THE ASSISTANT SECRETARY OF DEFENSE

1200 DEFENSE PENTAGON
WASHINGTON, DC 20301-1200

HEALTH AFFAIRS

18 July 2011

MEMORANDUM FOR ASSISTANT SECRETARY OF THE ARMY (M&RA)
ASSISTANT SECRETARY OF THE NAVY (M&RA)
ASSISTANT SECRETARY OF THE AIR FORCE (M&RA)
DEPUTY ASSISTANT SECRETARY OF DEFENSE (FORCE HEALTH PROTECTION AND READINESS)
DEPUTY ASSISTANT SECRETARY OF DEFENSE (CLINICAL POLICY AND PROGRAMS)
DEPUTY ASSISTANT SECRETARY OF DEFENSE (HEALTH BUDGETS AND FINANCIAL POLICY)
DEPUTY DIRECTOR, TRICARE MANAGEMENT ACTIVITY
JOINT STAFF SURGEON
COMMANDER, JOINT TASK FORCE NATIONAL CAPITAL REGION MEDICAL
CHIEF INFORMATION OFFICER, TRICARE MANAGEMENT ACTIVITY
PROGRAM EXECUTIVE OFFICER, JOINT MEDICAL INFORMATION SYSTEMS
PROGRAM EXECUTIVE OFFICER, DEFENSE HEALTH SERVICES SYSTEMS, CLINICAL SYSTEMS
DIRECTOR, MILITARY HEALTH SYSTEM ELECTRONIC HEALTH RECORD CENTER

SUBJECT: Policy for Military Health System Enterprise Architecture Principles, Version 1.0

I am pleased to announce the Military Health System (MHS) Enterprise Architecture (EA) Principles, Version 1.0 was approved by the MHS EA Committee under the MHS Chief Information Officer (CIO) Management Board on April 20, 2011. I would like to thank you for your staff's support and participation in the development of the MHS EA Principles, and look forward to more achievements as we continue to work together.

MHS EA Principles define high-level tenets, which will form the foundation for key design considerations, future architecture development, and decision-making for MHS Information Management and Information Technology (IM/IT) investments. MHS EA Principles are based on Federal, Department of Defense (DoD), and MHS policies, guidance, and commercial best practices, and provide a set of values that will guide the development of architecture, standards, and policy. MHS EA Principles directly align to the DoD Information Enterprise Architecture, DoD Net-Centric guidance, and MHS IM/IT Strategic Plan.

The Office of the Chief Information Officer (OCIO) for MHS will be incorporating EA Principles into architecture, contracts, policy, guidance, and architecture compliance frameworks to ensure their promulgation and application.

MHS EA Principles, Version 1.0 will remain in effect until superseded or rescinded. This document will be reviewed and updated on an annual basis and published after approval by the MHS Enterprise Architecture Committee.

The point of contact in the Office of the OCIO EA Division is Ms. Stephanie Boyles. Ms. Boyles can be reached at Stephanie.Boyles@tma.osd.mil, or (703) 681-8788.

Jonathan Woodson, M.D.

Attachment:
Military Health System Enterprise Architecture Principles, Version 1.0

Military Health System (MHS)
Office of the Chief Information Officer (OCIO)

MHS Enterprise Architecture Principles

Version 1.0

Prepared by:
MHS Enterprise Architecture Committee

04/20/2011

Stephanie S. Boyles — 20 April 2011

Stephanie Boyles — **Date Signed**

Military Heath System (MHS)

Office of the Chief Information Officer (OCIO)

Director, Enterprise Architecture Division (EAD)

DoD TRICARE Management Activity (TMA)

Alan T. Smith — 20 APR 11

COL Alan T. Smith — **Date Signed**

Military Heath System (MHS)

Office of the Assistant Secretary Defense (Health Affairs) (OASD (HA)/TMA)

Director, Information Management

DoD TRICARE Management Activity (TMA)

TABLE OF CONTENTS

1. INTRODUCTION 4

1.1 BACKGROUND 4
1.2 PURPOSE AND SCOPE 4
1.3 AUDIENCE 5
1.4 BUSINESS VALUE AND OBJECTIVES 5
1.5 PARTICIPATING ORGANIZATIONS 7

2. MHS ENTERPRISE ARCHITECTURE PRINCIPLES 7

3. SUMMARY OVERVIEW 8

3.1 SUMMARY OVERVIEW 8

4. APPENDICES 9

4.1 APPENDIX A: REFERENCE DOCUMENTS 9
4.2 APPENDIX B: ACRONYMS LIST 10
4.3 APPENDIX C: MHS EA PRINCIPLES 12
4.3.1 Data Principles 12
4.3.2 Information Assurance 18
4.3.3 Infrastructure Principles 37
4.3.4 Service Principles 42
4.3.5 Application Principles 50
4.3.6 Global Principles 54
4.3.7 Requirements Principles 56

Tables:

TABLE 1: MHS EA PRINCIPLES MAPPED TO MHS IM/IT STRATEGIC PLAN2010-2015 PRINCIPLES 6
TABLE 2: MHS PRINCIPLES AND DEFINITIONS 8

1. INTRODUCTION

1.1 BACKGROUND

The Military Health System (MHS) Enterprise Architecture (EA) formally defines and describes the military healthcare environment that enables the MHS to manage complexity, respond to change and perform its operations in the most efficient and effective manner. The MHS EA supports all aspects of the MHS Strategic Plan, the MHS Information Management /Information Technology (IM/IT) Strategic Plan, and is fully compliant with the Department of Defense Architecture Framework (DoDAF) and Federal Enterprise Architecture (FEA) guidance. The current MHS EA includes the following four core mission area segments: 1) Providing Access to Care, 2) Managing Provision of Health Services, 3) Performing Population Health Management, and 4) Managing Health Service Performance. Supporting these four core processes are the business, technical, and information architectures. The architectures provide the scope of the MHS business working from the bottom up, integrating the data and determining the business rules for the data. Moving to identifying business processes and applying the business rules to the business processes; also, going further to lead the services which complete these business processes and the systems that are being used to help accomplish the mission of the MHS.

The MHS EA vision is to develop a collaborative, agile, efficient, and high-quality medical enterprise that adapts to the changing needs of military medicine and maximizes the benefit of business and IT resources. The MHS EA frames and guides system design to aid the fielding of flexible and interoperable IT products that support the healthcare mission and operational imperatives across the MHS as well as strengthen our partnership with other federal health agencies (e.g., Veteran Affairs (VA), Military Services). MHS is fully engaged in supporting the President's Health IT initiatives in the development of a nationwide health information technology infrastructure based on recognized health IT standards and practices while still maintaining our mission responsibility to support the health of our Warfighters. MHS remains aggressive in working towards aligning and leveraging our IT investments consistent with the President's goals, and the supporting laws and regulations of 2009 and 2010, to provide higher quality, efficient, and cost-effective healthcare through the utilization of health IT.

As the future state MHS EA continues to evolve, it will further align with the MHS Quadruple Aim, the MHS Strategic Plan, the MHS 2010-2015 IM/IT Strategic Plan, MHS EA Principles, and the Enterprise Transition Plan. It will provide greater exposure to those components that support the electronic collection of data and use of data beyond direct patient care. It will reflect a line of sight vision from the strategic goals to actionable architecture. The future state MHS EA will further refine and incorporate the corroboration and partnerships with other federal agencies and healthcare organizations.

1.2 PURPOSE AND SCOPE

MHS Enterprise Architecture (EA) Principles are intended to express the MHS' intention on key issues to ensure design and investment decisions can be made from a common basis of understanding. Enterprise Architecture principles provide enduring guidelines that describe ways in which the MHS should fulfill its information management/information technology mission. The purpose of this document is to define the high-level principles (also known as tenets) that will provide a general roadmap for success in key design considerations, developing architectures, and enabling decision-making for MHS IM/IT investments. The associated

business rules for each principle (definitive statements that constrain operations to implement a principle) will be addressed in a future edition of this document.

1.3 AUDIENCE

The MHS EA Principles provides a common basis of understanding for key design considerations and investment decisions. The consumers of the MHS EA Principles include the following sets of customers:

1. Chief Information Officer Management Board (CIO-MB), Military Medical Services CIOs, Enterprise Architecture Committee, Portfolio Managers, Information Management, Program Managers, IT Solution and Product Managers.
2. IM/IT analyst, architects, engineers, and developers across the MHS IM/IT portfolio.

1.4 BUSINESS VALUE AND OBJECTIVES

The MHS EA Principles provide a common basis of understanding for requirements and key design and implementation considerations. They provide a set of values that guide IT decision-making and activities and form the foundation for IT architecture, standards, and policy development throughout the enterprise. Principles allow for diverse business, operational, and technical personnel in the enterprise or workgroup to develop a common language and shared understanding of the challenges faced, and are necessary to achieve the degree of organizational consensus required for an integrated and standards-based architecture.

The MHS EA guiding principles are drawn from Federal, DoD, and MHS policy and guidance, as well as commercially available best practices. These principles directly support the MHS alignment to the DoD Information Enterprise Architecture (DIEA), DoD net-centric guidance, and the MHS 2010-2015 IM/IT Strategic Plan Principles as shown in Table 1 below.

MHS IM/IT Strategic Plan 2010 -2015 Principles	MHS EA Principles						
	Data	Information Assurance	Infrastructure	Services	Applications/ Systems	Global	Requirements
Support the Warfighters and their families	X	X	X	X	X	X	X
Promote innovation						X	X
Adopt business process solution in concert with a technical solution	X	X	X		X	X	
Ensure information integrity and security	X	X		X		X	
Establish consistent, integrated, aligned, agile and interoperable enterprise architecture	X	X	X	X	X	X	X
Reduce complexity for the end-user				X		X	
Reduce time to implement functional capabilities	X		X	X	X	X	X
Use Industry standards and best practices				X	X	X	X

Table 1: MHS EA Principles Mapped to MHS IM/IT Strategic Plan 2010-2015 Principles

The goals and benefits of the MHS EA Principles are as follows:

1. Provide a basic set of criteria for which all MHS IT investments will comply.
2. Provide a core set of rules and guidelines which promote standardization and best practices within the organization.
3. Promote a general roadmap for success and a common basis of understanding for key design and implementation considerations, as well as decision making.
4. Provide a ready to use reference to ensure alignment both horizontally with enterprise capabilities and vertically with Federal and DoD strategic direction and federation partners.
5. Guide MHS initiatives, programs, and solutions in design and/or their successful alignment with MHS IM/IT goals.

1.5 PARTICIPATING ORGANIZATIONS

The MHS EA principles presented in this document were identified, reviewed, and agreed upon by a MHS EA Principles Tiger Team convened by the Office of the Chief Information Officer Management Board (CIO MB) Enterprise Architecture Committee (EAC). The EA Principles Tiger Team consisted of a group of representatives from different offices within the Military Health System who also contributes content for the overall MHS Enterprise Architecture. The skills and experience of the practitioners spanned across many of the core disciplines required for delivering healthcare information management and information technology to include: Enterprise Architecture, Project Management, Data Management, Software and Systems Engineering, Services, Network and Infrastructure, Application Development, Information Assurance, Business and Clinical Analysis, and Requirements Management, etc. Below is the list of participants for the EA Principles Tiger Team:

- Air Force Medical Service Enterprise Architecture (AFMS EA)
- Army Medical Department, Army Medical Command, Office of the Surgeon General (AMEDD OTSG)
- Deputy Assistant Secretary of Defense (DASD)/Information Management Directorate (IM)
- Program Executive Office (PEO), Defense Health Information Management System (DHIMS)
- Program Executive Office (PEO), Defense Health Service System (DHSS)
- MHS Chief Technology Officer (CTO)
- MHS Cyberinfrastructure Services (MCiS)
- Program Executive Office (PEO), MHS Joint Medical Information Systems Office (JMIS)
- Office of the Chief Information Officer Enterprise Architecture Division (OCIO EAD)
- Bureau of Medicine and Surgery (BUMED)
- Navy Information Systems Support Activity (NAVMISSA)

2. MHS ENTERPRISE ARCHITECTURE PRINCIPLES

The MHS EA principles provide a core set of rules and guidelines, which promote standardization and best practices within the organization. These principles provide context to help everyone from policy makers to system developers understand implications of design and implementation choices. Applied pragmatically, the MHS EA principles will drive common solutions and promote consistency and integration across key programs, applications, and services. Additional sample uses of these principles include EA development, EA compliance during the Defense Business IT Certification (DBITC), validation and verification of capabilities during Program Objective Memo (POM) review, Systems Engineering, Acquisition, JCIDS processes.

