VA ENTERPRISE DATA MANAGEMENT (VADM)

1. **REASON FOR ISSUE:** This directive establishes the Department of Veterans Affairs enterprise data management policy. VA's data is a strategic asset and critical resource for the Department's administration of benefits and the provision of services. As with any other strategic asset, data needs to be managed and this policy intends to set forth the overarching structure for enterprise data management. This directive applies to all data within the Department.

   By effectively managing VA's data over its lifecycle, the Department will improve data discovery, transparency, quality, consistency, access, use, and insight while realizing economic efficiencies and integrating security and privacy requirements. Effective lifecycle management enables better customer engagement and innovation. The Department will establish and use authoritative data sources and reduce duplicative collection. Finally, the Department will be able to create evidence and unlock insights to support operational, business, and strategic impact for the Department and Veterans. The policies set forth herein are based on best practices and address legislative and the Office of Management and Budget requirements.

2. **SUMMARY OF CONTENTS:** This directive:

   a. Provides enterprise policy, roles and responsibilities, rules, and principles; and establishes requirements for enabling the management of VA data as a strategic asset in a consistent, accurate, and holistic manner.

   b. Sets forth the responsibilities of the Administrations, Chief Information Officer (005), Chief Data Officer (008), and the Chief Data Technology Officer (005), and the Data Governance Council.

3. **RESPONSIBLE OFFICE:** Office of Enterprise Integration (008) and Office of Information and Technology (005).

4. **RELATED HANDBOOK:** None.

5. **RESCISSION:** VA Directive 6518, Enterprise Information Management dated February 20, 2015.

CERTIFIED BY:

/s/
Karen L. Brazell
Principal Executive Director, Office of Acquisition, Logistics and Construction and Chief Acquisition Officer, Performing the Delegable Duties of the Assistant Secretary for Enterprise Integration

BY DIRECTION OF THE SECRETARY OF VETERANS AFFAIRS:

/s/
Karen L. Brazell
Principal Executive Director, Office of Acquisition, Logistics and Construction and Chief Acquisition Officer, Performing the Delegable Duties of the Assistant Secretary for Enterprise Integration

DISTRIBUTION: Electronic only

TABLE OF CONTENTS

VA ENTERPRISE DATA MANAGEMENT (VADM)

1. PURPOSE.

a. To establish the US Department of Veterans Affairs (VA) requirements for the lifecycle management of data as a strategic asset to be used to support VA's Mission and values. VA's data is necessary in providing critical services and benefits to VA customers: US service members, Veterans, their beneficiaries, and their representatives.

b. Increase the value of data to VA and Veterans through enterprise-wide data lifecycle management, including responsible sharing and linkage with other data, safeguarding, and analytics and insights.

c. Set forth the overarching structure for enterprise data management within VA. The requirements of this structure will be developed and managed under the leadership of the Chief Data Officer (CDO) in partnership with the Data Governance Council (DGC).

d. Effectively manage VA's data as a strategic enterprise asset to improve data discovery, transparency, quality, consistency, access, and availability of data; while improving service to VA customers and realizing efficiencies via greater insights and the reduction of redundancies.

e. Establish the policies and processes for lifecycle data management, information sharing, supporting interoperability, and analytics; including coordinating and safeguarding policy activities to support efficient and effective administration of benefits and provision of services to Veterans.

f. Establish the roles and responsibilities of the DGC; and CDO, Chief Information Officer (CIO), DGC Co-Chair, Chief Data Technology Officer (CDTO), and other senior key officials in the Department.

g. Outline the collaboration structures and governance framework for coordinating and creating required policy and guidance.

