POLICY ON THE ACCESS, MAINTENANCE AND HANDLING OF CONFIDENTIAL DATA AND INFORMATION

I. Purpose

The purpose of this Policy is to identify information that is considered confidential and to establish the principles and guidelines on the access, maintenance and handling of such confidential information.

II. Scope

This Policy applies to all faculty, employees, administrators, schools, departments, divisions, units, institutes and centers of New York Medical College.

III. Definitions

Confidential information is defined as non-directory information pertaining to faculty, employees, students, alumni and all other sensitive and proprietary information of New York Medical College. Such confidential information includes without limitation the following:

- personnel records, payroll records and information regarding an employee's salary, length of service, performance or other personnel information;
- faculty appointment, promotion, termination and data records;
- personally identifiable information such as social security numbers, professional license numbers, names of spouses, children, parents, guardians, beneficiaries, marital status, physical description, education, financial matters, medical or employment history and other non public personal information pertaining to individual faculty, employees, students, alumni, donors, etc;
- student educational and financial records;
- research results not yet published, including manuscripts and correspondence;
- data concerning research subjects;
- medical information and information designated as "Protected Health Information" under the Health Insurance Portability and Accountability Act ("HIPAA");
- budgetary, business, financial, departmental, internal reports, memoranda, correspondence, contracts, strategic or planning reports and information, surveys, internal audit reports, etc;
- Information about or provided by third parties (e.g., information covered by non-disclosure agreements, contracts, business plans, non-public financial data, computer programs, etc;
- computer system passwords and security codes;
- donor and alumni information; and,

- litigation or other formal charges or complaints records and documents pending or in the process of investigation.

Such confidential information can be in any form including on printed media (e.g., forms, reports, memoranda, correspondence, microfilm, microfiche, books), computers, networks, magnetic or optical storage media (e.g., hard drive, zip drive, flash drive, memory card, diskette, tape, CD, DVD), physical storage environments (e.g., offices, filing cabinets, drawers), or in a person's memory.

Directory information regarding faculty and employees is defined as non confidential information which may be generally disclosed such as the name, faculty or job title, office address, office telephone number and College e-mail address.

Directory information regarding students and alumni is governed by the *Family Educational Rights and Privacy Act* ("FERPA") and by the regulations promulgated thereunder. Generally, this law permits the disclosure of directory information to third parties without a student's consent, unless otherwise requested, in writing, by the student involved, which information is defined by the College as including the student's name, address, telephone number, e-mail address, pager number, major field or program of study, name of the school enrolled in, dates of attendance, expected year of graduation and other similar information. All other student information cannot be disclosed to any other party without the prior written consent of the student. Specific questions concerning what information about a student may be obtained or disclosed must be directed to the Office of the Registrar.

Additional References:

Human Resources Policy 202, *Access to Employee's Personnel File*
Human Resources Policy 204, *Personal Data Changes*
Human Resources Policy 214, *Records Retention*
Information Services Policy 101, *Computer Usage, Authorized Access and Data Integrity*
Information Services Policy 102, *Network Access Rights and Network Security Implementation*
Information Services Policy 103, *Disaster Recovery-Networked and Local Information Backup*
Record Retention Policy

IV. Policy

It is the policy of New York Medical College that all confidential data and information as defined by this Policy shall be used, maintained, and handled by faculty and employees in a manner which protects the integrity of the data and information and the privacy of those associated with it and that confidential, sensitive and proprietary information shall be protected from unauthorized access and disclosure by faculty and employees consistent with the principles and requirements as specified by this Policy and as required by applicable law.

V. Responsibilities

1. General Principles

- All confidential information gathered and maintained by faculty and employees in the course of their duties and responsibilities for New York Medical College is considered institutional information and, as such, must be used, maintained and handled by faculty and employees as specified by and consistent with the authorization and in a manner that appropriately safeguards and secures such confidential information.
- All confidential information in electronic media must reside and be stored on the network servers of New York Medical College, and not on local work stations, personal computers, laptops, flash drives, etc.
- All confidential information in print or paper media must be stored in file cabinets that are secured and locked.
- All confidential information containing personally identifiable information must be accessed and used only by authorized employees of New York Medical College. Such confidential information shall be used for limited legitimate purposes of the College. Such confidential information containing personally identifiable information shall not be copied, stored, transferred, altered, destroyed or disclosed in any manner. Employees who are authorized to access and use such confidential information shall take all necessary precautions to assure that proper administrative, technical, and physical safeguards are established and followed in order to protect the confidentiality of such confidential information.
- All users of personal computers shall be responsible for adhering to all policies, standards and procedures for the use of information resources, including implementing security practices necessary to protect confidential data and information. Such personal computer users shall not access, acquire, use, copy, transfer or maintain confidential information on a personal computer and shall be held accountable for any loss or unauthorized disclosure of confidential information which is not on the College's network servers.

2. Responsibilities of Authorized Users of Confidential Information

Each authorized user of confidential information is responsible for understanding and complying with this Policy. Each authorized user accepts responsibility for the following:

- Access only the information authorized and reasonably necessary to perform his/her duties as an employee of New York Medical College;
- Maintain, use and handle confidential information consistent with the principles and guidelines set forth in this Policy;
- Take appropriate measures to protect confidential information wherever it is located, e.g., held on physical documents, stored on computer media, communicated over voice or data networks, exchanged in conversation, etc.;

- Safeguard the confidentiality of any security controls and passwords, e.g. physical key, ID card or computer/network account that allows access to confidential information;
- Report any suspected activities that may compromise confidential information to his/her immediate supervisor, department head, Information Services, Institutional Compliance Officer or Director, or the Office of General Counsel.

3. Responsibilities of Department Heads and Supervisors of Authorized Users of Confidential Information

Department Heads and Supervisors are responsible for establishing and maintaining security for confidential information within their areas of responsibility consistent with this Policy including the following:

- Require that only authorized users have access to confidential information and that he/she understands this Policy and his/her responsibilities in the handling of such information and materials;
- Identify confidential information and materials and implementing adequate controls to secure confidential data and information; and,
- Protect against the unauthorized disclosure of confidential information.

The responsibilities and obligations under this Policy shall survive the termination of employment with New York Medical College.

VI. Enforcement

Noncompliance with or violation of this Policy may result in serious disciplinary action, including suspension or termination of employment. It may also result in civil and/or criminal prosecution and penalties as applicable by law.

This policy shall be periodically reviewed by the Office of General Counsel and Institutional Compliance in consultation with the Human Resources and Information Services Departments.

All questions regarding this policy can be directed to the Office of General Counsel and Institutional Compliance.

Approved by:

Karl P. Adler, M.D.
President and Chief Executive Officer

10/01/07
Date