DEPARTMENT OF THE NAVY
BUREAU OF MEDICINE AND SURGERY
2300 E STREET NW
WASHINGTON DC 20372-5300

IN REPLY REFER TO
BUMEDINST 5370.4
BUMED-M82
1 Apr 2010

BUMED INSTRUCTION 5370.4

From: Chief, Bureau of Medicine and Surgery

Subj: NAVY MEDICINE ANTI-FRAUD PROGRAM

Ref: (a) DoD Instruction 5505.12 of 19 Oct 2006
(b) BUMEDINST 5200.13A
(c) BUMEDINST 4200.2B
(d) NAVSUPINST 4205.3C
(e) SECNAVINST 5430.92B
(f) 48 CFR § 3.104-1-9
(g) BUMEDINST 6320.66E
(h) BUMEDINST 6320.67A
(i) BUMEDINST 5370.3
(j) DoD Instruction 5505.2 of 6 Feb 2003
(k) DoD Directive 5500.7 of 29 Nov 2007
(l) SECNAV M-5214-1 of DEC 2005

Encl: (1) Appendix A: Preventing and Detecting Fraud on Contracts
(2) Appendix B: Preventing and Detecting Fraud in Other Key Programs
(3) Acronyms
(4) Definitions
(5) Anti-Fraud Resources
(6) Sample Referral Letter to TRICARE Management Activity Program Integrity Office

1. Purpose. To direct Navy Medicine commands to establish safeguards to prevent, detect, and report fraud. This instruction documents existing anti-fraud efforts and initiates new and enhanced efforts to implement reference (a) at Navy Medicine Medical Treatment Facilities (MTFs).

2. Applicability. Applies to all Navy Medicine commands.

3. Background

a. Fraud is any willful means of taking or attempting to take unfair advantage of the government, including but not limited to:

(1) The offer, payment, or acceptance of bribes or gratuities.

(2) Making of false statements, submission of false claims, or use of false weights or measures.

(3) Evasion or corruption of inspectors and other officials.

(4) Deceit by suppression of the truth or misrepresentation of a material fact.

(5) Adulteration or substitution of material.

(6) Falsification of records or accounts.

(7) Arrangements for secret profits, kickbacks, or commissions.

(8) Cases of conflict of interest, criminal irregularities, and unauthorized disclosure of official information connected with acquisition and disposal matters.

(9) Conspiracy to use any of these devices.

b. Navy Medicine is susceptible to fraud committed by government personnel (civilian and military), contractors, vendors, patients, or other outside parties.

c. Reference (b) directs commanders, commanding officers (COs), and officers in charge (OICs) within Navy Medicine to develop and maintain effective internal controls across their areas of responsibility (AOR). A system of effective internal controls is the basis for efforts to detect and prevent fraud. References (c) and (d) identify safeguards required to effectively monitor contracts for fraud. Reference (e) defines acquisition fraud and outlines policies and procedures for reporting suspected cases. Reference (f) identifies practices that may constitute acquisition fraud and required preventative and corrective actions. Reference (g) outlines credentialing and privileging policies and procedures. Reference (h) describes adverse privileging actions, peer review panel and reporting procedures that may be used for health care providers suspected of misconduct. Reference (i) outlines Navy Medical Inspector General (MEDINSGEN) responsibilities for implementing and sustaining a Hotline Program for reporting suspected fraud. Reference (j) outlines roles and responsibilities for investigating fraud. Reference (k) outlines the responsibility of all Department of Defense (DoD) employees to perform their official duties in an ethical manner and avoid any actions that may constitute fraud. Enclosures (1) and (2) provide examples of preventative and detective controls. Enclosures (3) and (4) provide clarification.

4. Policy. Fraud directly threatens our core mission of providing high-quality, economical health care to eligible beneficiaries. As such, all personnel within Navy Medicine must maintain constant vigilance to identify and report suspected fraud. Commanders, COs, and OICs must establish a tone across their AOR that fraud, regardless of magnitude, will not be tolerated. Accordingly, each command in Navy Medicine must develop an anti-fraud program that includes the following elements:

a. Fraud Risk Management Program. Each command must formally document its anti-fraud assets and efforts, including:

(1) A high-level command statement outlining the responsibility of all personnel to monitor against and prevent fraud (e.g., code of conduct, command policy, commander's note).

(2) The process for monitoring, reporting, and investigating fraud, with clearly defined roles and responsibilities.

(3) An anti-fraud program manager, appointed by the commander, CO, or OIC.

(4) Appropriate anti-fraud training.

