Department of Veterans Affairs
Washington, DC 20420

VA DIRECTIVE 6402
Transmittal Sheet
August 28, 2013

MODIFICATIONS TO STANDARDIZED NATIONAL SOFTWARE

1. REASON FOR ISSUE. To set forth policies and responsibilities that will govern local modifications to VistA National Software once sites are in compliance with the Gold Disk.

2. SUMMARY OF CONTENTS /MAJOR CHANGES. This Directive provides policy and processes that local facilities must follow to request evaluation and approval for modifications to standardized National Software, as well as requirements for annual certification of compliance.

3. RESPONSIBLE OFFICE. Assistant Secretary for Information and Technology (005), Service Delivery and Engineering (005OP) is responsible for the content contained in this Directive.

4. RELATED HANDBOOK. None.

5. RESCISSION. VHA 2004-038, Modifications to VHA Modifications to Class I Software dated July 23, 2004.

CERTIFIED BY:

/s/

Stephen W. Warren
Executive in Charge
and Chief Information Officer

BY DIRECTION OF THE SECRETARY OF VETERANS AFFAIRS:

/s/

Stephen W. Warren
Executive in Charge
and Chief Information Officer

Distribution: Electronic Only

MODIFICATIONS TO STANDARDIZED NATIONAL SOFTWARE

1. PURPOSE AND SCOPE. This Directive establishes mandatory Department-wide policy for implementing local software modifications to Veterans Health Information Systems and Technology Architecture (VistA) National 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. Unauthorized changes to VistA can disable or impair critical VHA functions and, in serious cases, result in patient safety incidents.

b. The Office of Information and Technology (OIT) is spearheading the VistA Open Source initiative, which is an effort to modernize the Department of Veterans Affairs (VA) electronic health record by opening VistA's software codebase so that the local field facilities as well as outside sources (industry, academia, etc.) may contribute to its development and increase innovation. The VistA code set will be certified and stored by the custodial agent Open Source Electronic Health Record Agent (OSEHRA). This partnership with OSEHRA is a key element of VA's effort to innovate in the Electronic Health Record software arena, including both VistA and our joint effort with the Department of Defense (DoD) to merge the agency's systems to support common clinical processes and implement an Integrated Electronic Health Record (iEHR) as directed by the Executive Branch. This move towards an iEHR requires rigorous and consistent software configuration at all VA Medical Centers (VAMC).

c. The Open Source VistA Gold Project is a component of the VistA Open Source initiative. A redacted version of the National Software is currently available to the public via the Freedom of Information Act (FOIA). The tenets of VistA Open Source are that all VAMCs will install and run the National Software located on the Gold Disk that has been certified by OSEHRA. Once standardization is achieved, VAMCs will adhere to the policies outlined within this Directive to implement local modifications to National Software.

2. POLICY.

a. It is OIT policy that all instances of VistA will install and run the certified National Software located on the Gold Disk. Upon fulfillment of gold disk standardization

requirements, sites must adhere to the following regulations regarding local software modifications:

(1) Local enhancements to, or modifications of, Protected National Software, in part or in whole, is prohibited. Refer to Appendix A for a complete list of Protected National Software.

(2) Local enhancements to, or modifications of, Non-Protected National Software is only allowed with an approved waiver by the Software Modification Waiver Committee (SMWC). Refer to Appendix B for the Waiver Process. Application of local modifications upon waiver approval must still adhere to the National Field Operations processes at http://vaww.sde.portal.va.gov/sites/fo/FOWiki/Wiki/Change%20Management.aspx.

(3) Local Software that does not modify the National Software in any way is not impacted by this directive. However, any such enhancement must still adhere to the National Field Operations processes at http://vaww.sde.portal.va.gov/sites/fo/FOWiki/Wiki/Change%20Management.aspx.

(4) Annual reports depicting adherence to this policy must be submitted by the OIT Regional Application Service Line Managers in accordance with the form in Appendix C.

3. RESPONSIBILITIES.

a. **Office of Information Technology (OIT) Chief Information Officer (CIO).** The OIT CIO or Designee will:

(1) Maintain partnership with OSHERA.

(2) Review annual compliance reports and ensure Medical Center compliance with this Directive.

b. **Office of Information Technology (OIT) Regional Director.** The OIT Regional Director will review the annual compliance report which must be submitted to the OIT CIO no later than October 31 of each year.

c. **Veterans Integrated Service Network (VISN) Chief Information Officers (CIO) and Facility CIO.** The VISN CIOs and Facility CIOs will establish controls that ensure all OIT staff are aware of the VA Protected National Software packages that are restricted from local modifications by this Directive. These controls must include periodic reviews, not to exceed an annual cycle, of facility-based modifications to determine if any violations have occurred.

