Department of Veterans Affairs
Washington, DC 20420

VA DIRECTIVE 6518
Transmittal Sheet
February 20, 2015

ENTERPRISE INFORMATION MANAGEMENT (EIM)

1. REASON FOR ISSUE: This Directive establishes Enterprise Information Management (EIM) policy for the US Department of Veterans Affairs. The VA's information assets are core resources of the Department, and their effective management is critical to the provision of services to our nation's Veterans. This Directive defines the objectives, establishes overarching principles and policy, assigns responsibilities, and delegates authority for the management and use of VA's information assets. Full implementation of this policy is necessary to enable VA to most effectively use resources to deliver an integrated, interoperable, Veteran-centric information environment.

2. SUMMARY OF CONTENTS: This Directive:

a. Provides enterprise rules and principles that enable management of VA information in a consistent, accurate, and holistic manner. These rules and principles serve as the baseline for alignment and prioritization of information capability initiatives across the VA.

b. Establishes information management roles and responsibilities between VA business units and OI&T. Implementation of this policy is a shared responsibility amongst all VA Administrations and staff offices.

3. **RESPONSIBLE OFFICE(S):** Department of Veterans Affairs Chief Information Officer (CIO) is responsible for the content of this policy.

4. **RELATED HANDBOOK:** None.

5. **RESCISSIONS:** None.

Certified By:

/s/
Stephen W. Warren
Executive in Charge and
Chief Information Officer
Office of Information and Technology

BY DIRECTION OF THE SECRETARY OF VETERANS AFFAIRS:

/s/
Stephen W. Warren
Executive in Charge and
Chief Information Officer
Office of Information and Technology

Distribution: Electronic Only

ENTERPRISE INFORMATION MANAGEMENT (EIM)

1. PURPOSE. To establish the importance of VA's information resources as strategic assets of the US Department of Veterans Affairs, necessary in providing critical, integrated services and benefits to US Service members, Veterans, their beneficiaries and other representatives, hereafter referred to collectively as "VA Customers". This Directive:

a. Establishes policy and assigns responsibilities to VA business units and OI&T to implement and enable a secure information sharing environment in the VA that supports delivery of services and benefits to VA Customers as well as the internal operations of the Department.

b. Provides enterprise rules and principles that enable management of VA information resources in a more consistent, accurate, and holistic manner. These rules and principles will serve as the baseline for alignment and prioritization of information capability initiatives across the VA.

c. Guides the use of information resources for implementing and enabling the sharing of information across the VA Enterprise, and with VA Customers and mission partners.

2. POLICY.

a. VA's information resources (all information collected, acquired, and stored by the Department in the course of conducting VA business and in serving VA Customers) are critical VA assets and shall be managed to provide the most integrated, efficient, and effective service possible to VA Customers.

b. All VA information shall be visible, accessible, and understandable in a secure environment throughout the information life-cycle to all authorized users including VA Customers, VA Employees, and VA mission partners.

c. The VA shall share and exchange information securely across the VA Enterprise and with its mission partners, as part of Department operations, in order to provide critical services to all VA Customers.

d. The VA will identify and designate Authoritative Data Sources (ADSs) which shall be officially registered, and used for all VA information to improve mission effectiveness by eliminating duplicative data sources and enabling the reuse of interoperable data.

e. All VA systems, services, and processes throughout the enterprise shall access VA data solely through official VA ADSs where available to ensure data quality, interoperability, and reuse.

f. The VA shall identify and designate as “common” all information that is used across multiple Administrations and staff offices to serve VA Customers or manage the internal operations of the Department. Business rules and standards for “common” information shall be defined and managed at the Department level.

g. All VA business processes shall be aligned with rules established around the creation, access, update and deletion of “common” information.

h. VA information shall be made open and available to other federal departments, agencies, mission partners, and the public to the maximum extent possible consistent within security and privacy laws and regulations and Department policies.

i. The VA shall adopt Federal information sharing standards to the maximum extent possible when implementing IT systems.

j. All new IT solutions , and all systems in production receiving development and modernization dollars for systems upgrades, shall be planned and designed in accordance with this policy, and will not be approved or funded unless those plans and designs comply with this policy.

