

<b>Number:</b>	<b>011-001</b>
<b>Section:</b>	<b>Institutional Policies Relative to GME</b>
<b>Title:</b>	<b>Intellectual Property Copyrights and Royalties</b>

**Effective Date:** 4/19/12

**Previous Review & Approval by GMEC:** 1/17/08

**Responsible Office:** NJMS Graduate Medical Education

**Update:** Every five years from effective date or as needed

**Purpose:** To set policy regarding copyrights and royalties for all copyrightable material created by Rutgers personnel related to or within the scope of their employment at the University.

**Scope:** This policy shall apply to full-time and part-time faculty, postdoctoral appointees, housestaff, non-faculty employees and student employees. Under the direction of the Executive Vice President for Academic Affairs, the Vice President for Research and Economic Development shall ensure compliance with this policy. The Dean, President/CEOs of the Healthcare Units and Vice Presidents in conjunction with the Director, Office of Technology Transfer and Business Development shall implement this policy. The Deans shall ensure that each new faculty member receives a copy of this policy or is directed to it on the University's web site.

**Definitions:**

1. **Housestaff/House Officer-** refers to all interns, residents and subspecialty residents (fellows) enrolled in a Rutgers New Jersey Medical School (Rutgers NJMS) graduate medical education program. A member of the housestaff may be referred to as a house officer.
2. **Designated Institutional Official (DIO)** – refers to the individual who has the authority and responsibility for the graduate medical education programs.
3. **Program** – refers to the structured medical education experience in graduate medical education which conforms to the Program Requirements of a particular specialty, the satisfactory completion of which may result in eligibility for board certification.
4. **Program Director** – the one physician designated to oversee and organize the activities for an educational program.
5. **Review Committee-** the Accreditation Council for Graduate Medical Education delegates authority to accredit programs/institutions to its Review Committees. The Review Committees are comprised of peer specialists in the field and resident physicians.

**Reference(s):**

1. Rutgers Policy ([policies.rutgers.edu](http://policies.rutgers.edu))

**Policy:**

- A. "Creator": Person who transforms ideas into a tangible form of expression thereby creating Copyrightable Material.
- B. "Copyrightable Material": Material that is subject to U.S. copyright laws, including, but not limited to, literary works, musical works, dramatic works, choreographic works, graphic works, photographic works, cardiographic, radiographic and pictorial works (e.g., x-rays, images), sculptural works, audiovisual and videotaped works, sound recordings, films, theses, and works in electronic media (e.g., digitized works and network transmission of digitized works, multimedia broadcast, web-based products, recorded materials, remote transmission of information, instructional software, CD-ROMs).

- C. "Derivative Works": Copyrightable Material based on or derived from one or more already existing copyrighted works. Derivative works include, but are not limited to, new versions, translations, dramatizations, fictionalizations, reproductions, compilations, revisions and condensations.
- D. "Traditional Works of Scholarship": Copyrightable Material reflecting research and/or creativity which is considered evidence of accomplishment in the Creator's academic discipline or professional field, and is specifically created for predominant use by persons or entities other than the University and/or its students. Such works include, but are not limited to, books, book chapters, journal articles, abstracts, student theses, plays, poems, pictorial and sculptural works, films, cassettes, musical compositions and other literary works.
- E. "Institutional Works": Copyrightable Material created (1) specifically or predominantly for use by or at the University, or (2) at the request or behest of the University, or (3) under the specific direction of the University, or (4) by a person acting within the scope of his or her employment at the University, or (5) under a written contract between the Creator and the University, or (6) under a contract between the University and an external agency. "Traditional Works of Scholarship" will not be considered "Institutional Works" for the purposes of this policy.
- F. "Instructional Materials": A type of "Institutional Work," including textbooks and study guides, used for the instruction of Rutgers students, housestaff and/or postdoctoral fellows.
- G. "Other Intellectual Property": Any Copyrightable Material other than Traditional Works of Scholarship, Institutional Works and Instructional Materials.
- H. "University Resources": Tangible resources provided by the University to a Creator, including funds, office space, lab space, equipment, electronic network resources (hardware and software), support personnel, secretarial support, research, teaching and lab assistants, assistance from medical students or residents, media specialists or illustrators, supplies, utilities. Funds include grants and contracts or awards made to the University by an extramural sponsor.
- I. Housestaff - refers to all interns, residents and fellows enrolled in a Rutgers New Jersey Medical School graduate medical education program. A member of the housestaff may be referred to as a house officer.

