ACQUISITION AND MANAGEMENT OF VA INFORMATION TECHNOLOGY RESOURCES

1. **REASON FOR ISSUE:** This Directive revises Directive 6008 issued in August 2016 and establishes policy for the acquisition and management of information technology (IT) related resources across the Department of Veterans Affairs (VA). VA's IT assets are core resources of the Department and their effective management is critical to the provision of services to our Nation's Veterans. This policy clarifies the scope of VA's IT resources subject to the oversight authority of VA's Chief Information Officer (CIO). This oversight is necessary to ensure alignment of these resources with enterprise IT, information management and information assurance policies, rules, standards and guidance. Additionally, this policy ensures that all VA IT related assets are acquired within the constraints and intent of the VA's IT Systems appropriation account, providing specific guidance as to when IT-related assets must be funded from the IT Systems appropriation account. All of VA's IT-related assets, resources and services are subject to all laws, executive mandates and VA CIO policy. This includes information assurance, security and privacy; enterprise architecture, standards and specifications; and IT management, technical and operational internal controls, regardless of the funding source. This policy, which replaces all previous memoranda on this subject, is necessitated by the growing magnitude and speed of change in information technologies, network-attached devices (i.e. the "Internet of Things"), and information security risks, procedures and regulations. Its full implementation will improve VA's effectiveness in the use of resources to deliver a standardized, integrated, interoperable and Veteran-centric information environment in accordance with all federal laws, regulations, and industry best practices.

2. **SUMMARY OF CONTENTS:** This Directive affirms the VA CIO's oversight authority over all information related assets as highlighted by the Federal Information Technology Acquisition Reform Act (FITARA), and establishes roles and responsibilities among VA administrations and staff offices, including the Office of Information & Technology (Ol&T).

    a. Specifies that any VA asset, resource, or service, IT or otherwise, that stores, transmits, manipulates or displays VA information shall comply with all laws, executive mandates and VA CIO policies regarding IT.

    b. Provides guidance and principles on the use of the VA IT Systems appropriation and other VA appropriations for the acquisition, development, and operation of VA IT assets in a secure, consistent, effective and efficient manner, as directed by congressional authority.

    c. Rules and standards relative to enterprise-wide management of IT resources are published as part of VA's Enterprise Architecture and governed by the IT Budget and Finance Board.

3. RESPONSIBLE OFFICE: Assistant Secretary for Information and Technology (005), ITRM (005F)

4. RELATED HANDBOOK: None

5. RESCISSIONS

   a. Rescinds any memoranda written prior to this Directive that authorizes the acquisition of IT resources by an organization other than the Office of Information and Technology. In addition, the following memoranda are rescinded:

   (1) VA Directive 6008 issued in August 2016 "Acquisition and Management of VA Information Technology Resources"

   (2) Use of the Information Technology (IT) Systems Appropriation, dated June 21, 2006

   (3) Use of Medical Care Funds to Develop Mobile Device Applications for Clinical Support, dated May 31, 2011

   (4) Use of Medical Care Funds for Development, Procurement and/or Support of Mobile Health Applications and Supporting Mobile Devices, dated July 16, 2013.

CERTIFIED BY: **BY DIRECTION OF THE DEPUTY SECRETARY OF VETERANS AFFAIRS**

/s/   **/s/**
Dat P. Tran   Scott R. Blackburn
Acting Assistant Secretary   Executive in Charge for the
Office of Enterprise Integration   Office of Information and Technology

Distribution: Electronic Only

ACQUISITION AND MANAGEMENT OF VA INFORMATION TECHNOLOGY ASSETS

1. PURPOSE AND SCOPE:

This Directive establishes policy for the development, acquisition, operations and management of information technology (IT) assets across the Department of Veterans Affairs (VA). As the statutorily accountable official for the management and security of all of VA's information resources, including VA operational information and associated resources such as personnel, equipment, funds, and IT, VA's Chief Information Officer (CIO) has authority over all information-related assets that are part of or interact with VA's information networks, services and capabilities. This policy:

a. Clarifies the scope of VA's IT assets.

b. Specifies that any VA asset, resource, or service, IT or otherwise, that stores, transmits, manipulates or displays VA information shall comply with all laws, executive mandates and VA CIO policies regarding IT.

(1) All assets must comply with all laws, executive mandates and VA CIO policy in regards to information assurance, security and privacy; enterprise architecture, standards, and specifications; and IT management, technical and operational controls, regardless of the funding source.

(2) IT assets funded by IT appropriations, as defined by this policy, must also comply with laws, executive mandates and VA CIO policy in regards to capital planning and investment control, investment management, and IT acquisitions.

(3) IT-related assets must conform to policies governing connection to the VA network.

c. Affirms all VA IT assets connecting to the VA Network, regardless of how they are funded or managed, are subject to those rules, standards and oversight processes as prescribed by the VA CIO. This policy clarifies and strengthens the ability of the VA CIO to manage enterprise compliance with value measurement, architecture, accessibility and information assurance standards, in accordance with Congressional intent and the highest standards of public transparency and resource stewardship.

d. Ensures all IT assets within VA are developed, procured and operated in the most effective and efficient manner possible within the legal limitations of VA appropriations and other relevant information resource management laws and regulations.

e. Defines those circumstances under which assets must be developed, acquired or operated with the IT Systems Appropriation (or other funding stream authorized to acquire IT assets) and those circumstances under which they may be acquired by VA organizations and facilities with other funds (e.g., Medical Equipment, including Medical Devices, Clinical Systems/ Medical Apps that meet the Food and Drug Administration (FDA) definition of a Medical Device). If any asset connects to the VA Network, IT policies governing security and maintenance will be followed.

f. Assigns roles and responsibilities related to the funding and management of VA's IT resources.