(5) Processes to promote fraud awareness among staff and outside parties (including vendors, patients, etc).

(6) Identification of available remedial actions when fraud occurs (e.g., criminal, civil and administrative penalties).

(7) Regular and active involvement of command senior leadership, including the Executive Steering Committee (ESC), on fraud issues and corrective actions.

b. Periodic Fraud Risk Assessment. A command's mission, size, complexity, organizational structure, and resources help determine its vulnerability to fraud. These factors differ at each command and vary over time. Periodically, but at least annually, each Navy Medicine command must assess and document its own fraud risk. Assessing fraud risk allows commands to focus internal control efforts where the likelihood and/or impact of fraud is greatest. Since prevention of fraud is one of the key objectives of internal controls, the fraud risk assessment should be a subset of a comprehensive internal control risk assessment.

(1) Information for this assessment can come from:

(a) Inspector General (IG) inspections and Hotline reports.

(b) Managers' Internal Control Program (MICP) assessments.

(c) Command Evaluation Program and other internal reviews.

(d) External audits, reports, and studies.

(e) Commanders, COs, and OICs and/or management observations and judgment.

(2) The assessment should identify the:

(a) Overall incentives, opportunities, and pressures to commit fraud.

(b) Programs where ineffective or nonexistent internal controls create opportunities for fraud.

(c) Likelihood and impact of fraud within those programs.

c. Prevention Techniques. An effective system of internal controls is the best means to prevent fraud. Although fraud of any magnitude negatively impacts mission accomplishment, each command must determine an acceptable level of risk and develop internal controls accordingly. Preventative controls must be focused on areas where the likelihood and/or impact of fraud is highest. Preventative controls can include policies, procedures, training, and communication. Examples of preventative controls can be found in enclosures (1) and (2).

d. Detection Techniques. For certain types of fraud, it is more effective to detect and address fraud after it occurs rather than trying to prevent it before it occurs. Detective controls are most effective for areas where the likelihood of fraud is low but potential impact is severe. They can also help assess the effectiveness of preventative controls. Detective controls are often clandestine in nature, to ensure they are not easily circumvented.

(1) Examples of detective controls can be found in enclosures (1) and (2). Other examples include:

(a) Unannounced inventory inspections.

(b) Reconciling accounting transactions with supporting documentation at random intervals.

(c) Ad hoc audits and analyses.

(d) Data mining.

(e) Automated system flags (e.g., disbursements over a certain dollar amount, excessive number of purchase card transactions to a single vendor).

(2) Potential fraud may also be detected during the course of internal reviews (including the command evaluation program) and external audits (e.g., IG inspections, Naval Audit Service audits).

e. Reporting, Investigative, and Corrective Action Process

(1) Navy Medicine personnel will report all suspected fraud for further analysis and investigation. If there is any doubt on whether or not something constitutes fraud, the incident should be reported. Enclosure (5) outlines the process for reporting potential fraud.

(2) Authorized IG investigators will evaluate all allegations of fraud and, if warranted, conduct a formal investigation, and consult with Command Counsel and/or Staff Judge Advocates as appropriate. References (i) and (j) will guide investigation of all fraud allegations reported to the MEDINSGEN Hotlines.

(3) Appropriate corrective action in response to substantive instances of fraud helps send a clear message across the organization that fraud will not be tolerated. That tone can help prevent fraud from occurring. Corrective action can include:

(a) Referral to law enforcement authorities for criminal or civil prosecution.

(b) Disciplinary action (e.g., termination, suspension, demotion, reassignment, reprimand, or counseling).

(c) Denied, reduced, suspended, or revoked privileging of health care providers for suspected misconduct (including fraud).

(d) Contract termination (in cases of acquisition fraud).

(e) Recommending Department of the Navy (DON) Acquisition Integrity Office (AIO) debarment of vendors who are suspected of committing fraud.

(f) Referring contract providers suspected of fraud to the TRICARE Management Activity (TMA) Program Integrity Office (see enclosure (6)).

(4) All substantive cases of fraud should trigger an analysis of the existence and effectiveness of associated preventative and detective internal controls. Systemic internal control failures should be reported, as appropriate, through the MICP.

(5) In addition to action against the perpetrators of fraud, the organization itself must undergo corrective action. This may include business process reengineering, revised policies and procedures, and/or enhanced internal controls. The ESC should be involved with all organizational corrective actions.

5. Responsibilities

a. Navy Medicine Regional Commanders will:

(1) Ensure compliance with this instruction across their AOR.

