General ADP Requirements

1.0. GENERAL

1.1. The Automated Data Processing Manual defines the contractor's responsibilities related to automated processing of health care information, and transmission of relevant data between the contractor, TRICARE Management Activity (TMA), and DEERS. It covers three major categories of information flowing between the contractor and TMA: health care service information, provider information (Chapter 7), and pricing information (Chapter 8). For each of these categories it presents specifics of submission, record and data element specifications, editing requirements, and TMA reporting of detected errors to the contractor. A separate chapter is devoted to beneficiary eligibility verification procedures (Chapter 9) and must be followed by the contractor.

1.2. This chapter addresses major functional and technical requirements related to the flow of health care related ADP information between the contractor and TMA. Health care service records as well as provider and pricing information must be submitted to TMA in electronic media. This information is essential to both the accounting and statistical needs of TMA in management of the TRICARE program and in required reports to Department of Defense, Congress, other governmental entities, and to the public. Technical requirements for the transmission of data between the contractor and TMA are presented in Section 2. The requirements for submission of health care service records and resubmission of records are outlined in Section 3, Section 4 and Section 5 address the TMA requirements related to submission and updating of provider and pricing information.

2.0. ADP REQUIREMENTS

It is the responsibility of the contractor to employ adequate hardware, software, personnel, procedures, controls, contingency plans and documentation to satisfy TMA data processing and reporting requirements. Items requiring special attention are listed below.

2.1. Backup System

2.1.1. Reliable backup for hardware, software, data files and personnel must be available to ensure continuous data processing when any of the listed primary components are not available for an extended period of time. These requirements can be satisfied by ensuring access to alternate hardware, regular backup procedures for application software and data files, and a backup plan of acquiring personnel in an emergency situation. All these measures must provide for timely recovery of data processing services following an interruption.

2.1.2. The contractor will conduct a test of the backup system within the first quarter of the initial health care delivery period and will continue to assure backup capabilities by testing or reviewing the availability and capability of the backup ADP system to process the TRICARE data and produce the expected results. Review of the primary ADP system configuration with the backup ADP system must be done at least semiannually. The contractor's testing of the backup system will be done at least once a year.

2.1.3. The test in the first quarter and the annual test must include a representative sampling of at least four hundred (400) of the various health care records routinely processed by the contractor. If the test does not produce results which are equal to those achieved on the contractor's primary system, the contractor shall take immediate steps, and within ninety (90) days reestablish a backup ADP system acceptable to TMA. In all cases, the results of the review and/or test results will be reported to Contract Management Division, TMA, within fifteen (15) days of conclusion of the review or test.

2.2. Security

2.2.1. The contractor has the responsibility to ensure that TRICARE program records in its custody, whether in machine readable form or hardcopy, are protected from unlawful disclosure, fraud or embezzlement. The Privacy Act of 1974 requirements must be applied to production test and distribution of hardcopy reports, to labeling and mailing of magnetic tapes, to restrictions of online access to data files, and to destruction of reports and magnetic tapes. These records must be protected from malicious or inadvertent destruction, and also from loss due to natural disasters.

2.2.2. OPM, Chapter 1, Section 5 outlines specific statutory requirements for control and/or release of information. The contractor, in processing TRICARE data, develops and maintains information files which fall within requirements of these laws. Control of access, either physically or electronically, to contractor's TRICARE program software, operational data files, documentation libraries and off-site storage areas must be limited to those persons with a legitimate need to access and use the information. All factors discussed above must form a basis for the contractor's security plan.

2.2.3. All systems processing sensitive but unclassified information or information subject to the Privacy Act of 1974 shall be protected. All contractors supporting TRICARE healthcare delivery programs (e.g., TRICARE Senior Prime) will comply with the security requirements process as defined by DoD 5200.40 (DoD Information Technology Security Certification and Accreditation Process (DITSCAP)), and as stated in this Manual.

2.2.4. Specific Security Requirements:

2.2.4.1. The contractor shall comply with DoD Minimum Security Requirements, DoD 5200.40 (DITSCAP), Health Insurance Portability and Accountability Act (HIPAA) (specifically the Administrative Simplification section of the Law, including the security, electronic signature, and privacy standards), Privacy Act Program Requirements (DoD 5400.11), Personnel Security Program (DoD 5200.2-R) and the MHS Information Assurance Policy Manual.

