CHAPTER 14

MEDICAL INFORMATION SYSTEM (MIS) PROGRAM

Section A. Medical Information Systems (MIS) Plan.

Section B. Medical Information System.

Section C. Medical Readiness Reporting System (MRRS).

Section D. Medical Information Implementation Guide (MIIG).

This page intentionally left blank

Section A. Medical Information Systems (MIS) Plan.

This page intentionally left blank.

A. Medical Information Systems (MIS) Plan.

1. Purpose. The Medical Information System (MIS) program described here follows the policy established by the Office of Health Services Commandant (CG-112), outlines systems and assigns responsibility for the administration of the MIS. The MIS is a key component for the overall management of CG clinics and sickbays. MIS is a dynamic tool, which will provide a comprehensive electronic solution for tracking operational medical readiness, health systems management, and patient access to care. The Health and Safety Directorate, HSWL SC, unit COs, and health care providers are responsible for ensuring successful implementation of the CG MIS.

2. Background.

   a. There is an ongoing need for Commandant, Area Commanders, and field level COs to assess medical and dental operational readiness. As one of the offshoots of this need, along with assurance of medical safety, the President and Congress have mandated the use of the Electronic Health Record (EHR) in military services. Additionally, the CG Health Services program needs to accurately capture workload, performance, and productivity through standardized methodology. Proper analysis of health care data provides the ability to realign assets where they are most needed to deliver timely, quality health care. The full implementation of the Composite Health Care System (CHCS), the military EHR, Armed Forces Health Longitudinal Technology Application (AHLTA), Medical Readiness Reporting System (MRRS), Dental Common Access System (DENCAS), and future enhancements to AHLTA will significantly enhance our ability to provide this information as needed.

   b. Federal statutes impose strict requirements for managing government information. The most pertinent Federal statutes that govern information include:

      (1) Federal Records Act (Public Law 81-754): Sets policy for and mandates establishment of agency programs for the management of Federal records.

      (2) Freedom of Information Act (Public Law 90-23): Provides policy to ensure public access to Federal government information.

      (3) Paperwork Reduction Act (Public Law 96-511): Recognizes information as a Federal resource and directs agencies to establish specific programs for management of the resource and associated elements.

      (4) Paperwork Reduction Reauthorization Act (Public Law 99-500): Defines information resources management and directs further program management requirements.

(5) A suspected or confirmed breach/compromise shall be reported in accordance with the Privacy Incident Response, Notification, and Reporting Procedures for Personally Identifiable Information (PII), COMDTINST 5260.5 (series).

(6) Privacy Act (Public Law 93-579): Provides policy and safeguards to protect privacy of individuals.

(7) Health Insurance Portability and Accountability Act (HIPAA), (Public Law 104-191): Requires health plans to assure the security and privacy of individually identifiable health information, and to use specified standards and code sets for electronic transactions involving medical information.

3. Privacy rights. CG policy concerning the privacy rights of individuals and the CG's responsibilities for compliance with operational requirements established by The Coast Guard Freedom of Information (FOIA) and Privacy Acts Manual, COMDTINST 5260.3 (series), Privacy Act and HIPAA are as follows:

a. Privacy.

(1) Protect, as required by the Privacy Act of 1974, as amended, and HIPAA, the privacy of individuals from unwarranted intrusion. Individuals covered by this protection are living citizens of the US and aliens lawfully admitted for permanent residence.

(2) Collect only the personal information about an individual that is legally authorized and necessary to support CG operations. Disclose this information only as authorized by the Privacy Act and HIPAA, and described in Chapter 4 of this Manual.

(3) Keep only personal information that is timely, accurate, complete, and relevant to the purpose for which it was collected.

(4) Safeguard personal information to prevent unauthorized use, access, disclosure, alteration, or destruction.

(5) Let individuals know what records the CG keeps on them and let them review or get copies of these records, subject to exemptions authorized by law.

(6) Permit individuals to amend records about themselves contained in CG systems of records, as authorized by HIPAA, which they can prove are factually in error, not up-to-date, not complete, or not relevant.

(7) Allow individuals to ask for an administrative review of decisions that deny them access to or the right to amend their records.

(8) Maintain only information about an individual that is relevant and necessary for CG purposes, as required to be accomplished by statute or Executive Order.

(9) Act on all requests promptly, accurately, and fairly.

b. Security.

(1) Facility Access Controls:

(a) The CG will continually access potential risks and vulnerabilities to individual protected health information in its possession, and develop, implement and maintain appropriate administrative, physical and technical security measures in accordance with HIPAA.

(b) Clearly define the security perimeter of the premises and building. Ensure that the perimeter is physically sound. Ensure all external doors are adequately secured against unauthorized access by installing locks, alarms or other access control devices.

(c) Define the instances in which visitors are allowed, including the areas they may visit and any escort requirements.

(d) Ensure all doors to interior areas requiring compartmentalization or added security are adequately protected against unauthorized access by installing locks, alarms, or other access control devices.

(2) Workstation Use and Security

(a) Comply with all applicable CG information system security policies.

(b) Log off every time prior to leaving the terminal

(c) Inspect the last logon information for consistency with actual last logon; report any discrepancies.