.

d. **Office of Information Technology (OIT) Application Service Line Managers (A-SLM).** The OIT A-SLM will:

(1) Work with Facility CIOs to establish and maintain controls to ensure all facility personnel are aware of the restrictions outlined by this Directive. These controls must:

(a) Include periodic reviews of local facility software and local modifications to Non-Protected National Software to determine if any violations have occurred

(b) Address actions to be taken to restore inappropriate modifications to Non-Protected National Software back to the national version.

(c) Establish policies and procedures that ensure the waiver process for local modifications to Non-Protected National Software changes follow this Directive.

(d) Take actions to restore Protected National Software to the nationally released version and prohibit future modifications to those applications.

(e) Identify and work with site subject matter experts/Automated Data Processing Application Coordinator (ADPAC) and/or Clinical Application Coordinator (CAC) to assess current modifications to Non-Protected National Software to determine continued need for enhancements.

(f) Submit waiver requests to SMWC for local enhancements to Non-Protected National Software that the site determines must continue.

(g) Support modification of Non-Protected National Software only when a waiver request has been approved.

(h) Promote local software to OSEHRA for certification and potential VA National adoption when multiple sites desire use of the product, or when the SMWC has requested it as part of the waiver approval.

(2) Restrict programmer access in VistA production accounts to valid OIT staff in accordance with VA Directive 6500, Managing Information Security Risk: VA Information Security Progr.am

(a) Assure annually that proper controls for programmer access are in place; validate continued need for programmer access for those with programmer access to the production account.

(3) Complete the annual certification letter for software certification and submit to the Regional OIT Director no later than October 31 of each year.

e. **Veterans Affairs Medical Centers (VAMC) Subject Matter Experts (ADPAC, CAC, etc).** The VAMC Subject Matter Experts will:

(1) Work with the local IT staff and Application Service Line Managers to assess the deviations made to their respective VistA software package(s).

(2) Provide documentation stating why the deviation is needed.

f. **Software Modification Waiver Committee.** The SMWC will:

(1) Disapprove waiver requests for local modifications to any Protected National Software.

(2) Assess whether waiver requests for local modifications to Non-Protected National Software are already available within the National Product, and provide remediation guidance back to the local facility.

(3) Review and assess each waiver to determine whether the modification to Non-Protected National Software is a local need or a national need.

(4) Approve permanent waivers for Non-Protected software when the need is local and there is no expectation that the solution would be desired on the national level.

(5) Approve temporary waivers for local modifications that are desired on the national level until the enhancements can be adopted as part of the National Software suite. This includes notifying facilities to submit the local enhancement to OSEHRA for certification so that VA may take steps to adopt it nationally.

(6) Disapprove the waiver request if the committee determines that the change is not needed/necessary.

4. REFERENCES.

a. Federal Manager’s Financial Integrity Act of 1982

b. Food, Drug and Cosmetics Act (establishes the FDA's authority over the VistA Software), specifically as referenced under Appendix A.

c. Government Accountability Office (GAO) Policy and Procedures manual for Guidance of Federal Agencies.

d. Office of Management and Budget (OMB) Circular A-123, Internal Control Systems.

e. OMB Internal Control Guidelines.

f. OMB Circular A-127, Financial Management Systems 31 U.S.C. 3512.

g. OMB Circular A-130, Federal Information Security. Management Act (FISMA).

h. The Computer Security Act of 1987.

i. VA Directive 6210, Automated Information Systems (AIS) Security.

j. VA Directive 6214, VA Information Technology Security Certification and Accreditation Program.

k. VA Directive 6500, Managing Information Security Risk: VA Information Security Program

5. DEFINITIONS

a. **Gold Disk.** Standardized version of VistA software certified by OSEHRA and adopted by VA for inclusion into the VistA suite of products.

b. **Local Software.** Products originating from any unrelated PD source including field developers, non-IT VA staff (e.g., physicians), vendors, open source, research, or educational organizations. Local Software products generally have a limited and non-standardized distribution across VA systems and are not automatically covered by Office of Information and Technology (OIT) Tier II and III support commitments.

c. **National Software.** Applications and Commercial Off the Shelf (COTS) product interfaces installed on or interacting with VA computing environments. National Software products have been created by or evaluated and certified by Product Development (PD) and Enterprise Systems Engineering (ESE) to comply with VA established criteria for the following:

(1) Architecture and technology

(2) Capacity and performance

(3) Coding standards

(4) Documentation

(5) Interagency Agreements

(6) Namespacing and interface control agreements

(7) Network capacity impacts

(8) OI Technical Reference Model (TRM)

(9) Privacy and confidentiality

(10) Section 508 accessibility

(11) Security

(12) Testing

National Software products are distributed for use at the enterprise level and PD is responsible for providing or arranging for the provision of customer support (Tier II) and maintenance (Tier III) support.

d. **Non-Protected National Software.** All National software not deemed as Protected in Appendix A of this directive.

e. **Protected National Software.** A subset of National Software as defined in Appendix A of this directive that represents the core of the VistA software. These products are restricted from local modifications of any type.

