OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE
HEALTH AFFAIRS
SKYLINE FIVE, SUITE 810, 5111 LEESBURG PIKE
FALLS CHURCH, VIRGINIA 22041-3206

TRICARE
MANAGEMENT
ACTIVITY

22 May 2012

MEMORANDUM FOR: SEE DISTRIBUTION

SUBJECT: Military Health System Cloud First Adoption Directive and Policy Guidance

References: See Attachment 1

1. INTRODUCTION

In December 2010, Vivek Kundra, U.S. Chief Information Officer (CIO), published the 25 Point Implementation Plan to Reform Federal Information Technology (IT) Management. A key component of this plan established a “Cloud First” policy mandating that government agencies “default to cloud-based solutions whenever a secure, reliable, cost-effective cloud option exists.”

As recently stated by the Federal CIO, Steven VanRoekel, in a December 8, 2011, memorandum to all Federal CIOs:

> Cloud computing offers a unique opportunity for the Federal Government to take advantage of cutting edge information technologies to dramatically reduce procurement and operating costs and greatly increase the efficiency and effectiveness of services provided to its citizens. …the Federal Risk and Authorization Management Program (FedRAMP) will provide a cost-effective, risk-based approach for the adoption and use of cloud services…

The National Defense Authorization Act for Fiscal Year (FY) 2012 mandates that the Department of Defense (DoD) and its agencies develop a strategy to migrate to using Cloud computing services. Against this backdrop, DoD released an IT Enterprise Strategy and Roadmap plan in September 2011 developed by the DoD CIO, Teri Takai. This memorandum is consistent with Federal and DoD strategies, directives, and plans as they relate to implementation of a Military Health System (MHS) Cloud First policy aligning with the MHS mission to:

> Provide the right information to the right customers at the right time to improve and maintain the health status of our beneficiaries across the entire continuum of health care operations.

2. PURPOSE

The purpose of this memorandum is to provide guidance on Cloud First adoption to MHS and IT organizations delivering health services to their constituents. Furthermore, this policy memorandum defines short-term actions that are required of the component CIOs relative to projects and programs, planned or in execution, related to the analysis, specification, acquisition, deployment, and consumption of Cloud computing technologies and services.

In addition, directional guidance is provided on the MHS Cloud First intent to establish an enterprise Cloud governance model, integrated with MHS IT governance, which provides policy and guidance for the full spectrum of Cloud governance requirements—from the MHS Cloud First Strategy, through requirements, architecture, acquisition, implementation, consumption, operations, management, and support.

3. SCOPE

This memorandum is applicable to any MHS IT organization delivering health services to their respective constituents. Any and all plans in process or in execution related to adoption or implementation of Cloud computing technologies, services, or virtualization solutions are within the scope of this memorandum. This includes technologies, services, and solutions including, but not limited to, the following: National Institute for Science and Technology (NIST) and industry definitions: Software as a Service, Platforms as a Service, Infrastructure as a Service, Desktop Virtualization, Cloud/Big Data Analytics, Virtualization Technologies, and IT Managed or Shared Services. The policy direction established in this memorandum will impact all current and future IT system deployments within MHS and its associated DoD health services components.

4. DIRECTIVE TO PLACE AN ADMINISTRATIVE HOLD ON CLOUD TECHNOLOGY PROGRAMS

To ensure uniform interpretation and adoption of the DoD and MHS Cloud First mandates, all current and/or planned efforts within the scope of this memorandum related to the planning, architecture adoption, acquisition, or operation of Cloud computing technologies will be evaluated. An administrative hold should be placed on any new or planned Cloud computing deployments. Any current or contractually obligated Cloud computing activities should continue; however, they will need to be reviewed for their fit into a broader, enterprise-wide MHS Cloud First initiative.

Within 60 days of issue of this memorandum, all activities related to the planning, architecture adoption, acquisition, or operation of Cloud computing technologies, services, and solutions must be reported to the MHS CIO office; a reporting format will be provided within 2 weeks of issuance of this policy memorandum. This reporting again will include current Cloud computing efforts, as well as those in the planning or pre-planning stages. For those Cloud computing activities in the planning or pre-planning stages, the underlying mission, business and

IT needs must be identified, along with an explanation of what Computing technologies, services, or solutions are being considered.