(2) Ensure practitioners assigned to fixed MTFs within their AOR are privileged per reference (g).

(3) Establish processes to prevent privileging of providers sanctioned by Department of Health and Human Services (HHS) and/or TMA.

b. Navy Medicine Support Command via Naval Medical Logistics Command (NMLC), will:

(1) Incorporate anti-fraud curriculum into the Contracting Officer's Representative (COR) training course.

(2) Prior to awarding a medical service contract:

(a) Verify that the company is not sanctioned by HHS or TMA, if the contract is with a company that provides health care workers.

(b) Verify that the individual provider is not sanctioned by HHS or TMA, for individual set aside (ISA) contracts.

(3) Prior to contract award, verify that the vendor is not in the Excluded Party List System (EPLS).

c. Commanders, COs, and OICs will:

(1) Formally establish and document a culture across their AOR that fosters constant vigilance against fraud, protects those who report fraud, and demands appropriate corrective action when fraud occurs.

(2) Implement a system of effective internal controls to detect and prevent fraud across the programs with the highest level of risk.

(3) Ensure full cooperation with all fraud investigations.

(4) Develop a comprehensive remedies plan, with appropriate corrective and disciplinary action, for all substantive fraud cases within their AOR.

(5) Review substantive cases of fraud for systemic internal control deficiencies and report, as appropriate, in the annual MICP Statement of Assurance (SOA), per reference (b).

(6) Appoint an Anti-Fraud Program Manager, from within the command's IG staff, to advise the command on anti-fraud matters.

(7) Ensure personnel complete mandatory annual anti-fraud training.

(8) Ensure full compliance with this instruction within their AOR.

d. All Navy Medicine Personnel (military and civilian) will:

(1) Exercise due diligence in monitoring for fraud.

(2) Report suspected fraud per this instruction.

(3) Complete mandatory annual anti-fraud training.

e. MTFs will: Ensure contract health care workers operating under definitive agency contracts (as defined in reference (c)), indefinite delivery indefinite quantity (IDIQ) contracts, clinical support agreements (CSAs), and blanket purchase agreements (BPAs) are not sanctioned by either TMA or HHS, prior to the workers coming onboard.

f. MEDINSGEN/Command IG Personnel will:

(1) Manage the Anti-Fraud Program within their respective AOR.

(2) Monitor Navy Medicine compliance with this instruction through command inspections.

(3) Establish and maintain a Hotline program, per reference (i), as a resource for reporting potential fraud.

(4) Develop and publicize Hotline fraud reporting procedures (e.g., command Web site, posters, and newsletters).

(5) Evaluate and report on the existence and effectiveness of internal controls designed to prevent and detect fraud through command inspections.

(6) Investigate substantive allegations of fraud in a timely and impartial manner, pursue corrective measures per applicable laws, regulations, directives, and instructions, and report the results of such investigations to law enforcement authorities, per reference (j), as appropriate.

(7) Report all substantive allegations of fraud involving health care providers working at Navy MTFs to the TMA Program Integrity Office, using the sample referral letter at enclosure (6). Provide documentation, as requested, to the Program Integrity Office.

(8) Provide an annual report to the commander, CO, or OIC, no later than 30 April, of all substantive fraud cases within the AOR.

g. The Anti-Fraud Program Manager will:

(1) Serve as senior advisor to management on fraud issues.

(2) Develop and implement initiatives to promote awareness across the AOR of means to detect, prevent, and report fraud.

(3) Provide periodic updates to the ESC (or equivalent) on fraud issues within the AOR.

(4) *(Echelon 2 Anti-Fraud Program Manager only)* Provide anti-fraud course content requirements to NMLC for inclusion in the COR training course.

(5) (*Echelon 2 Anti-Fraud Program Manager only)* Develop anti-fraud training for all Navy Medicine personnel in MTF and non-MTF-environments. Anti-fraud training should include, at a minimum:

(a) Legal definition of fraud.

(b) Areas of greatest fraud vulnerability within Navy Medicine.

(c) Responsibility of all personnel to monitor for and report suspected fraud.

(d) Signs of fraud.

(e) Ways to detect and prevent fraud.

(f) Ways to report suspected fraud.

(g) Potential criminal, civil, and administrative consequences of fraud.

(6) (*Echelon 3 and below Anti-Fraud Program Managers)* Supplement anti-fraud training curriculum with additional content, as needed, to address local anti-fraud training requirements.

h. Command Counsel and/or Staff Judge Advocates will:

(1) Perform a legal review on all investigations of fraud of a significant nature (e.g., cases resulting in disciplinary action, detachment for cause, or substantial monetary loss).

