

Department of Veterans Affairs  
Veterans Health Administration  
Washington, DC 20420

VHA HANDBOOK 1931.1  
Transmittal Sheet  
June 4, 2001

## INFORMATION RESOURCES MANAGEMENT SERVICE (IRMS)

**1. REASON FOR ISSUE:** This Veterans Health Administration (VHA) Handbook establishes operational guidelines for, and defines responsibilities of, Information Resources Management Service (IRMS), which unifies automated data processing (ADP), telecommunications, networking, office automation, information collection and management, and systems operations.

**2. SUMMARY OF CONTENTS/MAJOR CHANGES:** Significant changes in this policy include:

a. Impacts made by the reorganization of the Office of Information (OI) in support of information technology (IT) at VHA facilities.

b. Reflects the Veterans Integrated Service Network (VISN) structure.

**3. RELATED ISSUES:** VHA Directive 1900 dated January 26, 1999.

**4. RESPONSIBLE OFFICE:** The Office of the Associate Chief Information Officer for Customer Support (193) is responsible for the contents of this Handbook.

**5. DOCUMENT RESCINDED:** M-11, Chapter 17.

**6. RECERTIFICATION:** This document is scheduled for recertification on or before the last day of June 2006.

Thomas L. Garthwaite, M.D.  
Under Secretary for Health

**DISTRIBUTION:** CO: E-mailed 6/6/01  
FLD: VISN, MA, DO, OC, OCRO, and 200 E-mailed 6/6/01



**CONTENTS**

**INFORMATION RESOURCES MANAGEMENT SERVICE (IRMS)**

<b>PARAGRAPH</b>	<b>PAGE</b>
1. Purpose .....	1
2. Authority .....	1
3. Responsibilities .....	2
4. Procedures .....	3



## INFORMATION RESOURCES MANAGEMENT SERVICE (IRMS)

### 1. PURPOSE

This Veterans Health Administration (VHA) Handbook establishes operational guidelines for and defines responsibilities of IRMS, which unifies automated data processing (ADP), telecommunications, networking, office automation, information collection and management, and systems operations.

### 2. AUTHORITY

IRMS will provide the most effective and efficient use of IRM resources to the Department of Veterans Affairs (VA) health care facilities. IRMS functions include, but are not limited to the following areas:

- a. Performs administrative duties and tasks such as personnel management, special reports, fund control point management, planning, purchase of equipment, quality assurance, interaction with other services, support of health care facility committees, and other duties required to maintain the proper functioning of IRMS;
- b. Provides programming support to all Veterans Integrated Service Network (VISN) service/product lines for supplemental reports, local modifications, etc.;
- c. Plans and acquires ADP resources in accordance with policies defined by VISN management and VA and/or VHA mission and goals;
- d. Ensures the integrity and security of systems and databases in conformance with Federal laws and regulations, Office of Management and Budget (OMB) guidance, and VA and/or VHA policies and procedures;
- e. Ensures that Veterans Health Information Systems and Technology Architecture (VistA) services and mandated commercial software packages are made available to users to support VA and/or VHA missions and goals;
- f. Ensures that updated program versions and patches are installed;
- g. Ensures that appropriate backup procedures are accomplished, and that contingency management plans are developed, tested, and maintained;
- h. Provides sufficient security for sensitive data stored in the VistA system both to prevent inappropriate access and to allow ease of access to authorized users;
- i. Supports, to the extent possible within available resources, all VistA software by resolving problems and errors for which patches are not yet developed or available;
- j. Supports facility application coordinators with training on the use of VistA products;
- k. Supports areas outside mandated VistA applications by acquiring the software commercially or by developing non-verified software when hardware and staffing resources are available.

