

Supersedes: June 1, 2007

Effective: December 9, 2009

POLICY

Fairfield Medical Center computer access User ID, passwords and security codes will be issued for ALL Center employees, medical residents, graduate medical students and members of the Medical Staff and their employees after a security agreement is signed.

PURPOSE

The objective of this policy is to delineate guidelines for computer access so as to maintain security of data, protection of files and consistency of information regarding use of the system. This policy applies to all employees of the Center or its affiliates who have or are responsible for a computer account or any form of access that supports or requires a password on any system that resides at any Center facility, has access to the Center network or stores any non-public Center information.

PROCEDURE

I. ESTABLISHING USER ACCOUNTS

A. Fairfield Medical Center Staff – New Employee

1. All employees are required to electronically acknowledge the *Systems Access Security Agreement* form (see Attachment A) within Active Staffer in the orientation process.
2. Assignment of systems to be accessed by the user will be determined by the user's manager. A log of these preferences, organized by unit and position, will be kept in the Learning and Development Department and updated yearly.
3. Selection of the approved systems will be documented on the *New Employee Network Security Request Form* (see Attachment B) for each new user by the Learning and Development staff based on information from the log.
4. Learning and Development staff will forward complete forms to the Systems Department.
5. The *Systems Access Security Agreement* form will be electronically stored in Active Staffer until the employee resigns or is terminated.

B. Fairfield Medical Center Staff: Established Employee

1. Employees requiring additional or changed security access will need to apply for these privileges by having their manager place a request with the Help Desk. The Help Desk will create a ticket and forward it to the appropriate Systems administrator.
2. Systems staff will ensure the *Systems Access Security Agreement* form has previously been completed and is on file, or will have the user accept the Systems agreement form on Active Staffer. Systems staff will ensure that the access requested is appropriate.
3. The *Systems Access Security Agreement* form will be electronically stored in Active Staffer where it will be kept until the employee resigns or is terminated.

C. Physicians, Licensed Individual Practitioners (LIP) and Medical Students

1. The Medical Staff Office completes the *Request to Add New Physician* form (see Attachment C) and e-mails it to the Systems Programmer for physicians and LIP's.
2. After all requested computer accounts have been established, the Physician Clinical Analyst will share the usernames and passwords with the physician during their orientation and obtain their signature on the *Systems Access Security Agreement* form.
3. Medical Students and Residents will complete their orientation with the program coordinator. The *Systems Access Security Agreement* form will be completed at this time in paper format and electronically scanned to the Physician Clinical Analyst for account creation. Accounts will be established per the physician protocol. Usernames, passwords and computer training will be shared with the medical student or resident by the Physician Clinical Analyst following account creation.

Supersedes: June 1, 2007

Effective: December 10, 2009

4. The completed *Systems Access Security Agreement* form will be forwarded to the electronically shared folder where it will be kept until the practitioner is no longer affiliated with FMC.

D. Physician Office Staff and Other Entities Requesting Portal Access

1. Entities such as extended care facilities, home health care agencies, and medical offices using FMC for patient results and information necessary to care for their patients must obtain and complete or have on file a Business Agreement form prior to receiving systems access.
2. The request for access to the Center's portal is generated through a call to the Help Desk or through the Systems Physician Clinical Analyst who will create the Help Desk ticket.
3. The requesting office or facility will be sent a *Systems Access Security Agreement* form by the Help Desk, Portal Administrator or Physician Clinical Analyst upon receiving the request or Help Desk ticket. The completed form can be returned via fax, interoffice mail, or postal mail to the Systems department.
4. The Physician Clinical Analyst will telephone or visit the user to release their username and password and provide education as applicable to the individual's needs.

II. MANAGING USER ACCOUNTS

- A. Portal accounts not used in 90 days shall be disabled. The account may be reestablished by following the Established Employee protocol above.
- B. Physicians and LIP's will update their *Systems Access Security Agreement* form every three years upon their reapplication of privileges with the Center. This form will be included in their application packet.
- C. Employees will update their *Systems Access Security Agreement* form yearly by January 31 through Active Staffer. Failure to complete required annual systems access security agreement by January 31 will result in:
 1. A notice of delinquency will be sent to the employee and his/her manager, noting failure to complete required agreement by the deadline and giving notice of a grace period of 14 days in which to complete the required agreement. Employee will also receive an unacceptable rating on his/her next performance appraisal.
 2. If not completed by February 15, a second notice of delinquency will be sent to the employee, his/her manager and Human Resources. The notice will outline that the employee has failed to complete the required agreement for the year and is to be removed from the schedule immediately until completion of the required agreement. This will count as an attendance occurrence under FMC's Attendance Policy. The manager will notify the employee of his/her removal from the schedule.
 3. Once completed, the employee may return to work. The manager will notify Human Resources that the employee has returned to work.
 4. If the employee has not completed the required agreement by February 28, the employee will be removed from active status.
 5. An employee returning from LOA during December or January will have 30 days from his/her return to work date to complete the required agreement. The process listed above will be invoked should the employee not complete the required education within the 30-day period.
- D. All physician office staff and other outside agency staff will update a paper version of the *Systems Access Security Agreement* form yearly by January 31. Failure to meet this deadline will result in deactivation of their personal portal account.