(2) Serve as liaison to the DON AIO on acquisition fraud matters, per reference (e).

(3) Provide oversight and guidance on medico-legal aspects of the credentials review and privileging program with an emphasis on adverse privileging actions per reference (g), incidents of reportable misconduct, and separation or termination of employment due to disability of health care providers.

(4) Provide legal opinions on ethics standards of conduct issues, including gifts of travel, fundraising, relations with and support to nonfederal entities, use of government resources, conflicts of interest, government travel and transportation, political activities, and post-government employment. Review required financial disclosure reports.

i. The Bureau of Medicine and Surgery (BUMED) Deputy Chief for Resource Management/Comptroller (M8) will:

(1) Develop a methodology to monitor Navy Medicine compliance with this instruction through the MICP.

(2) Evaluate and report on the existence and effectiveness of internal controls designed to prevent and detect fraud through the MICP.

(3) Use the MICP to monitor programs across Navy Medicine with the greatest potential for fraud.

j. Comptrollers will:

(1) Review the adequacy of internal controls within accounting, budget, and financial systems to prevent and detect fraud.

(2) Report any significant internal control deficiencies through the annual SOA for the Federal Managers' Financial Integrity Act (FMFIA) overall process or FMFIA over financial reporting process, as appropriate.

k. CORs, Alternate Contracting Officer's Representatives (ACORs), and Technical Liaisons (TLs). CORs, ACORs, and TLs will follow the guidance in reference (c) and conduct due diligence in monitoring their assigned contracts for potential fraud. Additional steps to prevent and detect fraud on contracts can be found at enclosure (1).

6. Forms

a. DD Form 1173 (MAR 61), Uniformed Services Identification and Privilege Card, is a specialty form. It can be ordered using stock number 0102LF0042900 from Naval Forms Online at: https://forms.daps.dla.mil/order/.

b. DD Form 1173-1 (JUL 89), Department of Defense Guard and Reserve Family Member Identification Card, is a specialty form. It can be ordered using stock number 0102LF0085000 from Naval Forms Online at: https://forms.daps.dla.mil/order/.

c. NAVCOMPT Form 2282 (2-83), Overtime/Compensatory Time Request and Authorization, is available electronically from Naval Forms Online at: https://navalforms.daps.dla.mil/web/public/home.

7. Reports. The reporting requirements contained within this instruction are exempt from reports controlled per Part IV, paragraph 7k of reference (l).

A. M. Robinson, Jr.

A. M. ROBINSON, JR.

Distribution is electronic only via the Navy Medicine Web site:
http://www.med.navy.mil/directives/Pages/BUMEDDirectives.aspx

APPENDIX A
PREVENTING AND DETECTING FRAUD ON CONTRACTS

1. Navy Medicine relies on contracts to obtain goods and services essential to our mission in a cost-effective manner. Contracts also create opportunities for fraud. Unless otherwise directed by their contract administration plan (CAP) or contracting officer (KO), CORs, ACORs, and TLs will monitor their assigned contracts for potential fraud as follows:

a. Monitor contractor performance and reporting any potential fraud to the KO and other parties as detailed in enclosure (5), including:

(1) Upcoding actual services rendered (i.e., documenting higher level of service than those rendered).

(2) Billing for services rendered by MTF personnel.

(3) Using unauthorized or non-licensed staff to render care but representing services as being performed by authorized and licensed staff.

(4) Referral of MTF patients to own civilian practice.

(5) Invoicing for services in excess of those that could be reasonably accomplished (e.g., a contract employee billing for more than 24 hours of service in one day).

b. Review contractor invoices to ensure appropriateness of types and quantities of services being performed (i.e., are services performed reasonable and necessary?).

c. Notify the KO of anticipated and actual variance between quantity ordered and quantity delivered/performed.

d. Monitor the use of government furnished equipment (GFE), government furnished material (GFM) and government furnished property (GFP) in the possession of contractors to ensure use is per the terms of the contract. Contractor use of GFE, GFM, or GFP for uses outside the scope of the contract may constitute fraud (e.g., a contract radiologist using an MTF X-ray facility for private practice patients).

e. Inspect the credentials of contract employees to ensure they are accurate and current. Track expiring credentials to ensure contract compliance.

f. Comply with standards of conduct and avoid conflicts of interest as set forth in reference (k).

g. Reject any items of cost not specifically authorized by the contract or not in conformance with the terms of the contract (e.g., goods or services outside the scope of the contract, hours billed but not worked, goods or services billed but not received, substandard goods received).

h. Review the TMA Sanctioned Provider List and HHS, Office of Inspector General (OIG) Exclusion Program list (available online, with current links at enclosure (5)) and disallow payment to providers on either list.

i. Identify any irregularities in contractor performance in the annual report to the KO per the CAP, and to the chain of command and/or IG upon discovery.