(d) Comply with all applicable password policies and procedures, including not storing written passwords.

(e) Close files and systems not in immediate use.

(f) Perform memory-clearing functions to comply with security policies.

(3) Workforce Security

(a) Identify the extent of authorization each class of workforce members will require when accessing electronic protected health information, considering the criticality and sensitivity of the information to be handled.

(b) Workforce member, contractors and others shall access only those areas and the applicable health information to which they are authorized.

(c) Ensure appropriate training is completed before access to MIS components is granted or reinstated.

(4) Information Systems Activity Review

(a) Assign personnel to conduct a regular review of electronic protected health information systems' activities.

(b) Reviewers should have appropriate technical skills to access and interpret audit logs correctly.

(5) Contingency Plan

(a) Identify the hardware, software, applications and information sets that receive, manipulate, store and/or transmit electronic protected health information. Define information sets for the purpose of criticality rating.

(b) Identify backup methods and materials to be used, and the frequency of performing backups

(c) Monitor storage and removal of backups and ensure all applicable access controls are enforced.

4. Applicability and Scope. All health care facilities (clinics, satellite clinics, and sickbays) shall comply with the MIS operating guidelines as set forth. The MIS program described here contains the essential elements required at all CG facilities with medical personnel assigned and assigns responsibilities for the program's initiatives. The SHSO shall ensure all healthcare providers and support staff; which include Medical Officers, Dental Officers, Pharmacy Officers, Clinic Administrators, HS's; HSD's and Medical and Dental contractors; shall participate. Information technology is not static in nature but rapidly changing and dynamic, and requires the diligence of all concerned to create and maintain a sound program.

5. Objectives.

   a. The Director of Health and Safety Commandant (CG-11) has established a MIS that provides necessary tools and capabilities to assist in making sound business decisions for those Commands having healthcare facilities.

   b. Identify and justify resources required to maintain a quality MIS.

   c. Establish access and connectivity for CG-wide comprehensive utilization of AHLTA, ensuring local DoD host site affiliation for electronic referrals and consultations and access to the Central Data Repository for all military health system beneficiary medical records.

   d. Establish and maintain clinic and sickbay Microcomputer Allowance Lists (MAL) that provide appropriate access to medical information systems for managing clinical and administrative operations.

   e. Establish a standardized equipment list for peripherals. (e.g. pharmacy printers, Lab barcode readers, thin terminal clients devices, etc.).

   f. Identify systems training requirements and ensure required education and training standards are established and maintained.

   g. Provide direction as new adjuncts to existing programs are developed and deployed.

   h. Participate in DoD sponsored software and product development for use in the medical arena.

6. Definitions.

   a. The short list of acronyms and definitions below is provided for clarification of Chapter 14 terms:

      (1) Intranet. A privately owned network based on the Transmission Control Protocol/Internet Protocol (TCP/IP) suite.

      (2) Internet. A voluntary interconnected global network of computers based upon the TCP/IP protocol suite, originally developed by the U.S. Department of Defense Advanced Research Projects Agency.

      (3) NIPERNET. Non-Classified Internet Protocol Routing Network. The Defense Information Systems network (DISN) Internet line for unclassified DoD and federal agency Internet traffic.

      (4) CGDN+. CG Data Network Plus. The secure CG-wide area network (WAN).

(5) Firewall. Security measure which blocks unwanted/unauthorized entry to computer systems from outside the internal system.

(6) Host (site). Medical facility where a CHCS server platform resides.

(7) TelNet. Telecommunications Network. A protocol that facilitates remote logins to host site server and functions via the Internet. Restricted by CG IT authorities.

(8) IP address. Internet Provider address. An assignable 32 bit numeric identifier, which designates a device's location on an intranet network or on the Internet.

(9) LIU. Local Area Network Interface Unit. Device designed to provide external access and interface with the local area network (LAN).

7. Organizational Responsibilities. A detailed list of Organizational responsibilities and actions for each will be published in the Medical Information Implementation Guide (MIIG).

Section B. Medical Information System.

This page intentionally left blank.

B. Medical Information System.

1. Background. Information technology is dynamic in nature and rapidly changing. Commandant (CG-112) is responsible for ensuring that the Health, Safety, and Work-Life Directorate's MIS continues to evolve. The MIS has evolved from manual data collection systems to automated systems such as CLAMS to the DoD's hospital-based Composite Health Care System (CHCS). The advent of TRICARE in the mid 1990's necessitated integration of the CG's health care information with that of DoD's infrastructure.

2. Systems. The following outlines current automated information systems, applications and program components that come under the CG MIS program.

   a. Provider Graphic User Interface (PGUI) and AHLTA. A graphical user interface is software that makes CHCS easier to understand and use. The PGUI currently used in the CG will transition to AHLTA as DOD resolves the connectivity, efficiency, security, and other issues.

   b. Medical Readiness Reporting System (MRRS) . Section C of this Chapter provides further details.

   c. Dental Common Access System (DENCAS). The Dental Common Access System is an enterprise-wide, world class e-business system that functions seamlessly between ship and shore to provide a complete picture of Navy and CG personnel dental readiness. DENCAS also provides an accurate, real-time, comprehensive administrative reporting system.

   d. Protected Health Information Management Tool (PHIMT).