2. POLICY.

a. VA's data is a VA strategic asset and shall be managed consistently and across its lifecycle to:

(1) Enhance insight into the Veteran population to better understand their needs and desires; barriers and outcomes;

(2) Evaluate and improve the lifetime impact of VA services and benefits on the Veteran population; and

(3) Further strengthen proactive, efficient, and effective delivery of services and benefits to Veterans using authoritative data managed over its lifecycle.

b. References to data in this directive shall be construed to include all data created, collected, received, acquired, processed, derived, disseminated, stored, and disposed of by the Department in the course of conducting VA business and in serving VA customers.

c. All data in the Department shall be managed according to law, VA policy and standards including compliance with data quality and security requirements.

d. All data in the Department shall be available for responsible sharing as provided by law and in accordance with the VA's Ethical Principles for Access to and Use of Veteran Data while protecting privacy and confidentiality, and aligning with the appropriate standards, architectures, and models.

e. VA will establish a system that identifies individuals accessing confidential data and the project for which the data is required.

f. When authoritative data is identified, it is the responsibility of the data steward, data owner, and/or system owner to nominate the authoritative data source (ADS) for consideration to the DGC following the requirements for ADS identification and selection.

g. When VA has specific authoritative VA customer data within the VA information environment, VA will ensure this data is available via application programming interfaces (APIs) and leverage this authoritative data, within appropriate VADM practices, with a goal, whenever possible, of not asking for the same data again.

h. To the extent feasible, if VA has received authoritative data from the Department of Defense, or other external sources, within appropriate VADM practices, governing agreements and authorized user principles, VA will prioritize the use of this computable data and will not ask for the same data again.

i. References to data in this directive shall be construed to include data, information sharing, data interoperability, and analytics.

j. VA customers, individually and collectively, have an ongoing interest in their data and its management, quality, sharing, safeguarding, and use by VA.

k. The policies in this directive apply to the entire Department but are non-binding guidelines for the Office of Inspector General.

3. ROLES AND RESPONSIBILITIES.

a. **Secretary of Veterans Affairs shall** designate the CDO as the senior Department official responsible for execution and/or oversight of the Department's data assets and programs; and for guiding and instructing the Department's Data Owners and consumers to implement this directive.

b. **Assistant Secretary for Enterprise Integration shall:**

(1) Appoint the CDO to oversee and manage implementation of this directive.

(2) Oversee Department-wide policies and procedures to ensure the management of data as a strategic asset via the actions of the CDO.

(3) Integrate data management governance and policy within the broader VA governance and policy ecosystem.

c. **Assistant Secretary for Information and Technology / Chief Information Officer (CIO) shall:**

(1) Design, develop, implement and maintain VA's information technology systems, enterprise and technical architecture and infrastructure to meet the Department's data requirements as shaped by the CDO and Administrations.

(2) Set forth policy for data and system privacy and security in collaboration with Administration entities and for creating, maintaining, and documenting application programming interfaces through VA enterprise design patterns.

(3) Designate a Senior Official of the Office of Information Technology (OI&T) at the Deputy Assistant Secretary level or higher as the CDO day to day point of contact and the DGC Co-Chair, designate the Chief Data Technology Officer (CDTO), and support both designations with the necessary allocation of resources to fulfill the responsibilities of these roles.

(4) Ensure the efficiency and interoperability of the VA information environment consistent with FITARA and OMB A-130, promoting secure information sharing through the reuse of information resources, in consultation with the CDO and the OIT DGC Co-Chair.

d. **Under Secretaries, Assistant Secretaries, and Other Key Officials shall:**

(1) Implement this directive in their organizations within policy and guidance set by the CDO and the DGC Co-Chair.

(2) Designate a career Senior Official at the Senior Executive Service level to represent their organizational equities as a DGC voting member and

empower them to represent organizational equities within DGC deliberations.

(3) Designate a primary action officer to support their DGC representative and to participate in all applicable activities of the DGC including coordinating and/or participating in DGC subordinate working groups or forums; and coordinating DGC related actions by reaching back into the organization as needed.

(4) Establish resource coordination and governance, as needed, to support federated and aligned implementation of this directive within their organization, in line with data management functions and guidelines set forth by the CDO.

(5) Identify data stewards for the data within their organization and allocate the necessary resources for the implementation of data governance; management processes and authoritative data sources; and compliance with data policies within their Administrations/Staff Offices.

(6) Implement VADM policy and support implementation of VA's data strategy and roadmap including internal planning, programming, and resource allocation including the use of ADSs.