g. Specifies that acquisition of all IT-related assets shall be strictly limited to acquisition vehicles that adhere to VA IT policies such as cybersecurity and accommodation for persons with disabilities.

h. States user privilege levels for VA IT assets shall be managed exclusively by OI&T by ensuring proper privileges are assigned to non-IT staff so that Non-IT funded systems can be appropriately managed.

i. States that configuration of VA IT asset end user devices (if connected to the VA network), irrespective of funding source, shall be managed by OI&T unless properly isolated on the network according to VA Policy for Medical and General Device Isolation Architecture.

j. Updates governance of IT-related assets, operating guidelines and definitions.

k. Reinforces VA's use of life cycle management and total cost of ownership in the planning and management of all IT-related assets and services planned for or deployed in VA.

l. States that VA non-IT items/services are to be funded by the appropriate Administration or Staff Office with the allowable appropriation or funding stream (e.g. Non-IT consumable office equipment and office supplies; facility equipment; construction projects; specific miscellaneous VA non-IT items/services as identified in this policy; and Direct Medical (diagnostic or treatment) Systems, Equipment or Devices (DMSED) which meet the FDA definitions of a Medical Device and Direct Patient Care use. DMSED's must have an FDA product code number defining them as a medical device. (Any DMSED that does not have an FDA product code number must state in the funding vehicle the reason why it does not have an FDA product code number.)

2. POLICY

a. Funding

(1) Generally, only the IT Systems Appropriation, the Franchise Fund, Supply Fund, Canteen Fund, the OIG Appropriation, the VA/DoD Joint Incentive Fund and VA/DoD Federal Health Care Center Joint Fund have the legal authority to pay for VA IT items/services, subject to the laws and regulations governing these Funds.

(2) IT products for delivery to veterans provided by benefits programs under Title 38 authorities will not be charged to the IT appropriation, but have explicit legal authority to reimburse the IT account.

(3) VA non-IT items are to be funded by the requesting Administration or Staff Office, using its proper appropriation.

   b. **VA IT items and services include:**

   (1) All IT networks and equipment. This does not include clinical networks and
        equipment on the Medical Device Isolation Architecture (MDIA) used solely for
        Direct Patient Care; however, non-clinical applications on the MDIA are still an IT
        funding requirement;

   (2) All commercially developed software (with the exception of Commercial Off the Shelf
        (COTs) software used exclusively for Direct Patient Care and DMSED and that meet
        the FDA definition of a Medical Device. DMSED's must have an FDA product code
        number defining them as a medical device (any DMSED that does not have an FDA
        product code number must state in the funding vehicle the reason why it does not have
        an FDA product code number) ;

   (3) VA developed software application costs, including the development, acquisition,
        product support and management of the software applications, as well as any
        associated open source, innovations or pilots;

   (4) Any mechanism or service for providing access to applications in any IT environment
        operating under VA control, including private/commercial cloud operations;

   (5)   IT systems administration training, IT development and testing environments, IT
         performance testing, IT life cycle planning and IT technical requirements gathering
         (but not including business requirements gathering);

   (6) VA IT infrastructure (e.g., servers, storage, networks) required to maintain IT
        persistent data sources, both authoritative and non-authoritative, and legacy stores,
        including all data storage, backup and disaster recovery capabilities (except those
        items listed in section 2.c)

   (7) Voice, data and video telecommunications infrastructure (e.g., circuits and switches,
        wired cabling to the wall), regardless of whether the space is owned or leased by VA;

   (8) Telecommunications and telephony services and equipment except dedicated lines or
        services to patient residences for telemedicine;

   (9) All enterprise and limited number software and software licenses, enterprise and
        unique, (with the exception of those biomedical and clinical software items defined as
        DMSED). (DMSED items must have an FDA product code number defining them as
        a medical device; those that do not have an FDA product code number must state the
        reason why in the funding vehicle.);

(10) Employee and contractor support for IT help desk and customer service operations;

(11) Other service models used in VA's IT production environment, such as infrastructure-as-a-service (IAAS), platform-as-a-service (PAAS), and telecommunications-as-a-service, as defined by the National Institute of Standards and Technology's (NIST) guidelines, that require VA maintenance and/or interfaces to VA's IT production environment, applications or data stores; and

(12) All mixed-use systems, computers, and mixed-use servers, (i.e., those that support both a VA IT item/service and a VA non-IT item/service), are a VA IT funding requirement.

c.   VA non-IT items and services include Direct Medical (diagnostic, monitoring, or treatment) Systems, Equipment or Devices (DMSED), including but not limited to:

(1) Telehealth, radiology, cardiology, pulmonary, laboratory, intensive care unit and surgery systems;

(2) A Food and Drug Administration (FDA) approved medical device, which is defined as an instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, or a similar or related article, including a component part or accessory, which is:

(a) Recognized in the official National Formulary, the United States Pharmacopoeia or any supplement to them. Product codes for FDA approved medical devices may be found in the FDA's Product Classification Database. The product code assigned to a device therein is based upon the medical device product classification designated under 21 CFR Parts 862-892. The product code identifies the generic category of a device for FDA. If the item has been categorized as an FDA approved medical device with a product code, VA considers it to be a VA non-IT DMSED item; or

(b) Intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment or prevention of disease in man or other animals; or

(c) Intended to affect the structure or any function of the body of man or other animals, and which does not achieve any of its primary intended purposes through chemical action within or on the body of man or other animals and which is not dependent upon being metabolized for the achievement of any of its primary intended purposes; or

(d) A mobile medical application (app) which meets the FDA definition of a Medical Device and is intended for use in the diagnosis of disease or other conditions, or the cure, mitigation, treatment or prevention of disease. This includes the procurement, development and the ongoing maintenance and operations of this mobile medical app, but

not the app store itself, which is an IT "persistent data source" and as such requires IT management and funding; or