ATTACHMENT A

FAIRFIELD MEDICAL CENTER
SYSTEMS ACCESS SECURITY AGREEMENT

, have read, understand, and will comply with the following:

(Last name, First name, Middle initial)

- ____ I am the only person authorized to use my password(s) and user ID(s).
- ____ I will not disclose my password(s) or user ID(s) to anyone.
- ____ I will not attempt to learn another person's password(s)/user ID(s).
- ____ I will not attempt to access information by using a password(s) or user ID(s) other than my own.
- ____ I will retrieve or attempt to retrieve from the computer system only medical data that is directly related to the treatment of patients with whom I have a clinical relationship or those patients for whom I have been asked to provide a consultation or for approved educational or research purposes. I agree to maintain the confidentiality of all such patient data. I will access patient data only as required by my employment or medical staff responsibilities or for approved educational or research purposes.
- ____ It is my responsibility to log out of the system. I will not, under any circumstances, leave a computer terminal to which I have logged in unattended.
- ____ If I have reason to believe that the confidentiality of any of my password(s)/user ID(s) has been compromised, I will contact the Systems Department immediately so that my password(s)/user ID(s) can be deleted and a new password(s)/user ID(s) assigned to me.
- ____ I will immediately report any known or suspected breach of the confidentiality of the system or records/data obtained from it to the Medical Information Services manager.
- ____ I understand that my password(s)/user ID(s) will be deleted from the system when I am no longer employed or have privileges at this institution or when my job duties do not require access to the medical record database. I will immediately report any such status change to the Systems Department.
- ____ I understand my access will be automatically deactivated after 90 days of non-use.
- ____ I understand that medical records confidentiality is required by law, and that there are statutes specifically mandating the confidentiality of, among other areas, mental health, HIV, and drug and alcohol-related treatment records.
- ____ I understand that any fraudulent application, violation of confidentiality or any violation of the above provisions may result in disciplinary action from termination of access to the system or appropriate medical staff or University disciplinary measures up to and including termination of my employment with the University or the hospital.
- ____ I understand that the Systems department maintains an audit trail of accesses to patient information that records the user, date, and patient identification of all accesses to electronic medical records.
- ____ I understand that my access rights are subject to periodic review, revision and annual renewal.
- ____ I understand that if I do not accept these restrictions of access I may be denied access or have access terminated to relevant computer systems and networks.

Applicant Printed Name: _____

Office/Department/Unit: _____

Title/Position: _____

For Students: Start Date _____ End Date _____

Physician Preceptor:

E-Mail Address: _____

Telephone Number: _____

Signature

Date

Supervisor of Person Approving Issuance of this Account:

Name: _____

Telephone Number: _____

Title/Position: _____

Signature

Date

ATTACHMENT B

FAIRFIELD MEDICAL CENTER

**NEW EMPLOYEE
NETWORK SECURITY REQUEST FORM**

Department:

Dept. Code:

Date:

Manager/Supervisor (please print):

Ext:

User's Legal Name (please print):

First:

Middle Initial:

Last:

Credentials:

Position:

Employee #:

Security Access required for the following Applications (Manager/Supervisor should check all that apply):

- Network Login
- Portal
- PaceArt
- E-mail
- Network folder needed
- PMM/PFM
- Compliance Checker
- Encompass, MUSE
- Other: Wellness Connection, Synapse, Provation, HSM, PHS

Operations (AS400)

- AS400

- Horizon Expert Documentation (HED)
- ED Tracking Board
- Lab System

- API/Report Express
- Active Staffer

Help Desk

Username: _____ Password: _____

(You will be prompted to set your own password the first time you log in.)

Email Address: _____@fmchealth.org

Network Path: _____

Username: _____ Password: _____

Username: _____ Password: _____

Username: _____ Password: _____

Username: _____ Password: _____

Username: _____ Password: _____

Security Code: _____

Clinical Documentation

Username: _____ Password: _____

Username: _____ Password: _____

Lab

Username: _____ Password: _____

Accounting/Systems

Username: _____ Password: _____

ATTACHMENT C

Fairfield Medical Center Request to Add New Physician

Date Requested	
Physician Number	
Name (Last, First, Middle Initial)	
Physician Type (MD, DO, PA, etc)	
Office Address	
City, State, Zip	
Telephone Number (Including Area Code)	
Fax Number (Including Area Code)	
Date of Birth	
Date on Staff	
Status Code	
Medical Service Code	
Specialty Code	
State License Number	
Federal DEA Number	
Medicaid Provider Number	
Medicare Provider Number	
UPIN Number	
NPI Number	

Comments:

Physician Privileges:

✓	
	Admitting
	Discharge
	Ordering

Systems Requested:

✓	Request For:
	AS 400
	AD/PACS
	Portal

Orientation Date/Time: _____

Termination Date: _____

Date of Last Log In: _____