The major categories of EA principles are defined below in Table 2. A summarized set of principles are provided in Tables 2.1 through 2.7. The amplification and explanation of each principle is provided in Appendix C.

Principles	Description
Data Principles	Allows information, which is a strategic asset, to be visible, accessible, understood, and trusted to authorized users. Provides the foundation for moving the MHS to a Service Oriented Environment. Ensures data and services are decoupled from applications and systems.
Information Assurance Principles	Ensures data and services are secured and trusted, the proper security is provided, and security issues do not hinder access to information. Allows users to discover data and services, access them based on their authorization, and promotes permissions and authorizations following users wherever they are on the network.
Infrastructure Principles	Promotes IT capabilities that are survivable, resilient, redundant, and reliable to enable continuity of operations and disaster recovery in the presence of attack, failure, accident, and natural or man-made disaster. Ensures that a transport infrastructure is in place that provides adequate bandwidth and access to MHS and DoD capabilities.
Services Principles	Supports service-oriented definition and design, and the availability of authoritative investments in the net-centric environment through services.
Applications Principles	Fosters better application development, common interfaces, and integration, and redundant data entry.
Global Principles	Spans across the enterprise, are universal and cross-cutting all capabilities and ensures MHS governed resources are well conceived, designed, operated and managed to address the mission needs of the MHS.
Requirements Principles	Provides a framework for developing and managing requirements throughout the MHS enterprise. The outlined principles are derived from DoD guidance as well as best practices across many industries. The key principles for developing requirements ensures the solution meets the original needs of the end-user by having requirements that are testable, costable, traceable, adaptable and interoperable. Enterprise standards should be in place and used in order to provide quality requirements that align strategically to MHS strategic initiatives.

Table 2: MHS Principles and Definitions

3. SUMMARY OVERVIEW

3.1 SUMMARY OVERVIEW

The MHS EA Principles presented in this document were identified, reviewed, and agreed by Enterprise Architecture Principles Tiger Team. The EA Principles Tiger Team was convened by the CIO Management Board Enterprise (CIO MB) Architecture Committee (EAC) and represented by the functional and technical stakeholders of the Military Health System. This set of principles provides a common understanding for Data, Infrastructure, Service, Application, Global, Requirements, and Information Assurance. The MHS EA Principles provide an authoritative set of tenets to guide MHS initiatives, programs, and solutions in design and their successful alignment with MHS IM/IT goals. The principles will be presented to the MHS Enterprise Architecture Committee and recommended for adoption and promulgation to the MHS community.

4. APPENDICES

4.1 APPENDIX A: REFERENCE DOCUMENTS

- *Department of Defense Information Enterprise Architecture version 1.2,* May 07, 2010
- *National Institute of Health Enterprise Architecture Data Principles,* August 5, 2003
- *Recommendations for Implementing and Managing a Net-Centric Data Strategy in the MHS,* October 27, 2006
- *Net-centric Enterprise Solutions for Interoperability (NESI) version 3.2 or higher*, http://nesipublic.spawar.navy.mil/
- *Service-Oriented Architecture; Concepts, Technology and Design. Thomas Erl.* Prentice Hall, 2005
- *SOA Practitioners' Guide Part 2 SOA Reference Architecture*, 15 September 2006
- *OASIS Reference Architecture for Service Oriented Architecture Version 1.0 Public Review Draft 1,* 23 April 2008
- *The Open Group SOA Source Book 3rd Edition*, April 2009
- *OASIS Web Service Atomic Transaction (WS-AtomicTransaction),* Feb 2009
- *USD(AT&L) Memorandum, Subject: Amplifying DoDD 5000.1 Guidance Regarding Modular Open Systems Approach (MOSA) Implementation*, April 2004
- *DoD Systems 2020 initiative, Congressional Testimony*, May 18, 2010
- *DoD Net-Centric Data Strategy,* 09 May 2003
- *MHS IM/IT Strategic Plan, Defense Business Board "Task Group on Strengthening the DoD Enterprise Governance*", 2008
- *Acquisition Community Connection* - Defense Acquisition University, https://acc.dau.mil/
- *Business Analysis Body of Knowledge (BABOK Guide) V 2.0*
- *DoD Principal Accrediting Authorities (PAAs) Memorandum, Subject: DoD Information System Certification and Accreditation Reciprocity,* 23 July 2009

4.2 APPENDIX B: ACRONYMS LIST

ACRONYM	DESCRIPTION
AoA	Analysis of Alternatives
CIO	Chief Information Officer
CIR	Computing Infrastructure Readiness
COD	Capability on Demand
COOP	Continuity of Operations Plan
CPM	Capability Port Manager
CR	Communications Readiness
DBITC	Defense Business Information Technology Certification
DDR&E	Director of Defense Research and Engineering
DIEA/DoDIEA	Defense Information Enterprise Architecture
DoD	Department of Defense
DoD S&T	Department of Defense Science and Technology
DSD	Data and Services Deployment
EA	Enterprise Architecture
EAB	Enterprise Architecture Board
EAC	Enterprise Architecture Committee
EAD	Enterprise Architecture Division
EHR	Electronic Health Record
IA	Information Assurance
IM/IT	Information Management/Information Technology
IT	Information Technology
JCIDS	Joint Capabilities Integration and Development System
MHS	Military Health System
MBE	Military Based Engineered
MOSA	Modular Open Systems Approach
NIH	National Institute of Health

NESI	Net-Centric Enterprise Solutions for Interoperability
NOA	Network Operations Agility
OCIO	Office of the Chief Information Officer
OFI	Opportunity for Improvement
PBE	Platform Based Engineering
POC	Point of Contact
POM	Program Objective Memorandum
ROI	Return on Investment
SA	Secured Availability
SME	Subject Matter Expert
SOA	Service Oriented Architecture
TMA	TriCare Management Activity
TSD	Trusted Systems Design
USD (AT&L)	Under Secretary of Defense for Acquisition, Technology, and Logistics
VA	Veterans Affairs
VHA	Veterans Health Administration
WG	Working Group

4.3 APPENDIX C: MHS EA PRINCIPLES

4.3.1 Data Principles

The MHS Data Principles allow information, which is a strategic asset, to be visible, accessible, understood, and trusted to authorize users. These Principles provide the foundation for moving the MHS to a Service Oriented Environment. Additionally, they ensure data and services are decoupled from applications and systems.

Code	Title	Principle	Source	Definition	Amplification	Example
D-1	Net-Centric Data Strategy	Data should be accessible, interoperable, understandable, trusted, responsive to user needs, and discoverable by all authorized users.	DoD Defense Information Enterprise Architecture v1.2, May 07, 2010	**Accessible**: the ability to retrieve the data by a human, system or application. (source: DoD Directive 8320.02) **Interoperable:** the ability to communicate and exchange data accurately, effectively, securely, and consistently with different information technology systems, software applications, and networks in various settings, and exchange data such that clinical or operational purpose and meaning of the data are preserved and unaltered. (source: Executive Order 13410) **Understandable:** capable of being comprehended in terms of subject, specific content, relationships, sources, methods, quality, spatial and temporal dimensions, and other factors. (source: DoD Directive 8320.02) **Trusted:** Users and applications can determine and assess the authority of the source because the pedigree, security level, and access control level of each data asset is known and available. **Responsive to User Needs:** the quality of reacting quickly to fulfill users needs in terms of functionality, performance, content coverage and content quality. (source: NCES Techguide)	**Accessible:** Users and applications post data to a "shared space" in which (1) descriptive information about the asset (metadata) has been provided to a catalog that is visible to the Enterprise and (2) the data is stored such that users and applications in the Enterprise can access it. Data assets are made available to any user or application except when limited by policy, regulation, or security. **Interoperable:** Data assets are made interoperable through the use of data exchange syntax and semantics common used by a Community of Interest (COI), and by ensuring that the data exposure solution is compliant with any relevant standards and/or conventions. **Trusted:** Data assets shall have associated information assurance and security metadata, and an authoritative source shall be identified when appropriate. Responsive to User Needs: Perspectives of users, whether data consumers or data producers, are incorporated into data approaches via continual feedback to ensure satisfaction. **Discoverable:** Users and applications can discover the existence of data assets through catalogs, registries, and other search services. All data assets (intelligence, non-intelligence, raw, and processed) are advertised or "made visible" by providing metadata, describing the asset. **Understandable:** Users and applications can comprehend the data, both structurally and semantically, and readily determine how the data may be used for their specific needs through publication of rich descriptive metadata. Understandability is closely related to an aspect of transparency. The more	**If Implemented:** Patient medical data is collected and stored in a relational database. In order to meet the Net-centric data goals the following must occur: to provide accessibility, expose the data via a web service that can query the database upon user request, and provide the data in XML to the requesting application. Ensure the web service is WS-I compliant to provide interoperability. Understandability is accomplished by annotating the XML Schema, indicating what each term in the vocabulary meant and how it will be populated. Register the WSDL file and the XML schema to a metadata registry and the service endpoint with a service registry to achieve discoverability. A security service will be used that ensures only those who are authorized to access are able to do so (trusted). **If Not Implemented:** Patient medical data is collected and stored in a relational database supported by a legacy application. The data in the database is only accessible, discoverable, understandable, and trusted to a user coming in through the legacy application.

Code	Title	Principle	Source	Definition	Amplification	Example
				Discoverable: able to be seen, detected, or distinguished and to some extent characterized by humans and/or IT systems, applications, or other processes.	transparent the syntax and semantics associated with a given information sharing capability are, the easier it is to understand.	
D-2	Data-Centric Architecture	Data must be separate from applications.	DoD Defense Information Enterprise Architecture v1.2, May 07, 2010	**Data-centric:** Data is the most important part of the system, with the functionality grouped around the data, providing the user with different tools.	In a data centric architecture, the data is separated from the end-user application, usually with a services layer in between. Data is posted to a shared space, described using metadata. Applications post and pull data from a shared space so that multiple different ones can make use of the same data, promoting its re-use or re-purposing.	**If Implemented:** COTS dental digital imaging applications post imaging data to a repository that is available enterprise-wide via a registry (the shared space) to be pulled by a computer-aided diagnosis application that identifies oral pre-cancers. **If Not Implemented:** Create a point-to-point interface for the computer-aided diagnosis application with the COTS dental digital imaging application to get particular images. After this interface is complete, other applications are still unable to access the images.
D-3	Authoritative Data Source	All data must have an identified authoritative source.	DoD Defense Information Enterprise Architecture v1.2, May 07, 2010	**Authoritative source:** A source of data or information that is trusted because it is considered to be highly reliable or accurate or is from an official publication or reference. (source: DoD Directive 8320.02)	Data associated with an identified authoritative source can be re-used or re-purposed. It decreases duplicative data entry, data capture and reduces redundant information sources, providing improved efficiency.	**If Implemented:** Person information entered into DEERS (authoritative source). Same information is pulled from DEERS and used to populate Patient Registration. **If Not Implemented:** Person information entered into DEERS. Same information is manually entered into an MHS Patient Registration system ("min-reg"). Now same data exists in two places with possibility that the information is slightly different if it is not entered correctly.