(e) Mobile devices and accompanying data services (data plans) that are used to solely run mobile medical apps that are intended for use in the diagnosis of disease or other conditions, or the cure, mitigation, treatment or prevention of disease; any non-medical applications on a device (e.g. e-mail) must be funded by IT;

(3) Medical systems, equipment or devices required in support of medical training and simulation;

(4) Computers and servers which are strictly components of a medical device system (e.g. diagnostic imaging, PACS, Clinical Information Systems, etc.). Any non-medical applications on a device (e.g. e-mail) must be funded by the IT appropriation;

(5) Computers or mobile phones solely involved in running DMSED applications for use in direct patient care and tablets (e.g. iPads) predominantly involved in running DMSED applications for use in direct patient care; (any non-medical applications on these devices (e.g. e-mail) must be funded by the IT appropriation;

d. **Commercial Off the Shelf Software for Direct Patient Care**

Commercially developed software (i.e., commercial off-the-shelf (COTS)) purchased solely for purposes of direct patient care, as defined herein.

e. **Office Equipment and Office Supplies**

(1)   High-capacity multifunction devices that have copying, emailing and/or printing capabilities within one device and support a large office or workgroup are non-IT items.

(2)   Office supplies, including consumables and peripherals for end-users, are non-IT items. This includes anything that attaches to a computing device that does not store or process information, but rather serves just as an input or output device. Examples include privacy screens, bar code readers, monitors, headsets, insurance card readers, microphones, speakers, wireless keyboards, mice and mouse pads.

f. **Facility Equipment**

Facility equipment, including industrial control equipment, are non-IT items. This includes fire alarms, building security systems, nurse call systems, digital signage systems, energy efficient lighting monitors/transmitters, information boards/electronic signage and elevator systems.

g. **Construction Projects**

Construction projects, including modifications to a building's infrastructure even though required specifically for IT purposes, are VA non-IT items. Examples include: the acquisition and installation of a wire closet fiber optic infrastructure, power surge protection, distribution and battery backup systems and heating, ventilation and air conditioning (HVAC) equipment to comply with either operating requirements and/or manufacturer warranties. This includes construction of data centers. The cost of incidental cabling for IT equipment is an IT cost. However, the IT Systems Appropriation, Franchise Fund, Supply Fund or OIG Appropriation *do not* have the legal authority to incur any construction or cabling costs associated with major or minor construction, non-recurring maintenance projects and station level construction projects.

h. **Miscellaneous VA non-IT Items/Services**

(1) Information Technology Assets Purchased by a Vendor:

a.   IT related hardware procured by a vendor incident to a federal contract, and required to support the performance of that contract, will be funded by the same appropriation as the contract itself, as long as they are not used by any VA employee or connected to any VA network, except through an approve Virtual Private Network (VPN) such as the Citrix Access Gateway (CAG).

b. Any IT asset, as defined by this policy, procured by a vendor incident to a contract and intended to be turned over to the VA must comply with all VA asset management and security policies and be procured using an IT funding source.

(2) Software-as-a-Service (SaaS) solutions when the software is not owned or hosted by VA and no additional capabilities were added as a customization of the software and made part of the procurement are VA non-IT services. Also, the user must log on to a vendor site where all the functionality is made available and the vendor must be responsible for software, hardware, data security, help desk, etc. functions.

(3)   Initial costs of IT-related items and services funded by non-VA grants or other non-VA funding sources, such as non-VA research efforts, are considered VA non-IT items/services.

(4)   IT-related assets for delivery to Veterans provided by benefits programs under Title 38 authorities are VA non-IT items.

(5)   Business process re-engineering is VA non-IT. (This does not include associated software and infrastructure costs.)

(6)   End-user training costs, including train-the-trainer costs, are VA non-IT and are the responsibility of the benefitting organization(s) to pay for their users as the system is deployed.

(7)   Networks, wired or wireless, provided for patient care and therapeutic use for the benefit of veterans and/or their family that are not connected to any VA network are VA non-IT.

(8)   Web content development, services, and management. (NOTE: This only pertains to content development and does not pertain to software development of web sites).

(9)   Veterans Canteen Service (VCS)-Not connected to the VA network. All development and sustainment of VCS systems are not IT.

(10)   Compensated Work Therapy purchases exclusively supported by reimbursements from clients to support the program.

(11)   Specific bequests or gifts of funds to the VA for the purchase of IT products or services will be deposited in the General Post Fund and funded from the General Post Fund. This is a legally-authorized augmentation of the IT appropriation.

  i. Other Internal Controls

(1) The Chief Financial Officer (CFO) or other designated official for each VA Administrations and Staff Office must submit an annual certification letter to the Office of Information & Technology CFO. This letter shall state that to the best of their knowledge no funding outside of the IT Appropriation will be used to procure IT assets, as defined by this policy.

(2) Administration CFOs, other designated officials, and/or program managers shall immediately coordinate with the OI&T CFO should they become aware of any non-conformity to this policy.

3. RESPONSIBILITIES

a. The Assistant Secretary for Information and Technology, as the Department's CIO, in planning, managing and overseeing the VA's information resources, shall:

(1) Plan, program, budget and execute the IT Systems Appropriation;

(2) Manage approved reimbursable budget transfers when required to move the applicable funding between affected organizations;

(3)   Design, develop, implement and maintain a VA IT governance structure to:

(a) Ensure the proper use of the IT Systems Appropriation and acquisition of VA enterprise IT capabilities;

(b) Ensure that this policy is maintained and revised as required based on changing technologies**;**

(c) Authorize IT-Non-IT Workgroup to make recommendations about whether a specific project requires IT funding or is allowable for non-IT funding, when this policy does not allow for a clear determination. Additionally, the CIO implements policies to set criteria for whether a given asset is IT or not.