(7) Establish a data-driven culture including sustained engagement with their workforce that leverages data for the improvement of internal operations and services provided to VA customers.

(8) Develop and implement mechanisms for monitoring and enforcing data management policies and compliance with regulatory requirements.

e. **Chief Data Officer (CDO) shall:**

(1) With the CIO in collaboration with the policy leaders in the Office of the CIO; and the Evaluation Officer (EO), Statistical Official (SO), DGC and Chief Performance Officer (CPO) in the Office of Enterprise Integration; and Chief Architect in the Office of the CIO; and other stakeholders establish the Department's vision for its data; develop and maintain a data strategy, data strategy implementation roadmap, and business data architecture; and drive VA's evidence-based policymaking culture by integrating best data management practices to treat the Department data as a strategic asset.

(2) Oversee the implementation of VA's data strategy to ensure coherent strategic management and use of data across its entire lifecycle including data ownership, data stewardship responsibilities and decision rights.

(3) Provide to the Secretary a periodic assessment of VA's implementation of the strategy and roadmap including benefits, costs, challenges, and recommendations.

(4) Charter and execute the data governance function directly subordinate to the VA Operations Board; chair and consult with the DGC to ensure full representation of the Department's mission and business interests; lead the strategic and operational planning for the Department's data, including the identification of data stewards; establish guidelines and processes for the selection of ADS; champion the resource allocation for ADS within VA processes, make the official designations of ADS after DGC approval; and arbitrate cross-organizational and inter-agency data related issues.

(5) Lead VA data management maturity assessments to review data management capabilities for opportunities to improve data discoverability and access, process efficiency, cost savings, rationalize investments to maximize effectiveness, and serves, as a principal advisor to the CIO as it pertains to the resource requirements by guiding the development of business justifications and cost guidance for data related acquisitions and initiatives in the Department.

(6) Lead the open data initiative and guide data and analytics capabilities and further strengthen discoverability and accessibility of data.

(7) Coordinate existing and future policy, guidance, frameworks and standards to implement the policy of this directive.

(8) Focus data management functions for the Department through the establishment of data management goals, objectives, policy, and operating procedures for each step of the data lifecycle.

(9) Define the Department's data management organizational structure for business data architecture and coordinate the execution of those policies and processes.

(10) Review the impact of the infrastructure on data asset accessibility and coordinate with the CIO to improve such infrastructure to reduce barriers that inhibit data asset accessibility.

(11) Integrate VADM equities and support for evidence-based policymaking into VA governance and management processes including strategic planning, resource allocation, oversight of initiatives, risk management, and evaluation.

(12) Coordinate and align VADM policy, strategy, and processes with other federal agencies including the Department of Defense to advance integrated, effective, and efficient operations within VA and advancing Veterans' interests.

(13) Increase and promote the value of the Department's data as a strategic asset and communicate the benefits of VADM to ensure that the Department's data needs are met by the effective management and measurement thereof.

(14) Collaborate with the Senior Agency Official for Records, Senior Agency Official for Privacy, Chief Information Security Officer, CDTO, Chief Freedom of Information Act Officer, and Chief Privacy Officer or delegates, in addition to other data and information policy stakeholders, to coordinate policies and monitoring mechanisms of the necessary controls for the appropriate safeguarding and sharing of data assets through the data life cycle.

(15) Take responsibility for VA's Paperwork Reduction Act (PRA) efforts, including policy and organizational process improvements for PRA implementation and coordination with existing and future OIT efforts.

(16) On behalf of the Secretary, designate VA's SO to advise on statistical policy, techniques, and procedures and serve as an Agency consultant for the Department. The SO shall represent VA at the proceedings of the Interagency Council on Statistical Policy.

(17) Provide guidance and oversight across the Department's Data Analytics operations and workforce to align position descriptions, career paths, training opportunities, requirements, tools, methods, and analytical approaches used to develop evidence to support policy making and program evaluation, providing oversight for the implementation of the data analytics standards.

(18) Delegate responsibilities within VA, upon mutual agreement.