Code	Title	Principle	Source	Definition	Amplification	Example
D-4	Smart Data Pull	Data producers should be responsible for making the data accessible. Consumers should be responsible for determining the data that they need ("smart pull").	DoD Directive 8320.2, Data Sharing in a Net-Centric Department of Defense, December 02, 2004	**Smart pull:** a net-centric attribute in which users can find and directly subscribe or use value added services.	The data producer is not responsible for determining all the ultimate destinations of the data, only for posting it to an accessible shared space. The consumer determines that it has a need for the information and either pulls it directly or uses discovery services to pull it from the shared space. This principle does not rule out implementation of a publish-subscribe asynchronous mechanism for data transfer, even though such a pattern sometimes is referred to as a "push" (vs. a "pull" being a synchronous request-response pattern). Publish/subscribe still supports the unanticipated user—the consumers determine when they will become subscribers—the producers' only concern is to publish (post).	**If Implemented:** Raw disease surveillance data is posted to the shared space where it can be pulled by any data consumer with valid credentials and subsequently analyzed per the data consumer analysis needs. Data consumer determines need for data. New unanticipated users can access the data in the future without requiring further changes to the data provider. **If Not Implemented:** Raw disease surveillance data is processed and analyzed using a specific set of analysis protocols. The results are sent as a report to a predetermined list of recipients. Data producer determines need for data. Unanticipated users cannot access the data unless a change is made to the data provider.
D-5	Post Data in Parallel	Data should be widely available as soon as possible after it is committed.	DoD Directive 8320.2, Data Sharing in a Net-Centric Department of Defense, December 02, 2004	**Post in parallel:** a net-centric attribute in which the data producer makes data visible and accessible without delay so that users get it when and how needed.	Data should be available as soon as possible. Required analysis and further processing should not hold up availability of confirmed, validated data (this does not imply that uncommitted, preliminary data should be made available for sharing).	**If Implemented:** Raw disease surveillance data is posted to the shared space immediately after validation where it can be accessed by any data consumer with valid credentials, providing near-instantaneous data access. **If Not Implemented:** Raw disease surveillance data is processed and analyzed using a specific set of analysis protocols that are computationally intensive, requiring several days to complete. The results of the analysis are posted to the shared space as a report where it can be accessed. A significant delay in data access is introduced.

Code	Title	Principle	Source	Definition	Amplification	Example
D-6	Data Semantics & Syntax	Semantics and syntax for data sharing should be defined by communities of interest.	DoD Defense Information Enterprise Architecture v1.2, May 07, 2010	**Community of interest:** a collection of people who exchange information using a common vocabulary in support of shared missions, business processes, and objectives. (source: Department of Defense Net-Centric Data Strategy)	COIs bring together the user's needs and provider's capabilities and identify the most important data and the capabilities needed to support agile collaborative community business processes. The idea is to use COIs to delegate the structural (representation of data) and semantic (meaning of data) standardization down to a more manageable unit, instead of having to agree on a single data model across the DoD. The creation of MHS-related COIs should be driven by the need to support enterprise-wide interoperability rather than formed at an organization or geographic level such as an MTF.	**If Implemented:** Establish a MHS-wide Access to Care COI that defines structural and semantic standardization across the MHS and enables the exchange of information such as appointments, available schedules, and clinic and provider taxonomies across the enterprise. **If Not Implemented:** Define clinic, appointment, and provider taxonomies and semantics for each individual MTF.
D-7	Data Standards	Design and implementation shall use prescribed standards.	DoD Defense Information Enterprise Architecture v1.2, May 07, 2010	**Data Standard:** Data standards are defined as consensual specifications for the representation of data from different sources or settings. Standards are necessary for the sharing, portability, and reusability of data. The notion of standardized data includes specifications for both data fields (~variables) and value sets (~codes) that encode the data within these fields. (source: NCBI, NIH)	Standards establish uniform engineering and technical requirements for processes, procedures, practices, and methods. They provide a foundation for interoperability, ensure compliance with security and information assurance requirements, and govern the implementation of services and the operation of IT systems. Emerging or evolving standards relevant to IT systems should be considered.	**If Implemented:** ERCCR initiative uses the X12 275 message standard to transmit the CLR to the CDR so that any consult result from any MCSC can be stored, managed, and viewed in AHLTA. **If Not Implemented:** Laboratory test codes (Internal Exchange Numbers/IENs) in CHCS are not standardized so that each MTF must maintain its own list and the codes are not meaningful between MTFs.
D-8	Data Creation	Only handle information once. Information that exists should be reused rather than recreated.	DoD Defense Information Enterprise Architecture v1.2, May 07, 2010		This principle will promote the efficiency; accuracy and consistency of data.	
D-9	Data as a Business Asset	Data is a business asset and will be organized and managed to ensure that its value to the enterprise is maximized.	NIH EA Data Principles August 5, 2003		Organizing and managing the key data assets of the company drive the business processes needed to run the enterprise.	
D-10	Support Federal Mandates	Data supporting any federal government mandate is defined as enterprise data.	Recommendations for Implementing and Managing a Net-Centric Data Strategy in the MHS October 27, 2006		Policy makers and governance entities must insure DoD data standards and protocols are adopted, and that system development initiatives comply with these data standards.	

Code	Title	Principle	Source	Definition	Amplification	Example
D-11	Data Ownership	All enterprise data will have an identified business owner and a technical owner. The business owner will be responsible for defining and publishing the logical data, defining the sensitivity and criticality of the data and approving changes from a business perspective. The technical owner will define and publish the physical implementation of the logical data, adhering to the architectural data standards.	Recommendations for Implementing and Managing a Net-Centric Data Strategy in the MHS October 27, 2006		**Ownership and stewardship:** Accountability for the standardization and quality of data must reside with the business owners and stewards of the source data. Data owners/producers are responsible for making their data assets visible, accessible, and understandable.	
D-12	Standardization of Shared Data	Enterprise data standards should be identified when the value of interoperability with other information systems exceeds the value of uniqueness.	NIH EA Data Principles August 5, 2003		Standardization may reduce the duplication of effort and provide improved reporting. It may reduce the number of IC-managed systems.	
D-13	Standardization of Common Data	Enterprise data standards should be identified when the value of commonality across MHS exceeds the value of uniqueness.	NIH EA Data Principles August 5, 2003		Standardization may reduce the duplication of effort and provide improved reporting. It may reduce the number of IC-managed systems.	
D-14	Data Integrity	Authority to create and maintain the data will reside with those most knowledgeable about the data or those most able to control its accuracy.	Recommendations for Implementing and Managing a Net-Centric Data Strategy in the MHS October 27, 2006		For shared assets to be trusted, users and applications must be able to assess the authority of the source. Authoritative sources for key data assets in their shared data domain must be identified.	
D-15	Data Identifiers	Every object in the enterprise will contain a globally unique identifier.	Recommendations for Implementing and Managing a Net-Centric Data Strategy in the MHS October 27, 2006		In an integrated environment, it is frequently necessary to retrieve objects (or data) from other more authoritative sources for that information. To do that reliably requires that the requestor be able to make an unambiguous request. Unique identifiers provide an unambiguous name for the desired data	

Code	Title	Principle	Source	Definition	Amplification	Example
D-16	Data Tagging	Data in motion or at rest will adhere to Federal, DoD or industry data tagging rules and standards.	MHS Enterprise Architecture Workgroup February 2, 2011		Rules for content descriptors must be developed. Content descriptors provide "content-related" details about data assets, such as topics, keywords, context, and other content-related information that gives users and applications insight into the meaning and use of the data. Content metadata provides a basis for search engines to perform searches for data assets that address specific topics. Format descriptors may also be needed to convey the physical manifestation of an asset. For example, the format descriptors will provide information regarding the type of digital file. In addition, the format descriptors can contain optional information that describes the extent of the asset, such as file size, bit rate, and dimensions.	

4.3.2 Information Assurance

The MHS Information Assurance Principles ensure data and services are secured and trusted; the proper security is provided, and security issues do not hinder access to information. These principles focus on allowing users to discover data and services and access them based on their authorization. They promote permissions and authorizations following users wherever they are on the network.

Code	Title	Principle	Source	Definition	Amplification	Example
IA-1	Security Foundation	Establish a sound security policy as the "foundation" for design.	Principles for Information Technology Security (A Baseline for Achieving Security), Revision A	A security policy is an important document to develop while designing an information system. The security policy begins with the organization's basic commitment to information security formulated as a general policy statement. The policy is then applied to all aspects of the system design or security solution. The policy identifies security goals (e.g., confidentiality, integrity, availability, accountability, and assurance) the system should support and these goals guide the procedures, standards and controls used in the IT security architecture design. The policy also should require definition of critical assets, the perceived threat, and security-related roles and responsibilities.	DoD D number 8500.01 reference (A) / section 5.9.1	
	Security Foundation	Treat security as an integral part of the overall system design.	Principles for Information Technology Security (A Baseline for Achieving Security), Revision A	Security must be considered in information system design. Experience has shown it to be both difficult and costly to implement security measures properly and successfully after a system has been developed, so it should be integrated fully into the system life-cycle process. This includes establishing security policies, understanding the resulting security requirements, participating in the evaluation of security products, and finally in the engineering, design, implementation, and disposal of the system.	DoD D number 8500.01 reference (A)	

Code	Title	Principle	Source	Definition	Amplification	Example
	Security Foundation	Clearly delineate the physical and logical security boundaries governed by associated security policies.	Principles for Information Technology Security (A Baseline for Achieving Security), Revision A	Information technology exists in physical and logical locations, and boundaries exist between these locations. An understanding of what is to be protected from external factors can help ensure adequate protective measures are applied where they will be most effective Sometimes a boundary is defined by people, information, and information technology associated with one physical location. But this ignores the reality that, within a single location, many different security policies may be in place, some covering publicly accessible information and some covering sensitive unclassified information. Other times a boundary is defined by a security policy that governs a specific set of information and information technology that can cross physical boundaries. Further complicating the matter is that, many times, a single machine or server may house both public-access and sensitive unclassified information. As a result multiple security policies may apply to a single machine or within a single system. Therefore, when developing an information system, security boundaries must be considered and communicated in relevant system documentation and security policies.	DoDI 8500.2 reference E2.1.16.2.	
	Security Foundation	Ensure that developers are trained in how to develop secure software.	Principles for Information Technology Security (A Baseline for Achieving Security), Revision A	It is unwise to assume that developers know how to develop secure software. Therefore, ensure that developers are adequately trained in the development of secure software before developing the system. This includes application of	NIST SP 800-27 Rev A / DoDI 8500.2 section 5.7.7	

Code	Title	Principle	Source	Definition	Amplification	Example
				engineering disciplines to design, development, configuration control, and integration and testing.		
IA-2	Risk Based	Reduce risk to an acceptable level.	Principles for Information Technology Security (A Baseline for Achieving Security), Revision A	Risk is defined as the combination of (1) the likelihood that a particular threat source will exercise (intentionally exploit or unintentionally trigger) a particular information system vulnerability and (2) the resulting adverse impact on organizational operations, organizational assets, or individuals should this occur. Previously, risk avoidance was a common IT security goal. That changed as the nature of the risk became better understood. Today, it is recognized that elimination of all risk is not cost-effective. A cost-benefit analysis should be conducted for each proposed control. In some cases, the benefits of a more secure system may not justify the direct and indirect costs. Benefits include more than just prevention of monetary loss; for example, controls may be essential for maintaining public trust and confidence. Direct costs include the cost of purchasing and installing a given technology; indirect costs include decreased system performance and additional training. The goal is to enhance mission/business capabilities by mitigating mission/business risk to an acceptable level.	DoDI 8500.2 section 5.7.16	

Code	Title	Principle	Source	Definition	Amplification	Example
	Risk Based	Assume that external systems are insecure.	Principles for Information Technology Security (A Baseline for Achieving Security), Revision A	The term information domain arises from the practice of partitioning information resources according to access control, need, and levels of protection required. Organizations implement specific measures to enforce this partitioning and to provide for the deliberate flow of authorized information between information domains. The boundary of an information domain represents the security perimeter for that domain. An external domain is one that is not under your control. In general, external systems should be considered insecure. Until an external domain has been deemed "trusted," system engineers, architects, and IT specialists should presume the security measures of an external system are different than those of a trusted internal system and design the system security features accordingly.	DODI 8500.2 section E3.4.1.4	
	Risk Based	Identify potential trade-offs between reducing risk and increased costs and decrease in other aspects of operational effectiveness.	Principles for Information Technology Security (A Baseline for Achieving Security), Revision A	To meet stated security requirements, a systems designer, architect, or security practitioner will need to identify and address all competing operational needs. It may be necessary to modify or adjust (i.e., trade-off) security goals due to other operational requirements. In modifying or adjusting security goals, an acceptance of greater risk and cost may be inevitable. By identifying and addressing these trade-offs as early as possible, decision makers will have greater latitude and be able to achieve more effective systems.	Acquisition Management, 5000 series	

