Rancho Los Amigos National Rehabilitation Center

ADMINISTRATIVE POLICY AND PROCEDURE

SUBJECT: PHI SAFEGUARDS FOR MEDICAL EQUIPMENT

Policy No.: A157
Supersedes: NEW
Revision Date:

PURPOSE

The purpose of this policy is to establish guidelines and security measures for all equipment and or medical device(s) purchased, loaned, donated, or acquired through any form of grant/donation that transmits, retains, or displays Protected Health Information (PHI).

SCOPE

All equipment and medical devices acquired by Rancho Los Amigos National Rehabilitation Center (RLANRC) must be processed through Supply Chain Operations (SCO). Any equipment purchased outside of the standard procurement process such as personal funds, grants, or other funding must be reviewed and approved for acceptance by Information Management Services (IMS) and Bio Medical (Bio Med) department prior to installation.

Equipment and or devices installed without IMS/Bio Med consent cannot be supported by RLANRC, and will be immediately reported to the Department Head or Service Chief, CIO, and CEO. This includes equipment for demos, vendor evaluations, testing, etc.

POLICY

Any medical device and or equipment that transmits, retains, or displays PHI must conform to this policy. Adherence and use of this policy in acquisition and installation at RLANRC will ensure that appropriate technical safeguards are in place to provide for the security (confidentiality, integrity and availability) of PHI and other confidential information residing on facility-used equipment. This policy will also ensure all equipment received at RLANRC complies with administrative, technical, and physical safeguards mandated in accordance with federal patient privacy and security legislation.

Without the approval by Facility Security and Privacy (FSP) Officer – representing the combined review and assessment of IMS, SCO, and Bio Med - the equipment will not be accepted for use on the campus.

IMS in collaboration with SCO and Bio Med will ensure all required documentation and information to meet those safeguards are provided by the responsible parties (facility, vendor) prior to equipment acceptance.

PROCEDURE

A. Equipment Requisition Approval Process

1. In preparation for soliciting or acquiring new equipment, requestors are responsible for ensuring RLANRC Disclosure Statement for Medical Device Security (ATTACHMENT I) form is provided to the vendor/supplier for completion.

2. Once completed by the vendor, the form must be forwarded to the Facility Security and Privacy (FSP) Officer for review and approval. NOTE: Please include the original request (quote, system/equipment description) plus originating department name and contact.

3. If all components of the disclosure form are in compliance, the FSP Officer will sign and authorize the Disclosure for processing and return the form to requestor.

4. If components of the disclosure form are not in compliance, the FSP Officer will determine if the non-compliance issue can be addressed by alternate technology methods. This may require an assessment made by the Facility IMS Operations Manager.

   a. If the component/issue can be made compliant by another method, this is noted on the Disclosure and the form is returned to the requestor as "Approved" with the additional conditions/requirements noted.

   b. If the component/issue CANNOT be made compliant by other methodology, this is noted on the Disclosure and the form is returned to the requestor as "Not~~ed~~ Approved" with the reason noted.

5. The signed Disclosure must be submitted as an attachment through the Online Requisition System (OLR). Requestors must indicate items that retain PHI by selecting PHI within the Special Commodity field.

6. Acquisitions that are not processed through the OLR must still obtain the Disclosure form:

   a. **Fixed Assets or LACCAL.** All fixed asset requests will be required to submit a completed Disclosure attached to the Equipment Request Form (R-73).

   b. **Private Donations.** The Director of Volunteer Services will ensure the Disclosure is completed prior to acceptance of any equipment.

   c. **LAREI**. The Executive Director of Los Amigos Research and Education Institute will ensure the Disclosure is completed prior to acceptance of any equipment.

7. Requisitions submitted without a completed or unauthorized disclosure will be rejected by SCO.

8. Once a purchase order has been processed, SCO will document the information onto the Disclosure statement and forward to Bio Med.

B. Equipment Acceptance

For electrical safety, all equipment must meet Bio Med standards per Policy A419.

1. Upon receipt of equipment, the warehouse contacts Bio Med to ensure prompt inspection and acceptance of all equipment. Bio Med will complete an Equipment Acceptance Checklist (ATTACHMENT II). Any device determined to transmit, retain, or display PHI will require approval from IMS Operations Manager.

