medical facility must also complete and sign a portion of the form. All of this takes time, especially when you consider that individuals may be on leave or have changed duty stations. Completed documentation goes to the contracting officer for a decision or recommendation, depending on the amount of money involved. It takes time for the contracting officer to reach a decision or recommendation because he or she is usually busy awarding new contracts or administering existing contracts. If the contracting officer finds that the vendor should receive payment, the contracting office must wait for the budget office of the person who made the unauthorized commitment to provide a funding document with full funding certified for the proper fiscal year within which the unauthorized commitment occurred. The contracting officer must send the file to the legal office for review[29] to make sure the proposed payment is legal. It is common for a legal review to require a long time. It takes even more time if the file is legally insufficient and more documentation must be gathered. Once the file receives "legally sufficient" status, the contracting officer or a higher level contracting official signs the MEDCOM Form 747-R to approve the payment. The contracting officer must then issue a new contract vehicle to the vendor, or modify the existing contract to have a contract vehicle under which to make the payment. If the amount of the unauthorized commitment is $100,000 or more, the ratification process includes an in-person or video teleconference appearance by specific officials before the Head of the Contracting Activity (currently a dual-hatted responsibility of the Chief of Staff, MEDCOM) to explain the situation and remedial measures.[30] All of this processing time consumes taxpayers' money to pay many government employees to process unauthorized commitment forms, instead of paying them to do their "real" jobs.

Why Are Some Unauthorized Commitments Not Ratifiable?

The FAR requires legal review[29] of all proposed ratification actions because there are limitations on approving ratifications of unauthorized commitments. An unauthorized commitment cannot be legally ratified unless 7 specific conditions are satisfied.[31,32]

1. The vendor must have already provided the goods or services to the government, and the government must have already accepted them, or the government has otherwise obtained or will obtain a benefit from performance of the unauthorized commitment. If the vendor has not yet provided the goods or services, the unauthorized commitment cannot be legally ratified, regardless of the amount of expenses the vendor incurred in preparing to deliver the goods or services.

2. A government official must have proper authority to ratify an unauthorized commitment. Government officials do not have ratification authority based on their military rank or civil service grade. Only specified government officials with contracting authority have ratification authority. In addition, officials with ratification authority have limitations on the dollar amount they are authorized to ratify.[33] It is legally impermissible to split the unauthorized commitment for the purpose of avoiding an approval threshold.

3. The contract that results from the ratification action must have otherwise been proper if it had been originally made by an appropriate contracting officer. In other words, the unauthorized commitment cannot be properly ratified if contracting or fiscal law rules would have prohibited a contracting officer from entering into the original agreement on behalf of the government. One example: if contracting rules required the government to acquire the goods or services from a small business, but the unauthorized commitment is with a large business.

4. The contracting officer reviewing the unauthorized commitment must determine that the invoiced price is fair and reasonable. To make this determination, the contracting officer relies on market research,[18] personal knowledge, prices listed on existing contracts for the same or for similar goods or services, and other reasonable means. If the invoiced price is too high, the contracting officer has authority to negotiate a lower invoice price.

5. The contracting officer must recommend payment of the invoice, and legal counsel must concur in that recommendation. The contracting officer has a duty to gather the facts and comply with various contracting statutes, regulations, rules, and policies before making a recommendation. The legal counsel has a duty to review the file for legal sufficiency.

6. The correct amount and correct kind of government funds must have been available at the time the unauthorized commitment occurred, and those funds must be currently available to pay the invoiced amount. To know if the required funds were available and are still available, the contracting officer relies on a certification from a resource management official in the organization of the person who made the unauthorized commitment.

7. An unauthorized commitment cannot be legally ratified unless it complies with all other limitations prescribed under Army procedures. For example, local agency procedures could further restrict the dollar thresholds at which various contracting officials have authority to ratify the unauthorized commitment.

How to Reduce the Number of Unauthorized Commitments Within MEDCOM?

The number of unauthorized commitments may be reduced within MEDCOM by some or all of the following actions:

Education – This is the first step in knowing what comprises an unauthorized commitment, recognizing situations that are likely to result in an unauthorized commitment, and understanding why it is so important to avoid creating an unauthorized commitment. Without the education piece of the equation, government employees will not know what are unauthorized commitments, why they are highly undesirable, or how to avoid causing them to occur. Education is so important that all Office of the Surgeon General and MEDCOM employees are required to receive unauthorized commitment training as part of their annual ethics training.[34] The MEDCOM Health Care Acquisition Activity has created a video to facilitate this annual training and increase awareness of the need to avoid causing unauthorized commitments. Most unauthorized commitments occur because government employees are not aware that they lack authority to enter or change contracts on behalf of the government.

Attention to details – A lack of attention to details results in many unauthorized commitments. Too many government officials are paying inadequate attention to the terms and conditions of the existing contract, including the contract expiration date. As discussed earlier, ordering goods/services that are not included on the contract or continuing to order goods/services after the contract has expired will result in an unauthorized commitment. Paying closer attention to exactly what goods or services are covered by the contract and the available period for obtaining them will reduce the number of unauthorized commitments.

Planning – Some unauthorized commitments occur because of a lack of adequate planning to properly contract for the necessary goods or services before they are actually needed to accomplish the mission. Obviously, when individuals need something in their personal lives, they can make a quick trip to the store of their choice and purchase the item of their choice with personal funds. When the government needs something and will use appropriated funds to purchase the item, statute requires the government shopper to follow certain competition rules before obligating the government to part with taxpayers' money.[35] Depending on the amount of money involved, these competition rules require the government to give some degree of notice to the public so that interested sellers will have a fair opportunity to compete in the sale of their goods and services to the government. Compliance with the competition procedures takes time. This is why the customer sometimes assumes that a new contract is in place because the contracting office has had the requirement, the funding document, and the rest of the acquisition package for weeks, or even months. Advance planning is required to give the contracting office enough time to properly award a contract for the goods and services in routine situations. There are some sole-source, shortcut procedures for legitimate emergencies, but not for use when the customer creates the urgency by failing to perform adequate acquisition planning.[36]

Accountability – This is the final step in reducing the number of unauthorized commitments. Being held personally accountable for creating an unauthorized commitment should be an extra personal incentive for government employees to learn about unauthorized commitments and to avoid creating them. As can be easily imagined, increasing personal accountability by taking appropriate disciplinary actions against MEDCOM personnel who create unauthorized commitments is much more challenging when the offenders act solely for the benefit of the military mission and without any personal gain. To get the job done and the absence of personal gain are 2 consistent features of unauthorized commitments created in MEDCOM. While these 2 features may be admirable, they are totally irrelevant to the legal issue of whether an unauthorized commitment occurred.

Because health care costs tend to be relatively high, unauthorized commitments for health care goods and

services also tend to be relatively large. You may wonder how large is "relatively large." A review of MEDCOM Form 747-R submissions over the last decade determined that the most expensive unauthorized commitment in MEDCOM for that period occurred in 2006 in the amount of $656,483.40 for nucleic acid test kits and testing services for HIV-1, Hepatitis C, and the West Nile Virus (MEDCOM Form 747-R dated September 14, 2007). The single largest series of unauthorized commitments for the same goods and services during the last decade occurred from March 14, 2005 through July 6, 2005 when MEDCOM personnel made 365 unauthorized commitments totaling $646,168.89 to the same vendor for the same kind of goods and services for patient care of amputee patients of Operations Enduring Freedom/Iraqi Freedom (MEDCOM Form 747-R dated July 21, 2005). Although these goods and services were needed and were used to accomplish the mission in both situations, the unauthorized commitments could have been avoided by providing proper training, paying adequate attention to details, planning to meet the needs for future contract goods and services, and having a consistent history of holding individuals personally accountable for creating unauthorized commitments. There is seldom, if ever, a situation where an unauthorized commitment cannot be avoided. Customers should always contact their servicing contracting office when they have routine or urgent needs for goods or services that are not covered by an existing contract. The contracting officer has the authority to legally bind the government by creating a legal obligation for the government to pay for goods and services.

Conclusion

For all of the reasons presented in this article, when situations conducive to creating an unauthorized commitment occur, MEDCOM personnel must resist the temptation to take a chance on accomplishing the mission through unauthorized means. Instead of creating an unauthorized commitment to get the job done, MEDCOM personnel should contact their servicing contracting office, day or night, and acquire the goods and services through proper contracting means.

References

1. Federal Acquisition Regulation, Subchapter A, Part 1, Paragraph 1.602-3(a). https://www.acquisition.gov/far/loadmainre.html.
2. Defense Federal Acquisition Regulation Supplement. Washington, DC: US Dept of Defense; 1998 [2011 update]: Subpart 201.6. Available at: http://www.acq.osd.mil/dpap/dars/dfars/pdf/r20111004/201_6.pdf.
3. Army Federal Acquisition Regulation Supplement. Washington, DC: US Dept of the Army; 2001 (2010 update): Subsection 5101.602-3. Available at: http://farsite.hill.af.mil/reghtml/regs/other/afars/5101.htm#P225_28467.
4. Comptroller General of the United States. Unauthorized Commitments: An Abuse of Contracting Authority in the Department of Energy. Washington DC: US General Accounting Office; December 4, 1980. Report EMD-81-12. Available at: http://archive.gao.gov/f0202/114245.pdf. Accessed October 6, 2011.
5. Federal Acquisition Regulation, Subchapter A, Part 1, Paragraph 1.602-2(d). Available at: https://www.acquisition.gov/far/loadmainre.html.
6. Defense Federal Acquisition Regulation Supplement. Washington, DC: US Dept of Defense; 1998 [2011 update]: Paragraph 201.602-2(2). Available at: http://www.acq.osd.mil/dpap/dars/dfars/pdf/r20111004/201_6.pdf.
7. Deputy Secretary of Defense. Memorandum: Monitoring Contract Performance in Contracts for Services. Washington, DC: US Dept of Defense; August 22, 2008. Available at: https://acc.dau.mil/CommunityBrowser.aspx?id=278831. Accessed October 6, 2011.
8. *Army Regulation 70-13: Management and Oversight of Service Acquisitions.* Washington, DC: US Dept of the Army; July 30, 2010: paragraphs 2-2.f, 2-5.
9. Office of The Surgeon General. Memorandum: MEDCOM Policy on In-sourcing/Civilian Hiring Actions (CHA) and Service Contract Approval (SCA) Requests. Fort Sam Houston, TX: US Army Medical Command; February 26, 2010:2. OTSG/MEDCOM Policy Memo 10-007.
10. Federal Acquisition Regulation, Subchapter A, Part 1, Subparagraph 1.602-2(d)(1). Available at: https://www.acquisition.gov/far/loadmainre.html.
11. 31 USC §1342.
12. Comptroller General of the United States. Gifts of Goods and Services to the Government. Washington, DC: US General Accounting Office; March 4, 2002. Opinion B-289903. Available at: www.gao.gov/decisions/appro/289903.pdf. Accessed October 6, 2011.
13. Federal Acquisition Regulation, Subchapter A, Part 1, Paragraph 1.602-1(a). Available at: https://www.acquisition.gov/far/loadmainre.html.
14. Federal Acquisition Regulation, Subchapter A, Part 1, Paragraph 1.603-3(a). Available at: https://www.acquisition.gov/far/loadmainre.html.

15. Army Federal Acquisition Regulation Supplement. Washington, DC: US Dept of the Army; 2001 (2007 update): Subparagraph 5101.602-1(b)(2). Available at: http://farsite.hill.af.mil/reghtml/regs/other/afars/5101.htm#P225_28467.

16. Federal Acquisition Regulation, Subchapter C, Part 13, Subparagraph 13.303-3(a)(3). Available at: https://www.acquisition.gov/far/current/html/Subpart%2013_3.html#wp1092057.

17. Federal Acquisition Regulation, Subchapter C, Part 13, Subparagraph 13.303-3(a)(4). Available at: https://www.acquisition.gov/far/current/html/Subpart%2013_3.html#wp1092057.

18. Federal Acquisition Regulation, Subchapter B, Part 10. Available at: https://www.acquisition.gov/far/current/html/FARTOCP10.html#wp266706.

19. Army Federal Acquisition Regulation Supplement. Washington, DC: US Dept of the Army; 2001 (2010 update): Section 5110.002. Available at: http://farsite.hill.af.mil/reghtml/regs/other/afars/5110.htm#P3_34.

20. Federal Acquisition Regulation, Subchapter A, Part 1, Subparagraph 1.602-3(c)(6). Available at: https://www.acquisition.gov/far/loadmainre.html.

21. 31 USC §1502(a).

22. General Accounting Office. Principles of Federal Appropriations Law. Vol 1. 3rd ed. Washington DC: Office of the General Counsel, GAO; January 2004:5.11-5.15. Available at: http://www.gao.gov/special.pubs/d04261sp.pdf.

23. Federal Acquisition Regulation, Subchapter A, Part 1, Paragraph 1.602-1(b). Available at: https://www.acquisition.gov/far/loadmainre.html.

24. Federal Acquisition Regulation, Subchapter A, Part 1, Paragraph 1.602-3(b). Available at: https://www.acquisition.gov/far/loadmainre.html.

25. *Army Regulation 690-700: Personnel Relations and Services (General).* Washington, DC: US Dept of the Army; 1981. Available at: http://www.apd.army.mil/cpol/cpo.asp.

26. 64 Stat. 109, 10 USC, chap 47.

27. *MEDCOM Pamphlet 715-2: US Army Medical Command Request for Approval of Unauthorized Commitment Processing Ratifications.* Fort Sam Houston, Texas: Headquarters, US Army Medical Command; March 10, 2005.

28. 31 USC §3729.

29. Federal Acquisition Regulation, Subchapter A, Part 1, Subparagraph 1.602-3(c)(5). Available at: https://www.acquisition.gov/far/loadmainre.html.

30. Health Care Acquisition Activity Policy Letter 11-02: Policy and Procedures Regarding Unauthorized Commitments. Fort Sam Houston, Texas: Headquarters, US Army Medical Command; May 31, 2011:para 7g2.

31. Federal Acquisition Regulation, Subchapter A, Part 1, Paragraph 1.602-3(c). Available at: https://www.acquisition.gov/far/loadmainre.html.

32. Army Federal Acquisition Regulation Supplement. Washington, DC: US Dept of the Army; 2001 (2010 update): Paragraph 5101.602-3-90. Available at: http://farsite.hill.af.mil/reghtml/regs/other/afars/5101.htm#P225_28467.

33. Army Federal Acquisition Regulation Supplement. Washington, DC: US Dept of the Army; 2001 (2010 update): Paragraph 5101.602-3(b). Available at: http://farsite.hill.af.mil/reghtml/regs/other/afars/5101.htm#P225_28467.

34. Office of The Surgeon General. Memorandum: Policy and Procedures Regarding Unauthorized Commitment Training (UAT). Fort Sam Houston, Texas: US Army Medical Command; March 3, 2010. OTSG/MEDCOM Policy Memo 10-010.

35. 10 USC §2304(c).

36. Federal Acquisition Regulation, Subchapter B, Part 6, Section 6.301(c)(1). Available at: https://www.acquisition.gov/far/loadmainre.html. Available at: https://www.acquisition.gov/far/current/html/Subpart%206_3.html#wp1086841.

AUTHOR

Lt Col (Ret) Smith is a Contracts Law Attorney Advisor with the Office of the Staff Judge Advocate, US Army Medical Command, Fort Sam Houston, Texas.

Fiscal Law Overview

CPT Juan Lozada-Leoni, JAG, USA
Maurice A. Deaver, Jr, JD
MAJ Joseph B. Topinka, JAG, USA

Introduction

In these days of debt and budget issues facing our country, it is important for leaders, managers, and federal employees to have a solid understanding of fiscal law. Fiscal law is the body of law that governs the availability and use of federal funds. Fiscal law is derived from many sources, including the US Constitution, legislative appropriation acts and authorization acts passed by Congress and signed into law by the President, judicial court rulings, and Comptroller General Decisions pertaining to constitutional and congressional intent.

Congress

Only the US Congress has the ability to appropriate funds to be spent by the federal government, including the President. The constitutional basis for this power is rooted in a single sentence contained in the appropriation clause[1]:

> No money shall be drawn from the treasury, but in consequence of appropriation made by law.

Congress can decree, either in the appropriation itself or by separate statutory provisions, what is required to make the appropriation "legally available" for any expenditure. The power of the purse (or providing the money) belongs to Congress while the executive agencies, like the Department of Defense (DoD), carry out the laws with the money that Congress provides.

Judiciary

The judicial branch (the federal court system) also has a significant influence in fiscal law and the identified limitations on congressional spending power. Among these limitations are:

- The spending power must only be exercised in pursuit of the general welfare.
- The conditions imposed on the use of federal funds must be reasonably related to the articulated goals.
- The intent of Congress to impose conditions must be authoritative and unambiguous.
- The action in question must not be prohibited by the Constitution.

Unlike other areas where a leader, manager, or employee may have the latitude to do anything not expressly prohibited to complete the mission, fiscal law requires a person to have affirmative authority to use funds for a particular purpose. The US Supreme Court underscored this principle:

> The established rule is that the expenditure of public funds is proper only when authorized by Congress, not that public funds may be expended unless prohibited by Congress.[2]

In other words, the fact that funds are available and Congress has not expressly prohibited buying something does not constitute authority to buy it. Instead, a federal employee must be prepared to show how Congress has authorized and appropriated funds for the proposed expenditure.

Purpose and the Necessary Expense Rule

In 1809, Congress passed the Purpose Statute.[3] The text of the general provision of that statute is:

> Appropriations shall be applied only to the objects for which the appropriations were made except as otherwise provided by law.

Simply stated, the Purpose Statute says that public funds may be used only for the purpose or purposes for which they were appropriated. It prohibits charging authorized items to the wrong appropriation, and unauthorized items to any appropriation.

In 1954, the Comptroller General proposed a 3-part test[4] to determine whether expenditure is proper under the Purpose Statute:

1. The expenditure of an appropriation must be for a particular statutory purpose, or necessary and incident to proper execution of the general purpose of the appropriation.

2. The expenditure must not be prohibited by law.

3. The expenditure must not be otherwise provided for; it must not fall within the scope of some other appropriation.

In 1987, the Comptroller General determined that the first part of the test means that an expenditure is permissible if it is reasonably necessary to accomplish the objective of an appropriation, or will contribute materially to the accomplishment of that objective.[5] The Comptroller General developed this rule ("Necessary Expense Rule") because Congress is not required to specify every item of expenditure; it does not have the time, nor do we want it to specify every item. An agency wants and needs a certain amount of discretion to determine how it is going to accomplish its mission. The Necessary Expense Rule provides that flexibility. Unfortunately, what is "necessary" for one may seem like a luxury to another. That gap in perspective can get people into trouble.

The second part of the test is more straightforward. If the law specifically prohibits an expenditure, appropriated funds cannot be used for that particular purpose. Prohibitions may be found in appropriations acts, authorization acts, or other legislation. Since appropriations acts are made for a particular fiscal year, the presumption is that everything in the act applies only to the fiscal year covered. A provision contained in an annual appropriation act is not construed as permanent legislation unless the language used or the nature of the provision makes it clear that Congress intended it to be permanent.

The third part of the test relates to whether the expenditure is one that has been budgeted for or has typically been made from another more specific appropriation. In some cases, there may be 2 or more appropriations that are available for the expenditure, but that does not mean there is unfettered discretion.

An example of the third part of the test is the treatment of expenses and investments.[6] Expenses are those items that are consumed in operating and maintaining our agencies. Expenses are funded from operations and maintenance (O&M) accounts. Investments are those items acquired for their long-term use, eg, capital assets, such as equipment. Generally, procurement dollars are used for investments. Annual defense appropriations acts specifically allow investment purchases with a unit cost up to $250,000 to be funded with O&M appropriations. DoD has elected to do so in most cases. Thus, the rules on spending for these 2 types of items are[7]:

1. Procurement dollars must be used for purchase of an investment item that costs more than $250,000.

2. If the cost of an investment item is $250,000 or less, the purchaser must use O&M funds.

The funding test based on whether the unit cost of the investment exceeds $250,000 may sound simple, but it can become a problem in the purchase of computer systems. Today, we normally do not buy just one computer to be used by an individual as a word-processor. Rather, we usually buy computer systems: a network of computers with printers, internet access, and other peripherals. Because of this, we now have a test when it comes to purchases of computer (and other) systems: if the purchase is a system (a number of interconnected components designed to primarily function within the context of the whole), and the total cost of the system is over $250,000, the agency must use procurement dollars. If the purchase consists of a number of computers that will each operate independently, then there is no problem using O&M dollars for each piece, as long as each separate computer costs under $250,000.[8,9]

Representation funds are included within appropriations made available to the executive branch "for emergencies or extraordinary expenses."[10] Official representation funds are tightly regulated because of their limited availability and potential for abuse. Congress has long recognized that many agencies have a legitimate need for items that otherwise would be prohibited as entertainment, and has responded by making limited amounts available for official entertainment to those agencies that can justify the need. Entertainment appropriations originated from the need to permit officials of agencies whose activities involve substantial contact with foreign officials to reciprocate for courtesies extended to them by foreign officials. The Defense Department has its own authority. The Secretary of Defense, or the Secretary of a military department, within the limitations of appropriations made for that purpose, may use funds to "provide for any emergency or extraordinary expense which cannot be anticipated or classified."[10] When so provided in an appropriation, the official may spend the funds "for any purpose he determines to be proper."[10] Annual O&M appropriations include amounts for "emergencies and extraordinary expenses."[10]

Time

> Congress has the right to limit its appropriations to particular times as well as to particular objects, and when it has clearly done so, its will expressed in the law should be implicitly followed.[11]

The placing of time limits on the availability of appropriations is a primary means of congressional control.

By imposing a time limit, Congress reserves to itself the prerogative of periodically reviewing a given program or agency's activities. On the basis of time (duration), there are 3 types of appropriations: annual appropriations, multiyear appropriations, and no-year appropriations. These appropriations are either current, expired, or closed.

Annual appropriations are made for a specified fiscal year and are available for new obligations only during that fiscal year. Routine activities of the federal government are, for the most part, financed by annual appropriations. Personnel and O&M appropriations are annual appropriations. All appropriations are presumed to be annual appropriations unless the appropriation act expressly provides otherwise.

Multiple-year appropriations are available for new obligations for a definite period in excess of one fiscal year. Multiple-year appropriations are subject to the same principles applicable to annual appropriations. Multiple-year defense appropriations include: research, development, test and evaluation funds (2 years), procurement funds (3 years), and military construction funds (5 years).[6]

Current appropriations are monies for which availability for new obligations has not yet expired under the terms of the governing appropriations act. These funds may be obligated during the "present" period, but are subject to appropriation rules and laws.

Expired appropriations are monies for which availability has expired for new obligations, but which are available to adjust and liquidate previous obligations. All appropriations remain expired for 5 years.

Closed or cancelled appropriations are monies that are no longer available for any purpose. After 5 years, the agency must stop using these funds for any purpose. This means that the funds cannot be obligated, the funds cannot be used to adjust contracts, and they must become miscellaneous receipts to the US Treasury.

Bona Fide Needs Rule

Generally, the Bona Fide Needs Rule[11] states that a fiscal year appropriation may be obligated only to meet a legitimate, or bona fide, need arising in, or in some cases arising prior to but continuing to exist in, the fiscal year for which the appropriation was made. The rule does allow maintaining inventories at levels reasonably necessary to avoid disruption of operations, however, caution must be exercised so that the line between reasonable and excessive is not crossed.

Questions frequently arise regarding requirements that cover more than one fiscal year. In the typical situation, a contract is made in one fiscal year, with performance extending into part of the following year. In the case of service contracts, the Bona Fide Needs rule requires that contracts be performed only during the period of availability of the funds for new obligations. By statute,[12,13] however, Congress now also allows the use of funds, "for procurement of severable services for a period that begins in one fiscal year and ends in the next fiscal year if (without regard to any option to extend the period of the contract) the contract period does not exceed one year."[14] Severable services are those that are routine, repetitious services that can be divided by fiscal years because they involve a series of services such as janitorial work or grounds maintenance.