Code	Title	Principle	Source	Definition	Amplification	Example
	Risk Based	Implement tailored system security measures to meet organizational security goals.	Principles for Information Technology Security (A Baseline for Achieving Security), Revision A	In general, IT security measures are tailored according to an organization's unique needs. While numerous factors, such as the overriding mission requirements, and guidance, are to be considered, the fundamental issue is the protection of the mission or business from IT security-related, negative impacts. Because IT security needs are not uniform, system designers and security practitioners should consider the level of trust when connecting to other external networks and internal sub-domains. Recognizing the uniqueness of each system allows a layered security strategy to be used – implementing lower assurance solutions with lower costs to protect less critical systems and higher assurance solutions only at the most critical areas.	DODI 8500.2 section E3.3.2	
	Risk Based	Protect information while being processed, in transit, and in storage.	Principles for Information Technology Security (A Baseline for Achieving Security), Revision A	The risk of unauthorized modification or destruction of data, disclosure of information, and denial of access to data while in transit should be considered along with the risks associated with data that is in storage or being processed. Therefore, system engineers, architects, and IT specialists should implement security measures to preserve, as needed, the integrity, confidentiality, and availability of data, including application software, while the information is being processed, in transit, and in storage.	DODI 8500.2 section E2.1.17	

Code	Title	Principle	Source	Definition	Amplification	Example
	Risk Based	Consider custom products to achieve adequate security.	Principles for Information Technology Security (A Baseline for Achieving Security), Revision A	Designers should recognize that in some instances it will not be possible to meet security goals with systems constructed entirely from COTS products. In such instances, it will be necessary to augment COTS with non-COTS mechanisms.	DODI 8500.2	
	Risk Based	Protect against all likely classes of "attacks".	Principles for Information Technology Security (A Baseline for Achieving Security), Revision A	In designing the security controls, multiple classes of "attacks" need to be considered. Those classes that result in unacceptable risk need to be mitigated. Examples of "attack" classes are: Passive monitoring, active network attacks, exploitation by insiders, attacks requiring physical access or proximity, and the insertion of backdoors and malicious code during software development and/or distribution.	DODI 8500.2	
IA-3	Ease of Use	Where possible, base security on open standards for portability and interoperability.	Principles for Information Technology Security (A Baseline for Achieving Security), Revision A	Most organizations depend significantly on distributed information systems to perform their mission or business. These systems distribute information both across their own organization and to other organizations. For security capabilities to be effective in such environments, security program designers should make every effort to incorporate interoperability and portability into all security measures, including hardware and software, and implementation practices.	DODI 8500.2 E3.4.2.1	

Code	Title	Principle	Source	Definition	Amplification	Example
	Ease of Use	Use common language in developing security requirements.	Principles for Information Technology Security (A Baseline for Achieving Security), Revision A	The use of a common language when developing security requirements permits organizations to evaluate and compare security products and features evaluated in a common test environment. When a "common" evaluation process is based upon common requirements or criteria, a level of confidence can be established that ensures product security functions conform to an organization's security requirements. The Common Criteria provides a source of common expressions for common needs and supports a common assessment methodology.	DODI 8500.2 E2.1.3	
	Ease of Use	Design security to allow for regular adoption of new technology, including a secure and logical technology upgrade process.	Principles for Information Technology Security (A Baseline for Achieving Security), Revision A	As mission and business processes and the threat environment change, security requirements and technical protection methods must be updated. IT-related risks to the mission/business vary over time and undergo periodic assessment. Periodic assessment should be performed to enable system designers and managers to make informed risk management decisions on whether to accept or mitigate identified risks with changes or updates to the security capability. The lack of timely identification through consistent security solution re-evaluation and correction of evolving, applicable IT vulnerabilities results in false trust and increased risk. Each security mechanism should be able to support migration to new technology or upgrade of new features without requiring an entire system redesign. The security design should	DODI 8500.2	

Code	Title	Principle	Source	Definition	Amplification	Example
				be modular so that individual parts of the security design can be upgraded without the requirement to modify the entire system.		
	Ease of Use	Strive for operational ease of use.	Principles for Information Technology Security (A Baseline for Achieving Security), Revision A	The more difficult it is to maintain and operate a security control; the less effective that control is likely to be. Therefore, security controls should be designed to be consistent with the concept of operations and with ease-of-use as an important consideration. The experience and expertise of administrators and users should be appropriate and proportional to the operation of the security control. An organization must invest the resources necessary to ensure system administrators and users are properly trained. Moreover, administrator and user training costs along with the life-cycle operational costs should be considered when determining the cost effectiveness of the security control.	DODD 5000.1	
IA-4	Increase Resilience	Implement layered security. Ensure no single point of vulnerability.	Principles for Information Technology Security (A Baseline for Achieving Security),	Security designs should consider a layered approach to address or protect against a specific threat or to reduce vulnerability. For example, the use of a packet-filtering router	DODI 8500.2	

Code	Title	Principle	Source	Definition	Amplification	Example
			Revision A	in conjunction with an application gateway and an intrusion detection system combine to increase the work-factor an attacker must expend to successfully attack the system. Adding good password controls and adequate user training improves the system's security posture even more. The need for layered protections is especially important when commercial-off-the-shelf (COTS) products are used. Practical experience has shown that the current state-of-the-art for security quality in COTS products does not provide a high degree of protection against sophisticated attacks. It is possible to help mitigate this situation by placing several controls in series, requiring additional work by attackers to accomplish their goals.		
	Increase Resilience	Design and operate an IT system to limit damage and to be resilient in response.	Principles for Information Technology Security (A Baseline for Achieving Security), Revision A	Information systems should be resistant to attack, should limit damage, and should recover rapidly when attacks do occur. The principle suggested here recognizes the need for adequate protection technologies at all levels to ensure that any potential cyber attack will be countered effectively. There are vulnerabilities that cannot be fixed, those that have not yet been fixed, those that are not known, and those that could be fixed but are not (e.g., risky services allowed through firewalls) to allow increased operational capabilities. In addition to achieving a secure initial state, secure systems should have a well-defined status after failure, either to a secure failure state or via a recovery procedure to a known secure state.	DODI 8500.2	

Code	Title	Principle	Source	Definition	Amplification	Example
				Organizations should establish detect and respond capabilities, manage single points of failure in their systems, and implement a reporting and response strategy.		
	Increase Resilience	Provide assurance that the system is, and continues to be, resilient in the face of expected threats.	Principles for Information Technology Security (A Baseline for Achieving Security), Revision A	Assurance is the grounds for confidence that a system meets its security expectations. These expectations can typically be summarized as providing sufficient resistance to both direct penetration and attempts to circumvent security controls. Good understanding of the threat environment, evaluation of requirement sets, hardware and software engineering disciplines, and product and system evaluations are primary measures used to achieve assurance. Additionally, the documentation of the specific and evolving threats is important in making timely adjustments in applied security and strategically supporting incremental security enhancements.	DODI 8500.2	
	Increase Resilience	Limit or contain vulnerabilities.	Principles for Information Technology Security (A Baseline for Achieving Security),	Design systems to limit or contain vulnerabilities. If vulnerability does exist, damage can be limited or contained, allowing other information system elements to function properly. Limiting and containing	DODI 8500.2	

Code	Title	Principle	Source	Definition	Amplification	Example
			Revision A	insecurities also helps to focus response and reconstitution efforts to information system areas most in need.		
	Increase Resilience	Isolate public access systems from mission critical resources (e.g., data, processes, etc.).	Principles for Information Technology Security (A Baseline for Achieving Security), Revision A	While the trend toward shared infrastructure has considerable merit in many cases, it is not universally applicable. In cases where the sensitivity or criticality of the information is high, organizations may want to limit the number of systems on which that data is stored and isolate them, either physically or logically. Physical isolation may include ensuring that no physical connection exists between an organization's public access information resources and an organization's critical information. When implementing logical isolation solutions, layers of security services and mechanisms should be established between public systems and secure systems responsible for protecting mission critical resources. Security layers may include using network architecture designs such as demilitarized zones and screened subnets. Finally, system designers and administrators should enforce organizational security policies and procedures regarding use of public access systems.	DODI 8500.2	

Code	Title	Principle	Source	Definition	Amplification	Example
	Increase Resilience	Use boundary mechanisms to separate computing systems and network infrastructures.	Principles for Information Technology Security (A Baseline for Achieving Security), Revision A	To control the flow of information and access across network boundaries in computing and communications infrastructures, and to enforce the proper separation of user groups, a suite of access control devices and accompanying access control policies should be used. Determine the following for communications across network boundaries: • What external interfaces are required? • Whether information is pushed or pulled? • What ports, protocols, and network services are required? • What requirements exist for system information exchanges; for example, trust relationships, database replication services, and domain name resolution processes?	DODI 8500.2	
	Increase Resilience	Design and implement audit mechanisms to detect unauthorized use and to support incident investigations.	Principles for Information Technology Security (A Baseline for Achieving Security), Revision A	Organizations should monitor, record, and periodically review audit logs to identify unauthorized use and to ensure system resources are functioning properly. In some cases, organizations may be required to disclose information obtained through auditing mechanisms to appropriate third parties, including law enforcement authorities or Freedom of Information Act (FOIA) applicants. Many organizations have implemented consent to monitor policies which state that evidence of unauthorized use (e.g., audit trails) may be used to support administrative or criminal investigations.	DODI 8500.2	

Code	Title	Principle	Source	Definition	Amplification	Example
	Increase Resilience	Develop and exercise contingency or disaster recovery procedures to ensure appropriate availability.	Principles for Information Technology Security (A Baseline for Achieving Security), Revision A	Continuity of operations plans or disaster recovery procedures address continuance of an organization's operation in the event of a disaster or prolonged service interruption that affects the organization's mission. Such plans should address an emergency response phase, a recovery phase, and a return to normal operation phase. Personnel responsibilities during an incident and available resources should be identified. In reality, contingency and disaster recovery plans do not address every possible scenario or assumption. Rather, it focuses on the events most likely to occur and identifies an acceptable method of recovery. Periodically, the plans and procedures should be exercised to ensure that they are effective and well understood.	DODI 8500.2	
IA-5	Reduce Vulnerabilities	Strive for simplicity.	Principles for Information Technology Security (A Baseline for Achieving Security), Revision A	The more complex the mechanism, the more likely it may possess exploitable flaws. Simple mechanisms tend to have fewer exploitable flaws and require less maintenance. Further, because configuration management issues are simplified, updating or replacing a simple mechanism becomes a less intensive process.	DODD 8320.1	

Code	Title	Principle	Source	Definition	Amplification	Example
	Reduce Vulnerabilities	Minimize the system elements to be trusted.	Principles for Information Technology Security (A Baseline for Achieving Security), Revision A	Security measures include people, operations, and technology. Where technology is used, hardware, firmware, and software should be designed and implemented so that a minimum number of system elements need to be trusted in order to maintain protection. Further, to ensure cost-effective and timely certification of system security features, it is important to minimize the amount of software and hardware expected to provide the most secure functions for the system.	DODD 5200.28	
	Reduce Vulnerabilities	Implement least privilege.	Principles for Information Technology Security (A Baseline for Achieving Security), Revision A	The concept of limiting access, or "least privilege," is simply to provide no more authorizations than necessary to perform required functions. This is perhaps most often applied in the administration of the system. Its goal is to reduce risk by limiting the number of people with access to critical system security controls (i.e., controlling who is allowed to enable or disable system security features or change the privileges of users or programs). Best practice suggests it is better to have several administrators with limited access to security resources rather than one person with "super user" permissions. Consideration should be given to implementing role-based access controls for various aspects of system use, not only administration. The system security policy can identify and define the various roles of users or processes. Each role is assigned those permissions needed to perform its functions. Each permission specifies a permitted access to a particular resource (such as "read" and	DODI 8500.2	