      (1) The Privacy Rule of the Health Information Portability and Accountability Act (HIPAA) requires a covered entity (i.e., the CG Health Care Program) to maintain a history of when and to whom disclosures of Protected Health Information (PHI) are made for purposes other than for treatment, payment and health care operations. The covered entity must be able to provide an accounting of these disclosures to an individual upon their request. Authorizations and Restrictions to disclosures from an individual to a covered entity are included in the information that is required for accounting purposes. Disclosures that are permitted but also must be must be accounted for are those made within six years of the date of request, in the following 12 categories:

         (a) As required by law, statute, regulation or court orders.

         (b) For public health reports, communicable disease control, FDA reports, and OSHA reports.

         (c) To government authorities regarding victims of abuse or domestic violence.

(d) To health oversight agencies.

(e) To judicial or administrative proceedings through an order from a court or administrative tribunal (or a subpoena if notice to the individual is provided).

(f) As required by law or court order, to identify a suspect, or to alert law enforcement of a crime.

(g) To funeral directors, coroners or medical examiners as authorized by law.

(h) To facilitate organ, eye or tissue donation.

(i) For research, as approved by a Review Board.

(j) To prevent a serious threat to health or safety.

(k) For execution of the military mission and other essential government functions.

(l) To comply with workers' compensation laws.

(2) To comply with the requirements for accounting for disclosures, the TMA has developed and provided and electronic disclosure tracking tool. The Protected Health Information Management Tool (PHIMT) stores information about disclosures, Authorizations and Restrictions that are made for a particular patient. The PHIMT also has a functionality that can provide an accounting of disclosures by individual patient, upon request.

(3) Use of the PHIMT is password protected, and several user roles are defined:

(a) A regular user can create disclosures and Authorization/Restriction requests.

(b) A user administrator can add/modify users within their Service.

(c) A Privacy/Security Officer can approve/deny disclosures, Authorizations and Restrictions, and generate the associated letters.

(4) A User Guide and an Administrator Guide for the PHIMT can be accessed through the HIPAA Learning Management Tool at www.HIPAAtraining.tricare.osd.mil using the student ID and password used for the HIPAA Privacy training module.

Section C. Medical Readiness Reporting System (MRRS).

This page intentionally left blank.

C. Medical Readiness Reporting System (MRRS).

1. Description. The Medical Readiness Reporting System (MRRS) is the CG's medical readiness reporting system adopted from the Navy. It is designed for use by clinics, independent duty health services technicians and CG Personnel Command. MRRS contains the following functional elements:

   a. Immunization data.

   b. Primary Physical Exam data.

   c. Periodic Health Assessment data.

   d. Medical Readiness data.

   e. Blood type/ tests data.

   f. Visual Acuity/ insert requirements.

   g. Dental Exam and classification.

   h. Pre/Post Deployment History.

   i. Forms

   j. Health record tracking.

2. Recorded tests. MRRS is designed to track medical readiness parameters (e.g. HIV test, TST, DNA specimen submission, G6PD, sickle test, blood type, primary physical exam currency, periodic health assessment currency, and immunizations. The system is tailored to meet all Department of Defense (DoD) and CG medical readiness reporting requirements.

3. Questions related to MRRS. Questions on policy related to MRRS may be directed to COMDT (CG-1121).

4. Access Instructions. Members requiring access to MRRS need to request permissions from their local (clinic) MRRS Security Officer. Upon completion of mandatory MRRS training, members will receive access to MRRS after faxing or sending via electronic mail a completed DD-2875, System Access Request Form to the appropriate Security Officer. This form is available on the MRRS website at https://mrrs.sscno.nmci.navy.mil.

This page intentionally left blank.

Section D. Medical Information Implementation Guide (MIIG).

This page intentionally left blank.

D. Medical Information Implementation Guide (MIIG).

1. Background. The MIIG is a series of guides designed to assist commands in meeting the requirements of the Health Services MIS Program requirements and to augment policy that is outlined in the Medical Manual. Serving as both policy and guidelines, the MIIG utilizes the same principal used in the QI program (as contained in chapter 13), by outlining administrative requirements and by providing direction and policy for addressing critical MIS issues. The exercises provide generic frameworks adaptable to local conditions. In some cases, clinics may be required to submit evidence of completing an exercise to the HSWL SC for data evaluation purposes.

2. Responsibilities.

   a. Commandant (CG-112). Commandant (CG-112) develops exercises as needed on critical MIS issues for inclusion in the MIIG and posts them on http://www.uscg.mil/hq/cg1/cg112/cg1123/default.asp.

   b. HSWL SC. The HSWL SC ensures guides are available to Commands for all clinic personnel to complete and also reviews clinic's use of the MIIGs as part of the Operational Health Readiness Program.

   c. Unit Clinic Administrators (CA) & System Administrators (SA). Unit CA & SA shall ensure all clinic staff promptly comply with all MIIG guides and maintain a complete, updated MIIG folder.

This page intentionally left blank.