Protected National Software

1. The Veterans Health Information Systems and Technology Architecture (VistA) systems listed in this attachment are not to be modified in any manner; this is to ensure that patient care and business operations function as intended by the Veterans Health Administration (VHA). The Office of Information Technology (OIT) maintains this list on its VistA database administration web site under the "Protected Systems" title at http://vista.med.va.gov/dba/sensitive-systems.htm and will post updates to the web-based list as needed.

2. The designation of Protected National Software is prohibited from alterations as determined by the following:

a. Software which implements controlled procedures that support and ensure the financial integrity of the Department of Veterans Affairs (VA). For example, the Enhanced Time and Attendance software is used to establish employees' tours of duty and uses that control to manage actual employee time submitted. Any modification to this software, or others designated as protected by this directive, could negate the integrity of VA's payroll system.

b. Software which implements laws and regulations governing health records (and medical devices where such are used) or other laws and regulations affecting VA business operations. As an example, unauthorized modification to Food and Drug Administration (FDA) regulated software is a violation of the Code of Federal Regulations (CFR). At this time, two VistA software packages are subject to FDA oversight: Blood Bank and VistA Imaging. They are not to be modified in any manner outside the oversight of OIT.

c. Software that implements controls that governs and promotes consistency and data quality across VA, especially in critical areas such as workload reporting. As an example, there are standardized processes within VistA for capturing clinic visit information. Any local changes that alter workload reporting algorithms or influence workload reporting would be considered a violation of this Directive.

d. Software which implements controls and processes required to ensure adherence to VA and VHA Enterprise Architectures. For example, the Health Level 7 (HL7) system supports peer-to-peer messaging to ensure reliable data exchange across VHA systems. Since this system implements controls to ensure data

consistency and data quality, it is critical that this product continues to meet the Enterprise Architecture requirements.

e. Software which implements security, confidentiality, or privacy controls. For example, the Kernel system implements security, confidentiality, and privacy controls for VistA, including user authentication algorithms. Any local changes to the system could affect this tool since it provides safe construction of local software.

Protected National Software	
Accounts Receivable	This system implements sensitive VHA financial operations; it cannot be modified, and is subject to requirements of the Fiscal Integrity Act.
Bar Code Medication Administration	This system implements an automated method interfacing wireless point-of-care technology with an integrated bar code scanner to record the administration of patient medications. The product is a critical component necessary to meet requirements for patient safety.
Blood Bank	This system implements controls to manage blood products and implements several patient safety controls. Defined as a Food and Drug Administration (FDA) regulated medical device, it is subject to FDA certification. The entire package (all routines, files, hardware and/or system configurations) must not be altered in any way, as this system implements laws and regulations.
Computerized Patient Record System (CPRS) Order Entry Modules	The Order Entry Modules of CPRS improve the efficiency of processing orders in the patient's electronic record through order checking; order integration with progress notes, results, procedures, diagnosis, and problems; quick orders; order sets and time-delay orders. This module is a critical component necessary to meet requirements for patient safety.
Enhanced Time and Attendance	This system records time and attendance data and cannot be modified; it implements laws and regulations, and is subject to requirements of the Federal Managers Financial Integrity Act.

Protected National Software	
Fee Basis	This system implements sensitive VHA financial operations and cannot be modified; it implements laws and regulations, and is subject to requirements of the Fiscal Integrity Act.
Health Level Seven (HL7)	This system supports peer-to-peer messaging to ensure reliable data exchange across VHA systems. This system implements controls to ensure data consistency and data quality. The product is a critical component to meet requirements of Enterprise Architecture.
Integrated Funds Distribution, Control Point Activity, Accounting and Procurement Package (IFCAP)	This system implements sensitive VHA financial operations and cannot be modified; it implements laws and regulations, and is subject to requirements of the Fiscal Integrity Act.
Integrated Billing	This system implements sensitive VHA financial operations and cannot be modified; it implements laws and regulations, and is subject to requirements of the Fiscal Integrity Act.
Kernel	This system implements security, confidentiality, and privacy controls for VistA, including user authentication algorithms. It provides many tools for the safe construction of local software, and it implements many national control files, to include, but not limited to, New Person, Institution, State, etc. This system is a critical component in meeting the requirements of Enterprise Architecture.

