University of South Florida Physicians Group
3500 E. Fletcher Ave. Suite 400
Tampa, Fl. 33613

Name: _____

Position: _____

Supervisor: _____

Department/Company Name: _____

SECURITY POLICY

By the nature of the activities conducted in your position, you have access to information constituting privileged matter which is to be treated in a strictly confidential manner. The security of the computer systems is to be protected and maintained by the above noted individual.

1. The individual provided access to any area of the computer systems will select a personal password. This is to be a unique, confidential password. It is not to be initials or any other name or word easily associated with the individual.

2. The individual is responsible for the confidentiality of their password. The system will audit the activity of all users and any breach of policies or unauthorized access. NO passwords shall be programmed into a function key for sign-on.

3. No individual will share their password or sign-on to the system to allow access in any area to another individual for any reason. Any problem in achieving appropriate access will be resolved by the individual's supervisor or department head with the Director of Information Services.

4. No terminal or PC is to be left unattended without being logged off the system.

5. Any change in responsibility which alters the individuals required function and activity access will be reported through the individual's supervisor, department head, or project manager to the Director of Information Services, and subsequent changes will be made to the individual's security.

6. No individual shall use, alter, damage, take or destroy any data, database, computer program, computer system, computer network, and computer software or computer equipment without proper authorization. No individual will gain access or attempt to gain access to any computer, computer system or computer network without authorization.

7. No individual shall load non-approved or non-supported software on any system. A listing of approved and supported software may be obtained from the Department of Information Services.

8. No individual shall password-protect any files they have created or modified.

9. Any breach of the Information Services Security Policy shall constitute misconduct, subject to disciplinary action up to and including termination of the individual or contract with the individual and their organization.

I have read and I understand the above Information Services Security Policy, and I agree to adhere to the Policy as a condition of my employment with USF Physicians Group.

_____ _____

Employee Signature Date

PCIS Security Access Request Form

USF Health Information Systems

EMPLOYEE INFORMATION	
Last, First Name	Job/Title
Dept/Division	Location
Phone #	Employee Start Date
USF Health Network (HSCnet) Username	USF Health (HSCnet) Email Address
List Credentials- If there are no credentials please enter N/A	

TYPE OF REQUEST (If requesting a Reactivate, Deactivate or Modification please enter PCIS Username.)

Select Type of Access Request	PCIS User ID
Transferred to Department	
Legal Name Change to	

ROLES (Please select the role based on employee's job responsibilities)

Clinical Operations

- ☐ ARNP
- ☐ Clinical Care Specialist
- ☐ Fellow
- ☐ Medical Student
- ☐ Nurse (Supervisor)
- ☐ Physicians Assistant
- ☐ Physician

License #	UPIN #	DEA#	NPI#

- ☐ Resident
- ☐ Lab Staff
- ☐ Ancillary Staff
- ☐ BRIDGE

Revenue Cycle Operations

- ☐ Coder
- ☐ Coding Auditor
- ☐ Dept. Liaison Services
- ☐ Front Desk
- ☐ Front Desk Lead/Supervisor
- ☐ Financial Specialist
- ☐ RCO Staff (IRU, FRU, Pt. Services, Collectors)
- ☐ RCO Management (Manager, Supervisor, Asst. Director, Director)
- ☐ Payment Poster
- ☐ Registration Staff
- ☐ Registration Supervisor
- ☐ System Support Staff

Other (Justification required before access can be granted)

- ☐ Enter justification below

Administrative

- ☐ Auditing (F&A, Compliance)
- ☐ Department Administrator
- ☐ Department Administrative Asst./Secretary
- ☐ Early Steps Case Coordinator
- ☐ Reports – AES
- ☐ Reports – BAR
- ☐ Transcriptionist
- ☐ Professional Integrity Office
- ☐ External Contractor (May Require Prior Approval, please explain below)

Scheduling

- ☐ Scheduler
- ☐ Scheduling Manager
- ☐ Call Center
- ☐ Call Center Manager
- ☐ Schedule View

Medical Records

- ☐ Medical Records Staff
- ☐ Medical Records Management

Visiting Start Date Start Date: End Date End Date:

- ☐ Visiting Medical Student
- ☐ Visiting Resident/ Fellow

Research

- ☐ Clinical Research Coordinator
- ☐ Data Manager
- ☐ Nurse Coordinator
- ☐ Research Assistant
- ☐ Research Support Specialist
- ☐ Student Research/Assistant

Researchers requesting PCIS access must also provide the following (check if attached):

- ☐ *Copy of HEALS Report*
- ☐ *Human Subjects Protection Training*
- ☐ *IRB Letter*

PCIS Access Authorized By (REQUIRED)	
Last, First Name	Phone #
USF Health (HSCnet) Email	Title
Signature *	Date

*An authorized signature is required to process this form. Unsigned forms will result in access being delayed.

Once you have completed form, click icon below to print, sign and fax to (813) 396-9619.