2.2.4.2. All contractor or contract leased or supported IT systems that process, sort, transmit, or access sensitive but unclassified government information or information systems will obtain security certification and accreditation IAW DoD 5200.40 (DITSCAP) and the supporting guideline documents published by the Defense Information System Agency (DISA).

2.2.4.3. The MHS Information Assurance Team will provide guidance in the development of security documentation specified by the security references above in support of the certification and accreditation process.

2.2.4.4. Documentation includes an overall System Security Authorization Agreement (SSAA), a Vulnerability Assessment, Risk Analysis, Trusted Facilities Manual, Security Features User's Guide, and other security documents as defined within the referenced directives and standards.

2.2.4.4.1. Explanation of the System Security Authorization Agreement: The SSAA is a living document that represents the formal agreement among the Designated Approving Authority (DAA), Certifying Authority (CA), User Representative, and Program Manager. The SSAA is used throughout the entire DITSCAP to guide actions, document decisions, specify Information Technology Security (ITSEC) requirements, document certification tailoring and level of effort, identify potential solutions, and maintain operational systems security. The primary objectives of the SSAA are provided below:

- Document the formal agreement among the DAA(s), the CA, the user representative, and the program manager.

- Document all requirements necessary for accreditation.

- Document all security criteria for use throughout the IT system life cycle.

- Minimize documentation requirements by consolidating applicable information into the SSAA (security policy, concept of operations (CONOPS), plans, architecture description, etc.).

- Document the DITSCAP plan.

The SSAA is updated in each phase as the system development progresses and new information becomes available. The SSAA consolidates the system and security documentation into one document. This eliminates redundancy and potential confusion as multiple documents describe the system, security policy, system and security architecture. When feasible, the SSAA can be tailored to incorporate other documents as appendices or by reference to the pertinent document

2.2.4.4.2. System Security Authorization Agreement Appendices:

2.2.4.4.2.1. System Design Document: Describes the framework for the information system security architecture that includes a physical description of the hardware, software, firmware, interfaces, and Data flow.

- Hardware: Describes the hardware used and whether it is a standard commercial product, unique, or on the National Security Agency (NSA) Evaluated Products List (EPL). Include an equipment list and describe the target hardware and its function.

- Software: Describes the operating system(s), database management system(s), and applications. Documentation software includes the entire set of application programs, software procedures, software routines, and operating system software associated with the system. This includes manufacturer-supplied software, other commercial off-the-shelf software, and all programs generated applications software. The features of any security packages used on the system should be identified and described. Identify any software packages that are commercial off-the-shelf (COTS), government off-the-shelf (GOTS), and on the EPL and describe the target software and its intended use.

- Firmware: Describes the firmware used and whether it is a standard commercial product, unique, or on the EPL. For example, items such as Programmable Read-Only Memory (PROM) and erasable PROM (EPROM) devices are considered firmware. The software that is stored permanently in a hardware device that allows reading and executing the software, but not writing or modifying should be described.

- System interfaces and external connections: Describes the significant features of the communications layout. A high level diagram of the communications links and encryption techniques connecting the components of the information system, associated data communications, and networks should be included. Describe the system's external interfaces. The description should include a statement of the purpose of each external interface and the relationship between the interface and the system. Provide information on all Ports and Protocols used.

- Data flow: Describes the system's internal interfaces and data flows. The types of data and the general methods for data transmission should be stated. Diagrams or text to explain the flow of critical information from one component to another should be included.

2.2.4.4.2.2. System Rules of Behavior: This appendix provides an established set of rules of behavior concerning use of, security in, and the acceptable level of risk for, the system. The rules shall be based on the needs of the various users of the system. The security required by the rules shall be only as stringent as necessary to provide adequate security for information in the system. Such rules shall clearly delineate responsibilities and expected behavior of all individuals with access to the system. They shall include appropriate limits on interconnections to other systems and shall define service provision and restoration priorities. Finally, they shall be clear about the consequences of behavior not consistent with the rules.