(d) Ensure all VA information resources, including those funded outside the IT appropriation, are compliant with enterprise policy, rules, standards and guidance related to IT, information management (IM) and information security (IS).

(e) Provide visibility through the VA's enterprise architecture to all policy, rules, standards, guidance and configurations necessary to guide VA IT item design, acquisition, development and deployment;

(f) Develop, maintain and assure completeness and proper use of standard IT configurations; and

(g) Establish, maintain and make available bulk buy and enterprise purchase programs for IT related assets (including assets such as end user devices which may be purchased outside the IT appropriation) and services to ensure standardization, interoperability, economies of scale and accessibility of the VA information environment.

(h) Oversee and collaborate with VA stakeholders at the local level to ensure that IT-related capabilities funded and deployed at local sites are appropriately vetted and formally. Ensure alignment to enterprise policy, rules, standards and guidance. Ensure that acquisitions are available to all other local sites and not redundant, while making certain that operations and sustainment are properly funded and the proper appropriation is used.

(i) Integrate compliance with this policy within decision processes that OI&T oversees or participates in.

b.   **Under Secretaries, Assistant Secretaries, and Other Key Officials will:**

(1)   Ensure all VA IT and non-IT items/services which connect to any VA Network are subject to rules, standards and oversight processes as prescribed by the VA CIO in order to comply with information assurance, accessibility, security, privacy and enterprise architecture standards;

(2) Integrate compliance with this policy within established decision processes in which they oversee or participate;

(3) Maximize collaboration with the open source IT community; and

(4) Plan, program and budget for VA non-IT items/services to ensure they are supportive of VA Administration and staff office requirements.

c. **General Counsel:**

The Office of General Counsel shall, as necessary, provide appropriate legal advice and interpretation of appropriations law to assist in determining whether a given appropriation, or other fund stream, has legal authority to obtain the item in question. This advice and interpretation will also aid in determining whether an item must be purchased with the IT appropriation or not.

4. **REFERENCES**
    a. Federal Information Technology Acquisition Reform Act: Title VIII, Subtitle D of the National Defense Authorization Act for Fiscal Year 2015, Pub. L. No. 113-291
    b. 21 CFR Parts 862-892-FDA Medical Device Classification Panels
    c. 29 USC 794d : *Disabled VA Employees and Members of the Public*
    d. 40 USC §11101, *Definitions* and SUBTITLE III: *Information Technology Management, and The Clinger-Cohen Act of 1996*
    e. 44 USC chapter 35: *Information Resources Management*
    f. Title VIII, Subtitle D of the National Defense Authorization Act (NOAA) for Fiscal Year 2015, Pub. L. No. 11 3-291, *December 19, 2014*: *Federal Information Technology Acquisition Reform Act (FITARA) of 2014*
    g. 44 USC 3541-49, Dec 2014**: *Federal Information Security Modernization Act of 2014 (FISMA)***
    h. Public Law 107-347, December 2002: *E-Government Act of 2002*
    i. Public Law 109-114, November 30, 2005: *Military Quality of Life and Veterans Affairs Appropriations Act*
    j. 38 USC §§ 5705, 5701 and 7332: *Protection of Medical Records*
    k. 44 USC 3501-3521: *Paperwork Reduction Act of 1995 (PRA)*
    l. PL 111-352, Jan 2011: *Government Performance Results Act (GPRA) of 2010*
    m. OMB Memorandum M-15-14, June 10, 2015: *Management and Oversight of Federal Information Technology*
    n. OMB Circular No. A-11: *Preparation, Submission, and Execution of the Budget*
    o. OMB Circular No. A-130, *Management of Federal Information Resources*
    p. Consolidated Appropriations Act, 2002, S-515*, Information Quality Act (also known as the Data Quality Act)*
    q. OMB Memorandum M-12-18, Managing Government Records Directive, Aug 2012
    r. OMB Memorandum (M-06-16) Protection of Sensitive Agency Information (June 23, 2006)
    s. OMB Memorandum (M-15-14) Management and Oversight of Information Technology
    t. VA Directive 6300, Records and Information Management

u. VA Directive 6500, Managing Information Security Risk: VA Information Security
    Program
v. VA Directive 6550, Pre-Procurement Assessment for Medical Device/Systems
w. VA Directive 6518, Enterprise Information Management

5. DEFINITIONS

a. **Application.** (See OMB Circular A-130 Appendix III) The use of information resources
(information and information technology) to satisfy a specific set of user requirements.

b. **Authoritative Data Source**. A source of data or information designated and recognized as
official that is trusted, timely, secure and used within VA's information environment in support
of VA business processes. An authoritative data source is the one and only (logical) location
where a respective data element is created, updated and deleted. Administrations and staff
offices designate these sources within domains for which they are the stewards. The Office of
Information and Technology may develop and maintain technology solutions (e.g. services)
that use these sources. [VA Directive 6518, Enterprise Information Management Policy]

c. **Clinical.** Pertaining to actual observation and treatment of patients, as distinguished from
theoretical or experimental.

d. **Clinical Decision Support.** Clinical decision support (CDS) provides clinicians, staff,
patients or other individuals with knowledge and person-specific information, intelligently
filtered or presented at appropriate times, to enhance health and health care. CDS encompasses
a variety of tools to enhance decision-making in the clinical workflow. These tools include
computerized alerts and reminders to care providers and patients; clinical guidelines;
condition-specific order sets; focused patient data reports and summaries; documentation
templates; diagnostic support, and contextually relevant reference information, among other
tools. This does not include tools that only provide administrative support for clinical staff.