5. POLICY GUIDANCE

After assessing the current and planned activities with MHS, CIO will issue “Capstone” policy and guidance supporting the MHS Cloud First Strategy and adoption roadmap. This guidance will be consistent with Federal Agency mandates and will also be aligned with the standards and recommendations being developed by NIST, particularly those recommendations made in NIST Special Publications 500-291 and 500-293. The MHS Cloud Governance policy and guidance recommendations will also align with NIST Special Publication 500-292, defining a Cloud Computing Reference Architecture. Guidance on security requirements, as mandated by Health Insurance Portability and Accountability Act laws and regulations issued by the Department of Health and Human Services related to Protected Health Information, will be aligned with the FedRAMP initiative.

This MHS policy, when issued, will cover all aspects of MHS Cloud First adoption, including strategy, architecture, security, acquisition, onboarding, contracts, service level agreements, service catalogs, etc. An operational Cloud computing governance framework will be established covering all of the MHS Cloud First-related activities, and defining operational policies, enforcement mechanisms, and governance processes.

Jonathan Woodson, M.D.

Attachments:
1. References
2. “What is Cloud Computing?”

DISTRIBUTION:

DIRECTOR, DEFENSE CENTERS OF EXCELLENCE
DIRECTOR, VISION CENTER OF EXCELLENCE
DIRECTORS, TRICARE REGIONAL OFFICES
CHIEF INFORMATION OFFICER, TRICARE MANAGEMENT ACTIVITY
PROGRAM EXECUTIVE OFFICER, JOINT MEDICAL INFORMATION SYSTEMS
DEPUTY PROGRAM EXECUTIVE OFFICER, BUSINESS OPERATIONS AND PROCESS
  MANAGEMENT
PROGRAM MANAGER, DEFENSE HEALTH SERVICES SYSTEMS
PROGRAM MANAGER, DEFENSE HEALTH INFORMATION MANAGEMENT SYSTEM
DIRECTOR, MILITARY HEALTH SYSTEM CYBERINFRASTRUCTURE SERVICES
DIRECTOR, PORTFOLIO MANAGEMENT
DIRECTOR, EXTERNAL RELATIONSHIP MANAGEMENT
DIRECTOR, ENTERPRISE ARCHITECTURE
DIRECTOR, PERFORMANCE IMPROVEMENT
DIRECTOR, COMPUTER/ELECTRONIC ACCOMMODATIONS PROGRAM
DIRECTOR, TEST AND INDEPENDENT VERIFICATION AND VALIDATION
DIRECTOR, SYSTEMS INTEGRATION
DIRECTOR, ACQUISITION SUPPORT
DIRECTOR, MILITARY HEALTH SYSTEM ENTERPRISE ANALYSIS
DIRECTOR, MILITARY HEALTH SYSTEM ELECTRONIC HEALTH RECORD CENTER

ATTACHMENT 1

REFERENCES

(a) Federal Chief Information Officer Memorandum, “Security Authorization of Information Systems in Cloud Computing,” December 8, 2011

(b) U.S. Chief Information Officer Memorandum, “25 Point Implementation Plan to Reform Federal Information Technology Management,” December 9, 2010

(c) National Defense Authorization Act for Fiscal Year 2012

(d) Department of Defense IT Enterprise Strategy and Roadmap, Version (V) 1.0, September 6, 2011

(e) DoD Information Enterprise Strategic Plan, 2010–2012

(f) DoD IT Enterprise Technology and Roadmap, V 1.0, September 2011

(g) Military Health System 2010–2015 Information Management/Information Technology Strategic Plan

(h) CloudBuyersGuide.Org Publication, “Best Practices: Chief Information Officer/Chief Information Security Officer (CIO/CISO)”

(i) NIST Special Publication 500-291, “Cloud Computing Standards Roadmap”

(j) NIST Special Publication 500-292, “Cloud Computing Reference Architecture”

(k) NIST Special Publication 500-293, “U.S. Government Cloud Computing Technology Roadmap,” Volume I and II

ATTACHMENT 2

WHAT IS CLOUD COMPUTING?