2. Upon notification from Bio Med, the Operations Manager will review the Equipment Acceptance Checklist for PHI technical safeguards.

3. Deployment of the equipment will be coordinated by IMS, Bio Med, and/or SCO.

4. User testing is performed as required on the equipment.

5. After user testing has been completed and approved, the Operations Manager will then authorize the final acceptance of the equipment.

C. Equipment Documentation/Record Keeping

As part of Bio Med's internal control procedures, all related documentation will be scanned and recorded into the department's equipment management system (Tamis). This information is maintained by Bio Med indefinitely and is utilized for annual reviews, system upgrades, etc.

REFERENCES:

DHS Policies: 361.23, Safeguards for Protected Health Information (PHI)

Rancho Policies: Admin Policy A300, Computer Security and Protected Health Information Guidelines
Admin Policy A301, Vendor Relations
Admin Policy A419, Electrical Safety Policy

ATTACHMENTS

Attachment I – Disclosure Statement for Medical Device Security
Attachment II – BIO Med checklist

RANCHO LOS AMIGOS NATIONAL REHABILITATION CENTER
INFORMATION MANAGEMENT SERVICES

DISCLOSURE STATEMENT FOR MEDICAL DEVICE SECURITY

Manufacturer	Date	Requisition #/P.O #
Device Description	**Software Version** (If applicable)	**Software Release Date** (If applicable)

Manufacturer or Vendor Contact Information:	Name	Title	Department
	Company Name	Telephone #	e-mail

MANAGEMENT OF ELECTRONIC PROTECTED HEALTH INFORMATION (ePHI) As defined by HIPAA Security Rule, 45 CFR Part 164)	Yes No N/A Note
1. Can this device transmit, retain, or display electronic Protected Health Information (ePHI)? **(If answered No, disregard questions 2-20)**	
2. Types of ePHI data elements that can be maintained by the device:	
a. Demographic (e.g., name, address, location, unique identification number)?	
b. Medical record (e.g., medical record #, account #, test or treatment date, device identification number)?	
c. Diagnostic/therapeutic (e.g., photo/radiograph, test results, or physiologic data with identifying characteristics)?.	
d. Open, unstructured text entered by device user/operator?	
3. Maintaining ePHI: Can the device	
a. Maintain ePHI temporarily in volatile memory (i.e., until cleared on by power-off or reset)?.....	
b. Store ePHI persistently on local media?.....	
c. Import/export ePHI with other systems?	
4. Mechanisms used for the transmitting, importing/exporting of ePHI: Can the device	
a. Display ePHI (e.g., video display)?	
b. Generate hardcopy reports or images containing ePHI?	
c. Retrieve ePHI from or record ePHI to removable media (e.g., disk, DVD, CD-ROM, tape, CF/SD card, memory stick)?	
d. Transmit/receive or import/export ePHI via dedicated cable connection (e.g., IEEE 1073, serial port, USB, FireWire)?	
e. Transmit/receive ePHI via a network connection (e.g., LAN, WAN, VPN, intranet, Internet)?	
f. Transmit/receive ePHI via an integrated wireless connection (e.g., WiFi, Bluetooth, infrared)?.....	
g. Other_____?	

ADMINISTRATIVE SAFEGUARDS	Yes No N/A Note
5. Does manufacturer offer operator and technical support training or documentation on device security features?.....	
6. What underlying operating system(s) (including version number) are used by the device?.....	

PHYSICAL SAFEGUARDS	Yes No N/A Note
7. Are all device components maintaining ePHI (other than removable media) physically secure (i.e., cannot remove without tools)?	
8. Does the device have an integral data backup capability (i.e., backup onto removable media such as tape, disk)?	
9. Can the device boot from uncontrolled or removable media (i.e., a source other than an internal drive or memory component)?	