**STATEMENT OF PRINCIPLES**

The University encourages the dissemination of knowledge and development of creative work that fulfills its educational, research and service missions and benefits the public it serves. The University supports the preparation and publication of copyrightable works resulting from the teaching, research, scholarly and artistic endeavors of faculty, staff and students as part of their roles at the University. The University seeks to foster an intellectually stimulating environment in which creative efforts and innovations are encouraged and rewarded, the careers of its members are enhanced, and the University's reputation and prestige are furthered. The University respects, acknowledges and promotes the intellectual property rights in works created by its members. The University strives to maintain a balance among the interests of Creators, sponsoring bodies and the University in copyrightable material and income resulting from such works. All University personnel are encouraged to retain ownership of the copyright to Traditional Works of Scholarship (as defined herein) or to obtain a perpetual license from the copyright owner to reproduce, distribute, perform, and/or display the work and to make Derivative Works therefrom.

**POLICY/PROCEDURE**

- A. Copyright Ownership
  - 1. Institutional Works and Instructional Materials as defined herein shall be deemed as having been created within the scope of employment of the Creator. Copyright ownership of such works shall vest with the University unless otherwise agreed in writing. Rights associated with copyright ownership become enforceable where the University has sought and obtained a copyright, which shall be done where the University determines that the material is commercially viable.

2. Traditional Works of Scholarship as defined herein shall be deemed as having been created outside the scope of employment of the Creator. Copyright ownership of such works shall vest with the Creator.
  3. Ownership of the copyright in Other Intellectual Property will be determined by the University on a case-by-case basis, based upon the level of use of University Resources in its creation.
  4. Absent the establishment of such by law or contract, the University shall assert no ownership rights to any Copyrightable Material developed by a Creator before joining the University.
- B. Marking and Disclosure
1. Copyrightable Material shall be marked at the earliest possible opportunity with the copyright symbol "©" or the word "copyright" or the abbreviation "Copr.", the year of first production or publication, and the name of the owner of the copyright in the work.
  2. The Creator shall promptly file a copyright disclosure form with the Director, Office of Patents and Licensing for any (a) Institutional Works, (b) Instructional Materials and (c) Other Intellectual Property created with the use of University Resources.
    - a. The disclosure form shall be filed when the material is in final form or when it is close to completion. Should the Creator desire that the University release its ownership rights in the copyright in the disclosed work, the disclosure form should contain such a request.
    - b. The University may release its ownership rights to the Creator when, as determined by the Director, Office of Technology Transfer and Business Development (1) there are no overriding special obligations to a sponsor or other third party, and/or (2) the best interests of the University would be so served. The University shall make this decision within 90 days of receipt of the disclosure form.
    - c. If the Director denies the Creator's request that the University's ownership rights in the copyright be released to the Creator, the Creator may appeal this decision to the University Intellectual Property Faculty Committee for final decision. The University will endeavor to seek qualified faculty representation from all Rutgers Schools on this committee.
    - d. The Director, Office of Technology Transfer and Business Development shall file an application to register the University's copyright interest in the disclosed work when copyright ownership remains with the University.
- C. Rights to License, Market and Use Copyrightable Material
1. Traditional Works of Scholarship and Other Intellectual Property created without the use of University Resources:
    - a. The Creator has the right to determine his/her own licensing, marketing and use of these materials.
    - b. When a Creator departs from the University, she/he shall grant the University a license to distribute, display and reproduce this Copyrightable Material and to produce Derivative Works therefrom for educational and research purposes within Rutgers, except if copyright ownership of Traditional Works of Scholarship has been transferred to a publisher as a requirement of publication.
  2. Institutional Works, Instructional Materials and Other Intellectual Property created with the use of University Resources:
    - a. The University, through the Office of Technology Transfer and Business Development, shall have the right to determine the licensing, marketing and use of material for which the University has sought and obtained copyright ownership. This determination shall