When it comes to delivery of supplies beyond the fiscal year, the normal answer is that supplies are a bona fide need of the period in which the supplies will be used. That is, current funds generally cannot be used to purchase items beyond the time when the current need for materials exists. However, there are lead time and stock level exceptions to the rule which allow obligation of funds in one year and delivery of supplies in the next fiscal year.

Amount

The separation of powers doctrine established by the Constitution allows Congress to make laws and provide money to implement them. This same doctrine gives the executive branch the authority to carry out the laws with funds that are provided by Congress. Under this system, Congress must have the final word as to how much money can be spent by a given agency or on a given program. Congress generally does this through the making of appropriations and by specifically designating, or "earmarking" parts of general appropriations as maximum and/or minimum amounts for particular purposes.

Antideficiency Act

In 1870, 1905, and 1906, Congress passed the laws collectively known as the Antideficiency Act[15] (ADA) as a result of the obligation and spending of federal funds by executive branch agencies beyond their own budget estimates. They did so in the expectation that Congress would eventually make deficiency appropriations to pay for the needs of the departments, even when such expenditures exceeded estimates.

The ADA prohibits involving the government in a contract or obligation for the payment of money before an

appropriation is made unless authorized by law. It prohibits over-obligating an appropriation. The ADA is the principal law designed to protect Congress' power of the purse. It is the only fiscal statute that includes both civil and criminal penalties for violation.

The ADA consists of 4 major provisions:

1. An officer or employee of the United States may not make or authorize an expenditure or obligation that exceeds an appropriation. In other words, the agency cannot spend more than has been appropriated by Congress.

2. An officer or employee of the United States may not make or authorize an expenditure or obligation in advance of an appropriation, unless authorized by law. In other words, money cannot be spent until it is legally available.

3. An officer or employee of the United States may not accept voluntary services or employ personal services exceeding those authorized by law, except to save human life or prevent property damage. In other words, the government cannot receive services without paying for them.

4. An officer or employee of the United States may not make or authorize an expenditure or obligation that exceeds an apportionment or reapportionment, or in excess of the amount specified in a formal subdivision of funds in accordance with agency regulations. In other words, more money cannot be spent than has been identified for a command in a funding authorization document.

Voluntary Services

Title 31 USC §1342 prohibits the acceptance of voluntary services without specific statutory authority. The purpose of the prohibition is to preclude situations which might generate future claims for compensation and which might exceed an agency's available funds. The Government Accountability Office has frequently distinguished the acceptance of voluntary services from the acceptance of "gratuitous services" where it is clearly established by written agreement or by statute that no compensation is due or expected. However, the ADA is not the only constraint on voluntary services. If the work to be performed would normally be performed by the agency with its own personnel and appropriated funds, acceptance of "free" services to perform the same work would impermissibly augment the agency's appropriation. That is why it was necessary that the services not be ones that the agency would normally perform or fund, or, in the alternative, that specific statutory authority permit acceptance of the services. Some exceptions to the voluntary services prohibition which have been recognized by statute over the years include voluntary services in support of alternative dispute resolution; student intern programs; and voluntary services in support of medical care, museums, natural resources programs, and family support activities. In addition, the statute itself allows the acceptance of voluntary services for bona fide emergencies involving protection of human life or property and which are not part of the agency's regular functions.

Violations of the Antideficiency Act

When an organization within the Army believes a potential ADA violation has occurred, it will submit an initial report, usually called a "flash report," to the Assistant Secretary of the Army for Financial Management and Comptroller (ASA(FM&C)). This initial report is informal and merely sets forth the factual circumstances that led to the belief that a potential ADA violation occurred. If ASA(FM&C) determines that a further factual inquiry is warranted, a preliminary ADA review is conducted.[16] The preliminary report resulting from this review is submitted to ASA(FM&C), which, in consultation with the Army Office of General Counsel (OGC), determines whether an actual ADA violation has occurred and a formal investigation is required.

Where a formal investigation is warranted, an ADA investigator is assigned. The investigator has been trained in conducting ADA investigations and typically is from outside the activity under investigation. The investigator's role is to determine the event that caused the potential violation, the responsible individual(s), actions required to correct the violations, and action(s) taken to ensure that a similar violation does not occur in the future.

The formal investigation is intended to provide the investigator with the necessary facts in order to write the formal report. Using the preliminary report as a starting point, the investigator will determine what information is missing or what areas require a more in-depth examination in order to accomplish that task. The investigator will interview those involved in the transaction and carefully review the documentary evidence in order to trace and document the transactions, decisions, and circumstances that may have led to the violation. During this time, careful coordination with ASA(FM&C), as well as with counsel, will help the investigator maintain focus and not be drawn into unproductive lines of inquiry.

The formal report is submitted to ASA(FM&C) which obtains Army OGC review and coordinates with other

involved functional areas as appropriate. The final report is then submitted to the Under Secretary of Defense (Comptroller), who then submits it to the President, through the Director of the Office of Management and Budget, the President of the Senate, the Speaker of the House of Representatives, and the Comptroller General.

If at any time during the investigation it appears that a criminal violation may have occurred, the investigation is stopped and the matter referred to the US Army Criminal Investigation Command (USACIDC). While rare, such referrals do occur. If the facts indicate knowing and willful violations, the case will be referred to the Department of Justice (or the appropriate United States Attorney) for possible prosecution.

The *DoD Financial Management Regulation* requires that the person or persons who are named as responsible for the violation be administratively disciplined.[17] This discipline is administered on a case-by-case basis, taking into account the nature and seriousness of the offense, and the record, experience, and degree and level of responsibility of the person or persons responsible. For civilian employees, administrative discipline may range from a written reprimand or admonishment to removal from office. Military personnel may be subject to appropriate administrative discipline or to action under the Uniform Code of Military Justice.[18]

Conclusion

Fiscal law is a complex subject resulting from years of interaction between laws, policies, and judicial opinions focusing on the authority of Congress to use taxpayer funds. This article has attempted to identify the main issues that every leader, manager, or employee should know. A firm understanding of these issues can ensure proper financial management, avoidance of violations of the Antideficiency Act,[15] and possible disciplinary actions. In the final analysis, fiscal law is about spending the citizens' money for the appropriate purpose, during the appropriate time, and in the appropriate amount.

References

1. US Const Art 1, §9.
2. *United States v MacCollom*, 426 US 317,321 (1976).
3. 31 USC §1301.
4. Secretary of Interior, 34 Comp Gen 195,196 (1954).
5. Internal Revenue Serv Fed Credit Union-Provision of Automatic Teller Machine, 66 Comp Gen 356,359 (1987).
6. *Department of Defense Financial Management Regulation 7000.14-R*. Vol 2A. Washington, DC: Office of the Under Secretary of Defense (Comptroller); October 2008: para 010201.B. Available at: http://comptroller.defense.gov/fmr/02a/02a_01.pdf.
7. *Department of Defense Financial Management Regulation 7000.14-R*. Vol 2A. Washington, DC: Office of the Under Secretary of Defense (Comptroller); October 2008: para 010201.D.2.b. Available at: http://comptroller.defense.gov/fmr/02a/02a_01.pdf.
8. Appendix A, Expense/Investment Criteria. In: DFAS-IN Manual 37-100-03. Indianapolis, IN: Defense Finance and Accounting Service; 2003: sec D.3.c, D.6.A. Available at: https://dfas4dod.dfas.mil/centers/dfasin/library/regs.htm.
9. *Department of Defense Financial Management Regulation 7000.14-R*. Vol 2A. Washington, DC: Office of the Under Secretary of Defense (Comptroller); October 2008: para 010201.D.1.f.
10. 10 USC §127(a).
11. Comptroller General Decision B-130815, Contracts-Continuing Supply Contracts-Appropriations-Obligation-Bona Fide Need. Washington, DC: US Government Accountability Office; September 3, 1957. Available at: http://redbook.gao.gov/7/fl0030231.php.
12. 10 USC §2410 a.
13. 41 USC §253l.
14. Comptroller General Decision B-317636, Severable Services Contracts. Washington, DC: Government Accountability Office; April 21, 2009. Available at: http://www.gao.gov/decisions/appro/317636.htm.
15. 31 USC §§1341-1342, 1517.
16. Preliminary Reviews of Potential Violations. In: *Department of Defense Financial Management Regulation 7000.14-R*. Vol 14. Washington, DC: US Dept of Defense; November 2010:chap 3. Available at: http://comptroller.defense.gov/fmr/14/14_03.pdf.
17. Antideficiency Act Violations. In: *Department of Defense Financial Management Regulation 7000.14-R*. Vol 14. Washington, DC: US Dept of Defense; November 2010:chap 9. Available at: http://comptroller.defense.gov/fmr/14/14_09.pdf.
18. 64 Stat 109, 10 USC, chap 47.

Authors

CPT Lozada-Leoni is Assistant Staff Judge Advocate, US Army Medical Command, Fort Sam Houston, Texas.

Mr Deaver is Chief, Contract and Fiscal Law Division, US Army Medical Command, Fort Sam Houston, Texas.

MAJ Topinka is Deputy Staff Judge Advocate, US Army Medical Command, Fort Sam Houston, Texas.

Transitioning Third Party Collections from Third World Processes

Jackey D. Nichols, JD

Introduction

The Department of Defense Third Party Collection Program (TPCP) has been around for 20 years now.[1,2] Authorized by Congress, it allows the military services to recoup expenses for medical care provided to nonactive-duty beneficiaries when they have other health insurance. Often this program is confused with the Medical Affirmative Claims Program,[3] which seeks to recover money from third parties (not necessarily an insurance company) when any beneficiary seeks medical care because of the "third person's" action. The TPCP seeks recovery for any medical care given to any nonactive-duty beneficiary any time they have other insurance. The monies collected from the insurance companies are directed to the medical treatment facility (MTF) providing the care.[4] This can be a tremendous windfall to the MTF, especially in these fiscally challenging times. The hospital commanders may use this money to enhance patient care in a variety of ways. The total amount recouped by the Army has averaged around $100 million a year. Although that may seem like a lot of money, many think there is an opportunity to collect much more, and with good reason. First of all, our billing software program, Third Party Outpatient Collection System (TPOCS) is woefully out-of-date and not user-friendly.[5] It is also scheduled be removed from service in October 2013. At that point, the TRICARE Management Activity will end financial support for TPOCS. The Army Medical Command (MEDCOM) Chief of Staff and the Patient Administrative Division, along with many others, see this as a great opportunity for change.

The Problem

Unlike the 1960s and 1970s, when the military was on the leading edge of technology, today we often lag behind our civilian counterparts. In the area of medical billing, we are very far behind. While the medical industry has moved totally to electronic revenue cycle (billing and bill paying), many of our MTFs are still preparing hand-written notations of TPOCS-generated bills, stuffing envelopes, mailing them, and then waiting for a check to arrive in the mail, often a 45 to 60 day process. Meanwhile, our civilian counterparts e-bill their patient's insurance companies and get verification of coverage and electronic fund transfer payments within a few days of the initial encounter.

With improved computer applications come improved and streamlined processes. The commercial sector's programs can scan and catch many errors in the billing process before the bill is sent to the insurance company. Additionally, initial responses to insurance company questions or rejections can be automatically embedded in the program.

Billing the insurance company does not mean it will automatically pay. For years the MEDCOM legal community has reviewed the MTF-generated medical bills disputed by insurance companies. This normally occurs after the MTF's billing office has unsuccessfully tried to collect for 120 to 180 days.[6] The assumption is that the insurance company is legally obligated to pay, but refuses to do so. Unfortunately, this is not always the case. Often we see "disputed bills" which are based on an MTF clerical error, a program upgrade or change at an insurance company (which causes their computer not to recognize the Army as a proper payee), or other issues related to the fact we introduce hand-generated bills into a totally automated process. As a result, our "legal intervention" is not legal-oriented at all, it consists of performing the research and making phone calls for which the billing personnel do not have time. There are some existing legal issues that our legal counsel needs to address, but often in our current manual process those issues are buried under so many piles of paper that we cannot find them. This is all the more reason for change.

The Future

The MEDCOM leadership has authorized each of the 5 regional commands to come up with their own billing solution* to replace the TPOCS billing system.[7] The commands are expected to have their solution identified by the end of 2011. This short and tight timeline is driven by the rapidly approaching date when TPOCS will no longer be around to process our medical bills. As

*The policy supporting this action is currently under review within MEDCOM. As of this writing, there has been no official determination to change this policy.

such, it appears most regions will rely on a commercial vendor to supply the "software solution" to the demise of TPOCS.

Conclusion

Once MEDCOM regional staffs are manned with a Uniform Business Office* and legal counsel, we expect they will provide regional oversight over all the MTFs in their entire region's TPCP process.[8] Improved automation will allow trend analysis and identification of individual insurance company problems, in addition to a markedly shorter revenue cycle. In the end, our dedicated Uniform Business Office billing personnel will be able to join the rest of the country's medical billers with the latest and greatest tools instead of stubby pencils and legal tablets, thereby moving the Third Party Collection Program out of the third-world processes and into the 21st century. The result of this effort will put more dollars in the coffers of those MTFs whose commanders embrace, enforce, and support the Third Party Collection Program.

*The Uniform Business Office consolidates collection processing, analysis, and reporting of accounting related activities under one umbrella. Third party collections program, medical service accounts, and medical affirmative claims are the 3 services provided by the office.

References

1. Health Care Services Incurred on Behalf of Covered Beneficiaries: Collection From Third-Party Payers, 10 USC §1095.
2. Medical And Dental Care, Procedures for Charging Fees for Care Provided to Civilians; Retention and Use of Fees Collected, 10 USC §1079b.
3. Third Party Liability for Hospital and Medical Care, Recovery by United States, 42 USC §§2651-2653.
4. Collection from Third Party Payers of Reasonable Charges for Healthcare Services, 32 CFR §220, (2010).
5. Office of The Surgeon General. Memorandum: Third Party Collection Program (TPCP) Legal Follow-up Procedures. Fort Sam Houston, TX: US Army Medical Command; October 7, 2009. OTSG-MEDCOM Policy Memo 09-081.
6. *Department of Defense 6010-15-M: Medical Treatment Facility Uniform Business Office (UBO) Manual*. Washington, DC: US Dept of Defense; April 7, 2008. Available at: http://www.dtic.mil/whs/directives/corres/pdf/601015m.pdf. Accessed November 15, 2011.
7. Office of The Surgeon General. Memorandum: Regional Uniform Business Office (UBO) Implementation. Fort Sam Houston, TX: US Army Medical Command; July 28, 2010. OTSG-MEDCOM Policy Memo 10-051.
8. Office of The Surgeon General. Memorandum: Third Party Collection Program (TPCP) Procedures. Fort Sam Houston, TX: US Army Medical Command; October 19, 2011. OTSG-MEDCOM Policy Memo 11-087.

Author

Mr Nichols is Supervisor Attorney Claims Section, Office of the Staff Judge Advocate, US Army Medical Command, Fort Sam Houston, Texas.

Expanding Use of Technology Transfer Mechanisms Within the Army's Medical Treatment Facilities

Robert L. Charles, JD

Introduction and Background

Technology transfer involves sharing resources (eg, expertise, materials, personnel, or money) between entities to attempt technology discovery and/or improvement. The ultimate goal of technology transfer for US government laboratories is to meet their internal research and development missions. We are involved in technology transfer because we recognize the multidisciplinary requirements and complexity of today's scientific, engineering, regulatory, and commercial endeavors, and the inherent limitations of any one organization, including the US Government, to do it all.

Because of the importance of technology transfer to technological innovation and national economic well-being,[1] Congress has made it national policy that technology transfer is a responsibility of federal laboratory science and engineering professionals.[2] A great deal of technology transfer takes place informally, through scientific publications and meetings.[3]

Army medical centers have been involved in technology transfer activities as part of the Clinical Investigation Program (CIP) for many years. The Clinical Investigation Regulatory Office (CIRO), which oversees the CIP across the US Army Medical Command (MEDCOM), was designated a "federal laboratory" in the early 1990s. As a federal laboratory, the Director, CIRO was delegated authority to enter into technology transfer agreements. For internal policy reasons, CIRO, which was headquartered at Fort Sam Houston until 2010, chose to limit its exercise of technology transfer authority to research activities needing protocols within the CIP.

In October 2010, CIRO came under the command and control of US Army Medical Research and Materiel Command (USAMRMC) and relocated to Fort Detrick, Maryland. CIRO now operates as a USAMRMC laboratory for technology transfer purposes and has expanded its exercise of authority to include all technology transfer activities within the medical treatment facilities (MTFs).

The USAMRMC Office of the Staff Judge Advocate (OSJA) supervises and manages the administration, control, and coordination of all patent, copyright, and trademark activities within MEDCOM, as well as serving as the technology transfer legal technical channel supervisor for all MEDCOM units. Intellectual property licensing activities are carried out by the USAMRMC Office of Research and Technology Applications, which is located with and integrated into the OSJA.

Historically, researchers at MTFs who wished to enter into non-CIP cooperative research and development agreements and/or material transfer agreements ended up getting advice and assistance from the USAMRMC OSJA, because their local legal offices had no experience with these non-CIP agreements. In addition, all such agreements had to be staffed to and signed by The Surgeon General (TSG), because TSG was the only other designated authority or "laboratory" available. This greatly complicated and delayed the process. CIRO's role was expanded to include all technology transfer actions within the MTFs to encourage more non-CIP research collaborations by simplifying and speeding up the process of entering into appropriate agreements.

The purpose of this article is to encourage additional non-CIP technology transfer activities within Army MTFs. It briefly explains the 3 principal technology transfer mechanisms available to MTFs and their inventors/researchers for collaborations with nonfederal parties. Following that, examples of non-CIP collaborations are provided.

The Legal Mechanisms

The 3 principal mechanisms for research collaborations are called cooperative research and development agreements (CRADAs), material transfer agreements (MTAs), and nondisclosure agreements (NDAs). Authority for federal laboratories[4,5] to enter into CRADAs, MTAs, and NDAs comes from the same statutory source, the Federal Technology Transfer Act of 1986 (FTTA),[6] which

left it to the various federal agencies doing research and development (R&D) to designate those laboratories. While that statute speaks exclusively of CRADAs, it is important to recognize that MTAs and NDAs are just different types of CRADAs.

The fact that the CRADA law allows for a wide variety of collaborative R&D contractual arrangements often proves to be a mental hurdle to those only familiar with the more highly regulated and structured nature of government procurement practice under the Federal Acquisition Regulation (FAR).[7] However, Congress intended this new authority to be used by federal laboratories in a more flexible, industry-friendly way than is typical for government procurement practices. The FTTA

> authorizes a broad range of cooperative research and development arrangements where there is a mutual interest between the laboratory mission and other levels of government or private sector organizations.[8]

To understand how NDAs fit under CRADA authority, one need only look through the statutory definition of a CRADA.[9] Under that definition, a CRADA is any agreement between appropriate parties to share authorized resources "…*toward the conduct of* specified research and development *efforts*…" (emphasis added). The definition can be reasonably and fairly read to subsume both agreements for the precollaboration provision of resources in anticipation of a possible R&D collaboration agreement, as well as R&D collaboration agreements themselves. An NDA is an agreement *toward* (ie, in the direction of, in anticipation of) the conduct of specified research and development efforts. This interpretation would not be reasonable had Congress more narrowly defined a CRADA to be "an agreement…*to conduct* specified research and development."

Essentially, CRADAs, MTAs, and NDAs are research and development agreements that are distinguished from each other by the extent and nature of the collaborative activities that take place under them. They represent a spectrum of collaboration, and the line between where one mechanism stops and the next starts can easily get blurred.

As an example of this blurring, typically, MTAs and CRADAs have nondisclosure requirements written within them. As another example, a typical agency boilerplate may be labeled, "CRADA for Material Transfer."

Legal counsel should recognize that potential collaborators may insist on the use of their own templates, which will not use the labels that the government normally uses, but are otherwise quite legally acceptable. From the legal viewpoint, we are concerned that the intended activities fit within the legal bounds authorized, rather than what any particular document is called.

As a laboratory of USAMRMC, CIRO follows the policies and procedures set forth in *USAMRMC Regulation 70-57*.[10] Per that regulation, for those agreements that utilize its attached formats/templates, no further legal review is required by the USAMRMC OSJA before signature by the Director, CIRO. In practice, CIRO personnel frequently seek guidance and review as proposed agreements are being negotiated. While legal review at the USAMRMC level may not always be required, local policy at the MTF may require local JAG review.

Cooperative Research And Development Agreements

CRADAs are non–FAR-based R&D collaboration contracts that permit a wide variety of resource exchanges between the parties. To carry out the collaborations, federal laboratories may provide "personnel, services, facilities, equipment, intellectual property, or other resources with or without reimbursement (but not funds to nonfederal parties)." The nonfederal parties may provide the federal laboratories any of those resources, plus funds. (Since we are looking at non-CIP collaborations, the provision of *Army Regulation 40-38*[11] that prohibits the use of funds or other revenues provided by business groups operating for profit does not apply. The laboratories may accept, retain, and use these extramural resources without violating the Augmentation of Appropriations prohibitions.*)

Unlike FAR-based contracts or federal grants, no competition requirement exists for laboratories in choosing their CRADA collaborators. For researchers at MTFs contemplating collaborations with nonfederal parties, significant interrelated consequences flow from this:

- First, MTF researchers may and must communicate with potential collaborating parties to discuss possible collaborations.

- Second, the MTF researcher should ensure that he/she does not share any government-owned proprietary information, nor receive any of the

*Augmentation is a concept of appropriations law that is derived from statute, specifically 31 USC §3302(b) (miscellaneous receipts rule) and 31 USC §1301(a) (restricting the use of appropriated funds to their intended purposes). The Government Accountability Office has held that an agency may not augment its appropriations from outside sources without specific statutory authority. The objective of the rule against augmentation of appropriations is to prevent a government agency from undercutting the Congressional power of the purse by exceeding the amount Congress has appropriated for that activity.

collaborator's proprietary information, unless and until an NDA has been entered.

- Third, if the MTF researcher has an idea for an invention or has been working on a prototype for an invention, the researcher is required to take steps to help the Army protect any potential intellectual property,[12] and should do so before sharing any specific information with the non-federal party. That is most easily done by filing an invention disclosure.* As protection of intellectual property rights is often an essential element to successful commercialization, those rights are addressed in the CRADA statute and become an important part of the negotiations and agreement between the parties.[13]

Material Transfer Agreements

As noted earlier, an MTA (also known as a CRADA for material transfer) is authorized under the same legislation as a CRADA. As stipulated by *USAMRMC Regulation 70-57,*[10] it should:

> be used when (1) a party will be providing equipment, materiel, and/or information to the other party; (2) the receiving party will screen, test, evaluate, or otherwise use the equipment, material, and/or information, and may be required to provide a report of results to the party providing the equipment, material, and/or information; and (3) the parties are not bound to further collaboration unless another document providing for such collaboration is executed. Under a CRADA for Material Transfer, a USAMRMC laboratory may receive reimbursement for the cost of the material(s) it provides, or for the costs associated with screening, testing, or evaluating the equipment, material, and/or information and providing a report of results.[10(p3)]

Similar to CRADAs, MTAs for activities within MTFs must be signed by the Director, CIRO.

Nondisclosure Agreements

A common misunderstanding is that the government may not protect its own proprietary or commercial information from disclosure under a Freedom of Information Act (5 USC §552) request. In fact, federal courts considering the issue have provided very broad protection to such information where there are concerns that requiring disclosure would act to undermine the ability of federal laboratories to successfully perform their technology transfer mandate.[14,15]

In the private sector, NDAs, also known as confidential disclosure agreements, are commonly used as a prelude to entering into more substantive business discussions about a potential agreement. They are intended as a legal means to protect from public disclosure proprietary information such as recent unpublished research results; filed, but not issued patent applications; and confidential commercial information, which are provided to the potential partner for limited review, inspection, or preliminary testing. NDAs help each party evaluate what the other can bring to the negotiation table or lab bench that may be of interest. The promises made in an NDA serve to induce parties to share information.