e. **Clinical Information System.** A Clinical Information System (CIS) is a computer based
system that is designed for collecting, storing, manipulating and making available clinical
information concerning the diagnosis/treatment of patients' healthcare. Clinical Information
Systems provide a repository that stores clinical data, such as the patient's history of illness
and the interactions with care providers. The repository encodes information capable of
helping physicians decide about the patient's condition, treatment options, and wellness
activities as well as the status of decisions and actions undertake.

f. **Clinician.** A health professional, including physicians, psychiatrists, nurses and allied
health professionals, such as pharmacists and therapists.

g.   **Data.** An elementary description of things, events, activities and transactions recorded, classified and stored, but that may not be organized to convey any specific meaning. Data items can be numeric, alphabetic, figures, sounds or images. A database consists of stored data items organized for expeditious use, including reading, updating and deleting.

h.   **Data Store**. Any store of data intended to be persistent (i.e., non-volatile) or leaves residual memory trace of information for the purpose of later processing (creation, reading, updating or deleting), irrespective of its designation as authoritative or relation to a System of Record.

i.   **Direct Medical (diagnostic, monitoring, or treatment) Systems, Equipment or Devices (DMSED)** which meet the following criteria:

(1)   Direct medical diagnostic, monitoring, or treatment systems, including but not limited to telehealth, radiology, cardiology, pulmonary, anesthesia, laboratory, intensive care unit and surgery systems;

(2)   A Food and Drug Administration (FDA) approved medical device, which is defined as an instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, similar or related article, including a component part or accessory, which is:

(a)   Recognized in the official National Formulary, the United States Pharmacopoeia, or any supplement to them;

(b)   Used solely for Direct Patient Care and have an FDA product code number defining them as a medical device. (Any DMSED that does not have an FDA product code number must state the reason why in the funding vehicle.); any non-medical applications on a device (e.g. e-mail) must be funded by IT;

(c)   Intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment or prevention of disease in man or other animals; or intended to affect the structure or any function of the body of man or other animals, and which does not achieve any of its primary intended purposes through chemical action within or on the body of man or other animals and which is not dependent upon being metabolized for the achievement of any of its primary intended purposes.

(3)   FDA defined medical mobile apps are software programs that run on smartphones and other mobile communication devices. They can also be accessories that attach to a smartphone or other mobile communication devices, or a combination of accessories and software. Mobile medical apps are medical devices that are mobile apps, meet the definition of a medical device and are an accessory to a regulated medical device or transform a mobile platform into a regulated medical device.

(4)   Laptops and mobile phones that are supplied to a provider and used solely, and Tablets that are used predominantly, for diagnosis, treatment, cure, mitigation or prevention of disease, or used to gather patient information; any non-medical applications on a device (e.g. e-mail) must be funded by IT;

(5)   Development of medical applications for a mobile device, such as a smartphone or tablet, used directly by the patient to access VA medical systems and input medical information;

(6)   Telehealth equipment, which includes devices to report symptoms and measure vital signs for Veterans in their homes and the equipment necessary to connect Veterans and clinicians virtually via interactive video sessions, as well as the technology used to collect, store and forward telehealth information for clinical treatment purposes.

j.   Direct Patient Care. Care of a patient provided by a clinician or staff member. Direct patient care may involve many aspects of the health care of a patient, including monitoring, diagnosis, treatments (and execution of treatment plans, e.g. dietary restrictions, etc.), care plans, counseling, or self-care by a Veteran where medical devices are used in support of telecare (e.g. wound cameras), patient education and the administration of medication. This includes products or services which provide clinical decision support, such as those which support clinical telecare triage done by clinicians.

k.   Enterprise IT Capabilities. Enterprise level IT capabilities built using IT resources and data that are shared across two or more organizational components regardless of location. Within the VA this includes all IT related services for Veterans and eligible beneficiaries, support functions and resource management. Embodied in this concept are technical efforts such as infrastructure engineering for building, managing and evolving shared IT; IT or infrastructure operations for administering and monitoring the performance of the IT service being provided to the enterprise; and IT services management. Efforts such as IT strategy, portfolio management and IT governance enable this concept to function effectively.

l.   Information. Any communication or representation of knowledge such as facts or data, in any medium or form, including textual, numerical, graphic, cartographic, narrative or audiovisual forms. This definition includes information that an agency disseminates from a web page.

m.   Information Environment. The aggregate of the information created and used by an organization; the information architecture of the organization (models, authoritative and redundant data stores, data flows); the governance framework and policies and standards that ensure information is managed as an asset.

n.   Information Life-Cycle. The stages through which information passes, typically characterized as creation or collection, processing, dissemination, use, storage, and disposition.

o.   **Information Management.** The planning, budgeting, manipulating, and
controlling of information throughout its life cycle.

p.   **Information Resources.** (See 44 USC Section 3502) Information and related resources,
such as personnel, equipment, funds and information technology.

q.   **Infrastructure as a Service (IaaS).** The capability provided to the consumer to provision
processing, storage, networks and other fundamental computing resources where the consumer
is able to deploy and run any 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).

r.   **IT Asset.** Any equipment, interconnected system, or subsystem of equipment, which in
whole or by virtue of component parts, are used in the automatic acquisition, storage, analysis,
evaluation, manipulation, management, movement, control, display, switching, interchange,
transmission or reception of data or information by the Executive Agency

s.   **IT Infrastructure.** The term IT Infrastructure is applied to a group defined by OMB
Circular A-11 Section 300 to include infrastructure, office automation, and
telecommunications. These are defined in OMB Circular A-11 Section 300 as "… all IT
investments that support common user systems, communications, and computing
infrastructure. These investments usually involve multiple mission areas and might include
general LAN/WAN, desktops, data centers, and cross-cutting issues such as shared IT security
initiatives and telecommunications." [OMB A-11 Section 300]

t.   **IT Network.** The grouping of two or more computer systems that are physically or
virtually linked together.