- take into account the interests of the University, the public and the Creator, including the Creator's preferences.
- b. The Creator shall have the right to be identified or to refuse to be identified as the Creator by the University and by subsequent licensees and assignees, except as required by law.
- D. Royalties and Revenue Distribution
1. Traditional Works of Scholarship, and Other Intellectual Property that is created without the use of University Resources: All revenue from material within these categories belongs exclusively to the Creator.
  2. Institutional Works, Instructional Materials and Other Intellectual Property that is created with the Use of University Resources: A fee of 10% shall be paid to the Office of Technology Transfer and Business Development. This fee as well as other expenses (e.g., legal fees, registration fees, other licensing fees) shall be subtracted before revenue is distributed. The remaining revenue from material within these categories shall be divided as follows:
    - a. The Creator shall receive 40%.
    - b. The department/program/unit/center employing or contracting with the Creator shall receive 25%; primary consideration in the use of this portion of the revenues shall be given to support the Creator's further research or his/her other creative efforts at the University.
    - c. The School in which the Creator has an academic appointment or the administrative or patient care unit in which the Creator is employed shall receive 25%; this portion of the revenues shall be utilized at the discretion of the pertinent Dean, Vice President or President/CEO of the Healthcare Unit.
  3. In the event of the Creator's death, any compensation payable under this policy shall be paid to his/her estate or assigns.
- E. Traditional Works of Scholarship that are created as, or are transformed into, electronic media by faculty will be treated in a similar manner as other Traditional Works of Scholarship.
- F. Except where otherwise provided, resolution of disputes concerning the application of this policy or the ownership of copyrights shall be brought directly to the Vice President for Research, who shall, in consultation with the Senior Vice President and General Counsel and appropriate Dean or other Vice President, render a final decision within 30 calendar days.

<b>Number:</b>	<b>011-002</b>
<b>Section:</b>	<b>Institutional Policies Relative to GME</b>
<b>Title:</b>	<b>Patient Confidentiality and Health Information</b>

**Effective Date: 4/19/12**

**Previous Review & Approval by GMEC: 1/17/08**

**Responsible Office: NJMS Graduate Medical Education**

**Update: Every five years from effective date or as needed**

**Purpose:** To protect patient privacy as electronic health-care records and networked information systems are introduced into the University by ensuring the highest level of confidentiality of individually identifiable patient health-care information, whether paper or electronic, that is compatible with current technology and with legitimate needs for accessibility of the information.

**Scope:** This policy shall apply to health information that is generated during provision of health care to patients in any of the University's patient-care units, patient-care centers or faculty practices, as well as to clinical information generated from human subjects research under the auspices of the University or by any of its agents. Under the President, the Vice President/CEO of University Hospital (UH), the Vice President/CEO of University Behavioral HealthCare (UBHC) and the deans shall ensure compliance with this policy. Appropriate individuals at University Hospital, University Behavioral HealthCare, the schools and faculty practices, in conjunction with the Vice President for Information Systems & Technology (IST), shall implement the policy by means of unit-specific procedures and standards.

**Definitions:**

1. **Housestaff/House Officer-** refers to all interns, residents and subspecialty residents (fellows) enrolled in a Rutgers New Jersey Medical School (Rutgers NJMS) graduate medical education program. A member of the housestaff may be referred to as a house officer.
2. **Designated Institutional Official (DIO)** – refers to the individual who has the authority and responsibility for the graduate medical education programs.
3. **Program** – refers to the structured medical education experience in graduate medical education which conforms to the Program Requirements of a particular specialty, the satisfactory completion of which may result in eligibility for board certification.
4. **Program Director** – the one physician designated to oversee and organize the activities for an educational program.
5. **Review Committee-** the Accreditation Council for Graduate Medical Education delegates authority to accredit programs/institutions to its Review Committees. The Review Committees are comprised of peer specialists in the field and resident physicians.
6. **Privacy** is an individual's desire to limit the disclosure of personal information.
7. **Confidentiality** is a condition in which information is shared or released in a controlled manner.
8. **Security** consists of measures to protect the confidentiality, integrity and availability of information and the information systems used to access it.
9. **Electronic health information (such as electronic medical records)** is a computerized format of the health-care information in paper records that is used for the same range of purposes as paper records, namely to familiarize readers with the patient's status, to document care, to plan for discharge, to document the need for care, to assess the quality of care, to determine reimbursement rates, to justify reimbursement claims, to pursue clinical or epidemiological research, and to measure outcomes of the care process.