Code	Title	Principle	Source	Definition	Amplification	Example
				"write" access to a specified file or directory, "connect" access to a given host and port, etc.). Unless permission is granted explicitly, the user or process should not be able to access the protected resource. Additionally, identify the roles/responsibilities that, for security purposes, should remain separate, this is commonly termed "separation of duties".		
	Reduce Vulnerabilities	Do not implement unnecessary security mechanisms.	Principles for Information Technology Security (A Baseline for Achieving Security), Revision A	Every security mechanism should support a security service or set of services, and every security service should support one or more security goals. Extra measures should not be implemented if they do not support a recognized service or security goal. Such mechanisms could add unneeded complexity to the system and are potential sources of additional vulnerabilities. An example is file encryption supporting the access control service that in turn supports the goals of confidentiality and integrity by preventing unauthorized file access. If file encryption is a necessary part of accomplishing the goals, then the mechanism is appropriate. However, if these security goals are adequately supported without inclusion of file encryption, then that mechanism would be an unneeded system complexity.	DODI 8500.2	

Code	Title	Principle	Source	Definition	Amplification	Example
	Reduce Vulnerabilities	Ensure proper security in the shutdown or disposal of a system.	Principles for Information Technology Security (A Baseline for Achieving Security), Revision A	Although a system may be powered down, critical information still resides on the system and could be retrieved by an unauthorized user or organization. Access to critical information systems must be controlled at all times. At the end of a system's life-cycle, system designers should develop procedures to dispose of an information system's assets in a proper and secure fashion. Procedures must be implemented to ensure system hard drives, volatile memory, and other media are purged to an acceptable level and do not retain residual information.	DODI 8500.2	
	Reduce Vulnerabilities	Identify and prevent common errors and vulnerabilities.	Principles for Information Technology Security (A Baseline for Achieving Security), Revision A	Many errors reoccur with disturbing regularity - errors such as buffer overflows, race conditions, format string errors, failing to check input for validity, and programs being given excessive privileges. Learning from the past will improve future results.	DODI 8500.2	
	Design with Network in Mind	Implement security through a combination of measures distributed physically and logically.	Principles for Information Technology Security (A Baseline for Achieving Security), Revision A	Often, a single security service is achieved by cooperating elements existing on separate machines. For example, system authentication is typically accomplished using elements ranging from the user-interface on a workstation through the networking elements to an application on an authentication server. It is important to associate all elements with the security service they provide. These components are likely to be shared across systems to achieve security as infrastructure resources come under more senior budget	DODI 8500.2	

Code	Title	Principle	Source	Definition	Amplification	Example
				and operational control.		
IA-6	Design with Network in Mind	Formulate security measures to address multiple overlapping information domains.	Principles for Information Technology Security (A Baseline for Achieving Security), Revision A	An information domain is a set of active entities (person, process, or devices) and their data objects. A single information domain may be subject to multiple security policies. A single security policy may span multiple information domains. An efficient and cost effective security capability should be able to enforce multiple security policies to protect multiple information domains without the need to separate physically the information and respective information systems processing the data. This principle argues for moving away from the traditional practice of creating separate LANs and infrastructures for various sensitivity levels (e.g., security classification or business function such as proposal development) and moving toward solutions that enable the use of common, shared, infrastructures with appropriate protections at the operating system, application, and workstation level. Moreover, to accomplish missions and protect critical functions, government and private sector organizations have many types of information to safeguard. With this principle in mind, system engineers, architects, and IT specialists should develop a security capability that allows organizations with multiple levels of information sensitivity to achieve the basic security goals in an efficient manner.	DODI 8500.2	

Code	Title	Principle	Source	Definition	Amplification	Example
	Design with Network in Mind	Authenticate users and processes to ensure appropriate access control decisions both within and across domains.	Principles for Information Technology Security (A Baseline for Achieving Security), Revision A	Authentication is the process where a system establishes the validity of a transmission, message, or a means of verifying the eligibility of an individual, process, or machine to carry out a desired action, thereby ensuring that security is not compromised by a non-trusted source. It is essential that adequate authentication be achieved in order to implement security policies and achieve security goals. Additionally, level of trust is always an issue when dealing with cross-domain interactions. The solution is to establish an authentication policy and apply it to cross-domain interactions as required. Note: A user may have rights to use more than one name in multiple domains. Further, rights may differ among the domains, potentially leading to security policy violations.	DODI 8500.2	
	Design with Network in Mind	Use unique identities to ensure accountability.	Principles for Information Technology Security (A Baseline for Achieving Security), Revision A	An identity may represent an actual user or a process with its own identity (e.g., a program making a remote access). Unique identities are a required element in order to be able to: • Maintain accountability and traceability of a user or process. • Assign specific rights to an individual user or process. • Provide for non-repudiation. • Enforce access control decisions. • Establish the identity of a peer in a secure communications path. • Prevent unauthorized users from	DODI 8500.2	

Code	Title	Principle	Source	Definition	Amplification	Example
				masquerading as an authorized user.		
IA-7	DoD Information System Certification and Accreditation Reciprocity	Security terms and conditions to achieve reciprocity when a DoD Component deploys an Enterprise IS across the DoD Information Enterprise and receiving DoD Components.	DoD PAAs, Memorandum for Secretaries of the military departments Chairman of the Joint Chiefs of Staff. 23 July 2009	The timely deployment of information systems (ISs) is critical to attaining the Department's strategic vision of Net-Centricity. Reciprocity of accreditation decisions and the artifacts contributing to the accreditation decision will advance information sharing, reduce rework and cycle time when establishing Combined/Joint ISs/networks, and support DoD mission accomplishments. Reciprocity defines mutual agreement among participating enterprises to accept each other's security assessments in order.	DODI 8500.2 , DoD Directive 5000.01, DoD Directive 8000.01, 000 Directive 8500.01E,	

4.3.3 Infrastructure Principles

The MHS Infrastructure Principles promote IT capabilities that are survivable, resilient, redundant, and reliable to enable continuity of operations and disaster recovery in the presence of attack, failure, accident, and natural or man-made disaster. They ensure that a transport infrastructure is in place that provides adequate bandwidth and access to MHS and DoD capabilities.

Code	Title	Principle	Source	Definition	Amplification	Example
I-1	Shared Infrastructure Continuity of Operations	GIG infrastructure capabilities must be survivable, resilient, redundant, and reliable to enable continuity of operations and disaster recovery in the presence of attack, failure, accident, and natural or man-made disaster.	DoD Defense Information Enterprise Architecture (DIEA) v1.2, May 7, 2010 Source: Alliance for Telecommunication Industry Solutions (ATIS), an ANSI Accredited SDO	**Survivable:** A property of a system, subsystem, equipment, process, or procedure that provides a defined degree of assurance that the named entity will continue to function during and after a natural or man-made disturbance. **Resilient:** The ability to recover from a failure. The term may be applied to hardware, software, or data. **Redundant:** The surplus capability provided for a system to improve the reliability and quality of service. **Reliable:** The continuous availability of a service during normal operating conditions and under emergency circumstances with minimal disruption.	The Global Information Grid (GIG) provides the necessary physical computing infrastructure and related services to allow DoD to operate according to net-centric principles. It must be robust enough to deliver guaranteed levels of capability to consumers and providers of the Department's data and services.	**If Implemented:** • Survivability – Uninterruptible power supply keeps infrastructure working during electrical outage. • Resilient – Auto restart of failed server software, back in seconds. • Redundancy – Data stored in dual databases, with appropriate failover. • Reliability – Clustered and cached environment permits continued use even after a failure. **If Not Implemented:** • Survivability – Inability of hardware to perform during electrical outage. • Resilient – Server requires manual reboot after failure, with a delay of minutes to hours. • Redundancy – Mission-critical operation performed by a single server, with no other failover capability. • Reliable – Frequent unexpected downtime.
I-2	Shared Infrastructure Connectivity	The GIG shall enable connectivity to all authorized users.	DIEA v 1.2 7 May 2010		GIG communications systems shall provide the flexibility to support network connectivity to all GIG nodes and users, including those changing their points of attachment among alternate operational and network domains and/or COIs.	

Code	Title	Principle	Source	Definition	Amplification	Example
I-3	Shared Infrastructure Manageability	GIG infrastructure capabilities must be scalable, changeable, deployable and manageable rapidly while anticipating the effects of the unexpected user.	DIEA v 1.2 7 May 2010		GIG communications systems shall be designed and configured to be robust, adaptive, and reliable by employing network and configuration management, diverse path cable routing, and automatic rerouting features, ass applicable.	
I-4	Computing Infrastructure Readiness (CIR)	Computing infrastructure must support all missions of the Department, and provide the edge with effective, on-demand, secure access to shared spaces and information assets across functional, security, national, and interagency domains.	DIEA v 1.2 7 May 2010	CIR seeks to transform DoD GIG from a hardware- and program-centric infrastructure, to one that is dynamic, shared, adaptable and sufficient to support global net-centric operations.	Computing Infrastructure shall be consolidated, to the greatest extent possible, so that fixed global/regional and deployed virtual CI resources are used efficiently. Shared computing and data storage resources shall be capable of being discoverable and accessible for virtual management and control across the GiG. All GiG computing infrastructure facilities must be accredited, certified, and approved by DoD-designated authorities.	
I-5	CIR Node Consolidation	Consolidation of computing infrastructure fixed-node operations is a desired result for cost efficiencies. It shall not be accomplished, however, at the expense of degrading mission capabilities and operational effectiveness.	DIEA v 1.2 7 May 2010	**Consolidation:** The merging and/or joining of core computing assets.	Physical implementation of computing infrastructure shall include transparent interfaces to users to minimize, if not eliminate, degradation in performance and Quality of Service (QoS).	**If Implemented:** A new application is going to be deployed with a projected 3000 new users. Current shared computing resources are underutilized. The new application can tap into the shared resources, eliminating the need to purchase additional servers. **If Not Implemented:** A new application is going to be deployed with a projected 3000 new users. Even though all currently deployed servers are underutilized, 8 new servers are purchased to accommodate the needs of the new application.

Code	Title	Principle	Source	Definition	Amplification	Example
I-6	CIR Platform Agnostics & Independence	Computing infrastructure must be able to provide secure, dynamic, computing platform-agnostic and location-independent data storage.	DIEA v 1.2 7 May 2010	**Platform Agnostic:** The ability of software to run on any computer operating environment (e.g., Linux, Windows, Mac). **Location-Independent Storage:** Services and applications will share storage across multiple physical locations, allowing consolidation and efficient use of data storage resources. Likewise, users will be able to access information transparently from anywhere.	Computing infrastructure shall be computing platform agnostic and location independent in providing transparent real-time provisions and allocation of shared resources.	**If Implemented:** Computing and data storage needs increase significantly for a period of two months due to a new clinical guideline requiring all pre-menopausal females over 40 years to have a baseline breast MRI. Shared data storage and computing resources are dynamically allocated to accommodate the need. **If Not Implemented:** Computing and data storage needs increase significantly for a period of two months due to a new clinical guideline requiring all pre-menopausal females over 40 years to have a baseline breast MRI. The program-centric infrastructure can only handle half of the demand. Additional storage and computing power is purchased and installed, causing a delay. When the scanning is complete, the additional computing power sits idle.
I-7	CIR Hosting Environment	Computing infrastructure hosting environments must evolve and adapt to meet the emerging needs of applications and the demands of rapidly increasing services.	DIEA v 1.2 7 May 2010		Computing infrastructure shall be responsive to and supportive of the capability needs and requirements of the edge environment, despite intermittent connectivity or limited bandwidth. Computing infrastructure capabilities must be robust and agile to respond to increased computing demand, data storage, and shared space requirements.	

Code	Title	Principle	Source	Definition	Amplification	Example
I-8	NetOps Agility (NOA) Command & Control	The MHS shall operate and defend the GIG as a unified, agile, end-to-end information resource.	DIEA v 1.2 7 May 2010	Enables the continuous ability to easily access, manipulate, manage, and share any information, from any location at any time. NetOps Agility sets policies and priorities necessary to operate and defend the GIG. It establishes common processes and standards that govern operations, management, monitoring and response of the GIG.	Set policies and priorities necessary to operate and defend the GIG.	
I-9	NetOps Agility (NOA) Situational Awareness	Share NetOps information with the enterprise by making NetOps data, services, and applications visible and accessible and enable NetOps data to be understandable and trusted to authorized users.	DIEA v 1.2 7 May 2010	Enables the continuous ability to easily access, manipulate, manage, and share any information, from any location at any time. NetOps Agility sets policies and priorities necessary to operate and defend the GIG. It establishes common processes and standards that govern operations, management, monitoring and response of the GIG.	Enable the continuous ability to easily access, manipulate, manage and share any information, from any location at any time.	**If Implemented:** After an episode of decreased performance, NetOps data is available and reviewed, pinpointing the cause as a specific storage configuration issue. The issue is addressed quickly and performance is restored. **If Not Implemented:** After an episode of decreased performance, because of inadequate NetOps data, performance remains unacceptable, leading to end-user dissatisfaction and an attempt to completely revamp major portions of the architecture in order to improve performance, creating unnecessary costs and delays.