u.   **IT-Related.** Products and services that may have IT components but are not required to
be funded by the IT Systems Appropriation.

v.   **Information System.** (See 44 USC Section 3502) A discrete set of information
resources organized for the collection, processing, maintenance, transmission and
dissemination of information in accordance with defined procedures, whether automated or
manual.

w.   **Information Technology.** (See 40 USC Section 1110)

   (1)   With respect to an executive agency; any equipment, interconnected system or
   subsystem of equipment used in the automatic acquisition, storage, analysis, evaluation,
   manipulation, management, movement, control, display, switching, interchange,
   transmission or reception of data or information by the executive agency. This includes if

the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency that requires the use:

(a)   of that equipment; or

(b)   of that equipment to a significant extent in the performance of a service or the furnishing of a product.

(2)   Includes computers, ancillary equipment (including imaging peripherals, input, output and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support services), and related resources; but

(3)   Does not include any equipment acquired by a federal contractor incidental to a federal contract.

x.   Infrastructure. The substructure or underlying foundation, platform or network used for providing goods and services, including communications facilities, cable, wiring, data centers, power plants and communication systems.

y.   IT Project. Includes projects for software development, mobile applications, hardware installations, network upgrades, cloud computing/external hosting and virtualization rollouts, enterprise architecture, information assurance, business analytics, data management projects and the implementation of IT services.

z.   Medical Device. Any device or system that meets any of the following requirements:

(1)   Used in patient healthcare for diagnosis, treatment (therapeutic), or physiological monitoring of patients. This includes server-based medical equipment and clinical systems. Examples of medical devices/systems include, but are not limited to, physiological monitoring systems, ventilators, infusion pumps, Computed Tomography (CT) scanners, MUSE cardiology information system, Picture Archiving and Communication Systems (PACS), Clinical Information Systems (CIS), and laboratory analyzers. Medical devices directly connect to the patient; process human and other biologic specimens; create medical images, display electrophysiological waveforms; obtain physiologic measurements, or directly perform therapeutic-support to the patient.

(2)   The device/system has gone through the Food and Drug Administration's (FDA) Premarket Review or 510k Process.

(3)   Is incorporated as a component of a medical device system in such a fashion that if modified the device or system component could have a negative impact on the functionality or safety of the main medical device/system.

aa.   Multi-Function Device Printer. A free standing device that has copying, emailing and/or printing capabilities within one device and supports a large office or workgroup with high capacity functionality (i.e. # of pgs. per minute).

bb. Platform as a Service (PaaS). The capability provided to the consumer to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services 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.

cc. Redundant information. Multiple information stores of the same information that are synchronized and/or reconciled with one another for availability, integrity and continuity purposes.

dd. Service. A mechanism to enable access to a set of one or more capabilities, where the access is provided using a prescribed interface and is exercised consistent with constraints and policies as specified by the service description or contract.

ee. Software as a Service (SaaS). The capability provided to the consumer to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email) or a program interface. 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.

ff.   Software Development. The activity of computer programming, documenting, testing and bug fixing involved in creating and maintaining applications and software frameworks involved in a System Development Life Cycle (SDLC) and resulting in a software product. While the term refers to a process of writing and maintaining the source code, in a broader sense it includes all that is involved between the conception of the desired software through to the final manifestation of the software, ideally in a planned and structured process. Therefore, software development may include research, new development, prototyping, modification, reuse, re-engineering, maintenance or any other activities that result in **Software products.** All software development in the VA, whether Class 1, 2 or 3, shall fall under this policy guidance.

gg. System. The same as a General Support System defined in OMB Circular A-130-Appendix III, as an interconnected set of information resources under the same direct management control which shares common functionality. A system normally includes hardware, software, information, data, applications, communications and people. Some examples of systems are: a local area network (LAN) including smart terminals that supports a branch office; an agency-wide backbone; a communications network; a departmental data processing center including its operating system and utilities; a tactical radio network or shared information processing service organization.

hh. System Development Life Cycle (SDLC). Is a term used to describe a systematic approach and process for planning, creating, testing, deploying and retiring information systems.

ii. Telecommunications. A universal term that is used for a vast range of information-transmitting technologies such as mobile phones, land lines, VoIP and broadcast networks. It encompasses the infrastructure of a telecommunications network and includes any lines, apparatuses, towers, antennas or structures used, or for use in, a telecommunications network. In telecommunications, data is transmitted in the form of electrical signals known as carrier waves, which are modulated into analog or digital signals for transmitting information.

ACQUISITION AND MANAGEMENT OF VA INFORMATION TECHNOLOGY ASSETS

The chart below delineates products and services that are to be procured using the IT appropriations by OI&T and those that may be procured under Non-IT Appropriations by VHA, VBA, NCA, or Staff Offices.

Item Number	Item Description	Funding Source
HARDWARE		
1	PC, laptops, tablets, smartphones, cell phones (non-Smartphones), Satellite phones, [1]	IT
2	Thin Client[1]	IT
3	IT infrastructure (e.g., servers, storage, networks) required to maintain persistent data sources, both authoritative and non-authoritative, and legacy stores, including all data storage, backup and disaster recovery capabilities.[1]	IT
4	Printer[1]	IT
5	Tape Drive[1]	IT
6	Modem[1]	IT
7	Document Scanner	IT
8	Computer Room UPS/PDU Systems and UPS equipment for individual PCs, servers, etc.	Non-IT
9	Storage System (SAN, NAS)	IT
10	External Disk Drives	IT
11	Networking Equipment (WAN, LAN, WLAN)	IT
12	Cyber and Information Security Servers and Appliances	IT
13	Telephone Systems (PBX, KSU, IP)	IT
14	Two-way Radios (Police, Engineers, etc.)	Non-IT (Facility Equipment)
15	Pagers	IT
16	Handsets, Speakerphones, Conference Phones	IT
17	Videoconferencing Endpoints[3]	IT
18	Videoconferencing Bridges (MCUs)	IT
19	Peripherals (mouse, keyboard, PIV reader, bar code readers monitors, speakers, microphones, headphones, headsets, etc.)	Non-IT (Office Supplies)
20	Supplies and Consumables (Storage media (USB drives, CD/DVD-R/RW), paper, toner, batteries)	Non- IT (Office Supplies)
21	Digital Cameras (Clinical or otherwise), Editing Equipment	Non- IT