10. A **firewall** is a computer positioned at a single focused point of entry for external users over unsecured public networks, such as the Internet, into an internal trusted network; firewalls can be configured to monitor and regulate messages passing into and out of the private network, or prevent particular programs from passing through.

**Reference(s):**

1. Rutgers Policy 00-01-10-30:00
2. *For the Record: Protecting Electronic Health Information, National Research Council, 1997*

**Policy:**

A. General Principles:

1. Electronic health-care information has many advantages over paper records, including immediate availability to authorized individuals; clear organization; ready adaptability for analyses and research; legibility; and ability to provide alerts, suggestions, warnings, reminders, critical pathways and links to relevant literature. It will be the predominant form of health-care information at the University in the future. Properly implemented and managed, electronic health records have the potential to *increase* the security of health information and the privacy of patients over that in a paper-records environment.
2. Individuals have a fundamental right to control the dissemination and use of information about themselves, including health-care information. Individuals have the right to expect that their identifiable health information will not be disclosed without their express informed consent. Respect for patients' privacy is part of the ethical practice of the health-care professions.
3. The University is committed to providing appropriate safeguards for patient privacy and for confidential health-care information, consistent with available technology and with legitimate needs for accessibility of the information to authorized individuals for effective delivery of health care, for efficient functioning of the health-care delivery system (including audit and accreditation functions), for biomedical, behavioral, epidemiological and health services research, and for education.
4. Protection of health-care information depends on both technology and organizational measures to minimize potential abuse by authorized users, whether intentional or unintentional, and from outside attacks.
5. The technical and organizational security measures required to safeguard patient privacy and the confidentiality of health-care information must be balanced against: (a) costs (impediments to clinicians' access to information relevant to their decision-making; expense of purchase and of integration into the current system; costs of ongoing management, operations and maintenance; user frustrations with sub optimal interfaces and procedures; user time lost in satisfying security protections); (b) the need of authorized users to access critical information in a timely manner so that provision of health care is not compromised; (c) the need of researchers and educators for information that will further knowledge; (d) and the desire of payers not to be defrauded.
6. The University requires compliance with all state and federal laws, rules and regulations governing the confidentiality of patient medical records in any medium, as well as with the guidelines established by organizations such as the JCAHO.
7. Any individual who violates this policy or is responsible for unauthorized breaches of patient confidentiality shall be subject to discipline up to and including dismissal from the University as well as civil and criminal penalties. Sanctions shall be applied consistently to all violators regardless of job title or level in the organization.

B. Security breaches, violations of policy, unauthorized access, audit-trail data or other system warnings about unusual or inappropriate activity, and identified weaknesses in security measures shall promptly be reported by the assigned data steward or confidentiality officer to the pertinent dean or vice president and to the Vice President for IST.

- C. Mechanisms for protecting health information include *technical measures* for improving computer and network security, and *organizational measures* for ensuring that health-care workers understand their responsibility to protect information and that processes are in place for detecting and reporting violations:
1. Technical Practices and Procedures: The University and its patient-care units shall adopt the following technical security practices:
    - a. *Individual authentication of users.* In order to establish individual accountability for actions on-line and to implement access controls based on individual needs, every individual shall have a unique identifier or log-on ID for use in logging into patient-care information systems. Individuals shall be informed that it is a violation of this policy to share identifiers with others. Passwords shall be changed no less frequently than every six (6) months. Names, English-language words and common acronyms shall not be used as passwords. Passwords should include letters, numbers and other characters. There shall be strict procedures set up at each patient-care unit for issuing and revoking identifiers.
    - b. *Access controls.* As soon as current technology at the University permits, each patient-care unit, patient-care center and faculty practice shall develop procedures to ensure that users can access and retrieve only that information for which they have a legitimate need to know.
    - c. *Audit trails.* Each patient-care unit shall maintain in retrievable and usable form audit trails that log accesses to patient information. The logs may include information such as the date and time of access, the information or record accessed, the user ID under which access occurred, and if possible the reason for the access.