In the realm of federal technology transfer, the issue of NDAs commonly arises as a prelude to negotiations for a potential CRADA. Each party wants some written assurance that the information it plans to share with the other party will not be improperly divulged. Federal law prohibits and makes it a crime for a federal employee to wrongly disclose a collaborator's or potential collaborator's proprietary information.[16-19]

To address the need/desire of potential collaborators for assurance of confidentiality of their proprietary information before sharing it with government personnel, government counsel has drafted some boilerplate "acknowledgement of nondisclosure obligations," which are available in the *US Army Medical Command Legal Deskbook* (2008). These documents fall short of the creation of any contractual obligation on the government's part, and have the added benefit of allowing signature by the specific science and engineering personnel who are given access to the relevant information.

Individual government employees/researchers do not have authority to bind the government and, therefore, should not sign NDAs on behalf of a government entity. However, as NDAs are a type of CRADA, the Director, CIRO, can and does routinely sign these documents on behalf of MTF researchers. Government employees may acknowledge by signature having read and understood such documents.

Examples of Non-CIP Collaborations

A Better Wheelchair

MAJ Art Yeager is an occupational therapist currently assigned to Reynolds Army Community Hospital. While working with patients who used manual (nonelectric) wheelchairs, he saw 2 practical problems, both caused by gravity. First, when his patients were going up hills, which takes considerable strength, current wheelchair technology made it very difficult and awkward to stop without rolling or falling backwards. Second, when those

*Forms available at: https://technologytransfer.amedd.army.mil/ [Note: use the "For Our Inventors" button]

same patients were going downhill, current technology did little to assist the patients to adjust for the force of gravity, ie, slow the wheelchair to the desired speed.

MAJ Yeager, a former aviator, conceived 2 ideas to address these practical problems: first, a gravity-reacting antirollback brake, then a gravity-reacting automatic speed pacer. Working with patent counsel in the Legal Office at USAMRMC, MAJ Yeager's conceptions were filed as patent applications. Needing a private sector partner to further develop these technologies for potential commercialization, MAJ Yeager reached out under an NDA to Accessible Designs, Inc (ADI), a San Antonio-based designer and manufacturer of cutting-edge products for people with disabilities.

Working with the USAMRMC Office of Research and Technology Applications, the Army and ADI established a CRADA to design, engineer, and fabricate a prototype wheelchair that incorporates MAJ Yeager's technologies into ADI's own patented technology. The CRADA provides for ADI to seek further research and development funding, as well as to coordinate with outside organizations for prototype testing and evaluation. MAJ Yeager will continue to participate with ADI in the development of these important technologies.

Grants from Nonfederal Entities

Many for-profit and nonprofit entities provide grants for medical research activities that fall outside the scope of the CIP. These grants are contractual agreements that generally fit within the legal definition of a CRADA: the grantor organization provides the federal laboratory (in this case, the MTF as part of CIRO) money in exchange for the laboratory's agreement to carry out the specified research and provide a written report to the grantor and/or prepare a publication of the results. Personnel at MTFs have applied for and received such grants to perform research at their facilities. (Note: researchers should obtain approval from local authorities before submitting the grant application to be sure that the MTF will support the research should the grant be awarded.)

CIRO can sign the award documents on behalf of the Army. The relevant MTF's resource management office can accept the grant funds, which can then be spent, for example, to buy the supplies or pay the contractors to carry out the work, as needed.

Practice Makes Better

The AMEDD is at the forefront of national efforts to create simulators to provide its healthcare providers more and better opportunities to train in medical procedures before undertaking the procedures on patients, and to sharpen the skills of those already on the front lines of care. One example is the Mobile Obstetric Emergencies Simulator (MOES) system developed by LTC Shad Deering et al at the Madigan Army Medical Center. The system, along with its NOELLE simulator (Gaumard Scientific, Miami, FL), has been exclusively licensed by the Army to Gaumard. Practicing with MOES builds team and technical competency for obstetric emergencies. The need for such simulators throughout the medical community is obvious. Efforts by MTFs and their associated simulation centers to collaborate with nonfederal hospitals, academia, and the private sector to further develop such technologies is in everyone's best interest. NDAs and CRADAs are the mechanisms of choice to develop such relationships.

Useful USAMRMC Points of Contact

CIRO: 301-619-3069

Patent Counsel and for other IP issues:
301-619-7808

Office of Research and Technology Applications:
301-619-6975
https://technologytransfer.amedd.army.mil

Technology Transfer legal counsel:
301-619-7663

References

1. 15 USC §3701.
2. 15 USC §3710(a)(2).
3. Charles RL. Federal technology transfer: CRADAs, PLAs, and other mechanisms. *US Army Medical Command Legal Deskbook*. Fort Sam Houston, TX: US Army Medical Command; 2008.
4. 15 USC §3710a(d)(2).
5. *Department of Defense Instruction 5535.8: DoD Technology Transfer (T2) Program*. Washington, DC: US Dept of Defense; May 14, 1999.
6. Federal Technology Transfer Act, 15 USC §3710a (2004).
7. Federal Acquisition Regulation, 48 USC Part 27.3 (2004).
8. *Senate Report No. 383*, 99th Cong, 2nd Sess (1986).
9. 5 USC §3710a(d)(1).
10. *USAMRMC Regulation 70-57: Military Research, Development, and Acquisition; Military-Civilian Technology Transfer*. Fort Detrick, MD: US Army Medical Research and Materiel Command; February 8, 2007.

11. *Army Regulation 40-38: Clinical Investigation Program*. Washington, DC: US Dept of the Army; September 1, 1989: para 3-6(a)(8).

12. *Army Regulation 27-60: Intellectual Property*. Washington, DC: US Dept of the Army; June 1, 1993: para 2-5a.

13. 15 USC §3710a(b)(1)-(3)(D).

14. *Delorme Publishing Company, Inc v NOAA*, 917 F Supp 867 (D Maine 1996).

15. *Public Citizen Health Research Group v NIH and Johnson and Johnson*, 209 F Supp 2d 37 (D DC 2002).

16. Freedom of Information Act, 5 USC §552(b)(4).

17. Executive Order 12600, Predisclosure Notification Procedures for Confidential Commercial Information, 52 *Federal Register* 23781 (1987). Available at:http://www.archives.gov/federal-register/codification/executive-order/12600.html. Accessed November 1, 2011.

18. Trade Secrets Act, 18 USC §1905 et seq.

19. Economic Espionage Act of 1966, 18 USC §1831.

AUTHOR

Mr Charles is Chief, Medical Research Branch, Office of the Staff Judge Advocate, US Army Medical Research and Materiel Command, Fort Detrick, Maryland.

Social Media: Some Things to Consider Before Creating an Online Presence

CPT Adam Jonasz, JAG, USA

Introduction

One-way communication between military commands and their Soldiers, Family members, civilian employees, and the public is going the way of the VHS, the floppy disk, and the dinosaur. Command policies, safety briefs, training calendars, and traditional ways of conveying orders at daily formations, on bulletin boards, or through word of mouth is taking a back seat to more modern methods and mediums of communication. Soldiers, Family members, employees, and the public no longer just listen, and commands and commanders no longer just speak and expect to be heard; they now engage in a conversation. This conversation is not always a physical face-to-face exchange, but an increasingly virtual one over the internet through the use of "social media" forums like Facebook, Twitter, YouTube, and Flickr.

What is said on the parade ground is now posted on Facebook. What Soldiers and/or units do during training, in the field, or in the combat zone is now broadcast on YouTube. What Soldiers discussed at the chow hall or in the barracks now appears on Twitter. Comments are now memorialized on the internet, through posts, video, or audio, and all of it available to millions of users with the simple click of a mouse. Social media can be about engaging in conversation, changing the conversation, directing the conversation, listening to the conversation, responding to the conversation, starting the conversation, or just getting the word out.

Historically, commanders at all levels were able to determine the parameters of the relationship they had with their Soldiers and the Soldiers had with them. Now, because of the prevalence of social media and the Army's increasing use and reliance on it, Soldiers, Families, Army civilian employees, and the public are the ones who increasingly define how the unit or commander is perceived and the direction and course of their relationship.

Purpose

This article is an overview of social media and some of the many benefits, concerns, and legal issues to consider when deciding whether or not to create and maintain a government external official presence (EOP) within the social media world. In addition, it is the intent of this article to provide commanders, units, and organizations within the Army Medical Command (MEDCOM) tips on how to successfully ensure editorial control of your EOP. This article was not written with the intent of being an analysis of MEDCOM social media sites or as an in-depth report on the legal authority, laws, and guidance covering the use of social media. For guidance or details on how to set up a social media site, see *The Army Social Media Handbook 2011*[1] which contains guidance, many tips, and contact information to assist organizations with the implementation and maintenance of a social media page.

Overview

In order to fully grasp the idea of social media, it may help to parse the words. Media is the plural form of the word "medium," which in this context is a means of communication, such as radio, newspaper, the internet, or television that reach and influence people widely. Social media is therefore a social means of communication, in a 2-way environment as opposed to a one-way format. In the context of the internet: a website that does not simply present information, but allows for interaction while presenting information. This interaction can be as simple as asking for feedback or letting you vote on an issue, or it can be as complex as target advertising based on websites you previously visited or things purchased in the past.

Social media is a very broad term and, depending upon with whom you are speaking and for what purpose they engage in or use social media platforms, you may get a variety of definitions. For our purposes, however, social media usually refers to a large range of websites that allow online communications in which individuals shift fluidly and flexibly between the roles of audience and author. Social media can also be defined as the content created and shared by individuals on the web using freely available websites that allow users to create and post their images, video, and text information, and then share that with either the entire internet or just a select group, depending on security or privacy settings.

The Army's Use of Social Media

The Army has long recognized the extensive use of the internet and especially social media websites by society at large, but specifically Soldiers, Family members, potential recruits, and Army civilian employees. The Army presence in the social internet environment began in 2007 and has been increasing rapidly ever since, with EOPs being sponsored/maintained by general officers and commanders at all levels, including organizations down to platoon-size elements.[2]

The Army quickly recognized the importance of the fact that social media provides users the capability to rapidly and efficiently communicate with large numbers of people over a 2-way communications platform using multiple media such as audio, video, photo, and text. By using existing software platforms or websites such as Twitter, Flickr, YouTube, and Facebook, the Army can connect and interact with Soldiers, Families, Army civilians, and the public with little or no monetary investment. Most importantly, the Army is attempting to make use of social media platforms to affirmatively communicate the Army message to the public, Soldiers, Families, Army civilians, and people all over the world. The Army is taking control of the message, creating the conversation and listening to what is being said. As of October 2010, there were 1,076 registered EOP sites as follows: Facebook 713, Flickr 130, Twitter 162, and 71 on YouTube.[2(p3)]

On February 25, 2010, Department of Defense (DoD) Directive-Type Memorandum (DTM) 09-026[3] established DoD policy and assigned responsibilities for responsible and effective use of internet-based capabilities, including social networking services. The DTM also provided basic guidelines for military use of social media, and the use of an EOP. The policy went further by clearly stating:

> This policy recognizes that Internet-based capabilities are integral to operations across the Department of Defense.[3(p1)]

The DTM defined internet-based capabilities as:

> All publicly accessible information capabilities and applications available across the internet in locations not owned, operated, or controlled by the Department of Defense or the Federal Government. Internet based capabilities include collaborative tools such as SNS, social media, user generated content, social software, e-mail, instant messaging, and discussion forums (eg, YouTube, Facebook, MySpace, Twitter, Google Apps).[3(p1)]

It also defined external official presence as:

> Official public affairs activities conducted on non-DoD sites on the internet (eg, Combatant Commands on Facebook, Chairman of the Joint Chiefs of Staff on Twitter.)[3(p1)]

In addition, the Memorandum presented DoD policy as follows[3(p2)]:

> The NIPERNET* shall be configured to provide access to Internet-based capabilities across all DoD Components.
>
> Commanders at all levels and heads of DoD Components will continue to defend against malicious activity affecting DoD networks (eg, distributed denial of service attacks intrusions) and take immediate commensurate actions, as required to safeguard missions (eg, temporarily limiting access to the internet to preserve operations security or to address bandwidth constraints.
>
> Commanders at all levels and heads of DoD Components will continue to deny access to sites with prohibited content and to prohibit users from engaging in prohibited activity via social media sites (eg, pornography, gambling, hate-crime related activities).
>
> All use of internet-based capabilities shall comply with paragraph 2-301 of Chapter 2 of the Joint Ethics regulation…and the guidelines set forth in Attachment 2 [to the DTM].

On March 25, 2010, the Chief Information Officer of the Army issued a memorandum[4] which addressed establishing, maintaining, and reviewing social media sites, as well as operations security (OPSEC) awareness and training requirements.

On October 21, 2010, the Secretary of the Army issued a memorandum[5] establishing the delegation of authority for EOPs to the commanders of all Army commands, who may then redelegate the authority to subordinate commands, direct supporting units, and field operating agencies.

On March 1, 2011, the Deputy Secretary of Defense reauthorized Attachment 3 (Responsibilities) of DTM 09-026,[3] extending the DTM through January 2012 and outlining how the NIPERNET should be configured to allow access to Internet-based capabilities throughout the DoD components.

DoD and Department of the Army Regulatory and Policy Guidance on Social Media

At this point there are several regulations and directives that currently direct the Army's use of social media. According to the *Army Social Media Handbook 2011*,[1] the

*Nonsecure internet protocol router network

Assistant Secretary of Defense is currently working on an all-encompassing policy. Until that policy is issued, guidance is found in DTM 09-026[3]; a June 17, 2009 memorandum from the Office of the General Counsel of the Army[7] which recommended training for creators and maintainers of websites, content review for OPSEC, and other prohibited information and use disclaimers; and the following publications:

- *Army Regulation 25-1.*[6] Along with the Chief Information Officer (CIO)/G-6, the Chief of Public Affairs oversees and controls content on Army public websites. Only official Army information that is releasable and of value to the public may be released on these sites. Commanders and organization heads are to ensure that the Public Affairs Office and other appropriate designees review and clear web content and format before the content is posted on the Internet. The primary responsibility of the CIO/G6 is managing the Army's network, to include providing the appropriate amount of bandwidth to allow access to internet-based capabilities across the Army networks per DoD policy.

- *DA Pamphlet 25-1-1.*[8] Each Army organization that establishes a public website must have a clearly defined purpose and website plan that supports the organization's mission. All individuals appointed as webmasters or site maintainers, reviewers, and content managers must complete training and certification, as necessary, appropriate to the duties assigned to them.

- *Army Regulation 530-1.*[9] The regulation provides guidance to all Army Soldiers, civilians, and contractors to eliminate, reduce, or conceal indicators that could result in releasing critical and sensitive information. The regulation addresses the review requirements for releasing Army or government information through all types of media.

- *Army Regulation 360-1.*[10] Any official information intended for public release that pertains to military matters, national security issues, or subjects of significant concern to DoD must be cleared by appropriate security review and public affairs offices before release. This includes materials placed on the internet or released via similar electronic media. The Office of Public Affairs has the authority to release information about the Army as a whole; commanders below Headquarters, Department of the Army level can release information wholly within the mission and scope of their respective commands.

The Office of the Chief of Public Affairs (OCPA) has produced 3 documents to assist commands and organizations with their social media programs. On February 12, 2010, it released a Social Media Best Practices (Tactics, Techniques and Procedures) slideshow that outlined basic guidelines for public affairs social media strategies. On November 1, 2010, OCPA issued a memorandum titled "Standardizing Official US Army External Official Presences,"[11] in an attempt to standardize Army-wide EOPs. The OCPA published *The Army Social Media Handbook*[1] in January 2011, followed by a revised, updated version in August 2011.

As OCPA is also responsible for maintaining the Army social media registry, it apparently has taken the lead on developing policy and monitoring how social media is used in the Army. OCPA has also taken center stage in the effort to educate commanders and agencies on the use of social media and its potential pitfalls.

To establish a social media site, units/commanders must, at a minimum, consult the Secretary of the Army Memorandum: "Delegation of Authority – Approval of External Official Presences,"[12] and Attachment 2 (Guidelines For Use Of Internet-Based Capabilities) to DTM 09-026.[3] Units/organizations must receive command approval before establishing an EOP and it must be approved by the release authority (commanding officer or public affairs) before it can be registered (an EOP must be registered). When submitted for approval and registration an EOP plan must contain the following: a point of contact with a valid military (.mil) email address, a URL to an official Army website, a posted disclaimer which identifies the page as an "official" Army social media presence and disclaims any endorsement. The site must be clearly identified as official, unlocked and open to the public, use official seals, logos, be monitored and evaluated by DoD components for compliance with security requirements, and ensure info posted is accurate and relevant and does not provide personally identifiable information or information not approved for release. It is recommended that anyone considering establishing an EOP consult their public affairs office for advice and guidance. Public affairs plays a prominent role in the Army's use of social media and are constantly updating and implementing new ways to assist in the execution of Army regulations and DoD guidance.

LEGAL OVERVIEW

An overview of the legal principles that cover government sponsored social media include but are not limited to the following: the 1st Amendment to the US Constitution, copyright laws, the The Privacy Act of 1974,[13] the

Federal Open Records Act (Federal Records Act of 1950, 44 USC §§29,31,33), and defamation. Federal agency public web pages are required to comply with the provisions of section 508 of the Rehabilitation Act Amendments of 1998 (29 USC §794d). Public web pages must be equally accessible to disabled and nondisabled federal employees and members of the public. These legal issues should not inhibit or deter any organization from using social media to advance the unit mission, however, decision makers should be aware that social media does not exist in a vacuum. As a forum of media, many of the laws that apply to newspapers, television, radio, and magazines also apply to social media. Furthermore, when governmental agencies take part in social media, laws that relate to government action apply as well.

When a government actor creates a web presence, which is a forum for communication, it involves the 1st Amendment right to freedom of speech and expression. Therefore, the first issue to address is whether or not that agency's web page created a "public forum." A public forum is a US constitutional law term that describes a government-owned property that is open to public expression and assembly.[14] There are several types of public forums, each one expanding the right of public expression.

The most open forum is the traditional public forum, such as streets or parks that, by long tradition, have been devoted to the public for expressive use. In the traditional public forum, the government may not impose content-based restrictions on speech unless they are "necessary to achieve a compelling state interest and…narrowly drawn to achieve that end."[14] A social media page is unlikely to be designated a traditional public forum, as the US Supreme Court has restricted that category to property "historically" used for public expression (eg, public square in front of a court house or a municipal park).[14] Currently, social media space or the internet do not fall within that description. However, with time that may change as constitutional interpretation evolves.

The designated public forum, which "consists of property which the state has opened for use by the public as a place for expressive activity."[14] Examples include a public university "campus free speech zone" open to all speakers, or meeting rooms in a public library which is available to all members of the public. A designated public forum requires the government's clear intent to open one, however, it could be inferred based on the government's policies and practice. What the Supreme Court has termed the limited forum could be considered a subcategory of the designated public forum. The limited public forum is a place or space designated for speech by "certain groups" or for "discussion of certain topics." The government's establishment and application of content parameters in the limited public forum must be "reasonable in light of the purposes of the forum," and viewpoint neutral.[14]

The nonpublic forum refers to government property that "is not by tradition or designation a forum for public communication."[14] In a nonpublic forum, deference will be given to the government actor in deciding who may speak and what shall be said. The government may impose time, place, and manner restrictions, and may exclude speakers as long as that exclusion is reasonable.[14]

The last category is government speech. The concept behind this category is that governments must speak in order to govern, and they do so through agents whom they hire, pay, recruit, or subsidize. The government is permitted to use media to communicate its message and, when it does so, it does not have to include opposing viewpoints or allow for an exchange of idea or any interaction.[14] The ballot box is where the public has the opportunity to respond.

The type of public forum becomes important when deciding issues concerning whether defamatory or vulgar material would be protected by the 1st Amendment, what comments can be removed, what information may be retained or collected, and what information may be tracked. A question for commanders in regards to a social media platform is whether a commander or site maintainer can remove profanity or hate speech from a page? For example, can he or she order the removal of a post by someone who asks a controversial question, or makes a divisive or contentious remark?

The type of public forum created may very well determine the amount of editorial control and whether a post is actually a public record, and, if so, whether or not there is an obligation to maintain, release, and/or distribute. The type of social media presence maintained by the organization may be determined in part by the contents of any user agreement and its terms and conditions, disclaimers, and the stated purpose/scope of the site. Most government actors, including military organizations, create solely informational social media pages (eg, using Facebook without any interaction) and are engaging in purely government speech, and therefore retain editorial control of the page. The problems that usually arise concern EOPs that operate between the 2 extremes of no interactivity and complete interactivity. This gray area of having some interaction between web page creators and visitors to the site, but yet strictly controlling the conversation, scope of interaction, and/

or content makes it much more difficult to determine whether or not the government sponsored social media page is a public forum.[14]

Most of the time, the deciding factors will be the site's purpose, content, user policies, disclaimers, and the quantity and/or quality of communication between visitor and site creators/maintainers. At this point, there is no need for a constitutional law discussion about whether or not a particular EOP created a public forum. For purposes of this article, it is sufficient for the reader to be aware that, by their very nature, government-sponsored EOPs or web pages, regardless of purpose or content, fall under a constitutional umbrella which may or may not affect the extent to which a government actor, by its power to control the conversation, may utilize and control the capabilities of a social media site.

Retaining Editorial Control

If a government actor is very careful in setting up its social media site, it can usually guarantee that it is either government speech or a nonpublic forum and can therefore retain maximum control over the conversation that takes place. Lidsky[14] suggests the following combination of actions and common sense solutions for government agencies and commanders to ensure that their organization's site falls into a public forum that allows them to retain as much control as possible over the content and conversation:

- Establish a direction or purpose, a real objective that serves to advance your mission. The purpose may evolve as long as you develop a strategic plan to support it. Clearly state and post the purpose and the scope of site on the first page so that it is noticeable to visitors to the site. It should state that the use of social media by (name of entity) is for the purpose of obtaining or conveying information that is useful to or will further the goals of said entity.

- Plainly describe the terms and conditions of use so that a visitor to the site and/or user is on notice as to what kind of conduct and content is prohibited or permitted. Remind Soldiers that their conduct on the site is still regulated by the Uniform Code of Military Justice[15] and that they are expected to conduct themselves accordingly. Review the current applicable guidance and request advice from the public affairs office to ensure you are covering all of the Army specific requirements.

- Identify an administrator/maintainer in charge of the site. The maintainer should be well trained on all policies regarding EOPs, OPSEC regulations and concerns, and on reviewing content before it is posted. He/she should be intimately aware of the objective of the site. Require them to use their names and titles for official posts or responses.

- Establish a policy for the retention of records. This very simply means that anything posted by the organization or comments by the public should be retained in some form that, if needed, can be retrieved at a later date.

- Make sure that the administrators/maintainers understand the technology, how a site works, how to post, and how to remove posts. They must be knowledgeable about the subject matter, comprehend the commander's or unit's intent, and be able to apply that understanding responsibly to the web page. The administrators/maintainers must know the law, regulations, and guidelines before creating the site, as well as during its operation. Contact your local public affairs office, staff judge advocate and security officer for information and assistance.

- State clearly what kind of forum that you are creating. This could be done implicitly in the purpose/scope/policy statement. However, stating your intent to create a nonpublic or limited public forum immediately informs the visitor and user that there is no absolute 1st Amendment right to free speech or expression on the site.

- Train your people well and give them the time and resources to accomplish your site's stated purpose.

- Clearly post your disclaimers. They should include a general disclaimer, privacy and security disclaimer, copyright and trade mark disclaimer, moderated presence disclaimer, persistent cookie disclaimer, Freedom of Information Act (5 USC §552) and records management notice, external links and nonendorsement disclaimer, and all disclaimer/notices required by Army regulations. Include a disclaimer that states that any content posted by the public, Family member, Army civilian employee, and Soldier does not represent the opinion of the command.

- Clearly state user policies, terms and conditions, and enforcement methods such as no use of profanity; no personal attacks; no spam messages; no off-topic comments; no solicitations; failure to follow guidelines for posting comments may result in the deletion of comments without warning; and, based

on the discretion of site officials, comments may be deleted if they violate the Uniform Code of Military Justice,[15] disrupt good order and discipline, are discriminatory or offensive.

- Keep postings in official capacity. Do not speak/post/comment in an unofficial capacity, nor fluctuate between the 2 capacities.

