



**UNIVERSITY
PHYSICIANS**
BROOKLYN, INC.

STAFF CONFIDENTIALITY OF PROTECTED HEALTH INFORMATION

This statement should be signed by all UPB employees, physicians, volunteers, students, trainees, residents, interns, temporary personnel, consultants and contractors.

University Physicians of Brooklyn, Inc. is committed to protecting the privacy and confidentiality of health information about its patients. Protected health information is strictly confidential and should never be given, nor confirmed, to anyone who is not authorized under our policies or applicable law to receive this information.

Definitions:

Protected Health Information (PHI)- Any patient information, including very basic information such as their name or address, that (1) relates to the past, present or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present or future payment for the provision of health care to an individual, and (2) either identifies the individual or could reasonably be used to identify the individual.

Our policies apply to protected health information in any form, including spoken, written or electronic form. It is the responsibility of every practice staff member and medical staff member to protect the privacy and preserve the confidentiality of all protected health information. This includes, but is not limited to, compliance with the protective procedures below.

1. Public Viewing/Hearing

All UPB staff members are expected to keep protected health information out of public viewing and hearing. Protected health information should not be left in conference rooms, out on desks or on counters or other areas where the information may be accessible to the public or to other employees who do not have a need to know the protected health information. UPB staff members must also refrain from discussing protected health information in public areas, unless doing so is necessary to provide treatment to one or more patients. UPB staff members must review the patient's record for documented patient restrictions or objections before sharing information with friends and family of the patient.

2. Databases and Workstations

UPB staff members are expected to ensure that they exit any confidential database upon leaving their workstations so that protected health information is not left on a computer screen where it may be viewed by individuals who are not authorized to see the information. UPB staff members are also expected not to disclose or release to other persons any item or process which is used to verify their authority to access or amend protected health information, including but not limited to, any passwords, personal identification numbers, access cards or electronic signature. Staff members will be held liable for all activities occurring under his/ her account. These activities may be monitored.

3. Downloading, Copying or Removing

UPB staff members should not download, copy or remove from UPB any protected health information, except as necessary to perform their duties. Upon termination of employment or contract with UPB, or upon termination of authorization to access protected health information, staff members must return any and all copies of protected health information in their possession or under their control. In addition, staff members must ensure that all protected health information is disposed of in an appropriate manner. Health information in old PC's that are being removed must be deleted.

4. Emailing and Faxing Information

UPB staff members should not transmit protected health information over the Internet (including email) and other unsecured networks unless using a secure encryption procedure. Appropriate policies must be followed when faxing patient information, including using a cover sheet containing a confidentiality notice, ensuring that the fax machine is located in a secure location and verifying receipt with the intended recipient, when appropriate.

5. Curiosity or Concern

UPB staff members may not access, review or discuss information for purposes other than their stated duties. Staff members may not look up birth-dates, addresses of friends or relatives or review the record of a public personality.

6. Personal Gain or Malice

UPB staff members may not access, review or discuss patient information for personal gain or for malicious intent.

7. Policies & Procedures

UPB staff members must adhere to all of UPB's HIPAA privacy policies and procedures. The appropriate manager should be consulted if a staff member is unsure how to proceed in a specific circumstance.

VIOLATIONS

UPB staff members who violate this policy will be subject to disciplinary action, up to and including termination of employment. Staff members who have reason to believe that another person has violated UPB's policies should report the matter promptly to his/her manager. All reported matters will be investigated, and, where appropriate, steps will be taken to remedy the situation. UPB will make every effort to handle the reported matter confidentially. Any attempt to retaliate against a person for reporting a violation of UPB's policies may result in disciplinary action.

I agree to abide by the above statements and adhere to all of University Physicians of Brooklyn, Inc.'s HIPAA policies and procedures.

Print Name of Staff Member

Signature of Staff Member

Date