Audit-trail information shall be kept in a safe place to prevent erasure or modification. Procedures shall be established for regularly reviewing and analyzing audit logs or a random sample thereof to detect inappropriate accesses. Audit trails should be used together with system-generated prompts or warning screens informing users of the sensitive content of patient records and reminding them about audit logs and sanctions for unauthorized access.
    - d. *Physical security and disaster recovery.* IST and each patient-care unit shall: (1) limit unauthorized physical access to computer systems, displays, networks and health-care records; (2) position monitors and keyboards so they are not easily seen by anyone other than the user; (3) where appropriate, program workstations to display passworded screen savers if left idle for a specified period of time; (4) properly dispose of outdated equipment, tapes, disks, paper printouts and other media that contain confidential information; (5) establish plans for providing basic system functions and ensuring access to health-care records in the event of a natural emergency or mechanical or software failure by means such as redundant processing facilities, regular full-system back-ups and annual practice drills; (6) store back-up data in safe places or in encrypted form; and (7) ensure that contractors used to transport and store back-up tapes have adequate policies and procedures to protect the integrity and confidentiality of the information.
    - e. *Protection of remote access points.* IST shall install and monitor a firewall and/or other forms of protection that provide strong centralized security to host machines that allow external public or insecure connections such as the Internet or dial-in telephone lines. Outside access shall be allowed only to those systems critical to outside users or for the conduct of University business. There shall be an additional secure authentication process (either encrypted or single-session passwords) for remote and mobile users, such as those using home or portable computers, or remote access shall be allowed only over dedicated lines.
    - f. *Protection of external electronic communications.* In order to prevent interception by unauthorized individuals, all patient-identifiable information should be encrypted before transmission over open public networks such as

the Internet, or such transmission should be only over secure dedicated lines. The inclusion of patient-identifiable information in unencrypted E-mail is forbidden.

- g. *Software discipline.* IST shall ensure the installation of virus-checking programs on all servers University-wide. The University shall maintain an inventory of all software on all workstations and servers. Vendor licensing agreements must be adhered to.
- h. *System assessment and technological awareness.* IST shall formally assess the security and vulnerabilities of the University's information systems on an ongoing basis, e.g., running "hacker scripts" and password "crackers" against the systems, and routinely using software protection tools such as virus-detection software and software checksum protection. IST shall also continuously appraise the University's system architecture, hardware and software technologies, and procedures to eliminate outdated components and practices.

IST shall aggressively stay current with standards and technologies for security management, and make recommendations to the University's patient-care units concerning the *future* implementation of new security practices that become state of the art, such as strong authentication practices, University-wide authentication systems, access validation, expanded audit trails, electronic authentication of records via electronic signatures, cryptographic technologies.

- 2. Organizational Practices: The University and its patient-care units shall adopt the following organizational security practices:
  - a. *Unit-specific security and confidentiality procedures.* Each patient-care unit, patient-care center and faculty practice shall develop explicit and clear confidentiality procedures governing both paper and electronic media that:
    - (1) state the types of information considered confidential;
    - (2) stipulate who may have access to which elements of patient information for what purposes;
    - (3) identify the people authorized to release the information and the procedures that must be followed to make a release;
    - (4) identify the types of people authorized to receive information, under which circumstances, and when additional patient consent is required;
    - (5) specify a method of disposal of paper records containing patient identifiers that ensures their complete destruction (i.e., shredding or bonded disposal);
    - (6) enforce sanctions that will be applied for breaches of confidentiality and unauthorized access; and (7) set up training programs for staff, faculty and students in privacy, confidentiality and security. These policies and associated procedures should be reviewed annually and publicized regularly, preferably by senior management.
  - b. *Unit security and confidentiality committees.* Each patient-care unit, center and faculty practice shall establish a broadly based committee or assign a person or office to develop, implement, monitor and maintain the unit-specific procedures for protecting patient privacy and ensuring the security of information systems. Similarly, responsibility shall be assigned for granting and removing access privileges to/from users of the unit's information system.
  - c. *Education and training programs.* Each patient-care unit, patient-care center and faculty practice, in conjunction with IST, shall establish formal educational programs to ensure that all users of information systems receive the required training in professional responsibilities and personal accountability for security and confidentiality, in relevant security practices, and in existing confidentiality policies and proper procedures *before* being granted access to any health-information systems. Annual refresher courses should also be conducted with the participation of the medical staff leadership. Other

educational tools, such as in-service sessions, grand rounds, continuing medical education, selective use of one-on-one or small-group training for physicians, videos, pamphlets, posted reminders, on-line screens, memos and newsletters should be considered. System users requiring training include full-time, part-time, temporary and newly transferred employees, admitting and referring physicians, contractors, vendors, housestaff, students, volunteers, and outcomes or epidemiological researchers.