2.2.4.4.2.3. Contingency Plan(s): Describes the rapid recovery of a system in the event of an outage or interruption to automated mission operations. This document should describe the emergency responses, backup procedures, backup operations, and recovery. An outage or interruption may be caused by damage to facilities, equipment, software, or data that comprise the system or application. The plan provides an organized method for restoring automated mission operations to a useable level that will support crucial mission functions during times of emergency or until full and permanent operations can be restored. The plan defines the responsibilities of each person expected to play a role during the emergency and requirements for testing the plan. The detail of the contingency plan is influenced by the IT environment, the criticality of the functional applications being supported, and the user's requirements.

2.2.4.4.2.4. Security Awareness and Training Plan: Describes the security-training plan based on the written rules of the system. The type of training and the content should be specific to what each type of user needs to know to use the system securely. Documentation should include how specific groups of users will be trained and what that training will include. Subjects to be covered should include work at home, dial-in access, connection to the Internet, use of copyrighted works, unofficial use of government equipment, the assignment and limitation of system privileges, individual accountability, technical security controls (e.g., password use), proper use of applications, how to get help, and restoration of service as a concern of all users of the system or application.

2.2.4.4.2.5. Incident Response Plan: Describes policies and procedure for providing a capability to help users when a security incident occurs in the system and to share information concerning common vulnerabilities and threats. This capability should assist the organization in pursuing appropriate legal action if necessary. Documentation should address reporting requirements for security incidents and actions to be taken.

2.2.4.4.2.6. Configuration Management Plan: Describes the change management control or configuration control procedures. These procedures should identify and document the functional and physical characteristics of the system, control changes to those characteristics, and record and report change processing and implementation status.

2.2.4.4.2.7. Security Features Users Guide: Describes the User/Employee duties and responsibilities for security while using your network and consequences if they fail to follow the policies.

2.2.4.4.2.8. Trusted Facility Manual (TFM): Documents the cautions and privileges necessary to control the operations of a secure facility, and provides the procedures for managing system audits. Describes audit procedures, records, and actions associates with various types of audit events. The TFM focuses on system administration, not on computer security in general. The document briefly describes the system, details security mechanisms in place and defines procedures to securely administering the system. The document also discusses the philosophy of the system security design and control. The TFM describes security operations and roles and responsibilities associated with system administration.

2.2.4.4.2.9. Security Test Plan, Procedure and Results: This appendix describes both the expected and actual test outcomes for the security mechanisms or features, at both the system and application level. All security features must be tested at both the system and application level; this includes Audit, Discretionary Access Control, and Identification and Authentication, and Object Reuse. Test documentation describes the test plan; test logs, test reports, test procedures, and test results and explains how the security mechanisms were functionally tested.

2.2.4.4.2.10. Security Policy: This appendix does not have to be a separate document, but can be part of the core SSAA. This section describes what is and is not permitted in the field of security during the general operation of the system. The security policy section describes the exceptions to the policies contained in the laws, regulations, rules, and practices that regulate how an organization manages, protects, and distributes information. This section establishes policy precedence when more than one policy applies. A list of polices that apply to the system is provided. The primary thrust of this section is to develop mission-level security objectives through deductive reasoning. Security objectives are the top-most level of specifications and focus on the security related aspects of the identified mission. Security objectives must be concise, declarative sentences derived from analysis of mission information, threat, and umbrella security guidance. These security objectives should be written in terms independent of architecture and implementation. Each security objective should be justified by rationale. The rationale documents the mission objectives supported by that security objective, the threat driving the security objective, the consequences of not implementing the objective, and applicable umbrella security guidance supporting that security objective. The rationale binds each security objective to a mission objective and focuses attention on security at the mission level.

2.2.4.4.2.11. Memorandum of Agreement(s): This appendix contains all required memoranda of agreement (MOA). When systems managed by different DAAs are interfaced or networked, a MOA is required that addresses the accreditation requirements for each system involved. The MOA should include description and classification of the data, clearance levels of the users, designation of the DAA who shall resolve conflicts among the DAAs, and safeguards to be implemented before interfacing the systems. MOAs are required when one DoD component's system interfaces with another system within the same DoD component or in another DoD component and when a contractor's system interfaces with a DoD component's system or to another contractor's system.

2.2.4.4.2.12. Personnel Security Controls: This appendix provides a statement indicating the responsible organization complies with the appropriate personnel security requirements.