3. RESPONSIBILITIES.

a. VA Administrations and Staff Offices. In execution of their mission responsibilities the VA Administrations, staff offices and those who support them shall:

(1) Define and document (within the VA Enterprise Architecture (EA)) mission-specific business processes, and define business rules around the capture and usage of information within these processes.

(2) Align all business processes with rules established around the creation, update and deletion of “common” information.

(3) Develop information requirements and associated information quality standards (accuracy, consistency, timeliness) for running VA business operations based upon their defined business processes and mission requirements.

(4) Ensure that information gathered, provided and maintained within the VA information environment by their mission activities meets information quality standards as defined by the respective information quality office and/or information quality representative within each Administration.

(5) Define, document, implement and continually provide stewardship for authoritative data that are domain-specific to each administration and staff office, and promote adoption of standardized data across the enterprise.

(6) Provide and maintain all business information required for the development of enterprise-wide conceptual and logical data models. Where applicable, ensure adoption of these models within mission processes. Advocate for proper usage of appropriate industry standards in mission-specific areas.

(7) Evaluate all information resources within their mission scope with respect to Open Data and Open Government guidelines, and publish all information deemed appropriate for public release based on this evaluation.

(8) Ensure adherence to VA official guidance and policies, VA Information Privacy/Security policies and standards as well as Federal laws and regulations and National Institute of Standards and Technology (NIST) Publications.

(9) Integrate compliance with this policy within decision processes which they oversee.

b. The Office of Information and Technology (OI&T). In supporting the Administrations and staff offices in the delivery of mission capabilities OI&T shall:

(1) Design, develop, implement and maintain the VA's IT Systems environment to meet the Department's information requirements as defined by the VA's Administrations and staff offices.

(2) Ensure the efficiency and interoperability of the VA information environment, promoting secure information sharing through the reuse of information resources and the active identification and elimination of unnecessary duplicative information stores.

(3) Ensure that information design, configuration and storage within the VA information environment meets information quality standards as defined by the Administrations and staff offices

(4) Document (in collaboration with Administrations and staff offices) information flows within VA's information environment, including interactions with VA's mission partners.

(5) Develop and maintain the solutions (services, etc.) and informing technical specifications that deliver authoritative data within the VA information environment in support of VA business processes.

(6) Ensure and maintain the visibility, accessibility and secure use of authoritative data sources as defined by the Administrations and staff offices within the VA information environment.

(7) Drive (through collaboration with Administrations and staff offices) development, maintenance and adoption of VA-wide conceptual and logical data models.

(8) Develop and maintain physical data models of individual systems within VA's IT environment.

(9) Ensure adherence to Federal laws and regulations, NIST Publications, VA official guidance and policies, VA Information Privacy/Security Policies and Standards.

(10) Integrate compliance with this policy within decision processes which are overseen by OI&T.

4. REFERENCES.

a. Disabled VA Employees and Members of the Public; section 794d of Title 29, United States Code

b. The Federal Records Act of 1950

c. The Freedom of Information Act, July 4, 1966

d. The Privacy Act of 1974

e. The Office of Management and Budget (OMB) Privacy Act Implementation, Guidelines and Responsibilities, published in the Federal Register July 9, 1975

f. Paperwork Reduction Act of 1980

g. OMB Circular No. A-130, *Management of Federal Information Resources*.

h. The Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules

i. United States Code (USC), "Title 38 – Veteran's Benefits", "Chapter 3 Department of Veterans Affairs", "Section 310 - Chief Information Officer".

j. USC, "Title 40 – Public Buildings, Property, and Works", "Subtitle III – Information Technology Management".

k. USC, "Title 44 – Public Printing and Documents", "Chapter 35 – Coordination of Federal Information Policy", "Subchapter I – Federal Information Policy", "Section 3506 - Federal agency responsibilities, part (a)(2)".

l. OMB The Information Quality Act (also known as the Data Quality Act), January 3, 2002.

m. The Federal Information Security Management Act of 2002 (FISMA)

n. The Confidential Information Protection and Statistical Efficiency Act of 2002 (CIPSEA).

o. E-Government Act of 2002.

p. President Memorandum, *Transparency and Open Government* , January 21, 2009

q. VA Directive 6300, *Records and Information Management*, February 26, 2009.

r. OMB M-10-06, *Open Government Directive*, December 8, 2009.

s. OMB M-12-18, *Managing Government Records Directive*, August 24, 2012.

t. President Executive Order, *Making Open and Machine Readable the New Default for Government Information*, May 9, 2013.

u. OMB M-13-13, *Open Data Policy- Managing Information as an Asset*, May 9, 2013.