Log-in screens should be developed that remind users that health-care information is limited to legitimate health-care or research purposes, that misuse of health-care information is a violation of University policy and can lead to sanctions, and that audit logs record all user activities.

- d. *User confidentiality agreements.* Any individual (employee, student, volunteer, contract worker, vendor or other non-employee) accessing patient-information systems must sign a form stating that she or he has read, received a copy of, understood and will comply with this University policy and the patient-care unit's procedures. This form should be signed *prior to* access being given and retained in the pertinent department. The unit's data steward or confidentiality officer shall ensure the signing of these agreements and keep the forms on file.
- e. *Informing patients.* Each patient-care unit, patient-care center and faculty practice shall develop means to inform patients of the existence of electronic health records, to describe health-data flows within the unit and with external organizations, to describe the policies and procedures in place to protect patient privacy, to request additional patient authorizations for other proposed uses of their health information, and to inform patients of their rights of access to their health records. This information should list the types of organizations and individuals to whom identifiable and unidentifiable information is commonly released (such as insurers, managed care companies, responsible researchers with appropriate IRB approval and patient consent, certain government agencies, courts, accreditation and oversight bodies, authorized social-welfare agencies, etc.). Methods to accomplish this include disclosure authorization forms separate from other consent forms such as those for medical care or research. The time period for which authorizations are valid should be indicated.
- f. *Patient access to audit logs.* The University's health-care units, centers and faculty practices should give patients the right to request and review audits of all accesses to their health records, as well as the right to review the contents of their health records and annotate or supplement information they believe to be inaccurate, incorrect or incomplete (without removing any information). Patients' primary care physicians also have the right to review audit logs of their patients' health records.

<b>Number:</b>	<b>011-003</b>
<b>Section:</b>	<b>Institutional Policies Relative to GME</b>
<b>Title:</b>	<b>Rights and Responsibilities for the Use of the University Accessed Electronic Information System</b>

**Effective Date:** 4/19/12

**Previous Review & Approval by GMEC:** 1/17/08

**Responsible Office:** NJMS Graduate Medical Education

**Update:** Every five years from effective date or as needed

**Purpose:** To set policy for the use of the University's electronic information systems, broadly defined, including users' rights and responsibilities.

**Scope:** This policy applies to all individuals accessing and using computing, networking, telephony and information resources through any facility of the University. These individuals include students, faculty, visiting faculty, staff, volunteers, alumni, persons hired or retained to perform University work, external individuals and organizations, and any other person extended access and use privileges by the University under contractual agreements and obligations or otherwise. This policy covers all computing, networking, telephony and information resources owned by, procured through, operated or contracted by the University. Such resources include computing and networking systems (especially those connected to the University's telecommunications infrastructure---the University-wide and campus-wide backbones--as well as local area networks), public-access sites, shared computer systems, personal desktop computers, other computer hardware, software, databases stored on or accessible through the network, IST support personnel and services, physical facilities, and communications systems and services. Under the President the Vice President for Information Services & Technology (IST) shall ensure compliance with this policy. The Deans, Vice Presidents, IST Directors, Associate Deans for Student affairs, and individual managers shall implement the policy.

**Definitions:**

1. **Housestaff/House Officer-** refers to all interns, residents and subspecialty residents (fellows) enrolled in a Rutgers New Jersey Medical School (Rutgers NJMS) graduate medical education program. A member of the housestaff may be referred to as a house officer.
2. **Designated Institutional Official (DIO)** – refers to the individual who has the authority and responsibility for the graduate medical education programs.
3. **Program** – refers to the structured medical education experience in graduate medical education which conforms to the Program Requirements of a particular specialty, the satisfactory completion of which may result in eligibility for board certification.
4. **Program Director** – the one physician designated to oversee and organize the activities for an educational program.
5. **Review Committee-** the Accreditation Council for Graduate Medical Education delegates authority to accredit programs/institutions to its Review Committees. The Review Committees are comprised of peer specialists in the field and resident physicians.
6. **Internet-** a combination of international, national, state and local electronic networks employing a common set of protocols that enables people around the world rapidly and easily to access and exchange information, regardless of origin or location, and provide and receive services.
7. **World Wide Web-** is a client/server environment on the Internet that provides multimedia information and services with hypertext navigation.
8. **Information Owner** – a person designated by the Vice President of their respective organization and delegated the responsibility to manage and maintain the unit's information that is stored or processed by the business unit's application or by an application that is sued for a utility service.