One crucial indicator of the type of public forum your organization creates is the amount of interactivity that the site permits. Make an unambiguous resolution as to whether comments from the public, Soldiers, and/or Family members will be allowed. If allowed, develop standards that will limit topics, organizational subjects, or issues to those first posted by the command. As the strategic plan and/or the purpose of the site is under development, commands should determine how they will respond to posts and how much they will engage in conversation with the users.

The command must decide how to respond, or even whether to respond to questions or comments that are posted on the site. It must be determined how to manage unwanted or controversial comments or questions, or to leave them on the site either answered or unanswered. On some sites, other users may police such comments by either answering them (correctly or incorrectly) or by expressing disapproval of such comments or approval. Site administrators must decide at what point to remove divisive posts or to officially comment on them. The approach that a command adopts may change during the life of the site, depending upon the organization and the site's purpose/objective, negative or positive feedback from users, and/or the particular message or conversation.

Benefits And Challenges To Using Social Media

Before engaging in the use of social media, commanders and agencies in MEDCOM must first ask themselves whether the benefit received will warrant the time, expense, and effort involved in the creation and maintenance of an EOP on a social networking website.[14] They must seriously evaluate all the benefits and potential drawbacks or difficulties associated with having a presence on a social media website. Most importantly, before anything else, commanders and organizations must determine for what "purpose" they are undertaking this enterprise, ie, for what reason is a social media presence required? Commanders and organizations should not create social media web pages simply because other agencies are doing it, it is a modern form of media, or because it looks good on a résumé.

Once the purpose or objective has been determined, a strategic plan or social media strategy is necessary to establish how the purpose or objective will be achieved. A well organized and structured social media plan must address the following questions:

- What direct benefit does it offer the organization, agency, unit or command?
- What are the potential dangers, pitfalls or drawbacks?
- What are the legalities involved in operating a social media page?

In addition, commands should be knowledgeable about the process, requirements, and basic guidelines that govern the establishment, use, and maintenance of an EOP.

There are ample reasons why a commander, an organization, or even a platoon-size unit would want to use social media to enhance the mission. Social media is a powerful communication tool that can significantly increase the effectiveness of a command's interactions with Soldiers, Family members, civilian employees, and the public. Social media provides the command with the ability to reach larger audiences, including people with whom the command would not otherwise interact during the ordinary course of business. This communication can take place on a consistent basis, faster, and less expensively than with other forms of media. The quality of the communication is enhanced as well, through the use of video, audio, computer generated images, and photos. Today people can view social media anywhere at any time through desk tops, laptops, Ipads, Ipods, cell phones, at work, home, in the car, or while shopping. It can be used very effectively in crisis situations, to provide warnings and information, and manage a response. It can help build and maintain morale and esprit de corps by keeping the command and Soldiers connected.

Interactive social media can serve as a virtual town hall meeting, encouraging interaction between the command and its constituents. Social media also encourages the exchange of information and collaboration between the command and Soldiers, Families, and civilian employees, providing a continuous process of consultation. The command determines its amount of engagement. Social media can be used exclusively as an information outlet, or it can be used to solicit open-ended comment and expression, or to request more focused and limited avenues of feedback. The command can use it as a tool to encourage an exchange of ideas, to address relevant issues or concerns, monitor attitudes about certain issues,

and get a sense of the overall temperament across the target audience.

Commands can use social media sites to communicate with Soldiers, Families, and employees, directly eliminating intermediaries. Posts from the commander or command sergeant major are communicated directly and give an aura of straightforwardness without distortion. Social media fosters a spirit of engagement, accessibility, approachability, and the atmosphere of responsiveness between the command and its constituents.

Perhaps the greatest advantage of social media is that it allows the command to control the message. The message is whatever the command determines will promote or advance its mission. The message the command communicates is designed, tailored, and managed by the command. The command determines the message content, when, where, and how it is released, and the target audience. It may be as simple as posting information about organizational events, administrative necessities, or to congratulate a Soldier on a special occasion. The message can be directed at certain groups, individuals, or organizations; it could be to correct a wrongly perceived event or inaccurate news story. The message may be influenced by the kind of feedback the command receives from the message it posts. However, the means to track and measure feedback and the manner in which feedback is delivered are also controlled by the site administrators.

Not only can the command or organization dictate the message, it can control and/or limit the amount of interaction. In actuality the command shapes and manages the tone, quality, nature, and direction of the conversation that takes place by simply controlling the topic or subject of discussion; limiting the time allowed for comment; restricting the type of comments received (positive, constructive—not negative or divisive); establishing whether any comment is allowed; if allowed, the form of the comment (text, video, or a simple vote type response), and its length. The type of message and reply/comment environment may reflect the type of relationship the command has with its Soldiers, Family members, Army employees, and the public.

Drawbacks of Social Media Use in the Military

Although there are great benefits to using social media and it can be a force multiplier when used appropriately, in the context of government, especially the military, social media use comes at a price. Interactive social media can create or exert pressure to respond to user demands, comments, or questions. Site controllers must be careful what they ask for, or to what extent they open the conversation. Users and visitors are allowed their opinions. Obviously, Soldiers, Family members, Army civilians, and the public have 1st Amendment rights to free expression. The candid, uncensored exchange of ideas, and the freedom to express complaints, ask questions, and/or make comments is what has defined social media. However, that very characteristic is a potential game changer for military commands and organizations because the necessity to control the conversation is key. Even though the conversation occurs on an impersonal illuminated screen, there is still the requirement to maintain and convey the message of a command-driven relationship, with good order and discipline.

Many commands, organizations, and individual commanders choose not to respond to user comments or posts, but observe and listen. Even when comments or suggestions are requested, or questions are asked, those commands and/or individual commanders do not respond. Depending on an organization's strategic communications plan and social media purpose, such an approach can present a constant dilemma . Many users or visitors to a site will judge the site's credibility on the amount of interaction and conversation that occurs: how responsive is the site, is it consistently responding or not at all, is it merely an informational site, or does it support an actual exchange of ideas. Each command, organization, and/or commander must decide to what extent and when they will engage with a user based on upon their overall strategic plan. However, a site's perceived relevance to and prominence among its intended audience may depend upon how they view the site's credibility.

The most obvious and dangerous concern surrounding the use of social media in the government and specifically the military is the loss of sensitive or classified information. The internet is a powerful way to convey information quickly and efficiently. However, it also provides a potent instrument to adversaries to obtain, correlate, and evaluate an unprecedented volume of aggregate information regarding our operational capabilities, security limitations, and vulnerabilities. This spillage of information into the public arena can be used to assemble fragments of information to decipher the larger picture, draw conclusions, and deduct usable and actionable intelligence.

Maintaining operations security and the ability to manage the risks that result from the use of social media should be the number one priority of site controllers/maintainers. Information in the wrong hands can compromise ongoing operations, base security, or result in identity theft. Operations security includes information

concerning things such as: force protection measures; communications (information management, infrastructure information systems and networks equipment); logistics (movement of equipment and troops); personally identifiable information of Soldiers and Family members; operations (training missions, tactical and strategic operational military actions) and critical infrastructure (eg, bases, nuclear facilities, water plants).[9] Operations security concerns exist in what may seem like harmless photos, videos, news announcements, or status updates—not just folders clearly marked SECRET.

Operations security considerations should be part of any strategic social media plan. Site organizers must be aware of and knowledgeable about Army regulations that apply to classified and sensitive information, and who can approve the release of information. Operations security awareness training and specialized training for site maintainers and controllers is a must and should be included in the budget when determining the costs of establishing a site. Furthermore, site administrators/maintainers should be intimately familiar with the intent or purpose of the organization's social media page. Sometimes, unclassified information that might be considered harmless may not be conducive to the command's social media plan and should not be posted. The commander is ultimately responsible for the content of the organization's social media pages, including the problems that occur: a security violation, an offensive comment by a site official, or a simple mistake about the time and date of a social event.

Beyond the potentially dangerous reality of the release of OPSEC-related material via a social media site, site operators must be concerned with the dissemination of misinformation or a misrepresentation that may be posted by impostors or impersonators. In addition, site operators/maintainers must be trained on how and when to enforce site policies, user agreements, and disclaimers. For example, a site maintainer should be well trained regarding what posts or comments can be censored or deleted from the site, and when and if they need to be recorded and maintained.

Depending on the size of the organization and site's purpose, maintaining a social media presence can be a very time-consuming, labor-intensive endeavor. Social media page site operators must be trained not just on OPSEC issues, but in technical operation and maintenance, compliance with Army regulations and command policies, and site policies. The operators must design, create, manage, and promote the site. They must consistently review the site's content; keep the site interesting, people engaged, and information updated. The list of responsibilities goes on and on, and everything must be accounted for in the strategic plan, then resourced and funded.

Because the commander is personally responsible for the content, operation and maintenance of the site, he/she should be involved in or at least informed about its daily operations. Once a site operator publishes a post/comment, it becomes the commander's responsiblity. Once that comment, photo, or video is in the public domain, control over that post is basically lost; it can be downloaded, copied, and distributed at will. The command must also monitor the tone of its comments/posts (friendly but professional), review the photos, video, or text before publication. The sponsoring command must make every effort to not violate its own policies, protect copyright and trademark laws, and monitor and track feedback. If the purpose of the site is to connect with an audience with which the command does not interact on a regular basis, a poorly maintained or unremarkable site without much (or any) site/user interaction will not have many followers. It will lack credibility. A poorly organized and maintained site becomes irrelevant and may give a visitor/user a negative impression of the command and organization.

There are additional factors that an Army MEDCOM organization commander should consider when using or deciding whether or not to use social media are. The potential risk of an unauthorized release of personally identifiable information (PII) associated with patients' medical records/histories, civilian medical personnel, insurance providers, credentialing, investigations, lawsuits, and Family members is enormous.[16] Protection of personal information under the Privacy Act[13] and the Health Insurance Portability and Accountability Act (Pub L No. 104-191 (1996)) is an essential and basic responsibility of all MEDCOM organizations working with or connected to the provision of healthcare. It is usually these very kinds of organizations that could benefit the most from an open, uninhibited exchange with its users. However, the more open and engaging the site may be, the greater the potential risk for an unintended release of information. Unauthorized releases or a loss of PII is an extremely serious event, commands and site operators should refer to *OTSG/MEDCOM Policy Memorandum 11-070*[16] for reporting incidents when there is a suspected or actual loss, theft, or compromise of PII.

Records management is another factor that must be considered by organizations that provide healthcare. Records include all books, documents, videos, photos; indeed, anything made or received by the agency as evidence of the organization, function, policies, practices,

procedures, policies, operations, or other activities; or because of the informational data they may contain. The Federal records Act of 1950 contains the statutory authority for the Army Records Information Management System. Any electronic information generated by or contained in an information system or other automation source that is created or received during the conduct of business must be preserved. There are also restrictions on the collection of information from members of the public and how that information is stored. According to the Paperwork Reduction Act of 1995 (44 USC 3501 et seq), government agencies must get approval from the Office of Management and Budget prior to obtaining or soliciting "identical" information from 10 or more persons. The information must then be stored incompliance with the Privacy Act.[13]

The very nature of the medical field involves the use of copyright, trademark, and patent materials; equipment; instruments; and pharmaceuticals.[17] Site operators must be ever vigilant not to endorse, promote or show support for one product over the other. They must be mindful not to wrongfully use record, distribute or portray copyrighted material, patents or trademarks without acquiring the prior consent of the proprietor. For example photographs from media reporters working with units ("embedded") are copyrighted and cannot be publicly distributed without the written consent of the reporters.[17]

Conclusion

Like many other Army commands, MEDCOM organizations have turned to social media to distribute their message. In the MEDCOM there are numerous traditional websites and social media sites that span the spectrum of interactivity and communications. Because of their unique mission, many Warrior Transition Unit (WTU) sites have demonstrated a willingness to engage in conversation. Rather than waiting to be overwhelmed by questions and/or complaints from Soldiers, Family members, and/or interested third parties and see the reputation of the command suffer, some WTUs took a more proactive approach to establishing a communications platform for the command. Although social media has worked well for WTUs, that does not mean it will work, or is even a viable communications option, for all MEDCOM organizations.

Because of the nature of the Army's overall mission; the traditional, customary and legal restraints that surround open discourse within the military; and the necessary structure of the command/subordinate relationship, oftentimes the most advantageous social media site is one with restricted interactivity, offering informational and administrative necessities, while still providing a limited avenue of access to the command. Not all commands can afford to open themselves to full and free communication exchanges with users, for such openness of expression may negatively affect the way the command delivers its message, interacts with its subordinates, or even alter or inhibit the actual, intended purpose of the site.

Army MEDCOM organizations that already have an EOP in operation and those considering creating one should recognize and appreciate certain basic realities. The more an organization opens the site for a back and forth exchange of comments/posts, the more it is unable to control the conversation and messages of the forum. Consequently, it then becomes harder to manage the risks associated with OPSEC and PII. There is a greater obligation to maintain and keep records, protect 1st Amendment rights, and train and keep qualified personnel to monitor and maintain the social media platforms.

Finally, unfortunately, a simple fact that is often overlooked by too many organizations when sponsoring a social media page is that the command must determine how to keep the EOP relevant and prominent with users. Commands must consistently engage, participate (to a limited extent), influence, and monitor. The crucial element to a successful governmental or military social media site is "credibility." If users think a commander, command, or organizational site is credible, they will keep coming back—they will connect with it. The site will be relevant and take a prominent place in the user's choice of communications media within the command. A reliable site will attach an appearance of credibility to the command and/or organization. That perception alone has the potential to advance the mission.

The reader should recognize that all organizations do not require a social media site, nor is it to their advantage. Is it really necessary that we receive a tweet from a commander about what they had for breakfast or that a Soldier can become a fan of the command on Facebook? We certainly can read newsworthy articles on the organizational web page, in the newspaper, or in the base or organizational paper. Commanders can still get the message out at formations, bulletin boards, through town hall meeting, email, written correspondence, by phone, or face to face.

Commanders must consider how their organization's page will impact the larger picture, how it fits in with the overall Army message, and, most importantly, is a social media page really going to advance their units mission. Bottom line: considering all the legal implications,

benefits, and risks is creating an EOP really worth it, or can you simply do it the old fashioned way?

References

1. *The United States Army Social Media Handbook Version 2*. Washington, DC: Office of the Chief of Public affairs, US Dept of the Army; August 2011. Available at: http://www.slideshare.net/USArmySocialMedia/army-social-media-handbook-2011.
2. *The Army's Use of Social Media External Official Presence Sites*; Alexandria, VA; US Army Audit Agency; July 26, 2011. Audit Report; A-2011-0150-IET.
3. *Directive Type Memorandum (DTM) 09-026: Responsible use of Internet-based Capabilities.* Washington, DC: Deputy Secretary of Defense; February 25, 2011: Change 2. Available at: http://www.dtic.mil/whs/directives/corres/pdf/DTM-09-026.pdf.
4. Chief Information Officer/G-6 Memorandum: Responsible Use of Internet Capabilities. Washington, DC: Office of the Secretary of the Army; March 25, 2010. Available at: http://ciog6.army.mil/LinkClick.aspx?fileticket=Es8pnrXtvdU%3D&tabid=64.
5. Memorandum: Delegation of Authority–Approval of External Official Presences. Washington, DC: Secretary of the Army; October 21, 2010. Available at:http://www.slideshare.net/USArmySocialMedia/delegation-of-authority-social-media-use.
6. *Army Regulation 25-1: Army Knowledge Management and Information Technology.* Washington, DC: US Dept of the Army; December 4, 2008.
7. Office of the General Counsel Memorandum: Use of Social Media in the Army. Washington, DC: Dept of the Army; June 17, 2009.
8. *Department of the Army Pamphlet 25-1-1: Information Technology Support and Services.* Washington, DC: US Dept of the Army; October 25, 2006.
9. *Army Regulation 530-1: Operation Security.* Washington, DC: US Dept of the Army; April 19, 2007.
10. *Army Regulation 360-1: The Army Public Affairs Program*. Washington, DC: US Dept of the Army; May 25, 2011.
11. Department of the Army Memorandum: Standardizing official U.S. Army external official presences (social media). Washington, DC: Office of the Chief of Public Affairs, US Dept of the Army; November 1, 2010. Available at: http://corpslakes.usace.army.mil/socialmedia/Social%20Media%20Standard%20SOP.pdf.
12. Secretary of the Army Memorandum: Delegation of Authority–Approval of External Official Presences. Washington, DC: US Dept of the Army; October 21, 2010. Available at: http://www.slideshare.net/USArmySocialMedia/delegation-of-authority-social-media-use.
13. USC §552a (1974).
14. Lidsky LB. Government sponsored social media and public forum doctrine under the first amendment: perils and pitfalls. *The Public Lawyer.* 2011;19(2).
15. 64 Stat. 109, 10 USC, chap 47.
16. OTSG MEDCOM Policy Memorandum 11-070: Personally Identifiable Information (PII) Incident Reporting and Notification Procedures. Fort Sam Houston, TX: US Army Medical Command; August 19, 2011.
17. *Army Regulation 27-60: Intellectual Property,* Washington, DC: US Dept of the Army; June 1, 1993.

Author

CPT Jonasz is an Attorney-Advisor with the Office of the Staff Judge Advocate, US Army Medical Command, Fort Sam Houston, Texas.

Army Medical Training Agreements

Maurice A. Deaver, Jr, JD
Kendra J. Harris

Introduction

Army medical treatment facilities (MTFs) operate professional education programs to train military healthcare providers (HCPs).[1] To ensure sufficient training opportunities are available for military HCPs and to sustain viable in-house programs, MTFs enter into gratuitous training and affiliation agreements with civilian healthcare training institutions (TIs). The agreements allow military and civilian HCPs to train at each other's facilities. Gratuitous training agreements under which military HCPs train in civilian medical facilities are called medical training agreements (MTAs).[2] Gratuitous training agreements under which civilian HCPs train in Army MTFs are known as affiliation agreements.* This article summarizes the history of the Army MTA program from a legal perspective and discusses the current status of the program.

History

Historically, the primary legal issue in MTAs has been professional liability coverage for HCPs who may be sued in a personal capacity. Provision of liability coverage has always been problematic. The Department of Justice (DOJ) becomes involved by virtue of the statutory requirements under the Federal Tort Claims Act (FTCA).[3] In order for the FTCA to apply, DOJ or the appropriate US Attorney's Office must certify that the allegedly negligent HCP was acting within the scope of federal employment and move to substitute the United States as the defendant.[4] Upon substitution, the HCP is immune from personal liability.[4,5]

Prior to 1989, DOJ concluded that work performed by military members training at civilian facilities primarily benefited the TI and not the Army, finding that military HCP-trainees were not acting within the scope of employment. Without certification and substitution by DOJ, the individual military HCP-trainee would be left as the defendant in a lawsuit, responsible for his or her own defense and without any malpractice insurance other than that which he or she might have personally obtained. This result was untenable.

*The Air Force and Navy refer to both MTAs and affiliation agreements as training affiliation agreements.

In 1989, DOJ and legal representatives from the military services reached a consensus on defending these cases. The DOJ agreed to certify that the military HCP trainees were acting within the scope of their federal employment and substitute the United States as the defendant. In return, the services agreed to make every effort to ensure that the military HCPs training at TIs were covered under those institutions' insurance, rather than relying on the FTCA. In addition, the services agreed they would not accept one-sided agreements and would ensure the United States did not accept liability for civilian students at MTFs which was greater than the liability TIs accepted for military HCPs at their facilities. Finally, the services agreed to use all possible care in crafting agreements in order to maximize the defenses of the United States, particularly the "borrowed servant" defense. Under the borrowed servant defense, a special employer is liable for the negligent acts of the employee of another general employer when the employee is loaned to and supervised by the special employer. For example, a military HCP-trainee at a TI could be considered a borrowed servant from the MTF (general employer), and thus be covered by the TI's (special employer) professional liability coverage.

Despite the 1989 consensus, in subsequent years, lawsuits arose for professional negligence of military HCPs training in civilian TIs. In some instances, an MTA did not exist, was patently one-sided, did not maximize the ability of DOJ to assert the borrowed servant defense, or was otherwise ill-conceived. As the cases arose, DOJ raised the issue of noncompliance with the 1989 consensus, and raised the possibility that it might decline to certify and substitute if the services continued to fail to uphold their end of the arrangement to enter only into appropriate agreements. Such declinations have not, to the authors' knowledge, occurred.

Creation of Standard Format Medical Training Agreements

Continued friction over nonexistent and inadequate MTAs resulted in 2 standard MTA forms preapproved by DOJ. One form relies on professional liability coverage provided by the TI. The second form relies on the FTCA for professional liability protection. The Army distributed DOJ-approved model MTAs in 1994 and redistributed the same formats in 1996 and 2000. In

addition, The Surgeon General's Memorandum dated March 28, 2000,[6] delegated limited authority to regional medical commands (RMC) to enter into MTAs with local teaching hospitals for mission-essential skills augmentation/enhancement training. Two DOJ-approved model MTA formats attached to the Memorandum evolved into US Army Medical Command (MEDCOM) Model MTA Format 1 and Format 2. Format 1, shown in Figures 1 and 2, is favored because it is consistent with the consensus and it provides that the TI will cover the military HCPs with liability insurance. The second format provides for FTCA coverage and specifically sets up the "borrowed servant" defense. Format 2, shown in Figures 3 and 4, should only be entered in the event that the TI cannot or will not agree to provide liability insurance under Format 1.

Current Army policy requires that any agreement varying from DOJ models must be approved beforehand by the US Army Legal Services Agency Litigation Division, Tort Litigation Branch (LITDIV). However, the requirement has been neither well-publicized nor closely observed. In 2003, Army MTFs conducted a local review of MTAs and reported to MEDCOM and LITDIV that, of an estimated 300 agreements, 95% were compliant with the required format. Notably, LITDIV conducted a subsequent physical review of the agreements and documented a substantially lower level of compliance.

Recommendations for Army Regulations and Policies Affecting MTAs

In December 2004, LITDIV recounted the history of the Army's MTA Program in a memorandum to The Surgeon General. LITDIV noted inadequate and erroneous guidance in *Army Regulation 351-3*, and recommended Training Agreements be separated from that publication and placed in a standalone regulation. However, the current *Army Regulation 351-3*,[1] published in October 2007, still covers MTAs and affiliation agreements.

In February 2006, the MEDCOM Office of the Staff Judge Advocate made a 2-pronged recommendation to The Surgeon General: (1) request OTJAG support for a senior executive level request to DOJ to suspend DOJ agreement requirements for the duration of the Global War on Terror; and (2) direct the Commanding General, Army Medical Department Center and School (AMEDDC&S) to

- assume proponency for the Army Medical Training and Affiliation Agreement program;
- survey the field on the impact of DOJ Policy on training agreements across the Army;
- establish Army policy on MTAs and affiliation agreements in a new, standalone regulation.

On March 7, 2007, The Surgeon General executed memoranda consistent with that recommendation.