2.2.4.5. All electronic transmission of medical records and data over public unprotected and unapproved paths must be protected with FIPS 140-1 validated encryption technology that is interoperable with the DoD Public Key Infrastructure (PKI).

2.2.4.6. The Designated Approval Authority (DAA) as defined by the Lead Agent will serve as the accreditation official for Contractor information technology systems processing government sensitive but unclassified information.

2.2.4.7. All Contractor AISs, including stand-alone personal computers and laptops, that process government sensitive but unclassified information will be protected at the highest level of sensitivity of information processed, stored, transmitted, or accessed.

2.2.4.8. The Contractor shall establish and maintain standing operating procedures for safeguarding the security of the all sensitive but unclassified information, including privileged patient medical information and information subject to the Privacy Act, 1974, at a reasonable level of protection to preclude inadvertent disclosure to unauthorized sources.

2.2.4.9. These procedures shall include system auditing and routine review of audits, security awareness training, appropriate management of all system accounts and passwords, and providing access only to authorized personnel.

2.2.4.10. The Government reserves the right to specify what Government data/ information may be accessed by the Contractor. If at any time, classified national security information is discovered, a security breach is discovered, or unsuccessful attempts to access unauthorized information are noted, the Contractor shall secure the information and report the incident to the appropriate government representative.

2.2.4.11. The Contractor shall implement all required network security safeguards to protect the Contractor's AIS and sensitive information from unauthorized access, modification, or damage.

2.2.4.12. Specifically the Contractor shall implement network security measures to prevent unauthorized access via the Internet/DISN WAN and obtain certification and accreditation of the Contractor furnished network IAW DoD 5200.40 (DITSCAP), and the Information Assurance Technology Framework Forum (IATFF) ensuring compliance with the DoD Defense in Depth initiative.

2.2.4.13. The Contractor shall implement security measures to protect the system and data resources, procedures to react to Computer Emergency Response Team (CERT) security notices, and procedures designed to detect and correct security vulnerabilities.

2.2.4.14. All government provided information, or information relating to government sponsored personnel, that comes into the custody of the contractor remains the property of the U.S. Government and shall either be returned to the government or destroyed when directed by the appropriate government representative.

2.2.4.15. Personnel Security:

2.2.4.15.1. The contractor shall comply with the requirement to obtain the minimum personnel security investigations as prescribed by DoDD 5200.2-R based on the individual's responsibilities and access to sensitive but unclassified information.

2.2.4.15.2. This directive prescribes the level of security investigation required and the process for obtaining these security investigations.

2.2.4.15.3. All contractor personnel who have access to systems processing, storing, or transmitting sensitive but unclassified medical information shall be classified as ADP-I, ADP-II, or ADP-III as defined in DoDD 5200.2-R as dictated by their level of responsibility.

2.2.4.15.4. This classification determines the type of security investigation required.

2.2.4.15.5. Once personnel classification is determined, the appropriate investigation forms, finger print cards, and questionnaires shall be completed as required and submitted to the assigned Government AIS Security Officer for processing.

2.2.4.15.6. The appropriate government representative may authorize contractor personnel to temporarily occupy non-critical sensitive positions pending completion of the National Agency Check (NAC).

2.2.4.15.7. If at any time the individual receives unfavorable NAC adjudication, or if at any time information that would result in an unfavorable NAC becomes known, the Contractor shall immediately remove the employee from the non-critical-sensitive position.

2.2.4.15.8. All contractors and contractor sponsored personnel accessing Government systems are required to sign a non-disclosure agreement that will be retained as an official permanent record as determined by the sponsoring activity.

2.2.4.15.9. Security files on all Contractor personnel assigned to the contract shall be maintained by the contractor and made accessible to the appropriate government representative's Security Manager as required.

2.2.4.15.10. The Contractor shall report possible adverse information on contract employees occupying non-critical-sensitive positions through the ACOR to the appropriate government representative Security Manager.

2.2.5. Security activities are part of an ongoing process, even after certification and accreditation (C&A). Systems, processes, and personnel security must be maintained in accordance with DITSCAP and C&A approval packages. The Contractor will notify their Contracting Officers if/when they become aware of major modifications to their systems that may impact on their certification and accreditation.