Rancho Los Amigos National Rehabilitation Center
INFORMATION MANAGEMENT SERVICES
POLICY AND PROCEDURE

SUBJECT:	AFFINITY HIS SYSTEM ACCESS - ADMINISTRATION OF USERS AND PASSWORDS	Policy No.:	501
		Supersedes:	1/4/94,7/16/03
		Revision Date:	07/18/11
		Page:	1of3

I. PURPOSE:

Establish accountability and continuity in creating users, maintaining usercodes and passwords, deactivating users in the Affinity Health Information System (HIS) application, and assuring confidentiality of patient information. This policy will control access to the Affinity application.

II. POLICY:

A. Access Request

Controlling and issuing authorization to access Affinity is the responsibility of the Affinity System Manager. Only the System Management staff is to create new users and issue initial usercodes and passwords. User access is created upon receipt of a properly completed System Access Request (SAR) form (Attachment 1) that has been signed by the user and department head or delegate, and indicates training has been or will be provided. The System Management staff is:

System Manager, (562) 401-8471
Assistant to System Manager, (562) 401-7578
Operations Support Supervisor (562) 401-7455

B. Helping Users with Usercode and Password Problems

Usercode problems – the System Management staff can assist users with usercode problems because of the security level required.

Password problems – assistance with password problems is performed by authorized staff only. This includes staff designated as supersuers, Information Management Services (IMS) support staff and System Management staff. If a user does not know who the appropriate staff in their department, they are to contact their supervisor or the IMS Help Desk at x4357.

C. Reactivating Deactivated Users

The System Management staff is to assist users with usercode reactivation because of the security level required. Users can become deactivated due to disuse for 90 days, access security lockout function (when a user fails to gain access to Affinity after a certain number of attempts), or Human Resources Department indicates the user left the facility.

Ill. PROCEDURE- For all Approved Staff (excluding Licensed Medical Practitioners, covered in- section IV):

A. Creating User Access (System Management Staff only)

1. User's department staff generates the System Access Request (SAR) form, which is available on the Rancho Intranet. The form is forwarded to the Help Desk in building 100, room 012. Upon receipt, the Help Desk creates an Information Services Request (ISR), in the Portal system and faxes the SAR to the System Management staff.

2. System Management staff verifies the SAR is completed and signed by the Department Head or the designee (including the Training Certification section) and creates user account in Affinity. The SAR is filed in the Affinity Users binder.

3. System Management staff provides the user with Usercode and Password in a confidential envelope using the Acknowledgement form (refer to Attachment 2). This form includes basic guidelines for maintaining confidentiality of computer information.

   a. Usercodes- Effective January 1, 2004, new users are assigned a Usercode consisting of their first initial, followed by the last name, and if necessary followed by the numbers 1, 2, ,3 etc. to reach a minimum of 6 characters. For example, John Doe is JDoe12. Existing users have the option to keep their original Usercode or have it changed. If they want it changed, they can contact Systems Management staff at x7578 or 8471.

   b. Passwords -At the time of first login, the user must create their own password. Password rules are a minimum of 6 characters or numbers, in any combination. A change password tutorial is included on the back of the Acknowledgement form (Attachment 2). Passwords expire every 90 days. The same password cannot be used a second time.

   Note: Users can become deactivated due to the Access Security Lockout function (when a user fails to gain access to Affinity after a certain number of attempts). If this happens, the System Management staff must be notified to reactivate the user.

B. Helping Users with Password Problems (Approved Users, Help Desk, and System Management Staff)

The "CP- Change Password" procedure is used to re-set a user's password to a new-temporary password, such as Rancho1, Rancho2, etc. If the user has been deactivated, they cannot be seen in CP and the System Management staff must reactivate the user, while also re-setting the password.

C. Deactivating Users (System Management Staff)

The IMS Departmental secretary provides a copy of the monthly Human Resources Department report of County employees who have terminated their positions. These users are to be deactivated from the system within 48 hours of notification. The procedure followed by the System Management staff is as follows:

1. Receive monthly HR Termination Report, indicating employees who have terminated their positions.
2. Deactivate employees, except those who are nursing "other" reason, as they are often promotions.
3. Allow nursing superuser to identify nursing terminated with "other" reason that need to be terminated.
4. Move SAR from the active to the inactive binder.
5. File Termination report in binder for 1 year.

Note: Those departments that have <u>non-County staff</u> are to keep the System Management staff notified when those users no longer work for Rancho.

IV. PROCEDURE -For Appropriate Authorized Licensed Medical Practitioners:

The Licensed Provider Database (LPD) provides a list of licensed staff: physicians, licensed residents, fellows, and staff who are linked to a licensed physician: nurse practitioners, physician assistants, and clinical pharmacists who are determined to be authorized Affinity users. These users receive Affinity access approval by agreement with Medical Administration via the database.

