NewYork-Presbyterian Confidentiality, Privacy and Information Security Agreement

The processing of employee and patient information is a key function of NewYork-Presbyterian ("NYP"). In order to ensure the confidentiality of this information, each employee, student or trainee, affiliate, contractor, vendor or volunteer must read, sign and be governed by the following statements:

- Employee and patient records contain confidential information including but not limited to salaries, disciplinary actions, patient health information and patient financial information; they are privileged business documents belonging to NYP. Records include paper, printed and electronic files and documents.
- Privileged information encountered through routine review functions, such as those performed by NYP personnel must not be compromised or divulged. Discussion, access and/or reading of employee or patient records for non-job related reasons are prohibited. Under no circumstances should employee or patient information be discussed casually, socially, or in public areas.
- Requests for employee information should be directed to Human Resources. Requests for patient information should be directed to Health Information Management (Medical Records).
- All personnel are warned to be alert to any attempts by unauthorized persons to obtain employee or patient information though unscrupulous, devious or illegal means that are in violation of established policies of NYP. This information is valuable and confidential; and is protected by law and by strict NYP policies.
- Proprietary information such as financial and statistical records, purchasing and internal reports must also be kept confidential and only disseminated on a need to know basis.

Specific to patient privacy and safeguarding protected health information ("PHI"), you hereby attest to comply with the standards and expectations outlined below; and to appropriately use, disclose and safeguard PHI and the systems that maintain it.

Patient Privacy:

- Adhere to privacy laws and regulations, and applicable NYP policies and procedures
- Handle and maintain patient information in a confidential and secure manner
- Safeguard PHI, in any format (verbal, paper, electronic), and the systems you have access to
- Only use or disclose PHI as permissible by law
- Only access, use or disclose PHI as required to fulfill job duties and only for legitimate business purposes
- Only access, use or disclose the "*minimum necessary*" PHI to satisfy the intended purpose
- Avoid discussing PHI in public areas (elevators, cafeteria, public hallways/waiting areas, etc.)
- Obtain patient's permission prior to disclosing PHI in front of family or friends
- Seek guidance when uncertain about appropriate use or disclosure of PHI
- Avoid printing PHI, whenever possible, and appropriately secure when required for retention
- Shred or appropriately destroy all printed documentation and other media that contains PHI as required
- Avoid removing PHI from the facility (paper, on laptop, flash drive, etc.)
- Do not take pictures or videos of patients for personal use, or with a personal device
- Do not discuss patient information in social settings, with my family or friends; or post any patient information on social media
- Abide by special privacy protection provisions regarding "Sensitive Health Information" (Mental Health, Substance Abuse, HIV/Aids, Reproductive Health, Genetic information)

Information Security:

- Adhere to Information Security laws and regulations and applicable NYP policies and procedures
- Access systems containing employee and patient health information only as needed to perform your duties as defined by your relationship (faculty, employment, student, contract, etc.) with NYP.
    - You must not access employee or patient health information for which you have no legitimate business need

  - You must not use, disclose, copy, release, alter, revise, or destroy any employee or patient health information except as properly authorized within the scope of your relationship with NYP.
- Safeguard and protect your individual credentials (user ID and password) or any other user credentials that allow for access to employee or patient health information. You will be responsible for all activities undertaken using your credentials and other authorizations. o You must secure (lock or sign out) your system when not occupied; o You must sign off of computer systems after use;
  - You must not share or allow anyone access to systems containing employee or patient health information under your individual account; and
  - You must not use another user's individual account to access any systems
- Abide by NYP policies and procedures regarding use of any devices that may contain any employee and patient health information including the use of encryption or other equivalent method of protection when required.
- Upon termination of your relationship with NYP, you will return all institutional information and devices or dispose of them in accordance with hospital policies regarding the disposal of electronic equipment.
- Communication using the NYP network and systems is not private, and the institution may monitor the content of your communication to protect the confidentiality and security of NYP data.
- You have no right or ownership interest of any employee or patient health information. NYP may at any time revoke your employee account, other authorization, or access to employee and patient health information. At all times during your relationship with NYP, you will act in the best interests of NYP.
- You will be responsible for any misuse or wrongful disclosure of employee and patient health information and for any failure to safeguard your account credentials should they be used to access employee and patient health information.

Reporting Obligations:

You have an affirmative responsibility to report issues or concerns regarding employee and/or patient health information immediately to the Office of Corporate Compliance at (212) 746-1644. As such, you agree to:

- Report any suspicion or knowledge of unauthorized access to systems
- Report any misuse or disclosure of employee or patient health information
- Report, in accordance with NYP policies, activities by any individual that you suspect may compromise the confidentiality of employee or patient health information.

NYP prohibits retaliation in any form for good faith reporting of suspect activities and will maintain reported incidents in confidence to the extent permitted by law.

By signing this document, you agree to the requirements set forth within and understand that compliance with these provisions is a condition of your employment. In addition, you attest to understanding that failure to comply may result in disciplinary action up to and including loss of privileges and termination.