CURRENT ARMY MTA POLICY

As of this writing, portions of the Army policy on MTAs are found in *Army Regulation 351-3*, paragraph 4-7,[1(p11)] The Surgeon General Memorandum of March 28, 2000,[6] and MEDCOM Model MTA Formats 1 and 2. Paragraph 4-7 of *Army Regulation 351-3* sets out the policies, procedures, and responsibilities for what it describes as the Gratuitous Agreement Program, and defines a gratuitous agreement as:

> [a] contractual document to obtain short or long-term training for military residents/fellows at civilian or Federal educational institutions when these institutions agree to provide training at no cost to the Government.[1(p11)]

Short-term MTAs

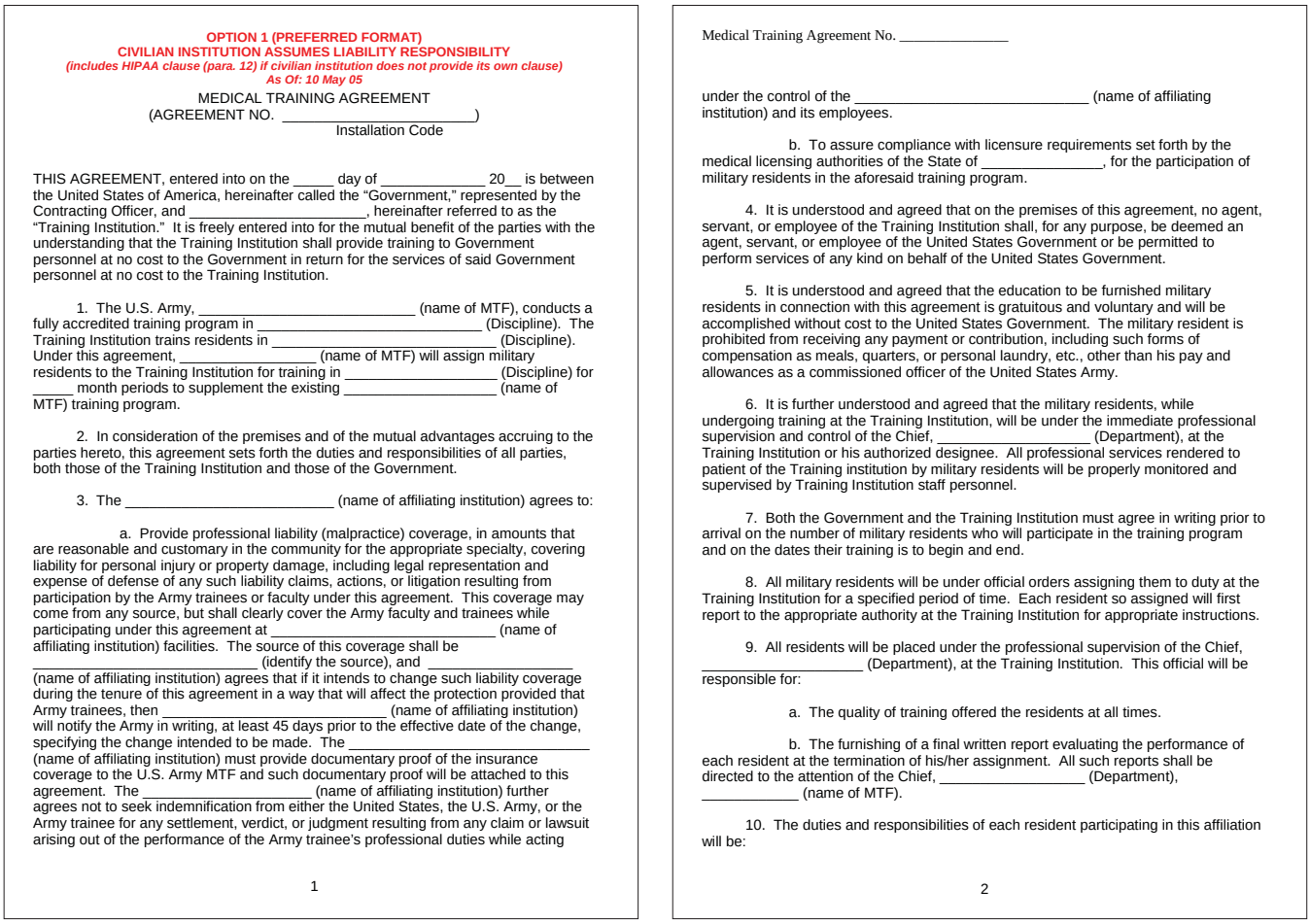
Major subordinate commanders are supervisory authorities of short-term MTAs for MTFs within their respective commands. The Commander, MEDCOM is the overall supervisory authority for all Army MTFs. The MEDCOM Assistant Chief of Staff for Resource Management provides oversight for gratuitous agreements through the MEDCOM Agreements Manager (MCRM-M). All proposed MTAs must be reviewed by the judge advocate office supporting the MTF and be signed by a US contracting officer. MTF commanders ensure adherence to the requirements of paragraph 4-7 of *Army Regulation 351-3*,[1(p11)] and its implementing guidance. Furthermore, "there will be no payment of" fees or charges "between the Army MTF and the" TI for short-term training. The Army and the Defense Federal Acquisition Regulation Supplements[7,8] provide limited additional guidance, respectively, for gratuitous agreements and the more general topic of educational service agreements.

Army Regulation 351-3 states that the format The Surgeon General has established:

> will afford the military trainee the benefits and protection normally afforded employees of the educational institution regarding liability insurance and legal representation.[1(p11)]

Thus, MTAs must follow the format prescribed in MEDCOM Model MTA Formats 1 and 2.* MTF commanders may approve, and contracting officers who support the

*The MEDCOM Model MTA formats are available from the MEDCOM Agreements Manager (MCRM-M).



OPTION 1 (PREFERRED FORMAT)
CIVILIAN INSTITUTION ASSUMES LIABILITY RESPONSIBILITY
(includes HIPAA clause (para. 12) if civilian institution does not provide its own clause)
As Of: 10 May 05

MEDICAL TRAINING AGREEMENT
(AGREEMENT NO. _____)
Installation Code

THIS AGREEMENT, entered into on the _____ day of _____ 20__ is between the United States of America, hereinafter called the "Government," represented by the Contracting Officer, and _____, hereinafter referred to as the "Training Institution." It is freely entered into for the mutual benefit of the parties with the understanding that the Training Institution shall provide training to Government personnel at no cost to the Government in return for the services of said Government personnel at no cost to the Training Institution.

1. The U.S. Army, _____ (name of MTF), conducts a fully accredited training program in _____ (Discipline). The Training Institution trains residents in _____ (Discipline). Under this agreement, _____ (name of MTF) will assign military residents to the Training Institution for training in _____ (Discipline) for _____ month periods to supplement the existing _____ (name of MTF) training program.

2. In consideration of the premises and of the mutual advantages accruing to the parties hereto, this agreement sets forth the duties and responsibilities of all parties, both those of the Training Institution and those of the Government.

3. The _____ (name of affiliating institution) agrees to:

a. Provide professional liability (malpractice) coverage, in amounts that are reasonable and customary in the community for the appropriate specialty, covering liability for personal injury or property damage, including legal representation and expense of defense of any such liability claims, actions, or litigation resulting from participation by the Army trainees or faculty under this agreement. This coverage may come from any source, but shall clearly cover the Army faculty and trainees while participating under this agreement at _____ (name of affiliating institution) facilities. The source of this coverage shall be _____ (identify the source), and _____ (name of affiliating institution) agrees that if it intends to change such liability coverage during the tenure of this agreement in a way that will affect the protection provided that Army trainees, then _____ (name of affiliating institution) will notify the Army in writing, at least 45 days prior to the effective date of the change, specifying the change intended to be made. The _____ (name of affiliating institution) must provide documentary proof of the insurance coverage to the U.S. Army MTF and such documentary proof will be attached to this agreement. The _____ (name of affiliating institution) further agrees not to seek indemnification from either the United States, the U.S. Army, or the Army trainee for any settlement, verdict, or judgment resulting from any claim or lawsuit arising out of the performance of the Army trainee's professional duties while acting

1

Medical Training Agreement No. _____

under the control of the _____ (name of affiliating institution) and its employees.

b. To assure compliance with licensure requirements set forth by the medical licensing authorities of the State of _____, for the participation of military residents in the aforesaid training program.

4. It is understood and agreed that on the premises of this agreement, no agent, servant, or employee of the Training Institution shall, for any purpose, be deemed an agent, servant, or employee of the United States Government or be permitted to perform services of any kind on behalf of the United States Government.

5. It is understood and agreed that the education to be furnished military residents in connection with this agreement is gratuitous and voluntary and will be accomplished without cost to the United States Government. The military resident is prohibited from receiving any payment or contribution, including such forms of compensation as meals, quarters, or personal laundry, etc., other than his pay and allowances as a commissioned officer of the United States Army.

6. It is further understood and agreed that the military residents, while undergoing training at the Training Institution, will be under the immediate professional supervision and control of the Chief, _____ (Department), at the Training Institution or his authorized designee. All professional services rendered to patient of the Training institution by military residents will be properly monitored and supervised by Training Institution staff personnel.

7. Both the Government and the Training Institution must agree in writing prior to arrival on the number of military residents who will participate in the training program and on the dates their training is to begin and end.

8. All military residents will be under official orders assigning them to duty at the Training Institution for a specified period of time. Each resident so assigned will first report to the appropriate authority at the Training Institution for appropriate instructions.

9. All residents will be placed under the professional supervision of the Chief, _____ (Department), at the Training Institution. This official will be responsible for:

a. The quality of training offered the residents at all times.

b. The furnishing of a final written report evaluating the performance of each resident at the termination of his/her assignment. All such reports shall be directed to the attention of the Chief, _____ (Department), _____ (name of MTF).

10. The duties and responsibilities of each resident participating in this affiliation will be:

2

Figure 1. Pages 1 and 2 of US Army Medical Command Model Military Training Agreement Format 1 (pages 3 and 4 are presented as Figure 2).

MTF commanders may execute, MTAs that conform to MEDCOM Model MTA Format 1 or Format 2. Both formats conform to DOJ guidance. Format 1 prescribes TI-provided liability coverage, legal representation, and no indemnification by the United States, the Army, or the military trainee.

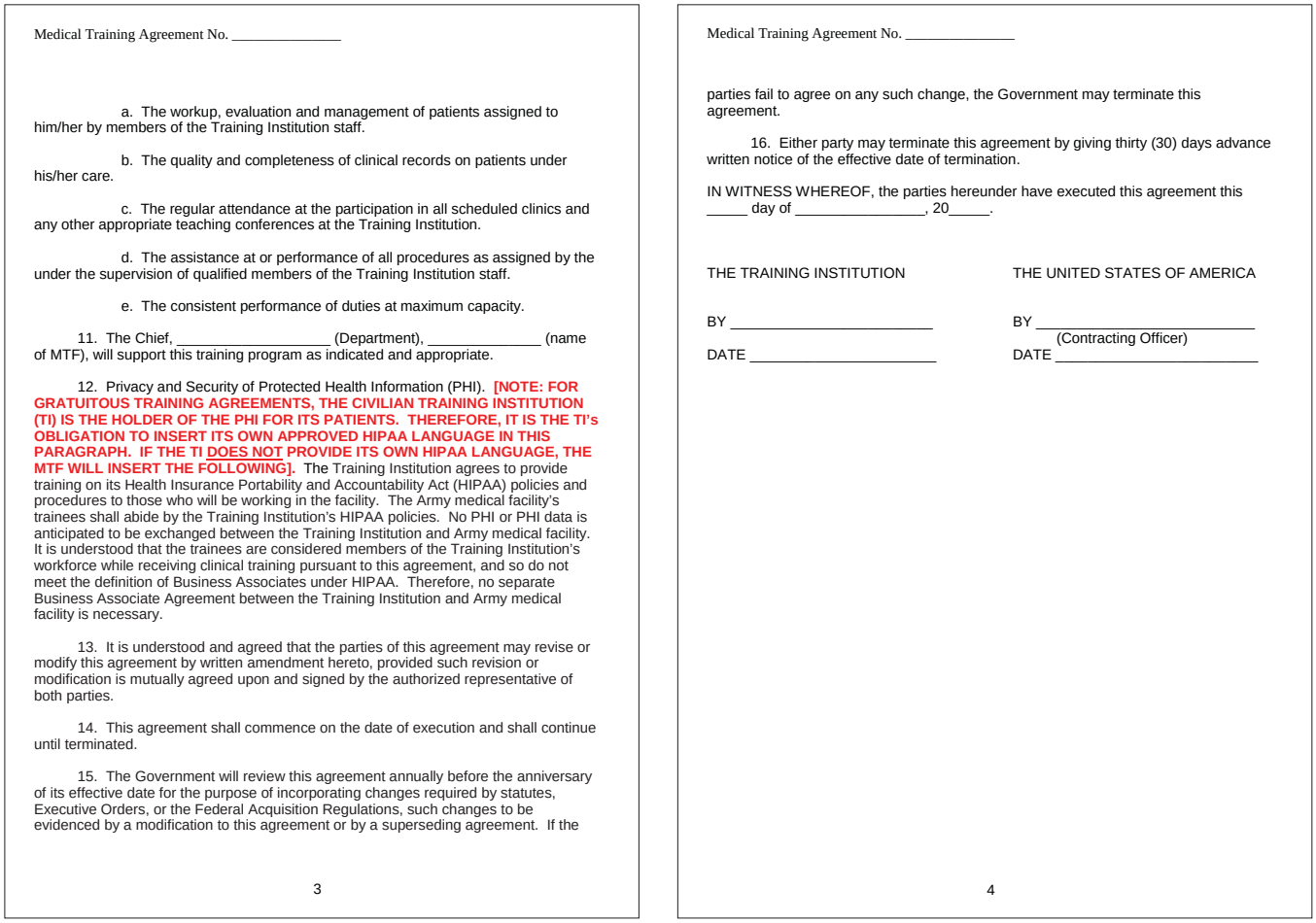
MTF commanders should attempt to agree upon MEDCOM Model MTA Format 1 with the TI because it is preferred. If the TI cannot or will not agree to Format 1, Format 2 may be used. Format 2 relies on the FTCA for liability protection of the military trainee and establishes the borrowed servant defense, to the extent it exists under applicable state law.

The oversight authority will coordinate with the MEDCOM Staff Judge Advocate (MCJA) to provide advance approval for all deviations from MEDCOM Model MTA Formats 1 and 2. MTFs and major subordinate commands must forward all MTAs that deviate from MEDCOM Model MTA Formats 1 and 2 through agreements manager channels to MCRM-M. In turn, MCRM-M will coordinate with the supervisory authority and MCJA. The oversight authority may approve nonsubstantive deviations from MEDCOM Model MTA Formats. Whenever there is a question as to whether proposed deviations are substantive, MCRM-M will coordinate through MCJA to contact LITDIV and/or the Department of Justice as necessary.

The local command authority issues temporary duty orders for military members in order to establish official duties under MTAs, and to identify the place, inclusive dates, and scope of training the duties will encompass. MTFs forward MTAs to the supervisory authority's support agreement manager within 5 days of execution or modification. MTFs also review existing MTAs annually. In addition to guidance on short-term MTAs, *Army Regulation 351-3*[1] provides instructions for long-term MTAs.

Long-term MTAs

The Office of the Surgeon General is the supervisory authority for long-term MTAs. *Army Regulation 351-3* assigns the AMEDDC&S Department of Health Education



Medical Training Agreement No. _____

a. The workup, evaluation and management of patients assigned to him/her by members of the Training Institution staff.

b. The quality and completeness of clinical records on patients under his/her care.

c. The regular attendance at the participation in all scheduled clinics and any other appropriate teaching conferences at the Training Institution.

d. The assistance at or performance of all procedures as assigned by the under the supervision of qualified members of the Training Institution staff.

e. The consistent performance of duties at maximum capacity.

11. The Chief, _____ (Department), _____ (name of MTF), will support this training program as indicated and appropriate.

12. Privacy and Security of Protected Health Information (PHI). **[NOTE: FOR GRATUITOUS TRAINING AGREEMENTS, THE CIVILIAN TRAINING INSTITUTION (TI) IS THE HOLDER OF THE PHI FOR ITS PATIENTS. THEREFORE, IT IS THE TI's OBLIGATION TO INSERT ITS OWN APPROVED HIPAA LANGUAGE IN THIS PARAGRAPH. IF THE TI DOES NOT PROVIDE ITS OWN HIPAA LANGUAGE, THE MTF WILL INSERT THE FOLLOWING].** The Training Institution agrees to provide training on its Health Insurance Portability and Accountability Act (HIPAA) policies and procedures to those who will be working in the facility. The Army medical facility's trainees shall abide by the Training Institution's HIPAA policies. No PHI or PHI data is anticipated to be exchanged between the Training Institution and Army medical facility. It is understood that the trainees are considered members of the Training Institution's workforce while receiving clinical training pursuant to this agreement, and so do not meet the definition of Business Associates under HIPAA. Therefore, no separate Business Associate Agreement between the Training Institution and Army medical facility is necessary.

13. It is understood and agreed that the parties of this agreement may revise or modify this agreement by written amendment hereto, provided such revision or modification is mutually agreed upon and signed by the authorized representative of both parties.

14. This agreement shall commence on the date of execution and shall continue until terminated.

15. The Government will review this agreement annually before the anniversary of its effective date for the purpose of incorporating changes required by statutes, Executive Orders, or the Federal Acquisition Regulations, such changes to be evidenced by a modification to this agreement or by a superseding agreement. If the

3

Medical Training Agreement No. _____

parties fail to agree on any such change, the Government may terminate this agreement.

16. Either party may terminate this agreement by giving thirty (30) days advance written notice of the effective date of termination.

IN WITNESS WHEREOF, the parties hereunder have executed this agreement this _____ day of _____, 20_____.

THE TRAINING INSTITUTION	THE UNITED STATES OF AMERICA
BY _____	BY _____
	(Contracting Officer)
DATE _____	DATE _____

4

Figure 2. Pages 3 and 4 of US Army Medical Command Model Military Training Agreement Format 1 (pages 1 and 2 are presented as Figure 1).

and Training responsibility for the preparation and execution of long-term MTAs.[1(p12)] Assignment of the military HCP-trainee will be by permanent change of station orders. There will be no payment of charges or fees between the government and the TI for training.

Long-term MTAs follow model MTA Formats prescribed by the Office of the Surgeon General and are executed by US contracting officers.

Staff Skills Augmentation Training Memorandum

The Surgeon General Memorandum of March 28, 2000,[6] delegates to commanders of regional medical commands the authority to enter MTAs for staff participation in necessary mission essential skills augmentation, maintenance, or enhancement training. The Memorandum includes the following prerequisites for staff training pursuant to an MTA:

1. The commander of the regional medical command must designate certain medical skills as mission essential for MTFs in the command.

2. The MTA must provide staff physicians with augmentation, maintenance, or enhancement training for the designated essential skills.

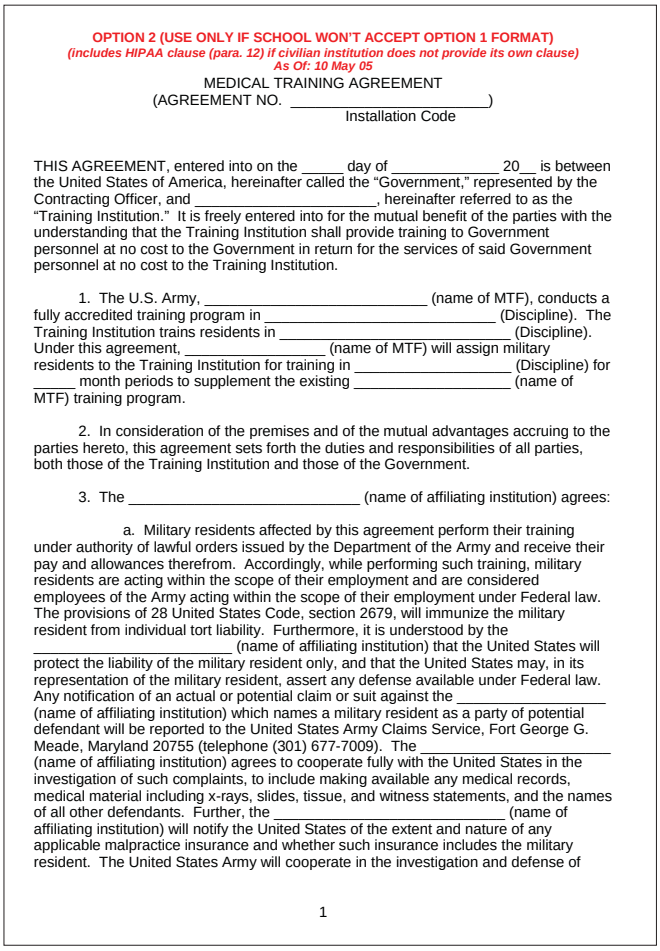
3. The MTA must be with a local teaching hospital.

4. The commander of the regional medical command must approve the act of entering into the MTA, which must be executed by a contracting officer.

5. Commanders of regional medical commands may allow MTF commanders to approve staff participation in training opportunities under MTAs previously entered into by the regional medical command.

6. The training must be within the United States.

7. Training duration should be no longer than a few weeks at any one time, and it should not result in additional certification by a recognized specialty or society board.



OPTION 2 (USE ONLY IF SCHOOL WON'T ACCEPT OPTION 1 FORMAT)
(includes HIPAA clause (para. 12) if civilian institution does not provide its own clause)
As Of: 10 May 05

MEDICAL TRAINING AGREEMENT
(AGREEMENT NO. _____)
Installation Code

THIS AGREEMENT, entered into on the _____ day of _____ 20__ is between the United States of America, hereinafter called the "Government," represented by the Contracting Officer, and _____, hereinafter referred to as the "Training Institution." It is freely entered into for the mutual benefit of the parties with the understanding that the Training Institution shall provide training to Government personnel at no cost to the Government in return for the services of said Government personnel at no cost to the Training Institution.

1. The U.S. Army, _____ (name of MTF), conducts a fully accredited training program in _____ (Discipline). The Training Institution trains residents in _____ (Discipline). Under this agreement, _____ (name of MTF) will assign military residents to the Training Institution for training in _____ (Discipline) for _____ month periods to supplement the existing _____ (name of MTF) training program.

2. In consideration of the premises and of the mutual advantages accruing to the parties hereto, this agreement sets forth the duties and responsibilities of all parties, both those of the Training Institution and those of the Government.

3. The _____ (name of affiliating institution) agrees:

a. Military residents affected by this agreement perform their training under authority of lawful orders issued by the Department of the Army and receive their pay and allowances therefrom. Accordingly, while performing such training, military residents are acting within the scope of their employment and are considered employees of the Army acting within the scope of their employment under Federal law. The provisions of 28 United States Code, section 2679, will immunize the military resident from individual tort liability. Furthermore, it is understood by the _____ (name of affiliating institution) that the United States will protect the liability of the military resident only, and that the United States may, in its representation of the military resident, assert any defense available under Federal law. Any notification of an actual or potential claim or suit against the _____ (name of affiliating institution) which names a military resident as a party of potential defendant will be reported to the United States Army Claims Service, Fort George G. Meade, Maryland 20755 (telephone (301) 677-7009). The _____ (name of affiliating institution) agrees to cooperate fully with the United States in the investigation of such complaints, to include making available any medical records, medical material including x-rays, slides, tissue, and witness statements, and the names of all other defendants. Further, the _____ (name of affiliating institution) will notify the United States of the extent and nature of any applicable malpractice insurance and whether such insurance includes the military resident. The United States Army will cooperate in the investigation and defense of

1

Medical Training Agreement No. _____

such complaints and where concurrence of the Attorney General is obtained will, upon request of the military resident, assist in the removal of the action to the appropriate Federal District Court with a view toward substituting the United States as a defendant in lieu of the military resident.

b. To assure compliance with licensure requirements set forth by the medical licensing authorities of the State of _____, for the participation of military residents in the aforesaid training program.

4. It is understood and agreed that on the premises of this agreement, no agent, servant, or employee of the Training Institution shall, for any purpose, be deemed an agent, servant, or employee of the United States Government or be permitted to perform services of any kind on behalf of the United States Government.

5. It is understood and agreed that the education to be furnished military residents in connection with this agreement is gratuitous and voluntary and will be accomplished without cost to the United States Government. The military resident is prohibited from receiving any payment or contribution, including such forms of compensation as meals, quarters, or personal laundry, etc., other than his pay and allowances as a commissioned officer of the United States Army.

6. It is further understood and agreed that the military residents, while undergoing training at the Training Institution, will be under the immediate professional supervision and control of the Chief, _____ (Department), at the Training Institution or his authorized designee. All professional services rendered to patient of the Training institution by military residents will be properly monitored and supervised by Training Institution staff personnel.

7. Both the Government and the Training Institution must agree in writing prior to arrival on the number of military residents who will participate in the training program and on the dates their training is to begin and end.

8. All military residents will be under official orders assigning them to duty at the Training Institution for a specified period of time. Each resident so assigned will first report to the appropriate authority at the Training Institution for appropriate instructions.

