

July 23, 2004

MODIFICATIONS TO VHA CLASS I SOFTWARE

1. PURPOSE: This Veterans Health Administration (VHA) Directive defines policy and procedures related to modifications to specific national Veterans Health Information Systems and Technology Architecture (VistA) software packages which have been designated as software prohibited from unauthorized alteration by VHA. *NOTE: National software, also known as Class I software, is fully supported by VHA's Office of Information (OI).*

2. BACKGROUND: 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. Local or unauthorized changes to VistA can disable or impair critical VHA functions and, in serious cases, result in patient safety incidents.

a. Designation of national software prohibited from unauthorized alteration is determined by the following:

(1) Software which implements controlled procedures that support and ensure the financial integrity of the Department of Veterans Affairs (VA). For example, the Personnel and Accounting Integrated Data (PAID) 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.

(2) Software which implements laws and regulations governing medical 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 OI.

(3) Software which implements controls that govern and promote information 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.

(4) 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.

THIS VHA DIRECTIVE EXPIRES JULY 31, 2009

VHA DIRECTIVE 2004-038

July 23, 2004

(5) 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.

b. VHA software prohibited from unauthorized alteration is subject to reviews that ensure the operational product matches the deployed product. Attachment A provides the initial listing of designated software and guidance for monitoring future changes to the listing.

c. While not specifically prohibited from modifying VistA software which does not appear in Attachment A, sites must proceed with extreme caution when adding to or modifying any VistA 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.

d. The need to balance protection of critical systems with support of local initiative is a difficult challenge. VHA encourages identification of local innovation that has national benefit. Facilities that believe local innovation falls into this category are urged to submit their proposals through the Informatics and Data Management Committee (IDMC) Screening Committee Request Proposal process. These requests need to be endorsed by the appropriate Veterans Integrated Service Network (VISN) Chief Information Officers (CIOs) and are to be reviewed in the context of all other national needs. Requests can be submitted using the Information Technology (IT) Service Requests process at <http://vista.med.va.gov/pas/ITServiceRequest.htm>.

3. POLICY. It is VHA policy that any nationally distributed software package, in part or in whole, may be designated as prohibited from unauthorized alteration outside VHA OI. **NOTE:** *This is to ensure that patient care and business operations function as intended by VHA.*

4. ACTION

a. **Office of Information (OI).** OI is responsible for:

(1) Identifying and notifying field activities of all software applications and functions that cannot be altered in any fashion by non-OI elements. **NOTE:** *The IDMC Screening Committee reviews the list of protected software and approves all designations.*

(2) Maintaining a listing of all identified software modules and functions (see Att. A for the initial list), and for publishing this list on the OI VistA web site.

(3) Reviewing all annual submissions certifying compliance with this Directive from VISN Directors.

(4) Contacting sites to require removal of any changes that OI determines as altering the intent of the national software, inappropriately modifying data, or in any way introducing patient safety issues.

(5) Maintaining certification and accreditation of Legacy VistA software in accordance with VA Directive 6214, to include conduct of Security Relevance Reviews for new releases and patches to existing software.

b. **Facility Directors.** VHA facility Directors who have a VistA system under their control are responsible for ensuring the monitoring, tracking, and documenting of all local changes to nationally-developed VistA to their VISN Director.

(1) **Documentation.** This documentation must include:

- (a) A description of the change.
- (b) Identification of modifications to software routines and databases.
- (c) Reason for change.
- (d) Description of test methodology.
- (e) Certification that changes do not:
 - 1. Alter the intent of the national software,
 - 2. Inappropriately modify data, or
 - 3. In any way introduce patient safety issues.
- (f) Completion of Security Relevance Review documents.

(2) **Exceptions**

(a) Software that is wholly a local development effort (i.e., Class III software that does not modify or replace national software) need not be reported.

(b) Software extensions that follow rules for local additions to national software (as noted in the VHA VistaA Database Administration Handbook) need not be reported. Extensions, or the implementation of additional features, must not impact the named software or functions designated by this directive.

