SECTION SEVEN: INSTITUTIONAL POLICIES RELATIVE TO GME PROGRAMS

POLICY NO: 7. 5
SUBJECT: CONFIDENTIALITY OF INFORMATION

POLICY

It is the policy of Saint Peter's University Hospital (SPUH) that all medical and/or personal information about any patient treated at this hospital and/or related off-site facilities be held in the strictest confidence by all employees and staff members. Failure to comply with this policy will result in disciplinary action up to and including termination.

PURPOSE

To ensure that the privacy and confidentiality of information about patients treated at Saint Peter's University Hospital is maintained by all personnel to comply with the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

RESPONSIBILITIES

Hospital Personnel shall:

- Be aware of and comply with the responsibilities of this policy and all SPUH policies relating to the HIPAA privacy and security standards.

- Treat all information received in the course of employment at SPUH, which relates to patients of the hospital as confidential and privileged information. Employees may exchange medical and/or personal information about patients only as it relates to the performance of their job duties.

- Refrain from discussing patients in public areas such as the Cafeteria, Coffee Shop, corridors, elevators, lounges, etc., or in any area of the hospital where a conversation may be overheard.

- Access patient information only if the employee has a need to know this information in order to perform job duties.

- Not disclose information regarding SPUH patients to any person or entity, other than as necessary to perform job duties and as permitted under SPUH policies, and then that which is minimally necessary for a specific disclosure.

- Not log on to any of the SPUH computer systems that currently exist or may exist in the future using a password and/or security code other than the employee's own passwords/security codes.

- Safeguard individually assigned computer passwords and/or security codes and not post passwords and/or security codes in a public place (such as on a computer monitor) or in a place where it will be easily lost or obtained such as on the employee's identification badge.

- Understand that computer passwords and/or security codes constitute the employees "signature" and the employee will be responsible for all entries made under that employee's particular access code(s).

- Not allow anyone, including other employees, to use individually assigned passwords and/or security code(s) to log on to the computer. Employees will log off the computer as soon as they are finished using it.

- Not take patient information from the premises of SPUH in paper or electronic form without receiving appropriate administrative permission.

- Refer all inquiries from the media regarding any patient to the Department of Community and Media Relations.

- Sign a new "Employee Confidentiality and Security Agreement" (attached) annually. This signed agreement shall be filed in the employee's file.

- Attend in-service on confidentiality once per year.

- Upon cessation of employment with SPUH, employees agree to maintain the confidentiality of any confidential information learned while an employee. Employees agree to turn over any keys, access cards, nametags, or any other device that would provide access to Saint Peter's University Hospital or its information.

Reviewed:7/2007