Code	Title	Principle	Source	Definition	Amplification	Example
I-10	Communications Readiness (CR)	The GiG communications infrastructure shall support full IP convergence of traffic (i.e., voice, video, and data) on a single network.	DIEA v 1.2 7 May 2010	CR focuses on the communications infrastructure and supporting processes that ensure information transport is available for all users (both fixed and mobile) across the GIG. This infrastructure includes physical networks, protocols, waveforms, transmission systems, facilities, associated spectrum management capabilities and other assets that provide: 1) wireless line of sight 2) SATCOM and other beyond line of sight, 3) fiber optic and traditional wire line, and all other physical transmission media.		

4.3.4 Service Principles

The MHS Service Principles support service-oriented definition and design, and the availability of authoritative investments in the net-centric environment through services.

Code	Title	Principle	Source	Definition	Amplification	Example
S-1	Service Orientation	The MHS should practice service-orientation.	NESI	**Service-orientation:** A design paradigm consisting of a distinct set of accepted design principles that advocate the representation of automation logic through highly independent and agnostic units called services.	A service-oriented approach supports DoD's ongoing effort to achieve net-centric operations. It establishes services as the means by which data producers and capability providers can make data assets and capabilities visible, accessible, and understandable across the enterprise and the means by which consumers can access and use these assets and capabilities. Wherever possible, information and functional capabilities should use existing services before creating duplicative capabilities and/or capabilities should be made available as reusable services.	The remaining principles in this section detail the desired design characteristics of services. Examples are provided for each of these.
S-2	Service Autonomy	Services should exercise a high level of control over their underlying execution environment.	NESI	**Autonomy:** For services to provide reliable, predictable performance they must exercise a significant degree of control over their underlying resources. Autonomy represents this degree of control measure and the principle emphasizes the need for individual services to possess high levels of individual autonomy.	When building an enterprise service inventory, there should be emphasis on positioning each member of the inventory as a standalone building block. Service autonomy should enable establishment of an execution environment that facilitates reuse because the service achieves increased independence and self-governance. There are multiple levels of service autonomy, including: **Service-level autonomy**: Service boundaries are distinct from each other, but the service may still share underlying resources. For example, a wrapper service that encapsulates a legacy environment that also is used independently from the service has service-level autonomy. It governs the legacy system, but also shares resources with other legacy clients. **Pure autonomy**: The underlying logic is under complete control and ownership of the service. This is typically the case when the logic is built from the ground up in support of the service. Service autonomy is not a binary yes/no quality but one in which there might be higher or lower degree of autonomy depending on the circumstances.	**If Implemented:** A service is created to wrap access to an enterprise repository. All data updates to and retrievals from the repository are performed via the service. (MHS CDR is a prime candidate to which the service autonomy principle should be applied.) **If Not Implemented:** A service is created to wrap access to an enterprise repository. However, many additional interfaces control the data in the repository, thus making the behavior of the service less predictable and more dependent on other interfaces.

Code	Title	Principle	Source	Definition	Amplification	Example
S-3	Service Loose Coupling	Service contracts impose low consumer coupling requirements and are themselves decoupled from their surrounding environment.	NESI	**Loose coupling:** Coupling between software programs can be viewed as representing a measure of dependency. The higher the dependency, the tighter the coupling. Loose coupling describes an approach where integration interfaces can be developed with minimal assumptions between the sending and receiving parties, thus reducing the risk that a change in one application or module will force a change in another application or module.	The message-based model, coupled with the mediation of the provider, makes it possible to create a system of loosely-coupled components. Service requesters will have to depend only on the interface described in the service contract and not on the service provider's implementation	**If Implemented:** A service is created with a service contract that does not depend on the underlying implementation. At a future date, a different implementation can be used to replace the old one with no impact on the service consumers. (Schedule Patient Appointment (SPA) service stores the scheduling information into CHCS. If in future this function is implemented by another EHR system, the use of loose-coupling principle will ensure that the user of the SPA service is not affected by this implementation change.) **If Not Implemented:** A web service is created by automatically generating WSDL from a particular set of classes that implement the logic. The service contract must be changed in the future when a different implementation is selected.
S-4	Service Abstraction	Service contracts only contain essential information, and information about services is limited to what is published in service contracts.	Thomas Erl, *Service-oriented Architecture; concepts, technology and design*. Prentice Hall, 2005. NESI, Dennis Wisnosky CTO under DoD Business Mission	**Abstraction:** Abstraction provides control of what parts of the underlying service logic are exposed to the outside world. By ensuring that these parts are designed in a generic manner so as to accommodate multiple potential service requestors, the service can be positioned as a reusable IT asset.	Service abstraction fosters reuse because it establishes the black box concept. Proprietary processing details should be hidden and potential consumers should only be made aware of an access point represented by a generic public interface.	**If Implemented:** A service is defined using commonly understood parameters that are independent of the underlying implementation. (The SPA service clearly defines input and output data in standardized XML constructs that are independent of any implementation specific data constructs.) **If Not Implemented:** A service is defined using parameters that are specific to the current underlying implementation. A change in the implementation would necessitate a change in the service definition.

Code	Title	Principle	Source	Definition	Amplification	Example
S-5	Standardized Service Contract	Services must conform to a published service contract. Within a service inventory, there is compliance to contract design standards.	NESI	**Contracts**: Services shall be formally defined using one or more service description documents.	In the Web services world, the technical service description documents are typically the WSDL definition and the XSD schema. Other documents that will be important are the policy, non-technical documents, legal agreements (such as SLAs) and any other service metadata. These documents can be collectively viewed as establishing a service contract—a set of terms and conditions that must be met and accepted by a potential service requestor in order to enable successful communication and interaction. A service contract can also can also include formal definitions of the service endpoint; each service operation; every input and output message supported by each operation; the data representation model of each message's contents; and the rules and characteristics of the service and its operations.	**If Implemented:** An enterprise-wide service contract template is utilized to formally define each service. (MHS wide service contract definition template is used to define the SPA service contract.) **If Not Implemented:** Services are created with varying degrees of specification for their contracts.
S-6	Service Composability	Services can be effective participants in a composition.	NESI	**Composability:** The ability of services to be reused by creating higher-level composite services that call multiple services and aggregate their logic.	As service portfolios grow in size, service compositions will become an unavoidable and increasingly important design aspect of building service-oriented solutions. The main reason this particular principle is so important is because it ensures that services are designed in such a manner so that they can participate as effective members, or controllers, of these compositions. The requirement for any service to be composable also places an emphasis on the design of service operations.	**If Implemented:** A complex functional process involves multiple semi-independent steps, each of which is handled by an existing service. A composite service is created that calls each of the atomic services and enables the end-to-end functional activity. (Manage Care business flow is exposed as a service that orchestrates calls to Order service and the Patient Demographics service.) **If Not Implemented:** Individual services are created without proper boundaries, such that there is some redundancy in their capabilities. This makes it difficult for a composite service to be created, reducing the opportunities for reuse.

Code	Title	Principle	Source	Definition	Amplification	Example
S-7	Service Reusability	Services contain and express reusable logic, and they can be positioned as reusable enterprise resources.	Thomas Erl, *Service-oriented Architecture; Concepts, Technology and Design*. Prentice Hall, 2005.	**Reuse:** The ability of a component to be utilized in contexts different that the initial circumstance it was built for.	Whenever possible, a Service should be constructed in a manner such that it is independent of context. This allows services to be reused in multiple implementations.	**If Implemented:** A service created to access clinical data from a repository for a case management application is later reused for a disability evaluation application. (Identity Management is offered as a service that is reusable in various business flows and service compositions.) **If Not Implemented:** A service is created without the ability to perform role-based access control, since it was not necessary for a particular application. This limits the reuse potential from other applications that necessitate it.
S-8	Service Statelessness	Services should maximize resource consumption by deferring the management of state information when necessary.	Thomas Erl, *Service-oriented Architecture; Concepts, Technology and Design*. Prentice Hall, 2005.	**Statelessness**: A service is stateless when it is not consuming memory related to the temporary storage and processing of state data. Whether or not a service enters into a stateless condition is determined by the functionality of the service capability that was invoked. As with autonomy, statelessness is a preferred condition for services and one that promotes reusability and scalability. For a service to retain as little state as possible, its underlying service logic needs to be designed with stateless processing considerations.	While a service is processing a message, it is temporarily stateful. If a service is responsible for retaining state for longer periods of time, its ability to remain available to other concurrent consumers will be impeded. If, however, services are designed to defer/delegate state (e.g., hand state information back to the consumer to take to whichever service it selects to process the next step of the transaction) then the service remains available to other consumers.	**If Implemented:** A service is created to manage a long-running activity (such as looking up historical medication profiles in a number of external entities—total response time might be many seconds or even minutes). The service defers its state to a temporary service state repository, so it can remain stateless longer (and thus releases memory resources for use by other consumers). **If Not Implemented:** The long-running service keeps its state information in memory for the entire duration of the activity.

Code	Title	Principle	Source	Definition	Amplification	Example
S-9	Service Discoverability	Services should be supplemented with communicative metadata by which they can be effectively discovered and interpreted.	NESI	**Discoverability:** Appropriate metadata is available such that a potential new service consumer can find and be able to reuse the service	The ability to register, discover, and govern services is an essential requirement for any Service Oriented Architecture (SOA) implementation. Centralized facilities for access and control of service metadata and artifacts become critical. A service registry provides these capabilities to publish interfaces and will be a key infrastructural component and cornerstone for SOA deployments. Web services registries, like other Web service components, need to be standards-based to foster interoperability across organizational boundaries.	**If Implemented:** A new service is added to the registry, with appropriate metadata. New consumers find out about the service from the registry and reuse occurs. (The SPA service is registered in the services repository and is discoverable for consumers.) **If Not Implemented:** A service is created by a program office, but its presence is unknown and, months later, a new service is created by a different group, duplicating efforts.
S-10	Transport Neutrality	Service definition should have clear separation between the service contract (input / output definition) and access mechanism.	SOA Practitioners' Guide Part 2 SOA Reference Architecture, 15 September 2006	**Transport Neutral:** Consumers shall not contain logic associated with the Provider's transport protocol. Likewise, the Provider shall not contain logic regarding the Consumer's transport protocol.	The logic of a service should be independent of the transport protocol for the endpoint. Protocol switching should be addressed outside of the service.	**If Implemented:** A Consumer sends a message to an endpoint unaware of the Provider's protocol choice. If the protocol of the Provider changes, the Consumer need not be adjusted. (The SPA service is invoked by consumer A using SOAP over HTTP while consumer B invokes the service using FTP.) **If Not Implemented:** A Consumer includes logic to do transformations associated with an endpoint protocol. The endpoint technology is changed. The service must now be rewritten to address the new technology.
S-11	Technology Neutrality	Service definition should be independent of the technology used to implement the service.	OAISIS Reference Architecture for Service Oriented Architecture Version 1.0 Public Review Draft 1 ; 23 April 2008	**Technology Neutral:** A service definition shall not use technology specific logic.	Building specifics of a technology into a service requires recoding should the technology changed. Service Oriented Architecture is by design to be independent of the underlying technology.	**If Implemented:** A service uses logic JMS for communication. The underlying technology is changed from WebSphereMQ to SonicMQ. The service does not require recoding. **If Not Implemented:** The service expects multipacket messages as constructed by WebSphereMQ. The logic for reassembling packets must be changed to address a change to SonicMQ.