Cloud computing, as defined by the National Institute of Standards and Technology (NIST)[1], is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models.

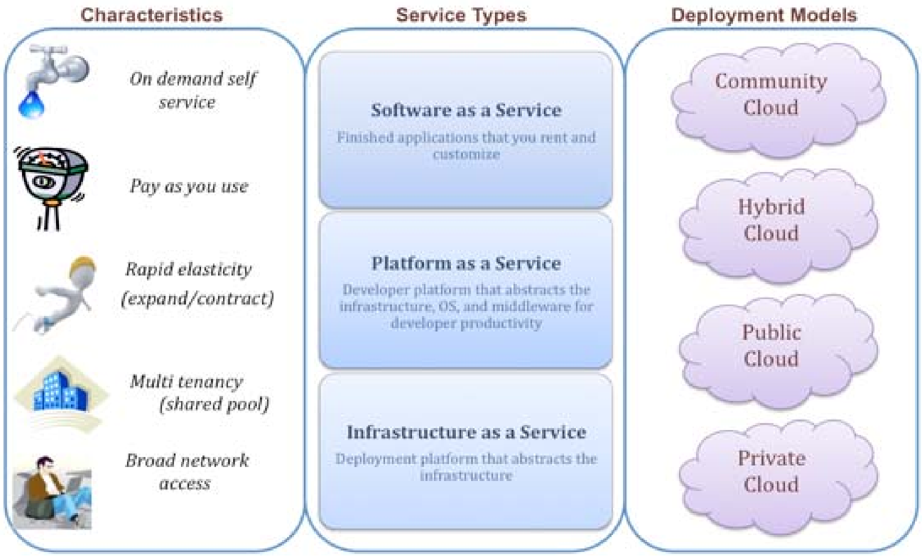
Characteristics
Service Types
Deployment Models
On demand self service
Pay as you use
Rapid elasticity (expand/contract)
Multi tenancy (shared pool)
Broad network access
Software as a Service
Finished applications that you rent and customize
Platform as a Service
Developer platform that abstracts the infrastructure, OS, and middleware for developer productivity
Infrastructure as a Service
Deployment platform that abstracts the infrastructure
Community Cloud
Hybrid Cloud
Public Cloud
Private Cloud

Figure 2: NIST definition of Cloud Computing

Cloud computing services can be described by their shared characteristics, by the computing resources provided as a service, and by the method of deployment. To provide a common basis for discussion within this strategy, we have tailored these concepts and definitions as follows.

Cloud Service Characteristics

NIST describes five essential characteristics of cloud computing services:

- **On demand self service:** A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service's provider.

[1] Definition of Cloud Computing, , as developed by NIST, the Cloud Computing Executive Steering Committee and the Cloud Computing Program Management Office , NIST Special Publication 800-145 Draft, January 2011, http://csrc.nist.gov/publications/drafts/800-145/Draft-SP-800-145_cloud-definition.pdf

- **Broad network access:** Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, laptops, and personal digital assistants).
- **Resource pooling:** The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, network bandwidth, and virtual machines.
- **Rapid elasticity:** Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out, and rapidly released to quickly scale in. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.
- **Measured Service:** Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

Cloud Service Models

According to NIST, cloud services fall into three service models characterized by the type of resource being provided:

- **Software-as-a-Service:** The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based e-mail). The consumer does not manage or control the underlying cloud infrastructure, including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.
- **Platform-as-a-Service:** The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure, including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations.
- **Infrastructure-as-a-Service:** The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and

possibly limited control of select networking components (e.g., host firewalls). Cloud Service Deployment Types

A cloud, and the services provided by it, can be further differentiated by how and where it is deployed. Clouds may be hosted internally or externally to the organization. NIST identifies four deployment types:

- **Private (or Enterprise) Cloud:** The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise.
- **Community Cloud:** The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party and may exist on premise or off premise.
- **Public Cloud:** The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.
- **Hybrid Cloud:** The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).