TECHNICAL SAFEGUARDS	Yes No N/A Note
10. Can software or hardware not authorized by the device manufacturer be installed on the device?.....	
11. Can the device be serviced remotely (i.e., maintenance activities performed by service person via network or remote connection)	
a. Can the device restrict remote access to specific devices or network locations (e.g., specific IP addresses)?	
b. Can the device log provide an audit trail of remote-service activity?	
c. Can security patches or other software be installed remotely?.....	
12. Level of owner/operator service access to device operating system: Can the device owner/operator	
a. Apply device manufacturer-validated security patches?	
b. Install or update antivirus software?	
c. Update virus definitions on manufacturer-installed antivirus software?	
d. Obtain administrative privileges (e.g., access operating system or application via local root or admin account)? ..	
13. Does the device support user/operator specific ID and password?	
14. Are access sessions terminated after a predetermined length of inactivity (e.g., auto logoff)?	
15. Events recorded in device audit log (e.g., user, date/time, action taken): Can the audit log record:	
a. Login and logout by users/operators?	
b. Viewing of ePHI?	
c. Creation, modification or deletion of ePHI?	
d. Import/export or transmittal/receipt of ePHI?	
16. Does the device incorporate an emergency access ("break-glass") feature that logs each instance of use?	
17. Can the device maintain ePHI (e.g., by internal battery) during power service interruptions?	
18. Controls when exchanging ePHI with other devices:	
a. Transmitted only via a physically secure connection (e.g., dedicated cable)?	
b. Encrypted prior to transmission via a network or removable media?	
c. Restricted to a fixed list of network addresses (i.e., host-based access control list)?	
19. Does the device ensure the integrity of the ePHI data with implicit or explicit error detection/correction technology?	
20. Does the software support encryption?.....	
21. If answered "No" to #20, will the software run on a Windows PC, which has been encrypted at the boot level?.....	

RANCHO LOS AMIGOS NATIONAL REHABILITATION CENTER
INFORMATION MANAGEMENT SERVICES

VENDOR DISCLOSURE STATEMENT FOR MEDICAL DEVICE SECURITY
Recommended Security Practices
Explanatory Notes (from questions 1-20): 1. 2. 3. 4. 5. 6. 7. 8. 9. 10. 11. 12. 13. 14. 15. 16. 17. 18. 19. 20.

----------**For Facility Security and Privacy Officer Use Only**----------

This device and/or system(s) referenced in this disclosure have been reviewed for applicable administrative, physical, and technical safeguards per HIPAA regulations.

D APPROVED - Additional conditions/requirements (if applicable) _____

_____

D NOT APPROVED - Reason: _____

_____

_____ _____

Facility Security and Privacy Officer Date

RANCHO LOS AMIGOS NATIONAL REHABILITATION CENTER

EQUIPMENT ACCEPTANCE CHECKLIST

DATE_____ CHECKED BY_____
Bio-Med Technician

ITEM_____ ASSIGNED DEPARTMENT_____

EQUIPMENT LOCATION_____ CONTACT PERSON_____
Building / Room #

MANUFACTURER_____

WEB ADDRESS_____ PHONE NUMBER_____

MODEL_____ SERIAL NUMBER_____

DESCRIPTION_____

CONTROL #_____ PO#_____

ELECTRICAL SAFETY REQUIREMENTS: PASS_____ FAIL_____

TESTING LABORATORY APPROVAL:_____

DOES THE UNIT OPERATE:_____

LITERATURE WITH UNIT (OPERATOR/SERVICE MANUAL):_____

IF YES, HARDCOPY OR DISC:_____

BIO-MED: ACCEPTED:_____ REJECTED:_____ PENDING:_____

CAN THIS DEVICE TRANSMIT OR MAINTAIN **ePHI:**_____
(IF THE DEVICE HANDLES **ePHI**, ACCEPTANCE IS PENDING IMS APPROVAL)

CONTACTED IMS (DATE)_____

DISCLOSURE STATEMENT ON FILE: YES_____ NO_____

ePHI TECHNICAL SAFEGUARDS:

-
-
-

OPERATING SYSTEM(S) INCLUDING SOFTWARE VERSION:_____

_____

COMMENTS: _____
_____
_____

IMS: ACCEPTED _____ REJECTED_____

DATE_____ SIGNATURE:_____
IMS TECHNICIAN