5. DEFINITIONS.

a. Accessible. Users and applications post data to a "shared space. Posting data implies that (1) descriptive information about the asset (metadata) has been provided to the Department's enterprise architecture, which 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.

b. Application. The use of information resources (information and information technology) to satisfy a specific set of user requirements.

c. 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. Administrations and staff offices designate these sources within domains for which they are the stewards. The Office of Information and Technology develops and maintains technology solutions (e.g. services) that use these sources.

d. Authorized User. A person who is granted access to information resources based upon clearance, need-to-know, organization security policy, and federal security and privacy laws.

e. Capability. The ability to achieve a Desired Effect under specified [performance] standards and conditions through combinations of ways and means [activities and resources] to perform a set of activities.

f. Common Information. Information that is both gathered and used by multiple Administrations, staff offices, or other organizational entities across the VA Enterprise to conduct business. Examples of such information include, but are not limited to:

(1) Identity
(2) Military Service Record
(3) Contact Information
(4) Demographic and Socio-economic.

g. Data. An elementary description of things, events, activities, and transactions that are recorded, classified, and stored, but not 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 retrieval.

h. Duplicative Data Sources and Information Stores. Multiple data sources or information stores of the same information that are in no way synchronized and/or reconciled with one another. This leads to multiple answers to the same question. Mirrored duplication of core information done for purposes of redundancy and resiliency of operations, and that are synchronized back to an authoritative source, are not “duplicative”.

i. Government Information. Information created, collected, processed, disseminated, or disposed of by or for the Federal Government.

j. 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, but does not include the provision of hyperlinks to information that others disseminate. This definition does not include opinions, where the agency's presentation makes it clear that what is being offered is someone's opinion rather than fact or the agency's views.

k. 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), and the governance framework, policies and standards that ensure information is managed as an asset.

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

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

n. Information Resources. Includes both government information and information technology.

o. Information Technology. The term "information technology" means any equipment or interconnected system or subsystem of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by an executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which (i) requires the use of such equipment, or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term "information technology" includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. The term "information technology" does not include any equipment that is acquired by a Federal contractor incidental to a Federal contract. The term "information technology" does not include national security systems as defined in the Clinger-Cohen Act of 1996 (40 U.S.C. 1452).

p. Interoperable*.* Many-to-many exchanges of data occur between systems, through interfaces that are sometimes predefined or sometimes unanticipated. Metadata is available to allow mediation or translation of data between interfaces, as needed.

q. Open Data. The Open Data Executive Order and the accompanying Open Data Policy released by OMB and Office of Science and Technology Policy that implements the Order—require that, going forward, newly generated government data shall be made freely available in open, machine-readable formats, while appropriately safeguarding privacy, confidentiality, and security. This requirement will help the Federal government achieve the goal of making previously inaccessible or unmanageable data easily available to entrepreneurs, innovators, researchers, and others who can use those data to generate new products and services, build businesses, and create jobs.

r. Open Government. Governing doctrine which holds that citizens have the right to access the documents and proceedings of the government to allow for effective public oversight. On December 8, 2009, the White House issued an “Open Government” Directive requiring federal agencies to take immediate, specific steps to achieve key milestones in transparency, participation, and collaboration. The Open Government Directive and all milestones and corresponding progress can be found on http://www.whitehouse.gov/open.

s. 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.

t. Strategic Asset. An asset that is required by an entity in order for it to maintain its ability to achieve future outcomes.

u. System or General Support System. 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. A system can be, for example, 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 a shared information processing service organization.

v. 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.

w. 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.

x. VA Customers. US Service members, Veterans, and their beneficiaries and representatives.

y. VA Mission Partners. Those with whom the Department of Veterans Affairs cooperates to achieve national goals, such as other departments and agencies of the U.S. Government; state and local governments; non-governmental organizations; and the private sector.

z. Visible. Users and applications can discover the existence of data assets through catalogs, registries, and other search services. All data assets (intelligence, nonintelligence, raw, and processed) are advertised or “made visible” by providing metadata, which describes the asset.