9. All residents will be placed under the professional supervision of the Chief, _____ (Department), at the Training Institution. This official will be responsible for:

a. The quality of training offered the residents at all times.

b. The furnishing of a final written report evaluating the performance of each resident at the termination of his/her assignment. All such reports shall be directed to the attention of the Chief, _____ (Department), _____ (name of MTF).

2

Figure 3. Pages 1 and 2 of US Army Medical Command Model Military Training Agreement Format 2 (pages 3 and 4 are presented as Figure 4).

8. TRICARE access standards must be maintained and participation in MTAs may not result in overall workload shifts to the managed care contractor.

The Memorandum requires appropriate legal review of the MTA, but the versions of MEDCOM MTA formats included as enclosures 1 and 2 to the Memorandum are outdated. The Memorandum does not include specific processing instructions, however all requirements described above for short-term MTAs apply.

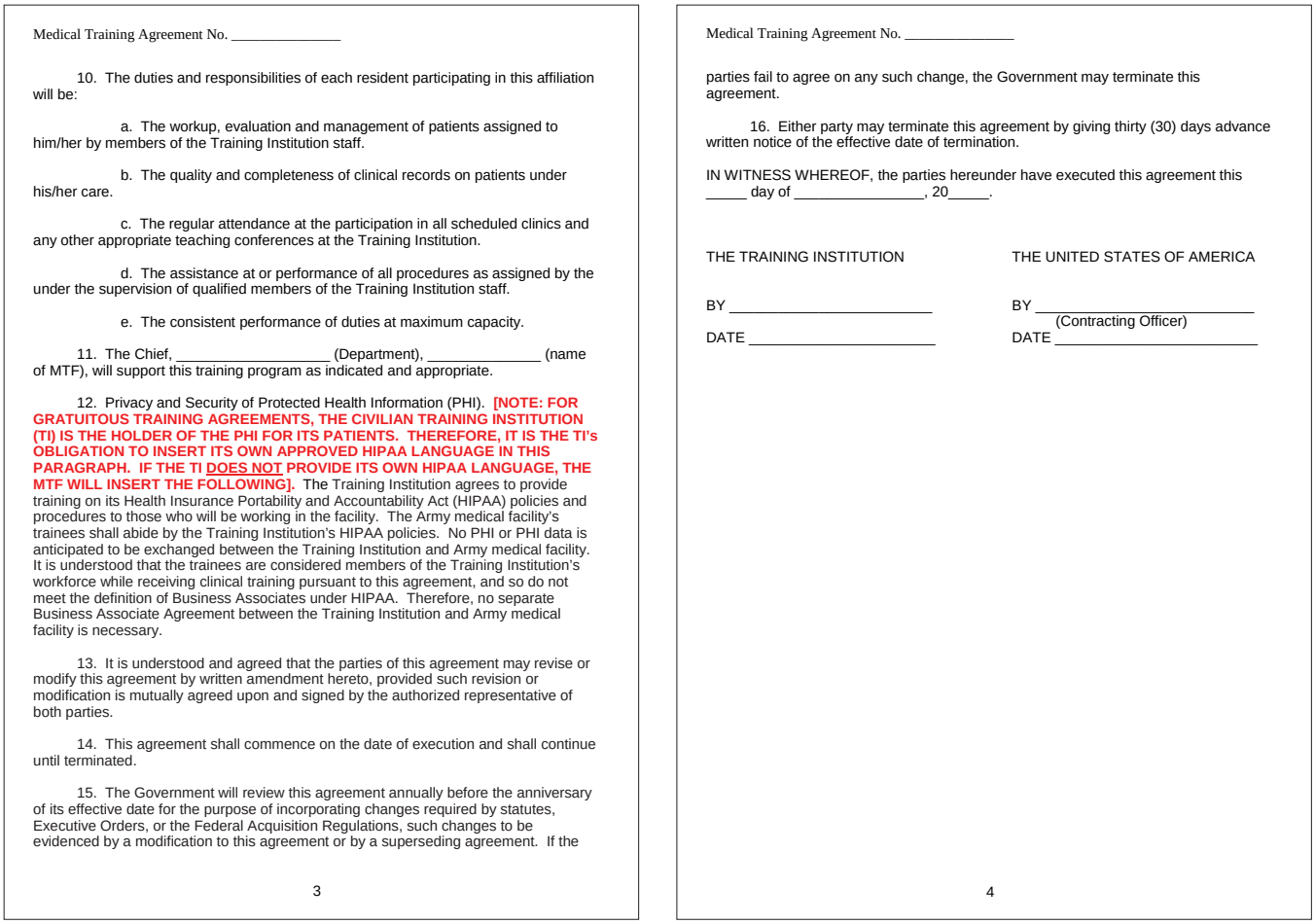
Because the Memorandum specifies several limitations on the grant of authority to commanders of regional medical commands, requests to deviate from those limitations must be approved. Such deviations might include entering into an MTA with a nonlocal teaching hospital, or entering an MTA for the purpose of enhancing skills of staff members other than physicians. The procedure for requesting approval of deviations is the same procedure used for deviations in short-term MTAs.

The Memorandum concludes by addressing civilian facilities without residency/fellowship training programs. The memorandum indicates the training with industry agreement may be more appropriate for such facilities. Neither MCJA nor LITDIV have any records which suggest that DOJ has ever approved the training with industry format included as enclosure 3 to the Memorandum. Accordingly, any request to use the training with industry format requires DOJ approval for deviations from one of the 2 MEDCOM Model MTA Formats.

OBSERVATIONS ON THE CURRENT ARMY MTA PROGRAM

Deviations from MEDCOM Model MTA Format 1

MEDCOM Model MTA Format 1 is appropriate when the TI provides professional liability coverage. In the past, LITDIV advised that MEDCOM Model MTA Format 1 provides guidance, but is not mandatory because the coverage is not being provided by the United States, but by the TI. When the TI provides coverage,



Medical Training Agreement No. _____

10. The duties and responsibilities of each resident participating in this affiliation will be:

a. The workup, evaluation and management of patients assigned to him/her by members of the Training Institution staff.

b. The quality and completeness of clinical records on patients under his/her care.

c. The regular attendance at the participation in all scheduled clinics and any other appropriate teaching conferences at the Training Institution.

d. The assistance at or performance of all procedures as assigned by the under the supervision of qualified members of the Training Institution staff.

e. The consistent performance of duties at maximum capacity.

11. The Chief, _____ (Department), _____ (name of MTF), will support this training program as indicated and appropriate.

12. Privacy and Security of Protected Health Information (PHI). **[NOTE: FOR GRATUITOUS TRAINING AGREEMENTS, THE CIVILIAN TRAINING INSTITUTION (TI) IS THE HOLDER OF THE PHI FOR ITS PATIENTS. THEREFORE, IT IS THE TI's OBLIGATION TO INSERT ITS OWN APPROVED HIPAA LANGUAGE IN THIS PARAGRAPH. IF THE TI DOES NOT PROVIDE ITS OWN HIPAA LANGUAGE, THE MTF WILL INSERT THE FOLLOWING].** The Training Institution agrees to provide training on its Health Insurance Portability and Accountability Act (HIPAA) policies and procedures to those who will be working in the facility. The Army medical facility's trainees shall abide by the Training Institution's HIPAA policies. No PHI or PHI data is anticipated to be exchanged between the Training Institution and Army medical facility. It is understood that the trainees are considered members of the Training Institution's workforce while receiving clinical training pursuant to this agreement, and so do not meet the definition of Business Associates under HIPAA. Therefore, no separate Business Associate Agreement between the Training Institution and Army medical facility is necessary.

13. It is understood and agreed that the parties of this agreement may revise or modify this agreement by written amendment hereto, provided such revision or modification is mutually agreed upon and signed by the authorized representative of both parties.

14. This agreement shall commence on the date of execution and shall continue until terminated.

15. The Government will review this agreement annually before the anniversary of its effective date for the purpose of incorporating changes required by statutes, Executive Orders, or the Federal Acquisition Regulations, such changes to be evidenced by a modification to this agreement or by a superseding agreement. If the

3

Medical Training Agreement No. _____

parties fail to agree on any such change, the Government may terminate this agreement.

16. Either party may terminate this agreement by giving thirty (30) days advance written notice of the effective date of termination.

IN WITNESS WHEREOF, the parties hereunder have executed this agreement this _____ day of _____, 20_____.

THE TRAINING INSTITUTION	THE UNITED STATES OF AMERICA
BY _____	BY _____ (Contracting Officer)
DATE _____	DATE _____

4

Figure 4. Pages 3 and 4 of US Army Medical Command Model Military Training Agreement Format 2 (pages 1 and 2 are presented as Figure 3).

the concerns are: (1) is there actually coverage; (2) does the coverage provide for legal representation; and (3) are there provisions for no recourse against the United States, the trainee, or other Army personnel in the event the TI-provided coverage actually pays out? As a consequence, substantial latitude is permitted within MEDCOM Model MTA Format 1, and most deviations are not deemed substantive.

Deviations from MEDCOM Model MTA Format 2

When the FTCA replaces liability coverage for the military trainee, MEDCOM Model MTA Format 2 should be used. Even small deviations from this form are frequently viewed as substantive. Attempts to "improve" the document by rewriting it are generally not well-received. Do not attempt to write a better document. Every change to MEDCOM Model MTA Format 2 must be viewed in the context of its impact on the borrowed servant doctrine. Any change which involves severing or weakening the chain of supervision between military trainees and the TI will likely be substantive. The form language of MTA Format 2 places military trainees under the

> immediate professional supervision and control of the Chief, [appropriate department] at the Training Institution…. All professional services rendered… by military residents will be properly monitored and supervised by TI staff personnel.[6]

Any changes in this language will almost certainly be deemed substantive.

Placing supervision responsibilities with personnel who are not employees of the TI (eg, independent contractors) breaks the supervisory chain within the TI and constitutes a substantive change. Similarly, inserting military personnel in the TI as instructors for military trainees also breaks the supervisory chain, as does the insertion of an independent government contractor as the instructor. Moving the responsibility for ensuring compliance with state licensure requirements from the TI to the government has been viewed as a substantive deviation. In one case, however, a change placing the burden on the

military trainee was accepted when the TI attorney produced the state statute explicitly placing the burden of compliance on the trainee. These are a few examples in which particular deviations from MEDCOM Model MTA Format 2 were disapproved. There are a number of other deviations that have been disapproved, including proposed MTAs that include numerous changes and additions to MEDCOM Model MTA Format 2, even though the many changes and additions had no apparent impact on the borrowed servant doctrine.

Liability Insurance

Training institutions are increasingly unwilling to pay for liability coverage. Such coverage generally comes in the form of commercial liability insurance, although state-owned TIs may rely on a state tort claims act. Government purchase of liability insurance for military trainees is an alternative. The United States is a self-insurer. On a number of occasions, the Comptroller General has determined that, absent a specific statutory grant of authority or other limited circumstances which are not applicable to MTFs, there is no authority for the United States to purchase liability insurance for its personnel. A federal statute[9] and a Department of Defense directive[10] specifically delegate authority to the Secretary of the Army to purchase liability insurance for medical personnel who are detailed for service with "other than a Federal Department." To the authors' knowledge, such authority has never been exercised or redelegated. Obviously, a general decision to fund commercial liability insurance for military trainees at TIs would have substantial fiscal implications.

To Whom Do the MTA Formats and Rules Apply?

While the MTA rules resulted from military physicians performing residencies in civilian medical TIs, the rules have generally been applied to any medical training in civilian organizations in which a military HCP or student military HCP engaged in clinical training. Notably, since *Army Regulation 351-3*[1] and The Surgeon General Memorandum of March 28, 2000[6] apply to physicians, MTAs for other than physicians require an approved deviation. MTA applicability includes public educational institutions as well as private institutions and commercial businesses that deliver healthcare. The rules apply to both military HCPs and student HCPs, covering ranges from student technicians and nurses through medical staff physicians in initial, advanced, or skills maintenance training. The rules apply to all forms of civilian facilities. In short, MTA format rules apply to all cases in which Army medical personnel deliver healthcare services outside of the MTF to people who are not military health system beneficiaries, because the authority for providing such care is based on the training benefits received by military HCPs. Such training, in turn, enables military HCPs to better deliver healthcare services to military health system beneficiaries.

Viability of the Borrowed Servant Doctrine

The borrowed servant doctrine is a creature of state law. If the doctrine is applied, a TI acting in the role of a special employer is vicariously liable for the negligent acts of military HCPs loaned from the general employer (the MTF) when the military trainees are supervised by the TI. One primary purpose for the development of the MTA format was to maximize coverage for military trainees using TI liability insurance and the borrowed servant defense. If the borrowed servant defense is not recognized and TIs do not independently agree to carry liability coverage, military HCPs must rely on protection under the FTCA. To the extent the state where the TI is located does not recognize the doctrine, an argument might be made that the underlying reason for requiring the model MTA format does not apply. The argument has to be made on a case-by-case basis through the request for approval of a deviation from the MEDCOM Model MTA Formats.

Comparison of Federal Tort Claims Act Protection vs Commercial Liability Insurance

Federal Tort Claims Act coverage for a military HCP is generally more advantageous than commercial liability insurance. For instance, under the FTCA, the military member is immune from liability and is no longer a defendant in the lawsuit. Commercial insurers are only liable up to the policy limit, and the military HCP is still personally liable. Thus, a reasonably well-informed military HCP trainee or a commercial insurer might demand DOJ certify the HCP is within the scope of federal employment in spite of coverage provided by commercial liability insurance.

Military HCP-trainee Duty Status

It is essential that the military HCP-trainee performing under the MTA do so in a duty status. Coverage under the FTCA is predicated on the HCP-trainee acting within the scope of his/her federal employment. DOJ advised in 1989 that it will issue scope of federal employment certifications only in those cases where the HCP-trainee took the actions subject to the complaint(s) pursuant to official orders. DOJ will not issue scope of federal employment certifications in cases where the military HCP-trainee was engaged in activity while on permissive TDY, on leave, or in some other nonduty status.

OTHER MILITARY SERVICE MEDICAL TRAINING AGREEMENTS

The Air Force and Navy published standalone directives covering affiliation agreements and MTAs (Army

terminology), or training affiliation agreements (Air Force and Navy terminology).[11,12] Those publications contain DOJ-approved model training affiliation agreement formats specific to each service.

REFERENCES

1. *Army Regulation 351-3: Professional Education and Training Programs of the Army Medical Department*. Washington, DC: US Dept of the Army; October 15, 2007.
2. 10 USC §4301.
3. 28 USC §2671-2680.
4. 28 USC §2679(d).
5. 10 USC §1089.
6. Office of The Surgeon General. Memorandum: Mission Essential Skills Augmentation/Enhancement Training. Washington, DC: US Dept of the Army; March 28, 2000.
7. *Army Federal Acquisition Regulation Supplement: Part 5101*. Washington, DC: US Dept of the Army; September 12, 2001 [rev 22]:151-152.
8. *Defense Federal Acquisition Regulation Supplement*. Washington, DC: US Dept of Defense; 1998 [update November 2011]: Subpart 237.72. Available at: www.acq.osd.mil/dpap/dars/dfars/html/r20090729/237_72.htm. Accessed November 4, 2011.
9. 10 USC §1089(f).
10. *Department of Defense Directive 6000.6: Defense of Certain Medical Malpractice Claims Against Department of Defense Healthcare Providers*. Washington, DC: US Dept of Defense; July 2, 2004 [recertified October 31, 2006]. Available at: http://www.dtic.mil/whs/directives/corres/pdf/600006p.pdf. Accessed November 4, 2011.
11. *Air Force Instruction 41-108: Training Affiliation Agreement Program*. Washington, DC: US Dept of the Air Force; May 4, 2011. Available at: http://www.e-publishing.af.mil. Accessed November 4, 2011.
12. *BUMED Instruction 7050.1B: Support Agreements*. Washington, DC: US Dept of the Navy; March 30, 2011. Available at http://www.med.navy.mil/directives/ExternalDirectives/7050.1B.pdf. Accessed November 4, 2011.

AUTHORS

Mr Deaver is Supervisory Attorney, Contract and Fiscal Law Division, Office of the Staff Judge Advocate, US Army Medical Command, Fort Sam Houston, Texas.

At the time this article was written, Ms Harris was a Legal Intern with the Office of the Staff Judge Advocate, US Army Medical Command, Fort Sam Houston, Texas.

Affiliation Agreements

David W. Claypool, JD

Generally speaking, federal agencies, including the Department of Defense (DoD) and the Army Medical Command, are prohibited by statute from accepting voluntary services. Section 1342 of Title 31 USC prohibits:

> [a]n officer or employee of the United States Government [from] … accept[ing] voluntary services … except for emergencies involving the safety of human life or the protection of property.

It is not difficult to discern the difficult questions that would arise if not for such a general prohibition. For instance: what would the status of the volunteer be; would he or she be limited to remedies provided by the Federal Employee Compensation Act (5 USC §§8101-8193) if injured on the job; what if he or she injured someone else while acting as an agent for the federal government? Moreover, on a more theoretical note, only Congress has authority to allocate resources that will be used to perform federal functions and services. This role that is reserved to the Congress would be diminished if federal officers had unbridled power to accept voluntary services.

Given the general prohibition, one might ask why it is that we see volunteers in our military treatment facilities. As with many statutory prohibitions, Congress has carved out specific exceptions to the general rule, and Army Medical Command benefits greatly from those exceptions. Section 1588 of Title 10 USC contains several exceptions that allow the military departments to accept voluntary services for a number of specific purposes, including "health care related services." (10 USC §1588(a)(1)) This article, however, deals with another narrow exception to the general prohibition; one that applies to the whole federal government and allows the Army Medical Command to participate more fully in the collegiality of the medical profession, and maybe even do a little recruiting. Section 3111 of Title 5 USC authorizes federal agencies "subject to regulations issued by the Office [of Personnel Management]" to accept voluntary service "performed by a student, with the permission of the institution at which the student is enrolled, as part of an agency program established for the purpose of providing educational experiences for the student" (para (b)(1)).

The Army Medical Command (MEDCOM) has taken advantage of the authority in 5 USC §3111 by establishing a program that permits students of accredited educational institutions to train at an Army medical facility. The vehicle by which this takes place is an affiliation agreement. The particulars of the Army's affiliation agreement program are found in chapters 15 (Affiliation Policy and Procedure) and 16 (Agreements) of *Army Regulation 351-3*.[1(pp58-69)] Since the regulation is comprehensive and reasonably short, this article is an introduction rather than an exhaustive treatment of all aspects of affiliation agreements.

Under *Army Regulation 351-3*, an affiliation agreement is a written memorandum of agreement between an Army medical facility and an accredited civilian educational institution.[1(p59)] The "student volunteers" appointed under an affiliation agreement are not federal employees. Congress has specifically addressed the questions noted earlier by designating student volunteers as employees for the purpose of workers compensation (if they are injured on the job) and federal tort claims (if they injure another) (5 USC §3111(c)(1)). Student volunteers, however, receive no other employee benefits or pay under the regulation.

The affiliation agreement may appear to represent a great opportunity to acquire no-cost, supplementary staff, but a cautionary note is appropriate here. It is important to keep in mind what this program is and what it is not. It is an opportunity to allow students to fulfill academic requirements in military treatment facilities. By allowing students this opportunity, we engage in the collegiality of the healthcare profession while also showcasing military medicine to potential future recruits or employees.[1(p59)] The affiliation agreement program is not an opportunity to supplement staff or to obtain staffing that is otherwise not authorized.[1(p59)] Title 5, Section 3111(b)(3) contains a specific prohibition against using student volunteers to displace any employee. It should also be noted that under *Army Regulation 351-3*,[1(p59)] "[a]ny work benefits derived [from an affiliation agreement] are incidental to training" and that in determining whether to enter into an affiliation agreement, facility commanders must assure that they "serve the best interest of the Army" and "do not detract from the medical mission of the Army medical facility or the education and training needs of AMEDD personnel." Programs established "for the sole benefit of the educational institution or its trainees" are specifically not authorized.

Moreover, commanders of medical treatment facilities must keep in mind that Section 3111 is an exception to a general prohibition against the acceptance of voluntary services. Any such exception should always be narrowly

interpreted, particularly so in this case since officers and employees of the US government who violate 31 USC §1342 are subject to criminal penalties under 31 USC §1350, which states that "[a]n officer or employee of the United States Government … [who] knowingly and willfully violat[es] section 1341(a) or 1342 of this title shall be fined not more than $5,000, imprisoned for not more than 2 years, or both." Therefore, care should be taken not to accept voluntary services other than in strict compliance with guidelines which implement 5 USC §3111 or 10 USC §1588. It may be instructive to note that Section 1342 immediately follows, and was enacted in tandem with Section 1341 (otherwise known as the Anti Deficiency Act). This implies that Congress attached as much importance to its prohibition of the acceptance of voluntary services as it did to its prohibition against the obligation of funds in excess of appropriations. It seems clear, therefore, that voluntary services should only be accepted in accordance with the guidelines that implement Section 3111 or 10 USC §1588. Otherwise, the protection of the exception(s) may be lost.

Memorandum of Agreement Approval and Execution

As stated above, affiliation agreements are memorialized by a memorandum of agreement (MOA) "between the educational institution and the Army medical facility."[1(p59)] Such an MOA is the only mechanism authorized for use "as the basis for the acceptance, appointment, and clinical assignment of the educational institution's trainees by the Army medical facility."[1(p59)] *Army Regulation 351-3* contains a prescribed format for an affiliation agreement MOA[1(pp61-65)] and local deviation from the prescribed format is not authorized without MEDCOM approval.[1(p59)] The regulation directs that the completed MOA "will be forwarded to reach the approving authority at least 30 days before the proposed starting date"[1(p59)] and "should be coordinated through" the staff judge advocate, civilian personnel officer, and resource management officer.[1(p59)] Although the regulation designates the commanding general of MEDCOM as the approving authority for affiliation agreements within MEDCOM, it also delegates approval authority "to commanders of Active Army medical and dental facilities … , provided the agreement is in the prescribed MEDCOM format."[1(p59)]

Once entered into, an affiliation agreement remains in effect until it is terminated by either party. Each agreement must be reviewed annually, however, "to determine whether it should remain in effect," and "[e]ither party may terminate the arrangements under this agreement by giving 30 days advance written notice of the effective date of termination." While the regulation encourages that such notice should "be given before the beginning of a training period," it recognizes that unusual circumstances may require shorter notice and specifically recognizes the right of the approving authority to terminate an agreement "at any time to meet the mission needs of the AMEDD."[1(pp59-60)]

Student Eligibility and Volunteer Status

In order to be eligible for appointment under an affiliation agreement an individual must meet the criteria and definition of a "student" under 5 USC §3111. The individual must be enrolled, at least half-time, "in a high school, trade school, technical or vocational institute, junior college, college, university, or comparable recognized educational institution" (para (a)) and have permission to participate from the educational institution at which he or she is enrolled (para (b)(1)). A break of 5 months or less between semesters does not affect the student's eligibility, so long as the "individual shows … a bona fide intention of continuing to pursue a course of study or training in the same or different educational institution during the school semester … immediately after the [break]" (para (a)).