(19) Advise VA leadership to support resolution of data-related disputes.

f. **CIO Appointed DGC Co-Chair shall:**

(1) Serve as the DGC co-chair and ensures participation of the offices within the Office of Information Technology, as needed, in support of the DGC, and its deliverables and decisions; including development and implementation of the VA's data strategy and roadmap.

(2) Coordinate Department level data policy and requirements, and coordinate information technology prioritization and resource allocation to achieve data-related business and mission requirements.

(3) Serve as the CDO's day to day point for coordination to leverage and strengthen alignment of OIT resources in support of implementing this Directive and execution of the CDO's responsibilities.

g. **Chief Data Technology Officer (CDTO) shall:**

(1) Serve as a principle technical advisor to the CIO, CDO, and DGC Co-Chair across all technical aspects of the data lifecycle.

(2) Coordinate guidance and policy across OIT information policy domains, internal governance and management processes, and product lines to engage, understand, and coordinate business and mission requirements including the implementation of authoritative data sources and information technology systems.

(3) Design and oversee delivery of aligned data and analytics technical infrastructure and capability including support for VADM processes to further strengthen discoverability and accessibility of data.

(4) Coordinate, design, and oversee delivery across OIT product lines of implementation and use of designated ADS.

(5) Drive and support OIT portfolios and product lines to align with policy and guidance for the management and use of VA's data as a strategic asset.

(6) Partner with and support the CDO by developing, operationalizing, and optimizing VADM capabilities and processes via VA's Information Architecture and through the DGC and subordinate forums and working groups.

(7) Drive towards interoperability by setting forth the requirements for systems documentation according to their maturity to include physical schemas, metadata, logical and physical models, as appropriate, and maintain them at the enterprise level repository to ensure transparency and visibility on the system's data, and authoritative data source implementation.

(8) Promote a secure information and data analytic infrastructure conducive to information sharing and data exchanges as well as to making use of data for analytic purposes aligned with this current policy.

(9) Ensure the semantic interoperability of the VA information environment, by ensuring compliance with all data requirements including the allocation of resources for ADS implementation.

(10) Supports the technical aspects of the VA strategy and roadmap for data integration, data sharing, data transformation, and data provenance across VA and with Federal agencies such as the Department of Defense.

h. **Data Governance Council (DGC) shall:**

(1) Create and maintain policy, processes, guidance, and standards to ensure that VA's data is managed to provide the most integrated, efficient, and effective service possible to VA customers and internal business operations.

(2) Advise and assist the CDO, DGC Co-Chair, CTO, CDTO, data owners and consumers with their roles and responsibilities.

(3) Seek to make decisions through consensus. If consensus is not achieved, the Chairs may call for a formal vote of the membership. Objections will be recorded and attributed in the minutes.

(4) When consensus is not reached, the CDO and DGC Co-Chair may take the issue to the VA Operation Board for Deputy Secretary of Veterans Affairs resolution.

(5) Coordinate data governance policy development and ensure that VA data management policies are consistent, and that implementation is transparent across all Data Owners.

(6) Charter and establish subordinate bodies as needed to support the work of the CDO, CTO, CDTO, and DGC.

(7) Negotiate Department-level data sharing agreements with external organizations for the interchange of data used by multiple Administrations and Staff Offices. The DGC may delegate sharing agreement responsibilities.

4. REFERENCES.

a. Department of Veterans Affairs Information Security Enhancement Act of 2006, 38 U.S.C. §§ 5721-28.

b. Paperwork Reduction Act of 1980.

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

d. U.S.C., "Title 40 – Public Buildings, Property, and Works", "Subtitle III – Information Technology Management".

e. U.S.C., "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)".

f. Information Quality Act (also known as the Data Quality Act), January 3, 2002.

g. U.S.C., "Title 44 – Public Printing and Documents", Chapters 29, 31 and 33

h. VA Directive 6300, Records and Information Management, September 21, 2018.

i. VA Directive 6500, Risk Management Framework for VA Information Systems - Tier 3: VA Information Security Program, March 10, 2015

j. Federal Information Acquisition Technology Reform Act of 2014 (National Defense Authorization Act for Fiscal Year 2015 (Title VIII, Subtitle D, H.R. 3979.))

