PURPOSE

To protect Morehouse School of Medicine ("MSM" or "School") employees, students and patients against a breach of privacy and/or confidentiality.

APPLICABILITY

This policy applies to all MSM employees, students, trainees, consultants, and volunteers.

DEFINITIONS

A. Breach: Accessing, sharing, reviewing, or disclosing oral, paper or electronic Confidential Information by an individual for purposes other than his/her job responsibility or for which s/he is authorized.

B. Confidential Information: Confidential Information is any communication, information, or reception of knowledge and includes facts, documents, data, or opinions that may consist of numerical, graphic or narrative forms-whether oral, printed, or electronic including in databases or on papers. Confidential Information includes but is not limited to patient records, student records, financial records, human resources/payroll records, legal documents, and research data.

C. Identifying Information: Identifying Information includes, but is not limited to, the following:

- Social security or employer taxpayer identification numbers
- Driver's license, state identification card, or passport numbers
- Checking account numbers
- Savings account numbers
- Credit card numbers
- Debit card numbers
- DEA numbers
- National Provider Identifier
- Personal Identification (PIN) Code which is a numeric and/or alphabetical code assigned to the cardholder of a financial transaction card by the issuer to permit authorized electronic use of that financial transaction card.
- Digital signatures
- Any other numbers or information that can be used to access a person's financial resources
- Biometric data

D. Personal Information: A person's first name or first initial and last name in combination with identifying information as defined above. Personal information does not include a publicly available directory containing information an individual has voluntarily consented to have publicly disseminated or listed, including name, address, and telephone number, and does not include information made lawfully available to the general public from federal, state, or local government records.

POLICY

During the course of employment, individuals may have access to Confidential Information. Any Confidential Information, whether oral, written, or electronic, should be maintained in a manner that ensures its confidentiality. The release of any such Confidential Information may result in negative financial or competitive action, productive loss, or cause legal or other non-beneficial impacts on MSM.

Confidential Information must be treated with respect and care by any workforce member who is authorized to have access to this information. Anyone who is authorized to use or disclose Confidential Information also has the responsibility to safeguard access to such information. Individuals who are authorized by MSM to access Confidential Information have a responsibility to limit access to those that are allowed by permission and/or by law. The access must be appropriate to the individual's job responsibility. A breach is a violation of this policy and/or state or federal regulatory requirements resulting in the unauthorized or inappropriate use, disclosure or access of Confidential Information.

MSM will safeguard confidential information concerning patients, students, employees, School business, and other matters. Confidential information includes, but is not limited to information concerning:

- Current, former and prospective students
- Current, former and prospective employees (employment, pay, health, insurance data, and other personnel information)
- Patients
- Alumni
- Board of Trustees' members
- School business, finances, or operations
- Intellectual property

Each employee, consultant, student, or person granted access to data and information holds a position of trust and must preserve the security and confidentiality of the information he/she uses. Users of School data and information are required to abide by all applicable Federal and State guidelines and School policies regarding confidentially of data, including, but not limited to the Family Educational Rights and Privacy Act of 1974 (FERPA), and the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

Any employee or person with authorized access to MSM's computer resources, information system, records or files is given access to use the School's data or files for the business of the School. Specifically, individuals should:

- Access data solely in order to perform his/her job responsibilities.
- Not seek personal benefit or permit others to benefit personally from any data that has come to them through their work assignments.
- Not make or merit unauthorized use of any information in the School's information system or records.
- Not enter, change, delete or add data to any information system or files outside the scope of their job responsibilities.
- Not include or cause to be included in any record or report, a false, inaccurate or misleading entry.
- Not alter or delete or cause to be altered or deleted from any record, report or information system, a true and correct entry.
- Not release School data other than what is required in completion of job responsibilities.
- Not exhibit or divulge the content of any record, file or information system to any person except as it is related to the completion of their job responsibilities.

Additionally, individuals are not permitted to operate or request others to operate any School data equipment for personal business, to make unauthorized copies of School software or related documentation, or use such equipment for any reason not specifically required by the individual's job description.

GUIDELINES

A. SECURE TECHNOLOGY

Each individual is responsible for protecting his/her password for access to School resources and information. Each user is responsible for all actions taken and uses of computer systems made under that individual's username. Faculty, staff, students and guests must keep all passwords confidential. At no time shall a password be written down on paper and/or post-it notes and passwords must not be stored in areas that are visible to others. Passwords must not be communicated to anyone, other than confirmed IT services personnel, except when otherwise directed by the Department of Human Resources. Users who have reason to believe that their password has been compromised must change it immediately.

MSM employs industry standard practices to keep non-public information as secure as possible. Despite this intention, it cannot assure members of the MSM community that their uses of School computing and communications resources will be completely private. Information and messages sent over the Internet can be intercepted in various ways. Therefore, users of MSM technology with access to the Internet cannot assume that information they send over the Internet will be or remain confidential and inaccessible to anyone other than the intended recipient. Information stored on School computing resources, or passed through communications networks may be accessible to the public through public record laws, subpoenas, interception, "hacking" or other means.

In general, information stored on computers is considered confidential, whether protected by the computer operating system or not, unless the owner intentionally makes that information available to other groups or individuals.

B. SUBPOENAS

Subpoenas and any other request or demand for the release of information for a legal proceeding must be referred to the Office of General Counsel before release of any information.

C. MEDIA CONTACTS

Employees may not comment on School business to representatives of the press (radio, television, or print media) without authorization from the Marketing and Communications department. Employees may not represent themselves as a spokesperson for MSM unless authorized to do so. If an issue arises that may result in engagement with the press, notification should be provided to the Vice President of Marketing and Communications for guidance.

D. RESTRICTIONS AND VIOLATIONS

Employees who receive requests for confidential information should seek direction from a supervisor. It is the employee's responsibility to report immediately to his/her supervisor any violation of this Policy or any other action, which violates confidentiality of data. **Employees who violate this Policy may be disciplined up to and including dismissal. Unauthorized accessing or disclosure of legally protected information may result in civil liability or criminal prosecution.**

REPORTING RESPONSIBILITIES

The individual, who commits, observes or becomes aware of an unauthorized or inappropriate access, use or disclosure of Confidential Information is responsible for promptly reporting such to one of the following:

- Immediate supervisor
- Department head or manager of the area in which the individual works
- Human Resources
- Compliance Office

The immediate supervisor or department management will coordinate a review of the potential breach with Human Resources and the Office of Compliance and, when applicable, review the circumstances surrounding the breach, mitigation steps and any harmful effect that may result from the breach. Department management in conjunction with Human Resources and Office of Compliance staff will determine appropriate sanctions concerning the breach.

Corrective action, if warranted, will be imposed based on the nature and severity of the violation, whether intentional or not, circumstances surrounding the breach or whether the violation demonstrates a pattern or practice of improper use or disclosure of Confidential Information on the part of the individual.

Nothing in this policy prohibits employees from discussing the terms and conditions of their employment as authorized by law.