Protected National Software	
Remote Procedure Call (RPC) Broker	This system supports client and/or server messaging used by Computerized Patient Record System (CPRS), Bar Code Medication Administration (BCMA), and others, to access the M database through application programmer interfaces (APIs). It provides a development kit for local development, and it implements security, confidentiality, and privacy controls. This system is a critical component in meeting the requirements of Enterprise Architecture.
VA FileMan	This system implements the VistA database engine and is the basis for several patient safety controls, as well as fiscal integrity controls. It implements security, confidentiality, and privacy controls, and is a critical component in meeting the requirements of Enterprise Architecture.
VistA Data Extraction Framework (VDEF)	This system implements the ability to transmit transaction-driven Health Level 7 (HL7) messages to recipient system. This application is part of the infrastructure software suite of VistA applications which enable an essential set of core functions for all VistA applications.
VistA Imaging	This system implements controls to manage medical images and implements several patient safety controls. Defined as a FDA-regulated medical device, it is subject to FDA certification. The entire package (all routines, files, hardware and/or system configurations) must not be altered in any way, as this system implements laws and regulations.

Protected National Software	
VistALink	This system supports client and/or server messaging used by rehosted HealtheVet-VistA applications by providing a method to access data between VistA and HealtheVet-VistA. This system is a critical component in meeting the requirements of Enterprise Architecture.

Waiver Process

1. While not specifically prohibited from modifying the certified Non-Protected National Software which does not appear in Appendix A, sites must proceed with extreme caution when adding to or modifying any program code or file structures. The interdependencies in this extremely complex system are long-established and constantly changing, and can be elusive and unclear without extensive documentation. It would be extremely easy to introduce errors that could have impacts on data quality and patient safety. While seemingly benign, even alteration of a default prompt from 'yes' to 'no' can have significant impact on user responses and corresponding aggregation of data. Modifications to Non-Protected National Software will require a waiver that will be approved by the SMWC. The SMWC will be comprised of OIT Product Development (PD), OIT Architecture, Strategy & Design (ASD), OIT Systems Design & Engineering (SDE), VHA Program Office, VHA clinical/business operations and Regional Application Service Line Managers. The waiver submission form is located on the Innovation and Development Request Portal (IDRP) at https://epas.r02.med.va.gov/apps/idrp.

a. As part of the Gold Disk installation, sites will be required to use the standardized National Software. Upon release of the Gold Disk and prior to the production implementation mandate, analysis will be conducted by the regional programmers in local test accounts to identify any local modifications to National Software.

b. The regional programmers will engage local subject matter experts (SME) to assess the local modification and determine the need for its continued use.

c. The regional programmers will remove any local modifications that local SMEs determine is no longer in use.

d. For functional enhancements that must continue, the regional application support team and the local SMEs will collaborate to submit a waiver request (found on the IDRP page https://epas.r02.med.va.gov/apps/idrp) to the SMWC.

e. The SMWC will review all waiver requests, taking the following actions:

(1) Utilize established Software Modification Acceptance Criteria (SMAC) to assess waiver requests found at http://vaww.vaco.portal.va.gov/sites/OIT/SMWV/default.aspx.

(2) Disapprove any waiver requests for local modifications to Protected National Software.

(3) Assess local functional modifications to determine if the National Package provides the functionality. In these situations, the SMWC will disapprove the waiver and

inform the local facility of the proper remediation activities to retain the functionality without modifying the National Software.

(4) Assess the waiver to determine if the need is to support local operations, or if the need is desired on a national basis.

(a). Approve permanent waivers for Non-Protected software when the need is local and there is no expectation that the solution would be desired on the national level.

(b). Approve temporary waivers for local modifications that are desired on the national level until the enhancements can be adopted as part of the National Software suite. This includes notifying regional Application Service Line Managers to submit the local enhancement to OSEHRA for certification so that the VA may take steps to adopt it nationally.

(5) Return waiver results to local facilities for action.

f. Application Service Line Managers will take the following action for all waiver decisions:

(1) Disallow application of local modifications to Protected National Software.

(2) Apply local modifications to Non-Protected National Software only when a waiver has been approved.

(3) Promote local software to OSEHRA for certification and potential VA National Adoption when multiple sites desire use of the product, or when the SMWC has requested it as part of the waiver approval.

Waiver requests can be submitted at https://epas.r02.med.va.gov/apps/idrp

Copy/paste onto VA letterhead; modify content based on specific information for your region

SAMPLE CERTIFICATION LETTER

(Date)

Chief Information Officer, 005

810 Vermont Avenue, NW

Washington, DC 20420

Subject: Certification of Waiver Approved Local Modifications to National Software

Region ___ (listed below) have completed the review of all local modifications to National Software distributed at the Department of Veterans Affairs (VA) Medical Centers in our Region.

We certify that no local modifications to Non-Protected National Software compromise the operation of VA.

We certify that all local modifications to Non-Protected National Software have approved waivers.

We certify that there are no local modifications to Protected National Software.

Software changes were made to the following Non-Protected packages:

List the VistA packages changed by each facility, along with the waiver approval date from the SMWC.

_____ (Signature of Regional Director) _____ (Date)

_____ (Signature of Regional ASLM) _____ (Date)