2. Executive Committees of the Medical Staff (ECOMS) and Executive Committees of the Dental Staff (ECODS), through Medical Staff Services Professionals (MSSPs), will verify the licensure and credentialing of each contract health care provider prior to privileging, per reference (f). Education should be primary source verified at time of accession. Licensure should be verified and documented every time the license is renewed or privileges are granted.

3. Ways to detect and prevent fraud on contracts:

a. Ensure segregation of duties for contract award, receipt, inspection, acceptance, and funds certification.

b. Perform periodic physical inventory of high risk items (e.g., high dollar value, pilferables, controlled substances) and reconcile against receiving reports and inventory records.

c. CORs should only accept goods and services on behalf of the government when they have adequate documentation indicating that the government received those goods and services.

d. Periodically review certified receiving reports on medical service contracts to ensure payments are not being made to sanctioned providers.

e. Reconcile Centralized Credentials Quality Assurance System (CCQAS) against the TMA and HHS sanction lists to ensure currently privileged providers have not been sanctioned. This can be done by:

(1) Receiving updates to the sanction lists and ensuring newly sanctioned providers do not show up as licensed or credentialed in CCQAS.

(2) Using random sampling to cross check active providers at the activity against CCQAS and the sanction lists.

f. Maximize primary source verification of credentials.

APPENDIX B
PREVENTING AND DETECTING FRAUD IN OTHER KEY PROGRAMS

1. Enterprise-Wide Anti-Fraud Efforts

a. Posters raising awareness of fraud and explaining how to report it (i.e., command IG Hotline).

b. Periodic e-mails or newsletters identifying specific types of fraud that may be or are occurring at the command, along with preventative/detective techniques.

c. Developing an effective system of internal controls designed to prevent and detect fraud and formally implementing those controls through policies, standard operating procedures (SOPs), and day-to-day business practices.

d. Ensure grade/rank of personnel conducting evaluations or oversight is appropriate for assigned duties (i.e., do not have an E-4 managing an in-depth travel expense audit on an O-6).

e. Make sure personnel responsible for oversight are themselves the subject of oversight – they can be a command's greatest asset in preventing fraud or its greatest liability.

2. Grants *(applicable only to Naval Medical Research Center activities)*

a. Require grantees to sign a certification statement declaring that the statements it makes in its grant application are true and correct and that any false statements made as a part of the certification can be prosecuted.

(1) If applicable, the grantee should be required to certify the completeness and accuracy of any data submitted in carrying out its grant activities.

(2) In lieu of using a generic certification for all grants, customize the certification statement to highlight specific requirements for each grant.

(3) If appropriate, require continuing certifications throughout the award period (i.e., in addition to the certification at the time of award), especially if supplemental funds are awarded.

b. Ensure the grantee provides all required deliverables (e.g., financial and progress reports) in a timely manner. Review reports to ensure performance is per the provisions of the grant, the grantee is meeting all required performance measures and there are no unusual or suspicious expenditures.

c. Promote anti-fraud awareness among grantees. This may include briefings, training sessions, workshops, bulletins, etc.

d. Include grant fraud content in the general anti-fraud course to target grant administrators.

e. Ensure grantees are aware of the Navy Medicine resources available for reporting fraud (e.g., IG hotline).

f. Maximize transparency over grant programs. This may include publishing grant awards and grantee progress reports on public Web sites.

g. Share information with other grant awarding agencies (e.g., medical research commands at other service medical activities) on problem grantees, reported cases of grant fraud, etc.

3. Information Technology

a. Review access that personnel have to key systems (e.g., Standardized Accounting and Reporting System - Field Level (STARS-FL), Composite Health Care System (CHCS), Armed Forces Health Longitudinal Technology Application (AHLTA), Wide Area Work Flow - Receipt and Acceptance (WAWF-RA), Standard Labor Data Collection and Distribution Application (SLDCADA), Defense Travel System (DTS)). Delete personnel who no longer require system access. Reconcile system access rosters with personnel rosters and remove system access for personnel who have left the command.

b. Monitor system access logs for unusual system usage patterns (i.e., usage outside of normal duty hours and on weekends).

c. Review system access logs for personnel with multiple user roles (e.g., an employee who is both a cardholder and approving official in the Government-wide Purchase Card commercial bank system).

d. Follow records retention standards. Maintain transaction-level documentation, as appropriate, to support entries into automated systems. Conduct periodic, random audits to "follow the paper trail" on a transaction.

e. Promote awareness of "phishing" schemes, including how personnel can recognize and report them. Send out an "all hands" message when a "phishing" attempt is made at the activity.