Code	Title	Principle	Source	Definition	Amplification	Example
				SOA Best Practices and Design Patterns		
SOA-1	Standards Based		NESI	**Standards Based:** A service should leverage standards whenever possible.	Usage of standards increases the likelihood of interoperability with internal and external partners. Standards exist for a number of aspects of service-orientation (metadata, data formats)	**If Implemented**: The services use NIEM compliant data structure. When working with external partners, the external partner may leverage the same format without negotiating a specific of type and semantics. **If Not Implemented:** The services use a proprietary data structure specific to MHS. A transformation layer must be built in order communications to occur with other partners.
SOA-2	Enterprise Focus		The Open Group SOA Source Book 3rd Edition; April 2009	**Enterprise Focus**: SOA should be designed with entire enterprise in mind. Services should be implementable across organizational boundaries.	SOA by design is intended to encompass the enterprise business needs. In order minimize recoding and maximize reuse, services in a multi-organization enterprise should use common design and messaging approaches. This is facilitated by an overarching governance structure such as an SOE.	**If Implemented**: Organizations within in an enterprise can share information with a minimum amount of negotiation. **If Not implemented:** Organizations may need to negotiate information sharing with all other organizations. Reuse would be minimal. Enterprise wide policies and governance would not be possible.
SOA-3	Governance		The Open Group SOA Source Book 3rd Edition; April 2010	**Governance:** SOA should provide design-time, run-time, and organizational governance to include QoS, security enforcement, and interoperability policies.	In order for SOA to provide the desired level of agility, design standards, security standards, and QoS policies should be in place. A governance board should be established in order define these standards. Based on the nature of the organization, training, and some restructuring should be considered.	**If Implemented:** A true SOA is implemented across the enterprise that manages policies and optimizes controls to improve business agility and reduce time for implementation. **If Not implemented:** SOA is reduced to a collection of independent services that have

Code	Title	Principle	Source	Definition	Amplification	Example
						implementation specific security, design, and run-time management. Reuse is minimized. Security standards and policies can become ad hoc. Different web service paradigms may be used (e.g. REST vs. SOAP).
SOA-4	Location Independence		NESI	**Location Independence:** Changes to endpoint locations should be invisible to Consumers and providers.	Endpoints should not be hard-coded. Discoverability address this to an extent, however, a bus technology may also be used to provide virtual endpoints and thus increasing the level of loose coupling between registries and endpoints.	**If Implemented:** Loose coupling between providers and consumers is improved. Changes to the provider endpoint are invisible to the consumer and the registry. Eliminating recoding. **If Not implemented:** Every time the endpoint is changed, the registry must be updated, the consumer may also need to be updated.
SOA-5	Data Transaction Management		OASIS Web Service Atomic Transaction (WS-AtomicTransaction) Feb 2009	**Data Transaction Management:** Data Transactions should be encapsulated in to a single service whenever possible. If not possible, WS-* policies should be used in conjunction with a transaction manager.	Cross service data transactions can be problematic for rollbacks. This can be eliminated by encapsulating a transaction in a single service. Otherwise, WS-* policies can be used to clearly define transaction boundaries and rollback approaches. Bus technology and Policy managers can be used to implement multi-phase/multi-service commits and rollbacks.	**If Implemented:** Data transactions can be managed in a manner similar to traditional applications. Commit and rollbacks are isolated in one place. **If Not Implemented:** Transaction boundaries cross services. Propagating commits and rollbacks across service becomes more dependent on the availability of the service, and the timeliness of the service.
SOA-6	Cardinality Independence		NESI	**Cardinality Independence:** Service Consumer and Provider logic should be independent of the number of endpoints.	A service should not contain logic to identify whether an endpoint corresponds to a single message recipient or multiple message recipients. This can be implemented by a service façade, or by publish-subscribe messaging using a bus.	**If Implemented:** As business or technical needs change, consumer requests may need to be published to one or more providers. The consumer implementation will not need to

Code	Title	Principle	Source	Definition	Amplification	Example
						change. **If Not Implemented:** Consumer code must be changed each time a provider is added or removed.
SOA-7	Taxonomy		The Open Group SOA Source Book 3rd Edition; April 2010	**Taxonomy/Semantics:** SOA should use a single taxonomy across the enterprise.	A single taxonomy removes the likelihood of misinterpretation of information between services. In particular, as services cross organization boundaries information semantics must be consistent.	**If Implemented:** Services do not require custom semantics to be defined. All information exchanged use the same names, types, and has the same meaning. Changes in the taxonomy are communicated to all services. **If Not Implemented:** Every interaction between services, most likely those that cross organizational boundaries, will require negotiation on semantics. As individual services change the semantics will have to be renegotiated.
SOA-8	Data Mediation		SOA Practitioners' Guide Part 2 SOA Reference Architecture, 15 September 2006	**Data Mediation:** Services shall avoid internal logic for data mediation whenever possible.	Data mediation can be externalized using a bus technology. Mediation occurring within Consumers and Providers increases the amount of recoding.	**If Implemented:** Consumer and Provider code need not be changed when data mediation changes. Changes can be localized to one location. **If Not Implemented:** The consumers and providers will need to address changes in data types individually, increasing the amount of recoding and the potential for error.

4.3.5 Application Principles

The MHS Application Principles foster better application development, common interfaces, and integration, and reduce redundant data entry.

Code	Title	Principle	Source	Definition	Amplification	Example
A-1	Open standards	Utilize standards based open architecture framework.	USD(AT&L) Modular Open Systems Approach (MOSA) Memo, DoD Net-centric Strategy, Technology Principles	The IT Application will use open industry standards, the system architecture based on loosely coupled interactions, enabling the internal components to map to well-defined external interfaces. Vendor neutrality and openness is advocated throughout technology architecture and realized through the adherence to open standards for consistent system and data interoperability. This is supported by the Standardized Service Contract principle but can also be associated with service-orientation as a whole when it represents the standard paradigm for solution design.	**Establish an Enabling Environment**: Must establish supportive requirements, business practices, and technology development, acquisition, test and evaluation, and product support strategies needed for effective development of open systems **Employ Modular Design:** Partitioning a system appropriately during the design process to isolate functionality makes the system easier to develop, maintain, and modify or upgrade Certify Conformance; Should prepare validation and verification mechanisms such as conformance certification and test plans to ensure that the system and its component modules conform to the external and internal open interfaces allowing plug-and-play of modules, net-centric information exchange, and re-configuration of mission capability in response to new threats and technologies. Open systems verification and validation must become an integral part of the overall organization change and configuration management processes.	
A-2	Ease of Use	Ensure applications are simple to use and transparent to users.	Common industry best practices for application design	**Simple to use:** From the user's point of view, an application should be more or less "invisible", enabling him/her to focus on executing tasks **Transparent:** Users can easily understand what is going on in an application with respect to executing tasks.	The user interface should be designed to enable a user to easily master use of the application, to focus on and execute his/her task efficiently and to be transparent so the user always what to do next and where to go next as well as the consequences of certain user actions. The IT Application should be kept as simple as possible while still meeting business and enterprise requirements. Where complexity is needed, it should be encapsulated to promote simplicity of solutions built on the Architecture.	**Positive:** A new user has had training on using MHS applications and is able to efficiently and effectively do his/her job with minimal disruption and when a new situation arises, he/she intuitively and successfully navigate the application to meet the need. **Negative:** A new user has had training on using MHS applications. The user has to take copious notes which he/she must refer to constantly. The user gets lost in the application frequently and each time a new situation arises he/she

Code	Title	Principle	Source	Definition	Amplification	Example
						must find a knowledgeable user to guide him/her through the new task.
A-3	Workflow Optimization	The user interface should support an integrated and seamless workflow.	Common industry best practices for application design, EHRWA Guiding Principle	Integrated and seamless workflow: a workflow comprised of disparate steps that appear as one and are completed without disruption.	The MHS has a very large end-user base. These users are the primary data producers and data consumers and their productivity depends heavily on a well-integrated and seamless workflow. As such, the user should be presented with one interface that provides access to the systems needed to conduct business. Conversely, using the different systems that comprise the MHS should not be disruptive to the workflow. EHRWA - Support and enhance clinical workflows.	**Positive:** The pharmacy clerk is servicing a patient at the pharmacy. The patient reports a change in her temporary address. The clerk immediately captures this information without having to switch applications. **Negative:** In the scenario above, the clerk needs to log into a separate application and bring up the patient in order to enter the new information.
A-4	Model-Based Engineered (MBE)	Apply modeling and simulation throughout the development process to foster more effective concept engineering and concurrent design, development, deployment and evolution.	DoD Systems 2020 initiative DDR&E, Congressional Testimony, May 18, 2010Initiative	MBE applies product, process, property, environment, and mission models to ensure rapid, concurrent, and integrated development of DoD systems that can adapt to foreseeable and unforeseeable change: – Innovative and Agile –Test Driven Design – Model Based Systems Engineering..	Using M&S for rapid and concurrent application/system development. This will impact Application Development, making it Fast and Flexible. The IT Application will readily support incorporation of new technologies to support business and technology innovation. Changing the traditional DoD requirements-delay-surprise acquisition game.	
A-5	Platform Based Engineered (PBE)	Apply architectural and automated design tools to the development of hybrid hardware, software, and networked systems as an enduring "platform" for evolving user capabilities.	DoD Systems 2020 initiative	The complement of MBE for portfolios or product lines, PBE invests in determining DoD-domain commonalities and variability, develops product-line architectures that package the commonalities into physical and informational platforms, and provides plug-compatible interfaces to the variable product line components: - Architecture Patterns - Intelligent Design Automation - Product Line Methodologies	– PBE will enable rapid changes to extensible product families to meet changing user environments and missions. – Will impact DEVELOP FAST, FLEX and ADAPT. Changing the traditional DoD stovepipe acquisition game.	

Code	Title	Principle	Source	Definition	Amplification	Example
				- Open Systems		
A-6	Capability on Demand (COD)	Design systems or services with the express intention of supporting adaptation in response to changes during operations.	DoD Systems 2020 initiative	COD provides technology support for evolutionary acquisition strategies that combine short, stabilized build-to-specification increment developments with concurrent change anticipation, analysis, and self-adaptation. This amplifies the effects of MBE and PBE capabilities for rapid new-component generation and integration- Service Oriented Design and Development Methodologies: – Self Healing Systems – Adaptive Algorithms – Autonomic Computing	– COD will allow fielded systems to rapidly respond to a changing environment as the mission evolves in unplanned, unforeseen ways. – Will impact ADAPT. Changing the traditional brittle DoD point-solution acquisition game.	
A-7	Trusted Systems Design (TSD):	Ensure secure system and subsystem design from unsecured vendors.	DoD Systems 2020 initiative	TSD includes up-front analysis and systems engineering of foreseeable threat patterns, uses MBE and PBE capabilities to build trust and assurance into DoD system architectures, and ensures that agile change adaptation fully addresses trust and assurance concerns. Designing secure systems from unsecured vendors and subsystems: –Composite Health Monitoring Systems –Design for Test Methodologies –Feedback Control (observability theory)	– Trusted Systems Design will allow us to take advantage of innovation in the global supply chain, while ensuring that our systems operate as intended. Composing assured systems from COTS will allow speedy adoption of COTS for the war-fighter/medic. – Will impact DEVELOP FAST. Changing the traditional slow DoD acquire-certify-patch security assurance game. This guiding principle states that the development and application of the BOE will incorporate IA requirements as a core part of the DoD infrastructure and in conformance with pre-defined security standards and directives.	
A-8	Scalability	Ensure applications are scalable.	DoD Net-centric Strategy	The ability of the application/service to handle the un-expected load (e.g., number of end-user consumers or number of calling services).		
A-9	Availability	The necessary availability to ensure un-interrupted business operations.	DoD Net-centric Strategy	Ability to run using a continuity of operations plan (COOP), ability to provide service during routine maintenance (hardware and software), and ability to provide service during catastrophic failures (e.g., massive outages of		

Code	Title	Principle	Source	Definition	Amplification	Example
				the power grid, physical destruction of the hosting facility).		

4.3.6 Global Principles

The MHS Global Principles span across the enterprise, are universal and cross-cutting all capabilities and ensure MHS governed resources are well conceived, designed, operated and managed to address the mission needs of the MHS.