22	Data Cables-incidental cables within IT workstations (copper, fiber, patch panels, etc.)	IT
23	Overhead Paging Systems	Non- IT (Facility Equipment)
24	Nurse Call Systems	Non-IT (Facility Equipment)
25	Direct Medical Diagnostic, Monitoring, or Treatment Systems - Bio-Medical Systems Equipment (PACS, BCMA, VBEC, ICU, CIS, ARK, MUSE, Lab, Rx, etc.)[2]	Non- IT (DMSED)
26	Dictation/Speech Recognition Systems requiring hardware/servers connected to VA network and software licenses	IT
27	Telemedicine Systems including Teleradiology, Telepathology, Telemental health, etc. (excluding video conferencing equipment[3])	Non-IT (DMSED)
28	Copiers	Non- IT (Office Equipment)
29	Desktop Fax Machines (does not include software/server based faxing solutions)	Non-IT (Office Equipment)
30	Multi-function Device, as defined	Non- IT (Office Equipment)
31	Facilities Management Systems (Building Controls, Digital Signage, Energy and Elevator Control Systems, Fire Alarm Systems, Building security (e.g. Video Surveillance, Physical Access Control, etc.), energy efficient lighting monitors[4]	Non-IT (Facility Equipment)
32	Satellite Communications (dishes/uplinks)	IT
33	Diagnostic Workstations (e.g. Radiology, Cardiology, Pathology)	Non-IT (DMSED)
SOFTWARE		
34	Interfaces, Middleware[2]	IT
35	Clinical Decision Support System (CDS) [2]	Non-IT (DMSED)
36	Clinical Information System (CIS) [2]	Non-IT (DMSED)
37	Operating Systems	IT
38	Diagnostic Tools[6]	IT
39	Cyber and Information Security Tools	IT
40	Office Automation (e.g. Acrobat, Illustrator, Creative Suite, OrgChartPro, staff scheduling etc.)	IT
41	Direct Medical Diagnostic or Treatment Systems - Bio-Medical Systems Software (OR, ICU, PACU, ED, Radiology, etc.) and Stand Alone Software used for direct patient care, excluding VA developed[5, 7]	Non-IT (DMSED)

42	Core Information Systems (VistA, VI, Exchange, Vetsnet, HDR, etc.)	IT
43	Electronic Media Subscriptions which require no software licenses.	Non-IT
44	Software as a Service (SaaS) [8]	Non- IT
45	Platform as a Service (PaaS) [8]	IT
46	Infrastructure as a Service (IaaS) [8]	IT
47	All software licenses, enterprise and unique, with the exception of biomedical and clinical software.	IT
48	USA Staffing: a web based HR assessment tool Subscription Service which requires no software licenses.	Non-IT
49	Real Time Locator System	Non-IT
Other		
50	Major/Minor/NRM/Station Projects, not specifically to serve IT (Excluding Activation)	Non-IT (Construction Projects)
51	Maintenance Contracts for IT Hardware and Software	IT
52	Microsoft Enterprise Licenses for Windows, Office, SMS, SQL, Exchange, etc.	IT
53	Cisco SmartNet Maintenance Contract	IT
54	VistA Maintenance & Expertise Center (VMEC)/VistA Imaging/Exchange	IT
55	Telecommunications Costs (Voice, Data and Video, both Local service and long distance telecommunications and telephony usage charges.) Telecommunications infrastructure (e.g., circuits and switches, wired cabling to the wall), regardless if the space is VA owned or leased.	IT
56	Release of Information (ROI) Software Maintenance	IT
57	Quality Enhancement Research Initiative (QUERI)	Non-IT (DMSED)
58	Cable Installation is IT, unless the cabling is associated with a non-IT project (e.g. Major/Minor Construction or NRM/Station-Level projects)	IT
59	Supply Fund Purchases of IT items/services for own use are not to be included in the IT systems appropriation.	Non-IT
60	Franchise Fund purchases of IT items/services for own use are not to be included in the IT systems appropriation.	Non-IT
61	All IT costs in support of VA mission-related operations incurred by VA Franchise Fund Enterprise Centers under OI&T management	IT

62	Web Development and Infrastructure	IT
63	Web **Content** Development, Management, and Services	Non-IT
64	Simulation equipment and programs used for clinician training	Non-IT
65	Veterans Canteen Service- Not connected to the VA Network. All development and sustainment of VCS systems are non-IT.	Non-IT (Non-VA IT Items/Services)
66	Compensated Work Therapy (CWT)	Non-IT (Non-VA IT Items/Services)
67	Printing and Reproduction	Non- IT (Office Supplies)
68	IT system administration training	IT
69	IT development and testing environments and performance testing	IT
70	IT life cycle planning, technical requirements gathering (not business requirements) and definition, and evaluation as necessary and incidental to the development, acquisition and operation of IT systems.	IT
71	End User Support Center operations for IT capabilities operated by VA.	IT
72	Applications end-user business process re-engineering.	Non-IT
73	Leased space or non-VA furnished space occupied only by OI&T employees whose salaries are paid by the IT Systems appropriation, not to include new construction.	IT
74	Initial costs of IT-related assets and services funded by grants or other non-VA funding sources, such as research efforts.	Non-IT
75	IT-related assets for delivery to Veterans provided by benefits programs under Title 38 authorities.	Non-IT
76	Construction projects[9]	Non-IT
77	Veterans/Guest Internet Access and Patient Disposable Phones	Non-IT
78	Costs of Background Investigations	Non-IT