### 3. RESPONSIBILITIES

a. The VHA Chief Information Officer (CIO) has oversight responsibility for VHA Information Technology (IT) operations.

b. The Associate CIO, Customer Support, has responsibility for the provision of technical support to ensure the continuity of IT systems and applications at the health care facility level.

c. The VISN CIO is responsible for managing IRM operations within the VISN. This responsibility includes:

(1) Ensuring the integrity and security of systems and databases within the VISN;

(2) Maintaining required operational records;

(3) Overseeing activities to ensure a constant state of readiness for external reviews and audits pertinent to information management, e.g., Joint Commission on Accreditation of Health Care Organizations, College of American Pathologists, and Food and Drug Administration (FDA);

(4) Providing a secure physical environment for the health care information system, including adequate air conditioning, fire protection, and backup, or emergency, power supplies;

(5) Advising management on the planning, acquisition, implementation, and management of automation and telecommunications resources at the health care facility or VISN; and

(6) Managing IRMS.

d. The Chief, IRM Service, will perform an annual risk analysis assessment and determine the proper backup schedule to meet the needs of the facility.

e. IRMS has the responsibility to:

(1) Perform complete system backups on a weekly basis, at a minimum and, as defined by software package documentation, maintain a journal of critical data;

(2) Ensure that access to the computer room and associated data storage area is strictly controlled;

(3) Permit access to data only in accordance with the existing VHA Automated Information Systems security policy;

(4) Ensure that all end users of the health care information system operate within the established VA Kernel security system;

(5) Conduct database integrity monitoring once per week, at a minimum, and correct any irregularities as soon as operationally possible; and

(6) Perform system capacity monitoring on an ongoing basis. In cases where the Chief, IRM Service, determines that a problem exists with system data storage capacity, the Chief, IRM Service, will follow the procedures outlined in the handbook on purging and archiving.

#### 4. PROCEDURES

##### a. Required Record Keeping

(1) A record of all users with access to the health care information system shall be securely maintained.

(2) A record of all devices connected to the main processing unit of the health care information system shall be maintained. The record must contain sufficient detail to allow the tracing of all cables from the computer room to the devices.

(3) A patch log for each software application program running under VistA shall be maintained. The patch log will contain the code before and after the patches are applied.

(4) Output from the system logs should be maintained for ready reference.

(5) Outdated records containing patient data or other sensitive information shall be disposed of in accordance with local policies on the disposal of sensitive documents.

(6) The software error log shall be printed weekly and stored in the appropriate system logbook. Only the most recent copy need be retained.

(7) A system downtime log that, at a minimum, contains the date, reason for downtime, whether it was scheduled or unscheduled, and the length of time the system was unavailable, shall be maintained. Only one log needs to be maintained for the entire health care information system.

(8) The Site Implementation Tracking system maintained on FORUM (the national electronic mail system) will be updated automatically as application packages/patches are installed into production. Site implementation tracking should be reviewed, at a minimum, on a monthly basis.

##### b. Patch and Version Management

(1) Patches to mandated VistA applications software and to the operating system must be applied in a timely fashion and documented by logging the updates.

(2) Notification of patch release will be made nationally on FORUM. Patches will be distributed electronically by Customer Support.

(3) Patches should be applied and discussed with the appropriate applications package coordinator, if possible, prior to installation.

(a) Patches should be applied in a test environment before introduction into the production account.

(b) Emergency patches must be applied within 24 hours of receipt.

(c) All other VistA patches should be applied to the production system within 30 days of receipt, per the decision of the VHA CIO Council Executive Board. More rapid installation of patches may be required for some mandates. ***NOTE:** When outstanding problems are reported, installation of patches is at the discretion of the Chief, IRM Service.*

(d) Patches to commercially-acquired software will be applied in a timely fashion, as required by the vendor. **NOTE:** *When outstanding problems are reported, installation of patches is at the discretion of the Chief, IRM Service.*

(4) Customer Support will provide support for all nationally released VistA patches.

c. **Required Written Guidelines**

(1) An operations manual outlining disaster recovery plans to ensure continued operation during failure of major system components must be developed and easily accessible to appropriate staff. The disaster recovery plan must be reviewed with facility and VISN personnel as required by the VISN CIO.

(2) Procedures for backup and restoration of production databases must be established and readily available to IRMS personnel.