4. Government Purchase Card (GPC) and Government Travel Charge Card (GTCC)

a. Conduct regular data mining to identify:

(1) Purchases against restricted and blocked merchant category codes.

(2) Cardholders making recurring purchases with the same vendor (GPC only).

(3) Purchases made when cardholder was not in temporary additional duty (TAD) status (GTCC only).

(4) GTCC balances paid without use of split disbursement. This may indicate use of the card for other than official purposes.

b. Monitor cardholder usage and deactivate, cancel or reduce credit limits on cards that are not being used (i.e., deactivate GTCCs when cardholder is not in TAD status; cancel GPCs not used in the past 6 months).

c. Track a traveler's itinerary to ensure tickets are either used or processed for refund (GTCC only).

d. Require use of electronic airline tickets unless mission will be adversely affected (GTCC only).

e. Maximize use of the individually billed account (IBA) vice the centrally billed account (CBA) (GTCC only).

5. Eligibility for Health Care *(References: NAVMEDCOMINST 6320.3B; DoDINST 1000.24)*

a. Perform Defense Enrollment Eligibility Reporting System (DEERS) check when patient schedules appointment (vice booking appointment and performing first DEERS check at time of appointment).

b. Perform DEERS and identification (ID) card (DD FORM 1173, Uniformed Services Identification and Privilege Card/CAC) check at Patient Administration on 100 percent of persons before nonemergency care is performed.

c. Perform DEERS and ID card (DD FORM 1173/CAC) check at specialty clinic (e.g., ophthalmology, pediatrics, OB/GYN) on 100 percent of persons before nonemergency care is performed. This checks eligibility for patients who bypass Patient Administration and go straight to the specialty clinic for an appointment.

d. Ensure patients who present a DD FORM 1173-1, Department of Defense Guard and Reserve Family Member Identification Card, also present additional documentation (either a copy of the service member's orders or a commissary privilege card). If the patient either does not show eligible in DEERS or does not have proper ID, follow procedures in NAVMEDCOMINST 6320.3B to either bill patient or deny treatment.

e. Check expiration date on all DD FORM 1173s/CACs

(1) If the card is expired, refer the patient to the nearest ID card office for a replacement.

(2) If the patient is a dependent and expiration date is blank or "INDEFINITE," confiscate the card and forward it to the local Personnel Support Detachment (PSD).

f. Perform physical review of all ID cards presented to establish eligibility for medical care to determine if:

(1) The photo on the ID card matches the beneficiary.

(2) The entitlement dates are appropriate (i.e., the card is not expired).

(3) The ID has not been tampered with.

g. Confiscate ID cards that appear to have been tampered with. Contact the command's servicing military criminal investigative organization. Mail the confiscated ID card, with delivery tracking, to the nearest DEERS/Realtime Automated Personnel Identification System (DEERS/RAPIDS) activity.

h. Pull random sample of recent patient visits (i.e., within the past week) and conduct retrospective DEERS eligibility checks. If patients received treatment but are not in DEERS, follow up with Patient Administration and/or specialty clinic to determine whether DEERS checks are being performed.

i. Post information in Patient Administration on how patients can update eligibility in DEERS due to life-changing events (e.g., births, deaths, divorces, adoptions).

6. Civilian Timekeeping. Conduct periodic, random audits to ensure timecards are substantiated by supporting documentation (e.g., approved leave requests; approved NAVCOMPT Form 2282, Overtime/Compensatory Time Request and Authorization for overtime and compensatory time; sign-in/sign-out sheets).

7. Personal Property/Inventory Accountability

a. Ensure receipt, inspection, and acceptance are not all performed by the same person.

b. Develop a list of "pilferable" items that need special attention and implement appropriate controls (i.e., periodic inventory, logging in property book, etc.). Examples may include:

(1) Information Technology (IT) assets (BlackBerrys, cell phones, laptops).

(2) Pharmaceuticals (especially Drugs with High Potential for Diversion).