[1] If the PC/server is dedicated to solely running non-IT (DMSED or Facility Software) software, then the PC/server is non-IT. If the PC/Server is used for both clinical and administrative functionality, then the DMSED/Facility Equipment software is non-IT, but the PC/Server is IT. However, tablets that are predominantly involved in running DMSED applications for use in direct patient care are non-IT. Otherwise, any device, system, service, or capability that connects to VA's IT networks to create, use, update, or delete information are IT, including: Desktop computers, Laptop computers, Mobile phones, Tablets, Video teleconferencing units, Analog telephones, Voice over Internet Protocol (VoIP) phones, Servers, routers and hubs, Desktop printers, desktop scanners, Intranet and internet.

[2] Medical devices and equipment that communicate with VA IT networks are non-IT (DMSED) if they directly interface with the patient for purpose of physiologic monitoring, diagnosis, treatment, or processing of human tissue or imaging of the human body or directly connect to the patient for the purpose of fluid resuscitation or pharmaceutical delivery. **This does not include systems that provide the**

administrative support of clinical/DMSED systems; these systems are IT. VA developed interfaces for the non-IT (DMSED) are IT. Vendor supplied interfaces, or upgrades to commercially produced software products with DMSED software are considered non-IT (subject to Appendix B review processes). Software maintenance procured as part of an acquisition of DMSED software is non-IT.
[3] Telemedicine modalities exclude videoconferencing equipment unless the videoconferencing equipment is exclusively used for patient care communications in real time, in which case it would be non-IT (DMSED).
[4] These systems are non-IT (facility equipment). VA developed interfaces for the non-IT (Facility Management) are IT. Vendor supplied interfaces, or upgrades to commercially produced software products, with Facility Management software are considered non-IT, but must comply with all VA IT standards. Software maintenance procured as part of an acquisition of Facility Management software is non-IT.
[5] All VA developed software costs will be considered IT; the development, acquisition, product support and management of software applications, including any open source, innovation, pilots, mechanisms and services for providing access to applications (e.g. mobile app store) in any IT environment operating under VA control, including private/commercial cloud operations is IT. Purchased Commercial Off The Shelf (COTS) software used for purposes of direct patient care is non-IT (DMSED). This includes acquisition, licensing and maintenance costs for this DMSED software. This DMSED software is non-IT even if it is not FDA regulated. It is non-IT (DMSED) even if it is run on a standard PC or server.
[6] This excludes diagnostic tools used exclusively to maintain non-IT (DMSED) items, which would be non-DMSED or systems used to maintain facility equipment, which are non-IT (facility equipment).
[7] Mobile health applications and associated devices are qualified as a "medical device", which are non-IT (DMSED) if they directly interface with the patient for purpose of physiologic monitoring, processing of human tissue or imaging of the human body or directly connect to the patient for the purpose of fluid resuscitation or pharmaceutical delivery. Per FDA guidance, "when the intended use of a mobile app is for the diagnosis of disease or other conditions, or the cure, mitigation, treatment, or prevention of disease, or is intended to affect the structure or any function of the body of man, the mobile app is a device." This includes the time to develop the application and integrate with the device, prior to it being placed into production usage. Associated data service (data plan) is also non-IT only if non-severable from the cost of the device.
[8] Software as a Service (SaaS) as defined by this policy in accordance with the National Institute of Standards and Technology's (NIST) guidelines (e.g. cannot be hosted on the VA network and no software can be downloaded from the service provider) are non-IT. Due to variants in SaaS offerings from industry, all funding request for SaaS projects must follow the SaaS approval process in Appendix B. Other service models used in VA's IT production environment such as infrastructure- (IAS), platform-(PAAS), and telecommunications-as-a-service, as defined by National Institute of Standards and Technology's (NIST) guidelines, that require VA maintenance and/or interfaces to VA IT production environment, applications or data stores are IT.
[9] Including modifications to a building's infrastructure, even though required specifically for IT purposes. Examples include: the acquisition and installation of a wire closet fiber optic infrastructure, power surge protection, distribution and battery backup systems, and heating, ventilation and air conditioning (HVAC) equipment to comply with either operating requirements and/or manufacturer warranties. This includes construction of data centers. The IT appropriation does not have the legal authority to incur any construction costs.

INTENTIONALLY LEFT BLANK

ACQUISITION AND MANAGEMENT OF VA INFORMATION TECHNOLOGY ASSETS

For specific questions concerning the proper funding for IT items/services please refer to the below linked documents.

1. **IT-Non-IT Workgroup (ITW) Processes and background information:**

    a. ITW Process Charter and How to submit projects to the ITW Link:
    b. IT-Non-IT Workgroup (ITW) meeting minutes, agendas, decisions and related documentation: Link:

2. **Medical Devices Review Process:**

    a. VA Directive 6550 Pre-Procurement Assessment for Medical Devices/Systems: LINK
    b. FDA Overview of Medical Devices and Medical Device Listing: Link

3. **Software as a Service (SaaS) and Non-IT funding requests Approval Process**

Starting with the VIP process to document your need, please refer to the instructions and Epic template to document the requirements, vendor name and product required to meet your objectives: Link. Once completed, forward your completed Epic to the appropriate IT Account Manager (ITAM) via your OI&T Local Deputy Chief Information Officer (DCIO).