The procedure followed by the System Management staff is as follows:

A. Creating User Access (System Management Staff only)

1. Open LPD database daily and look for the "New System Access Request (SARs) to Print" button, which indicates there are new users to be created.
2. Print the new SARs using the button "Print New SARS"

3. Create user accounts in Affinity, and file SAR in Affinity Users binder.

4. Provide user with Usercode and Password in a confidential envelope using the Acknowledgement form (refer to Attachment 3). This document also includes sample print-screens of the log-in prompt window and basic guidelines for maintaining confidentiality of computer information.

   a. Usercodes - Effective January 1, 2004, new users are assigned a Usercode consisting of their first initial, followed by the last name, and if necessary followed by the numbers 1, 2, ,3 etc. to reach a minimum of 6 characters. For example, John Doe is JDoe12. Existing users have the option to keep their original Usercode or have it changed. If they want it changed, they must contact System Management staff at x7578 or 8471.

   b. Passwords -At the time of first login, the user must create their own password. Password rules are a minimum of 6 characters or numbers, in any combination. A change password tutorial is included on the back of the Acknowledgement form (Attachment 3). Passwords expire every 90 days. The same password cannot be used a second time.

   Note: Users can become deactivated due to the Access Security Lockout function (when a user fails to gain access to Affinity after a certain number of attempts). If this happens, the System Management staff must be notified to reactivate the user.

B. Helping Users with Password Problems (Approved Users, Help Desk, and System Management Staff)

The "CP- Change Password" procedure is used to re-set a user's password to a new-temporary password, such as Rancho1, Rancho2, etc. If the user has been deactivated, they cannot be seen in CP and the System Management staff must reactivate the user, while also re-setting the password.

C. Deactivating Users (System Management Staff)

The LPD also provides a list of users to be removed from the system. The procedure followed by the System Management staff is as follows:

1. Open the LPD daily and look for the "Report of Deleted Providers" button, indicating there are users to be deactivated.
2. Print the report and deactivate the users in Affinity and WebRx (if appropriate) within 48 hours of notification.
3. Move SAR from the active to the inactive binder.

Attachment 1

RANCHO LOS AMIGOS

NATIONAL REHABILITATION CENTER

System Access Request

USER INFORMATION

Name (Last, First, MI)	Phone / Extension
Department / Unit	Employee Number
Work Location Building / Room	Job Title

NETWORK ACCESS [ ] Add [ ] Delete

E-MAIL ACCOUNT [ ] Add [ ] Delete

AFFINITY ACCESS [ ] Add [ ] Delete [ ] Change User Group (Menu)

User Group Name : ______________________________ (Or Same-As Person): ___________________

User's Primary Location: _________________________

QUANTIM/EDM ACCESS [ ] Add [ ] Delete [ ] Change Groups

User Groups (List) : _______________________________ (Or Same-As Person): _________________

Q/EDM E-Signature Required: Yes ___ No ___ (Authorized Medical Staff only)

RTIS.NET ACCESS [ ] Add [ ] Delete [ ] Change User Department

User Department: User Rights:

SYNAPSE ACCESS [ ] Add [ ] Delete

Residents/Fellows/Registry staff, please indicated expected Service End date: ____/____/________.

MPI SmartMerge / SmartID [ ] Add [ ] Delete User Role: ____________________

WEBRX [ ] Add [ ] Delete

OTHER (Specify) ___________________ [ ] Add [ ] Delete

PADI View [ ] Add [ ] Delete

(For TSO, please attach the ISD Registration for Downey Data Center)

SIGNATURES and Certifications

I, the undersigned, hereby certify that I have signed the eSignature Attestation Form (Admin Policy A433) and am compliant with provisions of the DHS Acceptable Use of Information and IT Resources policy (DHS 935.20). User Signature Date	Print Supervisor/Dept Head's Name: Phone#: Supervisor/ Dept Head Signature Date
Trainer Signature Date	This certifies the above user was (will be) trained on __________ for the Affinity Applications User Group/Menu requested above.

THIS SECTION TO COMPLETED BY IMS STAFF

Affinity/WebRX Security Officer	QEDM Security Officer	Network/E-Mail Security Officer	RTIS or ORSOS Security Officer
Date Received: ___________	Date Received: ___________	Date Received: ___________	Date Received: ___________
Date Processed: ___________	Date Processed:___________	Date Processed: ___________	Date Processed: ___________
Completed By: ___________	Completed By:___________	Completed By: ___________	Completed By:___________

NOTES