ACRONYMS

ACOR	Alternate Contracting Officer's Representative
AHLTA	Armed Forces Health Longitudinal Technology Application
AIO	Acquisition Integrity Office
AOR	Areas of Responsibility
BUMED	Bureau of Medicine and Surgery
BPA	Blanket Purchase Agreement
CAP	Contract Administration Plan
CBA	Centrally Billed Account
CCQAS	Centralized Credentials Quality Assurance System
CHCS	Composite Health Care System
CO	Commanding Officer
COR	Contracting Officer's Representative
CSA	Clinical Support Agreement
DEERS	Defense Enrollment Eligibility Reporting System
DMDC	Defense Manpower Data Center
DOD	Department of Defense
DON	Department of Navy
DTS	Defense Travel System
ECODS	Executive Committee of the Dental Staff
ECOMS	Executive Committee of the Medical Staff
EPLS	Excluded Party List System
ESC	Executive Steering Committee
FMFIA	Federal Managers' Financial Integrity Act
GFE	Government Furnished Equipment
GFM	Government Furnished Material
GFP	Government Furnished Property
GPC	Government Purchase Card
GTCC	Government Travel Charge Card
HHS	Department of Health and Human Services
IBA	Individually Billed Account
ID	Identification
IDIQ	Indefinite Delivery Indefinite Quantity
IG	Inspector General
ISA	Individual Set Aside
IT	Information Technology
KO	Contracting Officer
MEDINSGEN	Medical Inspector General
MHS	Military Health System
MICP	Managers' Internal Control Program
MSSP	Medical Staff Services Professional
MTF	Medical Treatment Facility

NMLC	Naval Medical Logistics Command
OIC	Officer in Charge
OIG	Office of Inspector General
PSD	Personnel Support Detachment
RAPIDS	Realtime Automated Personnel Identification System
SLDCADA	Standard Labor Data Collection and Distribution Application
SOA	Statement of Assurance
SOP	Standard Operating Procedure
STARS-FL	Standardized Accounting and Reporting System - Field Level
TAD	Temporary Additional Duty
TL	Technical Liaison
TMA	TRICARE Management Activity
WAWF-RA	Wide Area Work Flow - Receipt and Acceptance

DEFINITIONS

1. Credentials. Documents that constitute evidence of qualifying education, training, licensure, certification, experience, and expertise of health care providers.

2. Credentials Review. The application and screening process in which the credentials of health care providers are evaluated prior to being selected for service or employment by DON, granted clinical privileges or assigned patient care duties.

3. CCQAS. A Military Health System (MHS) Web-based, worldwide credentialing, privileging, risk management, and adverse actions application supporting medical personnel readiness. CCQAS also contains comprehensive data on licensure, education and training certifications, National Practitioner Data Bank findings, and medical personnel readiness data.

4. Grant. An authorized expenditure to a non-federal entity for a defined public or private purpose in which services are not rendered to the Federal government.

5. Grantee. A party receiving a grant. Grantees may include State or local governments, as well as foundations, educational institutions, or other private parties.

6. License. A grant of permission by an official agency of a State, the District of Columbia, a commonwealth, territory, or possession of the United States to provide health care within the scope of practice for a discipline. In the case of a physician, the physician license must be an active, current license that is unrestricted and not subject to limitation in the scope of practice ordinarily granted to other physicians, for a similar specialty, by the jurisdiction that grants the license. This includes, in the case of health care furnished in a foreign country by any person who is not a national of the United States, a grant of permission by an official agency of that foreign country for that person to provide health care independently as a health care professional. Authorized licensing jurisdictions for health care personnel are specified in reference (f). "License" and "licensure" includes certification and registration as appropriate for the provider type.

a. Active. An unrestricted license or registration not subject to limitation on the scope of practice ordinarily granted by the State.

b. Valid. The issuing authority accepts, investigates, and acts upon quality assurance information, such as practitioner professional performance, conduct, and ethics of practice, regardless of the practitioner's military status or residency.

c. Unrestricted. Not subject to limitations on the scope of practice ordinarily granted all other applicants for similar specialty in the granting jurisdiction.

ANTI-FRAUD RESOURCES

Question #1: How do I report a suspected case of fraud?

Answer #1:

Step 1: Report the allegation to your chain of command. If your chain of command is unresponsive or you fear reprisal, then;

Step 2: Report the allegation to an Inspector General. Your initial report should be to your command or installation Inspector General. After that, you can contact your regional Inspector General and finally, the Naval Inspector General.