**Reference(s):**

1. Rutgers Policy [00-01-05-30:00](#)
2. Rutgers Policy [00-01-35-60:00](#)
3. Rutgers Policy [00-01-40-60:00](#)

**Policy:**

**A. General Principles:**

1. The University owns its computing, networking, telephony and other communications systems and its information resources, and has the right to monitor them. The University also has various rights to the software and information residing on, developed on, or licensed for these computers and networks. The University has the responsibility for the security, integrity, maintenance and confidentiality of the electronic systems.
2. Computing, networking, telephony and information resources of the University, including access to local, national and international networks, exist to support students, faculty and staff as they carry out the education, research, health-care and public-service missions of the University, and its administration and management. Toward these ends, the University encourages and promotes the use of these resources by the University community. Access to and use of these resources for purposes or activities which do not support the University's missions are subject to regulation and restriction to ensure that they do not interfere with legitimate work; and any access to or use of these resources and services that interferes with the University's missions and goals is prohibited.
3. When demand for computing, networking, telephony and information resources exceeds available capacity or resources, priorities shall be established for allocating the resources, with a higher priority to activities essential to the missions of the University. The Deans and Vice Presidents, in conjunction with the Vice President for IST, shall set these priorities.
4. Information owners and system administrators shall develop and publicize specific written procedures to protect the rights of legitimate authorized users, to protect the integrity of the information and systems under their management, and to delineate the responsibilities of users. The University has the authority to control or refuse access to anyone who violates these procedures or threatens the rights of other users or the availability and integrity of the systems and the information. Actions that may be taken under this authority include deactivating accounts, access codes or security clearances; stopping processes; deleting affected files; and disabling access to computing, networking, telephony and information resources.
5. Users' expectation of electronic privacy must be balanced against the University's reasonable need to supervise, control and operate the University's information systems.
6. The University does not archive E-mail that has been sent or received by its systems. The user is responsible for archiving E-mail messages that the user wishes to retain.

**B. Rights of Users:**

1. *Privacy and confidentiality:* Because the primary use of the University's communications systems is to further the University's missions, members of the University community should not have the expectation of privacy in their communications, whether work-related or personal. By their nature, electronic communications, especially E-mail connected to the Internet, may not be secure from unauthorized access, viewing or infringement.

Although the University employs technologies to secure certain categories of electronic messages, as a rule confidentiality of E-mail and other electronic documents cannot be assumed. The University cannot and does not make any guarantee, explicit or implied, regarding the confidentiality of E-mail and other documents and messages stored in electronic media unless provisions, approved and maintained by the University, are specifically implemented to this

purpose. Users should not expect total privacy when using E-mail. Although the University will not monitor the content of electronic documents or messages as a routine matter, it reserves the right to examine all computer files in order to protect individuals and the University. In addition, during the course of routine conduct of University business, routine management of the University's computing and networking systems, as well as during emergencies, the University has the right to view or monitor users' files, data, messages or other activity for legitimate business purposes, with or without notice to users. Information seen in such a manner will ordinarily be kept confidential, but may under certain circumstances be used in disciplinary proceedings if appropriate. If an individual is suspected of violations of his/her responsibilities as described in this policy or of other misconduct, the University reserves the right to take any and all actions to abide by the law and maintain network integrity and the rights of access of others authorized to use the system. The University also reserves the right to access and disclose messages, data, files, and E-mail back-up or archives, if such exist, to law enforcement authorities and others as required by law, to respond to legal processes, and to fulfill its obligations to third parties. E-mail is subject to legal discovery during the course of litigation, even if deleted, by means of message archives, back-up tapes and un-deleting the messages. Therefore, good judgment dictates the creation only of electronic documents that may become public without embarrassment or harm.