Once selected for training, student volunteers are appointed in the same way as civil service employees. The requesting organization submits a Standard Form 52 (Request for Personnel Action) to the civilian personnel office that services the medical facility, which then uses a Standard Form 50 (Notification of Personnel Action), the same form used to appoint civil service employees, to effect the appointment.[1(p68)] The civilian personnel office also establishes an official personnel folder that contains:

- Copies of the appointment and termination Standard Form 50s.
- Copies of any license required for the category of position to which the student volunteer is appointed.
- A brief statement of the duties performed (which may be a standardized statement covering an entire trainee group).
- A record of time and attendance (which may be a format accepted by both the Army medical facility and the educational institution as long as it shows the dates and hours of training at the Army medical facility).[1(p68)]

To summarize, student volunteers are appointed using the same forms as civil service employees. As stated above, they are considered employees for the purposes of workers compensation laws, the Federal Tort Claims Act, and mass transit benefits. This is the extent of their similarity to federal employees. After appointment as

a student volunteer, the trainee serves without compensation and is not reimbursed for traveling or living expenses (see inset, Travel Expenses).[1(p59)] Student volunteers must not be used to staff a position that is a normal part of the medical treatment facility's workforce and must not displace any employee (para (b)(2)-(b)(3), 5 USC §3111; 5 CFR §308.101). Moreover, student volunteers under affiliation agreements are not "counted" as personnel, nor are positions created for them on tables of distribution and allowances.[1(p59)]

Although not employees for most purposes, student volunteers do receive a considerable amount of support in the form of close supervision. *Army Regulation 351-3* recognizes that the Army remains "responsible for health care provided in its facilities" and is mindful that student volunteers "could expose the United States to liability."[1(p59)] Therefore, it requires that student volunteers be closely "supervised by the Army medical facility staff while participating in the program" and stipulates that "[t]heir involvement in patient care will be governed by the Army medical facility's quality assurance program" under *Army Regulation 40-68*.[4]

Student volunteers may receive other kinds of support under the regulation s well. For example, the student will receive medical care for illness or injury suffered while undergoing training at an Army medical facility.[1(p68)] Army medical facilities may also provide student volunteers the following support when needed to support the training effort[1(p69)]:

- Meals, on a reimbursable basis at employee or guest rates, when the training schedule requires trainee presence during mealtime.
- Sleeping quarters in the facility during 24-hour call duty, when the training schedule requires the trainee to perform such duty.
- Transportation between Army medical facilities when required by the training schedule, but not from or to living quarters or the educational institution.
- Textbooks, supplies, and equipment required for use in training. Nonexpendable items will be hand-receipted and returned.
- Classroom, conference room, office, dressing room, locker, and storage space required for the conduct of training.

Travel Expenses

Congress has extended one other benefit to student volunteers. Public Law 107-296 amended 5 USC §3111 to specifically state that student volunteers are considered employees for the purposes of 5 USC §7905,88 the statute that authorizes mass transit benefits to offset commuting costs.[2] However, as of this writing, neither Army nor DoD regulations reflect this change. *Army Regulation 351-3* states that student volunteers are not entitled to travel benefits.[1(pp68-69)] This restriction is consistent with the eligibility criteria in the instruction that implements 5 USC §7905, *DoD Instruction 1000.27*,[3] which also specifically excludes students who provide voluntary services from eligibility for the mass transit benefits program.

Conclusion

So long as they are established for authorized reasons and in compliance with governing directives, affiliation agreements can be a useful exception to the general prohibition of the acceptance of voluntary services. They foster greater interaction between the military and civilian medical communities and serve as a recruiting opportunity, but are not a staffing opportunity. Like all other exceptions to general rules, however, they must be "handled with care." Those interested in establishing affiliation agreements should consult chapters 15 and 16 of *Army Regulation 351-3*,[1(pp58-69)] and seek advice from their servicing SJA, personnel, and training offices.

Acknowledgement

Special thanks to M. Louise Attaya, former attorney adviser at MEDCOM and author of "Affiliation Agreements," published in the 1999 *US Army Medical Command Legal Deskbook*, for providing a useful framework and knowledge used in writing this article.

References

1. *Army Regulation 351-3, Professional Education and Training Programs of the Army Medical Department.* Washington, DC: US Dept of the Army; October 15, 2007. Available at: http://www.apd.army.mil/pdffiles/r351_3.pdf.
2. The Homeland Security Act of 2002, Pub L No 107-296, Title XIII, Subtitle B, §1314.
3. *Department of Defense Instruction 1000.27: Mass Transportation Benefit Program.* Washington, DC: US Dept of Defense; October 28, 2008:13. Available at: http://www.dtic.mil/whs/directives/corres/pdf/100027p.pdf.
4. *Army Regulation 40-68: Clinical Quality Management.* Washington, DC: US Dept of the Army; February 26, 2004 [revised May 22, 2009]. Available at: http://www.apd.army.mil/pdffiles/r40_68.pdf.

Author

Mr Claypool is an Attorney Adviser, Office of the US Army Medical Command Staff Judge Advocate, Alexandria, Virginia.

Public Health Emergency Law: A Primer for Leaders and Managers in the Military

MAJ Joseph B. Topinka, JAG, USA
Ida Agamy, JD

Introduction

On March 5, 2010, the Department of Defense (DoD) reissued *DoD Instruction 6200.03, Public Health Emergency Management Within the Department of Defense*.[1] This comprehensive instruction addresses various subjects including public health emergency management roles and responsibilities for military commanders, as well as roles for military treatment facility (MTF) commanders, public health emergency officers, and MTF emergency managers. It also provides DoD guidance in accordance with applicable law. This article summarizes some of the major laws and provides a basic legal foundation for leaders and/or managers facing a public health emergency.

The Stafford Act

While this article's purpose is not to address DoD support to civil authorities, we cannot address public health legal authorities without first discussing the Robert T. Stafford Disaster Relief and Emergency Assistance Act (Stafford Act).[2] The Act allows the President to declare a major disaster or an emergency in response to an event (or threat) that overwhelms state or local government (to include a public health emergency). Ideally, the governor of a state must first respond to the disaster and execute the state's emergency plan before requesting that the President declare a major disaster or emergency, and the governor must certify that the emergency is in excess of the state's ability to handle it. But a governor's request is not necessary for the President to issue an emergency declaration if the emergency involves a federal primary responsibility, which is a situation where an emergency involves a subject area for which the United States exercises exclusive or preeminent responsibility and authority, such as a federal government building.

This declaration is vital in that it triggers access to federal disaster relief funds as appropriated by Congress, funds that can be used for many needs including:

- Public assistance, to include emergency work and permanent work to assist states, local government, and certain private, nonprofit organizations.
- Individual assistance, such as direct and financial assistance to individuals for housing and other disaster-related needs.
- Hazard mitigation to assist state and local governments to reduce the loss of life and property due to natural disasters, and enables mitigation measures to be implemented during the immediate recovery from a disaster.
- Emergency work to assist in meeting threats to life and property.
- Permanent work to repair, restore, and replace damaged facilities owned by state and local governments and eligible private nonprofit organizations.

A critical aspect of the Act is that the fund has several billion (10^9) dollars which may be immediately available for the emergency needs of state and local governments as appropriated by Congress in the Disaster Relief Fund.* Thus, from a fiscal law perspective, Disaster Relief Funds are only limited to those purposes authorized by the Stafford Act. The Act authorizes the Federal Emergency Management Agency (FEMA) to administer all disaster relief to the states.

Public Health Emergency Declaration

The Secretary of Health and Human Services can declare a public health emergency under Section 319 of the Public Health Services Act[3] (hereinafter referred to as Section 319), if the Secretary determines that:

- a disease or disorder presents a public health emergency; or

*The Stafford Act authorizes the President to issue a major disaster declaration to speed a wide range of federal aid to states determined to be overwhelmed by hurricanes or other catastrophes. Financing for the aid is appropriated to the Disaster Relief Fund (DRF), administered by the Department of Homeland Security. Funds appropriated to the DRF remain available until expended (a "no-year" account). The Stafford Act authorizes temporary housing, grants for immediate needs of families and individuals, the repair of public infrastructure, emergency communications systems, and other forms of assistance. Additional information at: http://www.fema.gov/pdf/about/stafford_act.pdf.

- a public health emergency, including significant outbreaks of infectious diseases or bioterrorist attacks, otherwise exists.

Such a broad definition gives the Secretary a great amount of flexibility. The Secretary also has the discretion to determine that a disease or condition presents a public health emergency, or a public health emergency otherwise exists, based on conditions that exist prior to the actual outbreak of disease or natural catastrophe. A public health emergency declaration lasts for 90 days, but can be terminated earlier if the Secretary determines that the emergency no longer exists. It can also be renewed by the Secretary for additional 90-day periods if the emergency persists.

A Presidential declaration under the Stafford Act and the public health declaration (PHD) under Section 319 are distinct and separate declarations, although often confused as being one and the same. One does not require the other, but in some situations, both are required in order for the Secretary to exercise certain additional authorities not otherwise provided under Section 319. For example, both a Presidential declaration under the Stafford Act (or the National Emergencies Act, 150 USC §§1621, 1631) and a PHD are required for the Secretary to waive or modify certain requirements under Section 1135 of the Social Security Act.[4] Once both are in place, the Secretary can waive or modify bed limits for critical access hospitals; and certain sanctions contained in the Emergency Medical Treatment and Active Labor Act[5] and the Health Insurance Portability and Accountability Act.[6]

In general, there is no requirement for a formal request to have such a declaration made by the Secretary. After a PHD has been issued, the Secretary has broad authority, including making grants, entering into contracts, conducting and supporting investigations, and accessing the Public Health Emergency Fund if appropriated by Congress. In addition, the Secretary has broad legal authority to provide assistance to state and local governments in the absence of a PHD, such as deploying the Strategic National Stockpile in advance of a public health emergency. Still, a PHD is a requirement for other authorities of the Secretary. One in particular involves emergency use authorization (EUA) of investigational medications. Under the Project Bioshield Act,[7] when the Secretary has made a PHD, the Food and Drug Administration may issue an EUA to allow the use of unapproved new drugs, off-label use of drugs approved for other purposes, unlicensed biological products, or medical devices not yet approved for the emergency. When the Secretary declares a PHD, the DoD "shall, to the extent practicable, act consistently with the applicable provisions of the declaration."[1(p5)]

Healthcare Labor

The Office of Personnel Management (OPM) develops regulations and federal job descriptions. They normally require a federal civilian healthcare employee to be licensed in any state. OPM determines qualifications and verifies those qualifications. Public health emergencies do not waive or preempt state licensing requirements for these employees.

The Federal Tort Claims Act (FTCA)[8] covers claims for property damage or personal injury or death caused by the negligence, wrongful act, or omission of a federal (military or civilian) employee acting within the scope of his/her employment. The FTCA coverage applies to an employee's official duties when the employee's actions in question are within the scope of employment. The FTCA does not apply to activities conducted outside the employee's official duties as a federal employee.

The Federal Employees' Compensation Act (FECA)[9] provides compensation benefits to federal civilian employees for disability due to personal injury sustained by an employee while in the performance of work-related duties. Benefits will not be paid, however, if the injury is caused by the willful misconduct or by the employee's intention to bring about his or her injury, or if intoxication is the proximate cause of the injury.

Overseas, the Foreign Claims Act[10] and the Military Claims Act,[11] as well as the North Atlantic Treaty Organization (NATO) Status of Forces Agreement (in accordance with the International Agreements Claims Act[12]) address issues of liability.

The Emergency System for Advanced Registration of Volunteer Health Professionals (ESAR-VHP)* is a system for advanced registration of healthcare providers developed by the Department of Health and Human Services to verify licensure, assign standardized credential levels, track hospital privileges, and mobilize volunteers. Registration with ESAR-VHP does not, in and of itself, constitute federal employment. Registration with ESAR-VHP does not qualify a public health professional for coverage under FTCA or FECA, and does require an additional mechanism for license reciprocity. However, upon declaration of an emergency, *DoD Instruction 6200.03*[1] does allow MTF commanders to supplement the available staff of healthcare personnel with volunteers, using information and documentation from the

*Information available at: http://www.phe.gov/esarvhp/pages/about.aspx.

ESAR-VHP. Such volunteers are considered employees of the DoD.[1(p29)]

For nonfederal employees, many states have provisions for some sort of liability protection for nonfederal healthcare providers. For example, Good Samaritan statutes may offer liability protection to healthcare workers, but differ by states in terms of breadth of coverage. The Federal Volunteer Protection Act[13] and certain state volunteer protection acts may provide liability protection for healthcare providers. The Emergency Management Assistance Compact,[14] of which all states are members, provides immunity to state officers and employees that other states share with an affected state pursuant to the compact. The Uniform Emergency Volunteer Health Practitioners Act* is a model law that addresses liability and licensing, but it has not been adopted by all states.

ISOLATION AND QUARANTINE

In general, under the police powers of the 10th Amendment to the US Constitution, the states have primary authority, including public health authority, for controlling the spread of communicable diseases within their borders. However, jurisdictional issues may arise when the spread of communicable diseases goes beyond state borders. Under Section 361 of the Public Health Services Act,[3] the Centers for Disease Control and Prevention (CDC) may apprehend, examine, detain, or conditionally release persons with certain communicable diseases that are listed by an executive order.† In addition, the CDC may apprehend and examine individuals traveling from one state into another if the CDC Director reasonably believes that such individuals may be infected with a quarantinable disease in its qualifying stage. A qualifying stage means that the disease is in a communicable stage, or a precommunicable stage, but only if the disease would be likely to cause a public health emergency if transmitted to other individuals.[15] Federal regulations governing quarantine and isolation are found in the Code of Federal Regulations at 42 CFR§§70 and 71. Part 70 governs interstate quarantine and isolation, while Part 71 deals with quarantine and isolation of foreign persons or imports into the United States or its possessions. Part 71 does not apply to isolation and quarantine in foreign lands, but rather addresses protection against the introduction, transmissions, and spread of communicable disease from foreign countries into the United States or its possessions.

In general, isolation is the separation of an individual or group infected and/or suspected to be infected with a communicable disease from those who are healthy, in such a place and manner to prevent the spread of that disease.[1(p37)] Quarantine deals with the separation of an individual or group that has been exposed to a communicable disease, but is not yet ill, from others who have not been so exposed, in such manner and place to prevent the possible spread of the communicable disease.[1(p38)] Both involve the restriction of the freedom of movement, a liberty interest protected by the due process clauses of the 5th and 14th Amendments to the US Constitution. Due process includes reasonable and adequate notice of the action that the government is taking, an opportunity to be heard on a timely basis, access to legal counsel, and review of the government's actions by an impartial decision-maker. *DoD Instruction 6200.03*[1] attempts to meet these due process requirements by ensuring that every individual or group subject to quarantine (and presumably isolation as well) is provided written notice of the reason for the quarantine and plan of examination, testing, and/or treatment designed to resolve the reason for the quarantine. The individual or group is allowed to provide information supporting an exemption or release. The military commander or designee shall review such information, and they will exercise independent judgment and promptly render a written decision on the need for the continued quarantine. Individuals and groups subject to the quarantine shall be advised that violators may be charged with a crime and subject to punishment of a fine or imprisonment for not more than one year.[16] In the case of military personnel, these potential sanctions are in addition to applicable actions by military legal authorities.

COMMAND AUTHORITY

Command authority in terms of a public health emergency has historically been a vague yet powerful concept. *DoD Instruction 6200.03*[1] has attempted to define that authority. One aspect of that authority involves the declaration of a public health emergency within the scope of the commander's authority and the implementation of relevant emergency health powers to achieve the greatest public health benefit while maintaining operational effectiveness. This authority will cover military personnel but may also include persons other than military personnel who are present on a DoD installation or in areas under DoD control. According to Enclosure 3 of *DoD Instruction 6200.03*[1(pp15-25)]:

*http://www2a.cdc.gov/phlp/docs/UEVHPA.pdf

†Federal quarantine and isolation authority is limited to those communicable diseases specified in an executive order of the President, ie, "quarantinable diseases." The most current list is found in Executive Order 13295, as amended by Executive Order 13375. These quarantinable diseases include cholera, diphtheria, infectious tuberculosis, plague, smallpox, yellow fever, viral hemorrhagic fevers, severe acute respiratory syndrome, and influenza caused by novel or reemerging influenza viruses that are causing or have the potential to cause a pandemic.

Emergency Health Powers many include:

(*a*) Collecting specimens and performing tests on any property or on any animal or disease vector, living or deceased, as reasonable and necessary for emergency response.

(*b*) Closing, directing the evacuation of, or decontaminating any asset or facility that endangers public health; decontaminating or destroying any material that endangers public health; or asserting control over any animal or disease, living or deceased, vector that endangers public health.

(*c*) Using facilities, materials, and services for purposes of communications, transportation, occupancy, fuel, food, clothing, health care, and other purposes, and controlling or restricting the distribution of commodities as reasonable and necessary for emergency response.

(*d*) Controlling evacuation routes on, and ingress and egress to and from, the affected DoD installation and/or military command.

(*e*) Taking measures to safely contain and dispose of infectious waste as may be reasonable and necessary for emergency response.

(*f*) Taking measures reasonable and necessary, pursuant to applicable law, to obtain needed health care supplies, and controlling use and distribution of such supplies.

(*g*) Directing US military personnel to submit to a medical examination and/or testing as necessary for diagnosis or treatment. Persons other than military personnel may be required as a condition of exemption or release from restrictions of movement to submit to a physical examination and/or testing as necessary to diagnose the person and prevent the transmission of a communicable disease and enhance public health and safety. Qualified personnel shall perform examinations and testing.

(*h*) Restricting movement to prevent the introduction, transmission, and spread of communicable diseases and/or any other hazardous substances that pose a threat to public health and safety. In the case of military personnel, restrictions of movement, including isolation, or any other measure necessary to prevent or limit transmitting a communicable disease and enhance public safety may be implemented. In the case of persons other than military personnel, restrictions of movement may include isolation or limiting ingress and egress to, from, or on a DoD installation and/or military command.

(*i*) Isolating individuals or groups to prevent the introduction, transmission, and spread of a communicable disease and/or any other hazardous substances that pose a threat to public health and safety. Isolation measures may be implemented in health care facilities, living quarters, or other buildings on a DoD installation and/or military command. Isolation measures do not lessen the responsibilities of the Military Health System (MHS) to provide medical care to infected and/or affected persons to the standard of care feasible given resources available.

CHALLENGES OVERSEAS

Because of the scope and variance among the laws in the various foreign countries in which the United States has military personnel, no attempt will be made here to discuss the particularities of dealing with a public health emergency in any specific country. Instead, a general overview is provided with citations to resources to assist in the creation of solid preparations and plans for a particular area of operations.

The greatest challenge for those working and stationed in foreign countries is that most of the authorities previously stated in this article do not apply. FEMA has no authority in foreign lands. There is no access to the Disaster Relief Fund (however, Overseas Humanitarian, Disaster, and Civic Assistance funds may be available to pay for humanitarian assistance operations and activities authorized by 10 USC §2651 and other authority). Information and resources are presented in the Figure.

With the possible exception of the land upon which our US embassies are situated, we typically have no "federal jurisdiction" on foreign soil. *DoD Instruction 6200.03*[1] does, however, apply to DoD facilities located both within the geographic United States and in foreign countries, but it clearly cautions that the instruction is limited in application for those outside of the United States:

> In areas outside the United States, this Instruction applies to the extent it is consistent with local conditions, and the requirements of applicable treaties, agreements, and other arrangements with foreign governments and allied forces. Implementation of these provisions at non-US installations and field activities shall require formal agreements with host-nation authorities as well as allied and coalition forces.[1(p3)]

It is, therefore, imperative for all leaders, managers, and legal advisors to be intimately familiar with the host nation's public health emergency laws, protocols, and procedures. The Department of State is the lead federal agency for requests for assistance originating outside of DoD. Commands and their public health emergency officers will closely coordinate with both the host nation authorities and the Department of State.

The following US laws and regulations do not apply on foreign soil:

- The Stafford Act, 42 USC §§5121-5207[2]
- 42 USC §5192
- 42 USC §5189e
- 42 USC §2811(b)(4)(B)
- Homeland Security Act of 2002, Pub L 107-296
- Executive Order 12148: Federal Emergency Management, July 20, 1979
- 42 USC §5170b
- 42 USC §5172
- 42 USC §311
- 44 CFR, Emergency Management and Assistance

Although not directly applicable to public health emergencies, good information and possible resources can be found by reviewing the Defense Threat Reduction Agency's Foreign Consequence Management Legal Deskbook, January 2007. Available at: http://www.dtra.mil/documents/business/current/FCMLegalDeskbook.pdf

Further Information Sources

International Law

Agreement Between the Parties to the North Atlantic Treaty Regarding the Status of their Forces, June 19, 1951 (NATO SOFA)

Agreement to Supplement the Agreement Between the Parties to the North Atlantic Treaty Regarding the Status of their Forces With Respect to Foreign Forces Stationed in the Federal Republic of Germany, August 3, 1959, revised effective March 29, 1998 (NATO SOFA Supplementary Agreement)

DoD Directive 5530.3: International Agreements, June 11, 1987, w/change 1, February 18, 1991

Chairman of the Joint Chiefs of Staff Instruction 2300.01C: International Agreements, March 15, 2006

Army Regulation 27-50: Status of Forces Policies, Procedures, and Information, December 15, 1989

Army Regulation 550-51: International Agreements, April 15, 1998

Rules for the Use of Force

Annex L (AT/FP Rules for the Use of Force) to *Army in Europe Regulation 525-13: Antiterrorism (AT)*, November 15, 2005 (pending revision)

10 USC §404 [Foreign Disaster Assistance, 2004]

10 USC §2551 [Humanitarian Assistance, 2004]

DoD Directive 6200.3: Emergency Health Powers on Military Installations, May12, 2003

Dept of the Army Installation Management Directive 6200.3: Implementation of DoD Directive 62003.3, Emergency Health Powers on Military Installations, January 27, 2004

Specific to Europe and European Command areas of responsibility, but useful for reference

US European Command Directive 5-13, International Agreements, Authorities and Responsibilities, January 27, 1994

US European Command Directive 45-3, Foreign Criminal Jurisdiction over US Personnel, March17, 2001

Army in Europe Regulation 1-3, International and Other Agreements, December 22, 2005

Army in Europe Regulation 550-50, Exercise of Foreign Criminal Jurisdiction over US Personnel, January 31, 2001

Army in Europe Regulation 550-56, Exercise of Jurisdiction by German Courts and Authorities Over US Personnel, December 11, 2009

Army in Europe Regulation 27-3, Sending State Forces Activities and Coordination, September 22, 2008

Information and resources regarding the authority and/or applicability of laws and military regulations in foreign countries.

Although there is a tendency to defer all legal issues in public health emergency law to the medical attorneys, to do so is a grave oversight. In overseas locations in particular, the scope of potential legal issues grows exponentially. Potential legal issues arising out of a broad scope public health emergency are, but are not limited to:

Contracts – failures of host nation contractors to comply with or complete contracts for fear of exposure; because of quarantine or isolation limitations; because of loss of capability due to involvement in the emergency (illness, deaths, or tasked for higher priority missions). For example, consider the implications of food

delivery to dining facilities and commissaries which is halted for any of the above reasons.

Legal Assistance – wills, powers of attorney, etc. But consider also the special requirements necessary to accommodate a sudden rise in the number of widows/widowers and orphans, abandoned property, retirees needing assistance, etc.

Labor Law – employees unable or unwilling to perform their duties; employees being required to work outside of their scope of employment; addressing volunteers, overtime, etc.

International Law – addressing issues pertaining to host nation employees; access to our installations; movement of personnel, property, etc; addressing concerns of US personnel living off installations; dealing with criminal sanctions against US personnel in host nation courts for failures to comply with host nation law.

Medical Law – examples include addressing issues of emergency health powers, emergency use authorizations, standards of care, Health Insurance Portability and Accountability Act (HIPAA)[6] and temporary waiver of HIPAA sanctions, medical malpractice, medical credentialing/privileging, etc.

Status of forces agreements (SOFAs) should be carefully reviewed to determine what language addresses public health emergencies. Article 53A of the German Supplement to the NATO SOFA, for example, provides that local, host nation, authorities may "regulate to protect health on US forces' installations." It is imperative that individuals have an advanced understanding as to how the respective host nation authorities interpret such words. Keep in mind, however, that SOFAs do not apply to US civilians not accompanying the forces (for example, expatriate US residents abroad), contractors, US civilians vacationing in the foreign country, or third country military personnel on leave (however, those on temporary duty may be covered).

Finally, perhaps the most useful resource is the International Health Regulations (IHRs),[17] developed by the World Health Assembly in 2005, which establishes an international legal framework to provide for a public health response to the international spread of disease. The IHRs constitute an international legal instrument that is binding on 194 countries across the globe, including all World Health Organization member states. The revised IHRs, which entered into force as international law on June 15, 2007, provide the legal framework to

> …prevent, protect against, control and provide a public health response to the international spread of disease in ways that are commensurate with and restricted to public health risks, and which avoid unnecessary interference with international traffic and trade.[17(p10)]

The IHRs have provisions for procedures at international airports and ports, refusal of entry quarantines, and tracing of contacts in times of emergency. Every leader and lawyer involved in public health emergency planning should avail themselves of this useful resource and determine its applicability within their host nation(s).