Navy Medical Inspector General Hotline

Telephone: 1-800-637-6175 (DSN 295-9019)
E-mail: MEDIG-Hotline@med.navy.mil

Mailing address: Navy Medical Inspector General
8901 Wisconsin Ave., Bldg. 1, 19th floor
Attn: Director of Special Inquiries/Investigator
Bethesda, MD 20889-5615

Navy Medicine West Inspector General Hotline

Telephone: 1-619-676-6068
E-mail: NMWestMEDIG@med.navy.mil
Fax: 1-619-767-6058

Mailing address: Navy Medicine West
Attn: NMW IG Hotline Coordinator
4170 Norman Scott Road, Bldg. 3232
San Diego, CA 92136

Navy Medicine East Inspector General Hotline

Telephone: 1-757-953-5800
E-mail: NAVMEDEast-HOTLINEDistributionList@med.navy.mil
Fax: 1-757-953-5799

Mailing address: Navy Medicine East
Attn: NME IG Hotline Coordinator
Bldg. 3, Suite 1400
620 John Paul Jones Circle
Portsmouth, VA 23708

Navy Medicine National Capital Area Inspector General Hotline

Telephone: 301-319-8990 (DSN 285-8990)
E-mail: NCAHotline@med.navy.mil
Fax: 301-319-8531

Mailing address: Navy Medicine National Capital Area (NMNCA)
Inspector General
8901 Wisconsin Ave., Bldg. 1, 9th Floor
Bethesda, MD 20889

Navy Medicine Support Command Inspector General Hotline

Telephone: 1-800-566-8494, ext. 8017 or 1-904-542-7200, ext. 8017
E-mail: IGHotline@med.navy.mil
Fax number: 1-904-542-9192

Mailing address: Navy Medicine Support Command (NMSC)
Inspector General
H2005 Knight Lane
P.O. Box 140
Jacksonville, FL 32212-0140

Note: In many cases, you can remain anonymous when you contact the IG Hotline.

Question #2: How do I check to see if a provider is sanctioned or excluded?

Answer #2: Check both of the following Web sites:

TMA Sanction List
http://www.tricare.mil/fraud/index.cfm?fuseaction=Sanction.search

U.S. Department of Health and Human Services, OIG Exclusion Program
http://www.oig.hhs.gov/fraud/exclusions.asp

Note: Any provider who is in the HHS Exclusion Program is also considered sanctioned by TMA.

Question #3: How do I update my TRICARE eligibility (e.g., birth, death, marriage, adoption, divorce, and proof of genetic relationship)?

Answer #3: You can visit the nearest ID card issuing facility at: www.dmdc.osd.mil/rsl or call the Defense Manpower Data Center (DMDC) Support Office at 1-800-538-9552.

Question #4: Where do I find out if a source is barred from receiving federal contracts?

Answer #4: Query the Excluded Parties List System (EPLS) at https://www.epls.gov/.

SAMPLE REFERRAL LETTER TO TRICARE MANAGEMENT ACTIVITY PROGRAM INTEGRITY OFFICE

Submission of Case Referral Supporting Findings of Suspected Aberrant, Abusive, or Fraudulent Billings for Case Development

Referral of Fraud or Abuse Allegation(s)
to the TRICARE Management Activity
Program Integrity Office

DATE:

CASE NAME: John Doe, M.D.

BRIEF DESCRIPTION OF THE ALLEGATION(S): The allegation is that John Doe, M.D., is billing for services actually rendered by a military physician.

PERSON/COMPANY INVOLVED: (e.g., Name, provider specialty, Tax ID #, address) John Doe, M.D., Tax ID No. 123456789. [MTF Address and civilian address if known] This provider has been a contracted provider since 01/01/04.

HOW ALLEGATION(S) WAS IDENTIFIED: Beneficiary complaint, analysis of billing records, and/or review of provider's workload. (Note: Provide details to allow TMA to appropriately assess and evaluate the case and its merits.)

EVIDENCE: (List all evidence included to support allegation): (Provide findings, copies of medical records, appointment logs, provider contract, etc. All relevant documentation that supports your referral and that will assist analysis of facts/findings.)

COMMANDING OFFICER COORDINATION: (Identify date referral coordinated with commanding officer):

POINT OF CONTACT: (Name, address, e-mail, and telephone number).

SUMBIT THIS DOCUMENT AND ATTACHMENTS TO:
TRICARE Management Activity
Program Integrity Office
16401 East Centretech Parkway
Aurora, CO 80011-9066
Fax: 1-303-676-3981
E-mail: Fraudline@tma.osd.mil