VHA DIRECTIVE 2004-038

July 23, 2004

c. **VISN Director.** Each VISN Director is responsible for:

a. Reporting to OI on an annual basis along with Director-level certification that any changes to the VistA system have been thoroughly tested and do not alter Federal, VA, or VHA policies and procedures.

b. Submitting an annual letter to OI certifying compliance of local changes made to VistA systems under their control (see Att. B). The letter certifying compliance must be received by OI no later than the 31st day of October of each year.

c. **VISN CIOs and Information Resource Management (IRM) Service Chiefs.** VISN CIOs with support from IRM Service Chiefs are responsible for establishing controls that ensure all IRM personnel are aware of VHA software modules and packages restricted from local alterations by this Directive. These controls must:

(1) Include periodic reviews, not to exceed an annual cycle, of facility-based software to determine if any violations have occurred.

(2) Address actions to be taken to restore any inappropriately modified software back to authorized versions.

(3) Establish policies and procedures that ensure all local changes to non-protected VistA components are fully documented and tested and that they do not:

- (a) Alter the intent of the national software,
- (b) Inappropriately modify data, or
- (c) In any way introduce patient safety issues.

(4) Review all facility submissions within VISN control, and prepare an annual reporting letter summarizing local changes to VistA software for signature by the VISN Director.

5. REFERENCES

- a. Office of Management and Budget (OMB) Circular A-123 Internal Control Systems.
- b. OMB Internal Control Guidelines.
- c. OMB Circular A-127, Financial Management Systems.
- d. OMB Circular A-130, Management of Federal Information Resources.
- e. General Accounting Office (GAO) Policy and Procedures manual for Guidance of Federal Agencies.

- f. Federal Manager's Financial Integrity Act of 1982.
- g. The Computer Security Act of 1987.
- h. VA Directive 6210, Automated Information Systems (AIS) Security.
- i. VA Directive 6214, VA Information Technology Security Certification and Accreditation Program.
- j. VHA Directive 6210, Automated Information Systems (AIS) Security.
- k. MP-6, Part 1, Chapter 2.
- l. Food, Drug and Cosmetics Act (establishes the FDA's authority over the VistA software), specifically as referenced under Section 3, Policy.

6. FOLLOW UP RESPONSIBILITY: The Chief Information Office (19) is responsible for the contents of this Directive. Questions may be addressed to 727-319-1121.

7. RESCISSIONS: VHA Directive 10-93-142 is rescinded. This VHA Directive expires July 31, 2009.

S/ Arthur S. Hamerschlag for
Jonathan B. Perlin, MD, PhD, MSHA, FACP
Acting Under Secretary for Health

Attachments

DISTRIBUTION: CO: E-mailed 7/23/2004
FLD: VISN, MA, DO, OC, OCRO, and 200 – E-mailed 7/23/2004

ATTACHMENT A

NATIONALLY SUPPORTED VHA PROTECTED SYSTEMS

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 (OI) maintains this list on its VistA database administration web site under the "Protected Systems" title at <http://vista.med.va.gov/dba/> and will post updates to the web-based list as needed.

- 1. Accounts Receivable.** This system implements sensitive VHA financial operations; it cannot be modified, and is subject to requirements of the Fiscal Integrity Act.
- 2. 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.
- 3. 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.
- 4. 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.
- 5. 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.
- 6. 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.
- 7. 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.

VHA DIRECTIVE 2004-038

July 23, 2004

8. 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.

9. 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.

10. Personnel and Accounting Integrated Data (PAID) Time and Attendance. 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.

11. 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.

12. 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.

13. 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.

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

ATTACHMENT B

SAMPLE CERTIFICATION LETTER

(Date)

Chief Information Officer
VHA Office of Information (19)
810 Vermont Avenue, NW
Washington, DC 20420

Subject: Certification of Local Modifications to Veterans Health Information Systems and
Technology Architecture (VistA) Software

VISN __ (number or name) __ has completed the review of all local changes to the nationally
distributed VistA software at the Department of Veterans Affairs (VA) Medical Centers in our
VISN.

We certify that no local changes compromise the operation of VA.

Software changes were made to the following packages:

(List the VistA packages changed by each facility.)

_____ (Signature of VISN Director) _____

_____ (Date) _____

_____ (Typed Name of VISN Director) _____

VISN __ (Number of VISN) __