Code	Title	Principle	Source	Definition	Amplification	Example
G-1	Interoperability	Interoperability of solutions across the MHS (to internal DoD, Veteran Affairs (VA), Federal, and other external partners) is a strategic goal.	DIEA v 1.2 7 May 2010	The ability of systems, units, or forces to provide data, information, materiel, and services to and accept the same from other systems, units, or forces and to use the data, information, materiel, and services so exchanged to enable them to operate effectively together. National Security System (NSS) and Information Technology System (ITS) interoperability includes both the technical exchange of information and the end-to-end operational effectiveness of that exchanged information as required for mission accomplishment. (source: CJCSI 3170.01G)	All Program Offices, OCIO divisions and entities of Military Health System (MHS) must work together to achieve interoperability goal. Information is made interoperable by following the rules for net-centric sharing of data and services across the enterprise. DoD achieves infrastructure interoperability through definition and enforcement of standards and interface profiles and implementation guidance.	**Positive:** Utilizing common data standards, interface/ integration profiles and implementation guides helps programs to enable effective information sharing capabilities among data trading partners. For example, Virtual Longitudinal Electronic Record (VLER) Health program uses Health Information Technology Standards Panel (HITSP) Patient Summary (C32) and supporting Integrated Health Enterprise (IHE) implementation guides. **Negative:** Results in establishing information silos, point-to-point expensive data interface, and high interface maintenance costs.
G-2	Information Sharing	Improving the Military Health System (MHS)'s ability to share information helps the MHS realize the power of information as a strategic asset.	DIEA v 1.2 7 May 2010, DoD Information Strategy May 4, 2007	Information Sharing is defined as "making information available to participants (people, processes, or systems)." Information sharing includes the cultural, managerial, and technical behaviors by which one participant leverages information held or created by another participant. This DoD Strategy establishes the vision for the future: Deliver the power of information to ensure mission success through an agile enterprise with freedom of maneuverability across the information environment. (source: DoD Information Sharing Strategy, May 4, 2011)	The MHS OCIO will provide a secure environment for collaborative sharing of information assets (information, services, policies) with MHS's external partners, including Veteran Affairs (VA), other Federal Departments and Communities of Interest (e.g., Department of Homeland Security, the Intelligence Community), state and local governments, allied, coalition, non-governmental organizations (NGOs), academic, research, and business partners. Benefits include, but are not limited to: (1) Achieving unity of effort across mission and coalition operations, (2) Improving the speed and execution of decisions, (3) Achieving rapid adaptability across mission and coalition operations, and (4) Improving the ability to anticipate events and resource needs, providing an initial situational advantage and setting the conditions for success.	Information Sharing capabilities can be realized when the dissemination of information is supported at all organizational levels. For example, utilizing an online based content management tool, similar to DKO and/or DCO or Forge.mil, will benefit the teams to collaborate and share information in a seamless way rather than using shared drives or e-mail system.

Code	Title	Principle	Source	Definition	Amplification	Example
G-3	Service-Orientation	The MHS should practice service-orientation.	DoD Net-centric Strategy, Technology principles, NESI	Through SOA, the DoD's business IT solutions are being united via an infrastructure and standards-based pattern termed the Business Operating Environment (BOE). The IT Application and components built upon it should be viewed as a set of independent services that can be composed to provide a solution. how the program will make its unique services/applications available to the GIG community.	In support of attaining the goals of DoD Business Transformation and carrying out various related activities (including those described in the DoD Net-Centric Data Strategy and the DoD Net-Centric Services Strategy), business data and services need to be easily located, understood, and reused by authorized users. The Net-centric Design Tenets provide more specific, technical direction to remote realization of the net-centric aspects of the GIG architecture, per reference (XX), through the evolution of legacy systems and the development of new systems that comply with DoD net-centric direction, as well as achieve technology investment reuse, enhanced integration and interoperability and take advantage of core enterprise services such as those provided by the NCES program.	
G-4	Joint Governance	In support of IM/IT initiatives and programs, MHS should employ Joint Governance Structure among Medical Services division.	MHS IM/IT Strategic Plan, Defense Business Board "Task Group on Strengthening the DoD Enterprise Governance", 2008	Governance means establishing and enforcing how DoD Components and mission partners, on behalf of the Mission Areas, agree to provide, secure, use, and operate services. There are three elements to governance: 1) Identifying the attributes for providing, securing, using, and operating services that have to be governed and what level of governance is required 2) Establishing lines of responsibility, authority, and communication for making decisions about services across the lifecycle of services 3) Establishing the measurement, policy, and incentive/control mechanisms to ensure that individuals and organizations carry out their responsibilities. (source: DoD Net-Centric Services Strategy, 2007).	During the new initiative/ program development, MHS OCIO divisions and programs should work with Medical Services departments to define joint governance structure to coordinate on shared processes, tools and resources.	**Positive:** • Designed to focus on an organization's core functions • Uses an "output-focused" strategy to ensure measurable execution • Led by strong leadership that encourages tough questions during a deliberative decision-making process • Develops a process to monitor execution, measure output, promote accountability, receive feedback, and analyze the results of decisions **Negative:** • Decision by consensus - eliminates "constructive tension"\ • Numerous and overlapping items on the agenda • Insufficient delegation

4.3.7 Requirements Principles

The MHS Requirements Principles provide a framework for developing and managing requirements throughout the MHS enterprise. The outlined principles are derived from DoD guidance as well as best practices across many industries. The key principles for developing requirements ensure the solution meets the original needs of the end-user by having requirements that are testable, costable, traceable, adaptable and interoperable. Enterprise standards should be in place and used in order to provide quality requirements that align strategically to MHS strategic initiatives.

Code	Title	Principle	Source	Definition	Amplification	Example
R-1	Strategic Alignment of Requirements	Strategic alignment of requirements and solutions.	Acquisition Community Connection - Defense Acquisition University	Requirements and solutions are aligned to strategic directions, imperative, initiatives and mission tasks.		
R-2	Governance of Requirements	Decisions during requirements development and management occur in the appropriate forum.	Acquisition Community Connection - Defense Acquisition University	Governance is an overarching process through which decisions are made, oversight is performed, and trust is promoted.	Governance can provide a forum for bidirectional and continuous feedback throughout development and management of requirements.	
R-3	Engaged Key Requirement Stakeholder	Key stakeholders are identified early and engaged in developing the requirements.	Business Analysis Body of Knowledge (BABOK Guide) V 2.0		Key stakeholders are engaged for better understanding of their sought benefits and how the system can derive their benefits. Determine which set of requirements are relevant to a particular stakeholder group.	Stakeholders are responsible for formally approving requirements documentation. It beneficial to have stakeholders involved in the process well before approval so they are familiar and comfortable with the requirements set.
R-4	Requirement Stakeholder Roles and Responsibility	Roles of the key stakeholders are indentified and responsibilities of the stakeholders are defined.	Business Analysis Body of Knowledge (BABOK Guide) V 2.0	Description of who the stakeholders are, their interests in the system and how they use the system.	Key stakeholders may include: customers, suppliers and end-users.	Examples of key stakeholder's roles: Domain Subject Matter Expert (SME), Implementation SME, Analyst, Project Manager, Sponsor, Tester and end-user.
R-5	Requirements Change Management	Change management approach is in place and used.	Business Analysis Body of Knowledge (BABOK Guide) V 2.0	Requirements Management must control and manage the impact of changes to the defined operational need.		How to handle changes that fall in scope and out of scope of the project.
R-6	Requirements Risk Management	Risk management approach is in place and used.	Business Analysis Body of Knowledge (BABOK Guide) V 2.0	Uncertainties that arise in the system requirements can focus the attention of stakeholders on unrealistic user requirements and may highlight ambiguity and lack of consistency.		Indentifying assumptions and constraints mitigates risk.
R-7	Requirements Tools	Tools are identified and available to use.	Acquisition Community Connection - Defense Acquisition University		Tools are important in techniques, methodologies and analyses.	

Code	Title	Principle	Source	Definition	Amplification	Example
R-8	Capability Based Planning for Requirements	Requirements are aligned with the Capability Based Planning Framework.	Acquisition Community Connection - Defense Acquisition University	The Capability Based Planning Framework is used in order to achieve a business goal or objective.	Includes following the scope and direction of the Capabilities Based Assessment (CBA) and Joint Capability Integration and Development System (JCIDS).	
R-9	Enterprise Standards for Requirements	Use of enterprise standards for the structure and content of each requirements specification.	Business Analysis Body of Knowledge (BABOK Guide) V 2.0	Standards are used for statement formation, terminology and mutually exclusive requirements. Requirements align with National standards.		Use of templates, consistent set of models, documents and National standards such as the HL-7 functional model.
R-10	Planning, Programming, Budgeting and Execution (PPBE) for Requirements	Requirements align with PPBE decision making process.	Acquisition Community Connection - Defense Acquisition University	PPBE is the process used to allocate resources within the DoD.	A cyclic process that provides the mechanisms for decision making and provides the opportunity to reexamine prior decisions regarding changes in the environment.	
R-11	Requirements Quality Assurance	Use of high quality standards for the structure and content of each requirements specification.	Business Analysis Body of Knowledge (BABOK Guide) V 2.0	Quality Assurance is a process used to ensure quality.	Ongoing process that ensures the requirements supports the delivery of value to stakeholders.	Use of enterprise standards ensures quality.
R-12	Requirements Traceability	Requirements are able to be traced back to the business objective by being explicit, quantified and testable.	Business Analysis Body of Knowledge (BABOK Guide) V 2.0	Traceability identifies and documents the linage of each requirement and its relationship to other requirements.		Backward traceability (derivation) and forward traceability (allocation).
R-13	Requirements Adaptability	Requirements are adaptable throughout process.	Business Analysis Body of Knowledge (BABOK Guide) V 2.0	Adaptable requirements can be changed or modified in order to meet the needs of the end-user.		Baselining is a way to view requirements at a point in time to be agreed upon before further development.
R-14	Stakeholder Value for Requirements	Requirements meet the needs of the end-user.	Business Analysis Body of Knowledge (BABOK Guide) V 2.0		Ease of use and minimized errors for intended end-users provide value to stakeholders.	Prototyping is a way for the end-user the desired outcome before implementation.
R-15	Requirements Agile Approach	Requirements are developed and managed using an agile approach.	Business Analysis Body of Knowledge (BABOK Guide) V 2.0	Agile is the methodology where requirements and solutions use iterative and incremental development.		
R-16	Requirements Analysis	The use of appropriate analysis methodologies for requirements.	Acquisition Community Connection - Defense Acquisition University	Analysis of requirements involves making sure that the requirements are written to be useable, costable and testable.	Analysis includes use cases and business requirements specifications.	A use case describes the tasks the system will perform for the actors and the expected outcome.
R-17	Requirements Verification	Requirements are verified by appropriate stakeholders.	Business Analysis Body of Knowledge (BABOK Guide) V 2.0		Ensures the requirements have been defined correctly.	Verification involves a final check by analyst and key stakeholders that the requirements are ready for review and final approval.

Code	Title	Principle	Source	Definition	Amplification	Example
R-18	Requirements Validation	Requirements are validated by product or solution.	Business Analysis Body of Knowledge (BABOK Guide) V 2.0	Validation ensures that the stated requirements support and are aligned with the goals and objectives of the business.	Measures how well the requirements met the original need of stakeholders.	
R-19	Requirements Interoperability	Requirements are designed to integrate with, interoperate with, and interface with other capabilities.	Business Analysis Body of Knowledge (BABOK Guide) V 2.0	Interoperability is the ability of systems to communicate by exchanging data or services.		Indentify and address ability to integrate requirements to ensure a system to system solution.
R-20	Prioritized Requirements	Requirements are prioritized.	Business Analysis Body of Knowledge (BABOK Guide) V 2.0	Prioritization determines the relative importance of a set of requirements.	A method to specify when requirements will be addressed.	Structured requirements that are broken down and organized by subject or category.
R-21	Requirement Business Rules	Business Rules are developed and used to manage requirements.	Business Analysis Body of Knowledge (BABOK Guide) V 2.0	A Business Rules supports or constrains functionality of solution.	Ensures the solution interprets the converted data correctly.	Uses appropriate terminology that enables domain SMEs to validate the rules.