CONCLUSION

All leaders and managers in the DoD should be familiar with *DoD Instruction 6200.03*.[1] It is a critical tool in planning for a public health emergency. In addition, they need to have a solid understanding of the federal laws which are behind this instruction; some of which have been addressed in this article. Ultimately, reacting to a public emergency will be a team approach. The authors have some parting recommendations to leaders and managers as you plan for dealing with a public health emergency:

1. Become familiar with the CDC's *Frequently Asked Questions about Federal Public Health Emergency Law* (available at http://www2a.cdc.gov/phlp/emergencyprep/FPHELfaq.asp). It is a comprehensive collection of easily located, specific information on subjects covered in this article, and more.

2. Know your supporting legal counsel and establish a relationship early on. Train with counsel. Incorporate him/her into your exercises and your real-life situations.

3. Have a basic understanding of the legal framework both in the military and civilian environment. Even though this article has addressed federal, state, local, and, overseas legal issues, host nation issues may arise as well. In other words, what happens outside the military installation's gate must not be ignored. Cooperation with local leaders and managers in a public health emergency is critical.

4. Get the facts before making any decisions. The law is only as good as the facts to which the law is applied. Incomplete facts will result in incomplete and possibly detrimental decisions and negative public health consequences.

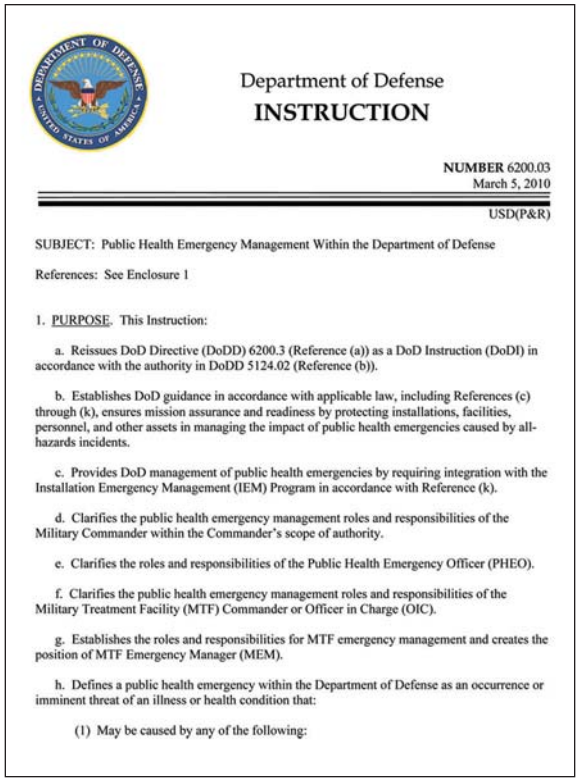
REFERENCES

1. *Department of Defense Instruction 6200.03: Public Health Emergency Management Within the Department of Defense*. Washington, DC: US Dept of Defense; March 5, 2011. Available at: http://www.dtic.mil/whs/directives/corres/pdf/620003p.pdf.
2. 42 USC §§5121-5207.
3. 42 USC §247d
4. 42 USC §1320b-5.
5. 42 USC §1395dd.
6. Pub L No 104-191, 110 Stat 1936.
7. 21 USC §360bbb-3.
8. 28 USC §§2672-2680, §1346(b).
9. 5 USC §81 et seq.
10. 10 USC §2734.
11. 10 USC §2733.
12. 10 USC §2734a, §2734b
13. 42 USC §§14501-14505.
14. Pub L No 104-321.
15. 42 USC §264.
16. 42 USC §271 as implemented by 42 CFR, Part 71.2.
17. *International Health Regulations.* 2nd ed. Geneva, Switzerland: World Health Organization; 2005. Available at: http://www.who.int/ihr/9789241596664/en/index.html. Accessed November 10, 2011.

AUTHORS

MAJ Topinka is Deputy Staff Judge Advocate, US Army Medical Command, Fort Sam Houston, Texas.

Ms Agamy is Deputy Command Judge Advocate, US Army Europe Regional Medical Command, Heidelberg, Germany.



Department of Defense
INSTRUCTION

NUMBER 6200.03
March 5, 2010
USD(P&R)

SUBJECT: Public Health Emergency Management Within the Department of Defense

References: See Enclosure 1

1. PURPOSE. This Instruction:

a. Reissues DoD Directive (DoDD) 6200.3 (Reference (a)) as a DoD Instruction (DoDI) in accordance with the authority in DoDD 5124.02 (Reference (b)).

b. Establishes DoD guidance in accordance with applicable law, including References (c) through (k), ensures mission assurance and readiness by protecting installations, facilities, personnel, and other assets in managing the impact of public health emergencies caused by all-hazards incidents.

c. Provides DoD management of public health emergencies by requiring integration with the Installation Emergency Management (IEM) Program in accordance with Reference (k).

d. Clarifies the public health emergency management roles and responsibilities of the Military Commander within the Commander's scope of authority.

e. Clarifies the roles and responsibilities of the Public Health Emergency Officer (PHEO).

f. Clarifies the public health emergency management roles and responsibilities of the Military Treatment Facility (MTF) Commander or Officer in Charge (OIC).

g. Establishes the roles and responsibilities for MTF emergency management and creates the position of MTF Emergency Manager (MEM).

h. Defines a public health emergency within the Department of Defense as an occurrence or imminent threat of an illness or health condition that:

(1) May be caused by any of the following:

Army Paralegals and Paralegal Specialists

MSG Christopher Chouinard, USA

Introduction

As the US Army Medical Command's Chief Paralegal Noncommissioned Officer, I have had the opportunity to talk and get to know a phenomenal group of Soldiers and civilian personnel who make up this command's paralegal workforce. These paralegal specialists (military occupational specialty 27D) and civilian paralegals are well educated, professional, and hard-working. Unfortunately, they are unknown to many within MEDCOM. Some of them are heroes in disguise. Some of them are heroes waiting to be challenged. In any event, these paralegals specialists and paralegals are a resource which should not be ignored and which I encourage all leaders and personnel within this command to utilize to their fullest potential.

Training and Experience

Military paralegal specialists provide valuable services, and are an integral part of the Army's legal system. They provide legal and administrative support in such diverse areas as criminal law, ethics, administrative law, contract law, fiscal law, and, yes, health law. They are highly skilled and highly trained. Paralegal specialists require 10 weeks of advanced individual training and on-the-job instruction in such matters as legal terminology, research techniques, preparing legal documents, interviewing witnesses, and transcription. By the time paralegal specialists are assigned to a medical center or a medical region, they have had years of experience and can provide in-depth legal support to MEDCOM commanders, staff, and personnel.

Paralegals, like paralegal specialists, also provide invaluable legal services in many of the same areas described earlier. However, the status of the individual specialist is based on the state in which he or she was trained. Some may have a paralegal certificate which is usually the result of a program that targets those who already possess a college degree or prior legal experience. The certificate program focuses heavily on litigation, research, writing, ethics, and legal documentation. Others may have an associate degree in applied science in paralegal studies which requires courses in civil litigation, legal research, legal analysis and writing, and ethics. These courses are supplemented by requirements determined by the student's specialization. Some of these programs require an externship in order to provide hands-on job experience in the legal field. Finally, there is the bachelor's degree in paralegal studies. This degree offers the most complete education for those with no prior experience in the legal industry. The primary advantage of a bachelor's degree program over the associate's and certificate programs is the focus on the actual execution of the skills rather than a simple understanding of the ideas and principles.

Importance of Role

Paralegal specialists and paralegals have been a mainstay in the Army Judge Advocate General's (JAG) Corps since World War II. Regardless of the type of command, they have been a multiplier that correlates to mission success. They both provide direct support to the military and civilian attorneys within the command. They very often are the "boots on the ground" representative of the Judge Advocate General and the Corps Regimental Command Sergeant Major in dealings with commanders and staff. They have the ability to function in any given environment. They have the ability to do everything that an attorney can, with the exception of practicing law. They can research any given subject. They can draft legal documentation on any given topic. The can answer complex questions.

The Future

Within the MEDCOM, over 50 civilian and military paralegals work in unison to provide MEDCOM with unparalleled support. As diverse as the practice of medicine and its many disciplines, paralegal specialists and paralegals can adapt to any scenario. As the Army Medical Command grows, the need for operational and sustained legal support will increase. The increased demand for comprehensive health law support will create a greater demand for paralegal specialist and paralegal support. It is without question that there will be a paralegal specialist or paralegal involved in each and every decision as MEDCOM becomes an even greater combat asset.

If the noncommissioned officer is the backbone of the US Army, the paralegal specialist and paralegal are the nerve that provides an electric spark which makes the JAG Corps work. MEDCOM has been graced with many professional and hardworking Paralegals that are committed to mission success. Their level of expertise and knowledge is unsurpassed and makes me proud to be part of this tremendous organization. While it is always easy to "call the lawyer," it is even easier to just call your paralegal. They are the consummate professionals and the foundation upon which the Army Judge Advocate General's Corps is built.

The Judge Advocate General's Corps of the United States Army

The Judge Advocate General's Corps of the United States Army is composed of Army officers who are lawyers and who provide legal services to the Army at all levels of command. The Judge Advocate General's Legal Service includes judge advocates, warrant officers, paralegal noncommissioned officers and junior enlisted personnel, and civilian employees. The Judge Advocate General is a lieutenant general. All military officers are appointed by the US President subject to the advice and consent of the Senate, but the Judge Advocate General is one of the few positions in the Army explicitly provided for by law in Title 10 of the United States Code and which requires a distinct appointment.

The Judge Advocate General

General George Washington founded the US Army JAG Corps on July 29, 1775, with the appointment of William Tudor as the Judge Advocate General. The Army Judge Advocate General's Corps is the oldest of the judge advocate communities in the US armed forces, as well as the oldest "law firm" in the United States. The Judge Advocate General serves a term of 4 years. LTG Dana K. Chipman, appointed in October 2009, is the 38th Judge Advocate General of the Army.

Mission

Judge advocates serve in the position of Staff Judge Advocate on the special and personal staff of general officers in command who are general court-martial convening authorities (the authority to convene a general court-martial). Staff Judge Advocates advise commanders on the full range of legal matters encountered in government legal practice and provide advice on courts-martial as required by the Uniform Code of Military Justice. Subordinate judge advocates prosecute courts-martial, and others, assigned to the independent US Army Trial Defense Service and US Army Trial Judiciary, serve as defense counsel and judges. The almost 2,000 full-time judge advocates and civilian attorneys who serve The Judge Advocate General's Corps comprise the largest group of attorneys who serve the US Army. Several hundred other attorneys practice under the Chief Counsel of the United States Army Corps of Engineers and the Command Counsel of the United States Army Materiel Command.

Judge advocates are deployed throughout the United States and around the world, including Japan, South Korea, Germany, Kosovo, Iraq, Afghanistan, Kuwait, and Qatar. They provide legal assistance to soldiers, adjudicate claims against the Army, advise commands on targeting decisions and other aspects of operational law, and assist the command in administering military justice by preparing nonjudicial punishment actions, administrative separation actions, and trying criminal cases at court-martial.

In addition to the active component judge advocates, there are approximately 5,000 attorneys who serve in the US Army Reserve and the Army National Guard. Several hundred Reserve and National Guard attorneys have left their civilian practices to serve in support of Operations Iraqi Freedom and Enduring Freedom.

Legal Center and School

The Judge Advocate General's School began in World War II at the University of Michigan to train new judge advocates as the Judge Advocate General's Department rapidly expanded. It was disestablished for a short time after the war. It was then reestablished at Fort Myer in Arlington, Virginia, but, after a short stay, was relocated to the University of Virginia in Charlottesville in 1951. The Judge Advocate General's Legal Center and School adjoins, but is distinct from, the University of Virginia School of Law. The Commandant of the Judge Advocate General's School is authorized by Congress to award a Master of Laws degree. The school is the only federal institution to have American Bar Association accreditation as an America's law schools. Judge Advocates from all 5 armed forces of the United States and international students attend the annual Judge Advocate Officer Graduate Course in which the Master's degree is awarded. The Legal Center and School also trains the Army's new judge advocates, provides continuing legal education for judge advocates and lawyers from throughout the United States government, and trains the Army's paralegal noncommissioned officers and court reporters. The School trains those officers appointed military judges, irrespective of service.

Insignia

The branch insignia consists of a gold pen crossed above a gold sword, superimposed over a laurel wreath. The pen signifies the recording of testimony, the sword represents the military character of the JAG Corps, and the wreath indicates honor. The insignia was created in May 1890 in silver and changed to gold in 1899.

The US Army Medical Department Regiment

The US Army Medical Department was formed on July 27, 1775, when the Continental Congress authorized a Medical Service for an army of 20,000 men. It created the Hospital Department and named Dr Benjamin Church of Boston as Director General and Chief Physician. On 14 April, 1818 the Congress passed an Act which reorganized the staff departments of the Army. The Act provided for a Medical Department to be headed by a Surgeon General. Dr Joseph Lovell, appointed Surgeon General of the United States Army in April 1818, was the first to hold this position in the new organization. The passage of this law marks the beginning of the modern Medical Department of the United States Army.

Throughout its early history, the size and mission of the US Army Medical Department would wax and wane in response to military events around the world. There was, however, no formal regimental organization until World War I. Then, in the late 1950s, the brigade replaced the regiment as a tactical unit. In the reorganization that followed, some Army units lost their identity, their lineage, their history. This loss did not go unnoticed. The US Army Regimental System was created in 1981 to provide soldiers with continuous identification with a single regiment. Department of the Army Regulation 600-82, The US Army Regimental System, states the mission of the regiment is to enhance combat effectiveness through a framework that provides the opportunity for affiliation, develops loyalty and commitment, fosters a sense of belonging, improves unit esprit, and institutionalizes the war-fighting ethos.

The US Army Medical Department Regiment was activated on July 28, 1986, during ceremonies at Fort Sam Houston in San Antonio, Texas, the "Home of Army Medicine." Lieutenant General Quinn H. Becker, the US Army Surgeon General and AMEDD Regimental Commander, was the reviewing officer. He was joined by general officers of the US Army Reserves and the Army National Guard, representing the significant contributions and manpower of the reserve forces in the Total Army concept.

Insignia

The AMEDD Regimental Distinctive Insignia was designed by the Institute of Heraldry and is one of the oldest crests In the Army today. The 20 stars on the crest correspond to the number of states in the Union between December 10, 1817, and December 3, 1818. The origin of the crest dates from the Act of April 14, 1818, by which the Medical Department of the Army was first organized.

The alternating red and white stripes on the left side of the shield are the 13 stripes of the American Flag. The green staff is the staff of Asclepius (according to Greek mythology, the first healer, the son of Apollo, the sun god); and green was a color associated with the Medical Corps during the last half of the 19th century. The phrase "To Conserve Fighting Strength" gives testimony to our mission as combat multipliers and guardians of our Nation's strength and peace.

Information

The Regimental web site (http://ameddregiment.amedd.army.mil/default.asp) is designed to provide you with useful information about the US Army Medical Department (AMEDD) Regiment. Through the web site, you can learn the history of the AMEDD Regiment, the symbolism behind our heraldic items, how to wear the Regimental Distinctive insignia, and various programs available to you and your unit.

The Office of the AMEDD Regiment is located in Aabel Hall, Building 2840, on Fort Sam Houston, Texas. The Regimental staff can provide further information pertaining to the history of the Army Medical Department and the AMEDD Regiment, and assist with any of the services described in the web page.

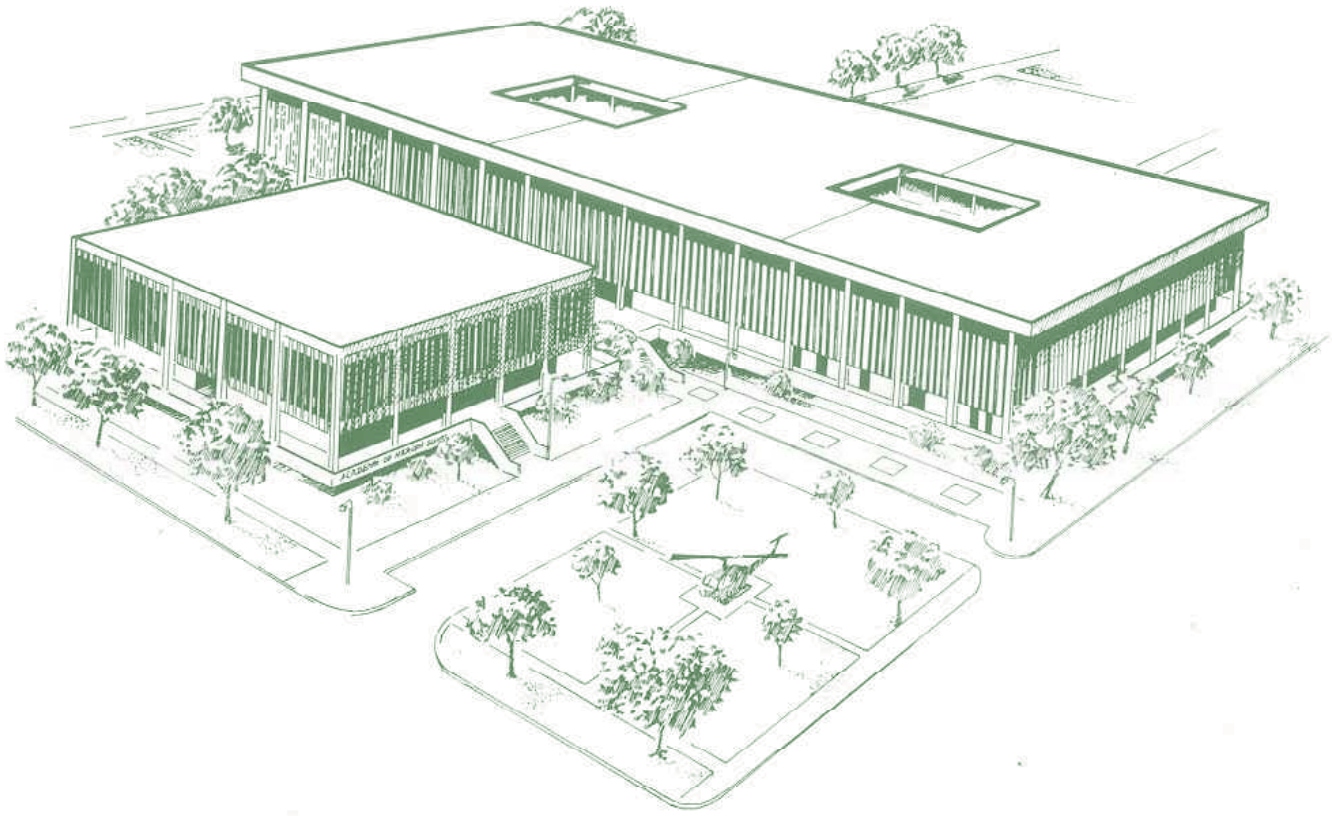
For additional information please contact the Army Medical Department Regimental Office at the following address:

Commander
US Army Medical Department Regiment
ATTN: MCCS-GAR
2250 Stanley Road
Fort Sam Houston, Texas 78234-6100

The telephone number is (210) 221-8455 or DSN 471-8455, fax 8697.

Internet: http://ameddregiment.amedd.army.mil/

Email: amedd.regiment@amedd.army.mil



The headquarters and primary instructional facility of the Army Medical Department Center and School, located on the Military Medical Education and Training Campus, Fort Sam Houston, Texas.

SUBMISSION OF MANUSCRIPTS TO THE *ARMY MEDICAL DEPARTMENT JOURNAL*

The *United States Army Medical Department Journal* is published quarterly to expand knowledge of domestic and international military medical issues and technological advances; promote collaborative partnerships among the Services, components, Corps, and specialties; convey clinical and health service support information; and provide a professional, high quality, peer reviewed print medium to encourage dialogue concerning health care issues and initiatives.

REVIEW POLICY

All manuscripts will be reviewed by the *AMEDD Journal*'s Editorial Review Board and, if required, forwarded to the appropriate subject matter expert for further review and assessment.

IDENTIFICATION OF POTENTIAL CONFLICTS OF INTEREST

1. **Related to individual authors' commitments:** Each author is responsible for the full disclosure of all financial and personal relationships that might bias the work or information presented in the manuscript. To prevent ambiguity, authors must state explicitly whether potential conflicts do or do not exist. Authors should do so in the manuscript on a conflict-of-interest notification section on the title page, providing additional detail, if necessary, in a cover letter that accompanies the manuscript.
2. **Assistance:** Authors should identify Individuals who provide writing or other assistance and disclose the funding source for this assistance, if any.
3. **Investigators:** Potential conflicts must be disclosed to study participants. Authors must clearly state whether they have done so in the manuscript.
4. **Related to project support:** Authors should describe the role of the study sponsor, if any, in study design; collection, analysis, and interpretation of data; writing the report; and the decision to submit the report for publication. If the supporting source had no such involvement, the authors should so state.

PROTECTION OF HUMAN SUBJECTS AND ANIMALS IN RESEARCH

When reporting experiments on human subjects, authors must indicate whether the procedures followed were in accordance with the ethical standards of the responsible committee on human experimentation (institutional and national) and with the Helsinki Declaration of 1975, as revised in 2000. If doubt exists whether the research was conducted in accordance with the Helsinki Declaration, the authors must explain the rationale for their approach and demonstrate that the institutional review body explicitly approved the doubtful aspects of the study. When reporting experiments on animals, authors should indicate whether the institutional and national guide for the care and use of laboratory animals was followed.

INFORMED CONSENT

Identifying information, including names, initials, or hospital numbers, should not be published in written descriptions, photographs, or pedigrees unless the information is essential for scientific purposes and the patient (or parent or guardian) gives written informed consent for publication. Informed consent for this purpose requires that an identifiable patient be shown the manuscript to be published. Authors should disclose to these patients whether any potential identifiable material might be available via the Internet as well as in print after publication. Patient consent should be written and archived, either with the *Journal*, the authors, or both, as dictated by local regulations or laws.

GUIDELINES FOR MANUSCRIPT SUBMISSIONS

1. Articles should be submitted in digital format (preferably an MS Word document on CD or floppy disk) with one printed copy of the manuscript. Ideally, a manuscript should be no longer than 24 double-spaced pages. However, exceptions will always be considered on a case-by-case basis.
2. The *American Medical Association Manual of Style* governs formatting in the preparation of text and references. All articles should conform to those guidelines as closely as possible. Abbreviations/acronyms should be limited as much as possible. Inclusion of a list of article acronyms and abbreviations can be very helpful in the review process and is strongly encouraged.
3. A complete list of references cited in the article must be provided with the manuscript, with the following required data:
   - Reference citations of published articles must include the authors' surnames and initials, article title, publication title, year of publication, volume, and page numbers.
   - Reference citations of books must include the authors' surnames and initials, book title, volume and/or edition if appropriate, place of publication, publisher, year of copyright, and specific page numbers if cited.
   - Reference citations for presentations, unpublished papers, conferences, symposia, etc, must include as much identifying information as possible (location, dates, presenters, sponsors, titles).
4. Either color or black and white photographs may be submitted with the manuscript. Color produces the best print reproduction quality, but please avoid excessive use of multiple colors and shading. Digital graphic formats (JPG, GIF, BMP) and MS Word photo files are preferred. Prints of photographs are acceptable. Please do not send photos embedded in PowerPoint. Images submitted on slides, negatives, or copies of X-ray film will not be published. For clarity, please mark the top of each photographic print on the back. Tape captions to the back of photos or submit them on a separate sheet. Ensure captions and photos are indexed to each other. Clearly indicate the desired position of each photo within the manuscript.
5. The authors' names, ranks or academic/certification credentials, titles or positions, current unit of assignment, and contact information must be included on the title page of the manuscript.
6. Submit manuscripts to:

EDITOR, AMEDD JOURNAL
AHS CDD BLDG 4011
2377 GREELEY RD STE T
FORT SAM HOUSTON, TX 78234-7584

DSN 471-6301
Comm 210-221-6301
Email: amedd.journal@amedd.army.mil

PIN: 10242-000