k. Foundations for Evidence-Based Policymaking Act of 2018 (Pub. L. 115–435).

l. Geospatial Data Act of 2018.

m. OMB M-19-23, Phase 1 Implementation of the Foundations for Evidence-Based Policymaking Act of 2018: Learning Agendas, Personnel, and Planning Guidance.

n. OMB M-20-12, Phase 4 Implementation of the Foundations for Evidence-Based Policymaking Act of 2018: Program Evaluation Standards and Practices.

o. OMB M-13-13, Open Data Policy - Managing Information as an Asset.

p. Executive Order 13642, *Making Open and Machine Readable the New Default for Government Information.*

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 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.

b. **Authoritative Data Source.** A source of data or information designated as official source of data after recognition by the DGC and endorsement by the CDO and is recognized as trusted, timely, and secure and is used within VA's information environment in support of VA business processes. Administrations and Staff Offices nominate these sources within domains for which they are the stewards. OIT develops and maintains technology solutions (e.g. services) that use these sources.

c. **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.

d. **Business Architecture**. A depiction of the various components of VA’s business and their relationships to each other.

e. **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 or in line processing.

f. **Data Architecture**. A perspective of the overall agency EA providing the information about the agency's baseline and target data architectures.

g. **Data Asset.** A collection of data elements or sets that may be grouped together and represents a work product generated by a VA employee or VA-affiliated entity.

h. **Data Quality.** A measure of the condition of data based on factors such as accuracy, completeness, consistency and reliability.

i. **Data Governance.** The exercise of authority, control, and shared decision-making planning, monitoring, management and enforcement over data assets.

j. **Data Lifecycle.** The stages through which data passes, typically characterized as creation or collection, processing, dissemination, use, storage, and disposition.

k. **Data Management**. The set of disciplines and techniques used to process, store and organize data.

l. **Data Owner.** An agency official with statutory or operational authority for specified information and responsibility for establishing the criteria for its creation, collection, processing, dissemination, or disposal. Responsibilities may extend to interconnected systems or groups of interconnected systems.

m. **Data Stewardship.** The formal, specifically assigned and entrusted accountability for business (non-technical) responsibilities ensuring effective control and use of data and information assets implemented by formally assigning and entrusting its responsibilities to data stewards.

n. **Enterprise Architecture.** EA is a management practice focused on performance improvement through the alignment of strategic objectives, business needs, and information technology capabilities. EA identifies whether its resources are properly aligned to the agency's mission and strategic goals and objectives. EA is used to drive business decisions toward a more effective and efficient agency performance.

o. **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. Information usually but not always has associated meta-data, or data that helps to characterize and provide context.

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

q. **Information Resources.** Includes both government information and information technology.

r. **Interoperability**. The ability of a system to securely exchange information with, and use information from, other systems without special effort by the user. (IEEE)

s. **Open Data**. Under the OPEN Government Data Act, government data shall be made freely available in machine-readable formats, while appropriately safeguarding privacy, confidentiality, and security in order to be easily available to entrepreneurs, academia, researchers, and others who can use those data to generate new products and services. An enterprise-wide data inventory will be maintained to include a list of data assets and associated metadata for public, non-public, and restricted public data assets.

t. **Record.** As defined in 44 U.S.C. 3301, records are all books, papers, maps, photographs, machine readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the United States Government under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the Government or because of the informational value of the data in them.

u. **Safeguarding.** Safeguarding relates to the measures used to deter, detect, and prevent against the loss, misuse, theft, unauthorized access, unauthorized modification, unauthorized disclosure, or unauthorized use of classified, controlled unclassified information (CUI), and other unclassified information of a sensitive nature, and the protections afforded to information systems/networks on which such information resides. Safeguarding encompasses - but is not limited to - counterintelligence, information assurance, information security, operational, administrative, personnel, and physical security, as well as privacy, civil rights, and civil liberties protections.

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

w. **VA Customers**. US service members, Veterans, and their beneficiaries and representatives and employees.

x. **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.