Department of Veterans Affairs
Washington, DC 20420

VA DIRECTIVE 6402
Transmittal Sheet
December 29, 2022

LOCAL MODIFICATIONS TO NATIONALLY RELEASED VISTA SOFTWARE

1. **REASON FOR ISSUE.** This Directive sets forth policies and responsibilities that will govern Office of Information and Technology (OIT) modifications to Veterans Health Information Systems and Technology Architecture (VistA) Software.

2. **SUMMARY OF CONTENTS/MAJOR CHANGES.** This Directive revises policy, processes and responsibilities that the Department of Veterans Affairs (VA) Medical Centers (VAMCs) and OIT must follow to request evaluation and approval for modifications to standardized VistA software, regional-supported Class II, Class III and compliance scanning for VistA standardization.

3. **RESPONSIBLE OFFICE.** Office of Information and Technology (005), Software Product Management (SPM) (005S), VistA Office (VO).

4. **RELATED HANDBOOK.** None.

5. **RESCISSION.** VA Directive 6402, Modifications to Standardized National Software, dated August 28, 2013.

CERTIFIED BY:

/s/
Guy T. Kiyokawa
Assistant Secretary for
Enterprise Integration

BY DIRECTION OF THE SECRETARY OF VETERANS AFFAIRS:

/s/
Kurt D. DelBene
Assistant Secretary for
Information and Technology and
Chief Information Officer

Distribution: Electronic Only

LOCAL MODIFICATIONS TO NATIONALLY RELEASED VISTA SOFTWARE

1. **PURPOSE AND SCOPE.** The purpose of this directive is to control variation in nationally released Veterans Health Information Systems and Technology Architecture (VistA) software through defined, mandatory governance channels. The scope of this directive addresses non-standardized changes to National Class I Software.

   a. Veterans Health Administration (VHA) clinical and management operations rely on accurate and consistent support from a suite of information systems. Of these, VistA represents the major system. VistA is used to implement regulations, processes and controls that must be applied consistently across VHA.

   b. This directive does not impact:

      (1) Any VistA application parameter/package setup performed by the VHA Office of Health Informatics staff and/or activities required to implement the new Electronic Health Record (EHR).

      (2) Any processes for developing or governing nationally released VistA software.

      (3) Requirements for VistA data storage required by the National Archives and Records Administration approved records schedule found in Record Control Schedule 10-1 dated January 2020.

2. **POLICY.** It is VA policy that all instances of VistA will install the National VistA Software. At the conclusion of the VistA Standardization Project (2013-2018), all currently approved waivers shall remain in effect until each VAMC has transitioned to the new Electronic Health Record Modernization (EHRM) software. All VAMC facilities and their OIT support must adhere to the following regulations regarding software modification:

   a. Specific VistA instance enhancements to, or modifications of, in part or in whole, is prohibited.

   b. All Class II and Class III new software requests for local modifications shall be submitted and documented through the Innovation and Development Request available at the Innovation and Development Request Portal. This includes any Class I routine that is copied to a regional/VAMC VistA instance-specific namespace as well as any menu options associated to the copied routine(s). All regional/VistA instance-specific software must follow all OIT programming standards. All innovations or Class III Commercial Off-The-Shelf (COTS) modifications that are not approved for national release must be removed from the specific VistA instance(s) and restored back to the VistA gold standard.

c. All requests for local modifications to accommodate EHRM efforts will be governed by the Veteran-Focused Integration Process (VIP) used by EHRM.

d. The waiver process was discontinued as of November 2018. Existing software waiver approvals and exemptions prior to November 2018 remain in effect until either a permanent solution removes the need for these modifications or each VAMC has migrated to the new EHR.

e. If a non-compliant modification is discovered and the VAMC facility Director determines that the non-compliant modification supports important operational capability, the OIT VistA support team will work with the facility and governance referenced in this policy to resolve the non-compliance in a manner that minimizes adverse effects on operations, staff and Veterans.

3. RESPONSIBILITIES.

a. **Under Secretaries, Assistant Secretaries and Other Key Officials** are responsible for ensuring compliance with this Directive within their respective Administrations, Staff Organizations and Program Offices by coordinating and collaborating with Office of Information and Technology officials.

b. **Assistant Secretary for Information and Technology and Chief Information Officer (CIO).** The CIO is the senior agency official responsible for the implementation of this directive. The CIO shall review and evaluate compliance with this directive.

c. **Applications Service Line (ASL) Manager, OIT, SPM.** The ASL Manager shall monitor, process and approve or disapprove all new software requests entered via the Innovation and Development Requests available at the Innovation and Development Request Portal.

d. **Director VO, OIT, SPM.** The VO Director shall maintain a partnership with all programs that impact changes to VistA software, including but not limited to VHA, OIT, EHRM, the Financial Management Business Transformation/Integrated Financial and Acquisition Management System and Defense Medical Logistics Standard Support.

e. **Director, VAMC.** The VHA VAMC Director shall submit new software requests for the VAMC and associated outpatient clinics through the Innovation and Development Requests available at the Innovation and Development Request Portal. The Director will also decide the significance of the impact of removing a non-compliant modification on operations, staff and Veterans.

f. **VHA Chief Informatics Officer.** The VHA Chief Informatics Officer shall manage functional governance for VHA through approved VHA committees.

4. DEFINITIONS.

a. **National Class I Software.** Nationally released OIT SPM VistA software includes all interfaces installed on or interacting with VA computing environments. National Software has been created by or evaluated and certified by OIT to comply with VA established criteria listed below. (Source: VistA Office)

(1) Architecture and technology

(2) Capacity and performance

(3) Coding standards

(4) Documentation

(5) Interagency agreements

(6) Name spacing and interface control agreements

(7) Network capacity impacts

(8) OIT Technical Reference Model (TRM)

(9) Privacy and confidentiality

(10) Section 508 accessibility

(11) Security

(12) Testing

g. **Class II Software.** Represents a Class III product that has been verified as compliant with established standards. These are products coming out of field development (FD) and are certified and approved for Class II deployment and follow-on support by FD. (Source: VistA Office)

h. **Class III Software.** Products originating from any unrelated OIT SPM source, including field developers, non-Information Technology (IT) VA staff (e.g., physicians), vendors, open source, research, or educational organizations located on a VAMC-specific VistA instance. These software products generally have a limited and non-standardized distribution across VA systems and are not covered by OIT SPM support commitments. (Source: VistA Office)

5. REFERENCES.

a. P.L. 97-255, Federal Managers Financial Integrity Act of 1982, published September 8, 1982.

b. Food, Drug and Cosmetics Act (FD&C Act), published March 29, 2018. The Act establishes the Food and Drug Administration's (FDA's) authority over the VistA Software.

c. Government Accountability Office Policy and Procedures Manual for Guidance of Federal Agencies, published on May 18, 1993.

d. Office of Management and Budget (OMB) Memorandum M-16-17, OMB Circular No. A-123, Management's Responsibility for Enterprise Risk Management and Internal Control, published July 15, 2016.

e. OMB Circular A-127, Financial Management Systems 31 U.S.C. 3512, published August 13, 1999.

f. OMB Circular A-130, Managing Information as a Strategic Resource, published July 28, 2016.

g. P.L. 100-235, Computer Security Act of 1987, published January 8, 1988.

h. VA Records Control Schedule 10-1, dated January 2021.

i. VA Directive 6500, VA Cybersecurity Program, published February 24, 2021.

j. VistA Standardization and Virtualization Software Waiver Exemption, dated June 2020. (Rescinded)