2. *Safety:* Unwanted communications and offensive or objectionable materials are available through the Internet and may be blocked or regulated by the University. The University accepts no responsibility for the content of electronic mail received. However threatening, harassing or offensive communications received by University personnel over the network should be reported to IST, Public Safety and, if appropriate, to the Office of Workplace Diversity.
3. *Intellectual freedom:* The network is a free and open forum for the expression of ideas. The University will not prevent expressions of academic opinions on the network as long as these opinions are not represented as the views of the University and are not in conflict with University policies or state and federal laws. Even with disclaimers about not representing the views of the University, appropriate language, behavior and style should still be used in communications distributed on the University's computing and networking facilities. It should be remembered that certain categories of speech---defamation, obscenity and incitement to lawlessness---are not protected by the Constitution. The University reserves the right, at its sole discretion, to decline to post, to remove posted pages or to restrict University Web sites or computer accounts which contain or are used for personal expressions of a non-academic nature.

**C. Responsibilities of Users:**

1. Individuals with access to the University's computing, networking, telephony and information resources have the responsibility to use them in a professional, ethical and legal manner. Users are required to take reasonable and necessary measures to safeguard the operating integrity of the systems and their accessibility by others, while acting in a manner to maintain an academic and work environment conducive to carrying out the University's missions efficiently and productively. Specifically, responsibilities of users include:
  - a. Respecting the rights of others, including intellectual property, privacy, freedom from harassment, and academic freedom;
  - b. Safeguarding the confidentiality of certain information and the privacy of patients;
  - c. Using systems and resources so as not to interfere with or disrupt their normal operations or their access use and use by others so authorized;
  - d. Protecting the security of University electronic systems and the integrity of information stored there;

- e. Knowing and obeying University and unit-specific policies and procedures governing access and use of electronic systems and of information.
2. Individuals are prohibited from sharing passwords or log-in IDs or otherwise giving others access to any system for which they are not the data stewards or system administrators with appropriate authority. Users are responsible for any activity conducted with their computer accounts and are responsible for the security of their passwords.
3. Individuals may not use another person's network account or try to obtain password or access code to another's network account to send or receive messages.
4. Individuals must identify themselves and their affiliation accurately and appropriately in electronic communications and may not disguise the identity of the network account assigned to them or represent themselves as someone else.
5. The University's communications systems may not be used to harass, intimidate, threaten or insult others; to interfere with another's work or education; to create an intimidating, hostile or offensive working or learning environment; or to conduct illegal or unethical activities.
6. The University's networks may not be used to gain or attempt to gain unauthorized access to remote networks or computer systems.
7. Individuals are prohibited from deliberately disrupting the normal operations of the University's computers, workstations, terminals, peripherals or networks.
8. Individuals may not run or install on any University computer system a program that may result in intentional damage to a file, or that may intentionally compromise the integrity of the University's systems or the integrity of other computing environments via the University's network (e.g., computer viruses, Trojan horses, worms or other rogue programs).
9. Individuals are prohibited from circumventing access and use authentication systems, data-protection mechanisms, or other security safeguards.
10. Individuals must abide by all applicable copyright laws and licenses, and respect other intellectual-property rights. Information and software accessible on the Internet is subject to copyright or other intellectual-property-right protection. University policy and the law forbid the unauthorized copying of software that has not been placed in the public domain and distributed as "freeware." Therefore nothing should be downloaded or copied from the Internet for use within the University unless express permission to do so is stated by or received from the owner of the material, and the owner's requirements or limitations on use of the material are observed. The use of software on more than the licensed number of computers, unauthorized installation of unlicensed software on University computers, plagiarism and invasion of privacy are also prohibited. "Shareware" users must abide by the requirements of the shareware agreement.
11. Activities that waste or unfairly monopolize computing resources (such as unauthorized mass mailings; electronic chain letters, junk mail and other types of broadcast messages; unnecessary multiple processes, output or traffic; exceeding network directory space limitations; excessive game-playing or other trivial applications; and excessive printing) are prohibited.
12. Reading, copying, changing or deleting programs or files that belong to another person or to the University without permission is prohibited.
13. The University's computing resources may not be used for commercial purposes or personal financial gain.
14. All network communications exiting the University are subject to the acceptable-use policies of the network through which they flow.
15. Use of the University's systems that violates local, state or national laws or regulations or University policies, standards of conduct, or guidelines is prohibited.
16. Confidential information should be encrypted before transmission over open public networks such as the Internet, or such transmission should only be over secure dedicated lines. Including confidential University information in unencrypted E-mail is forbidden.

**D. E-mail and other electronic communications (Internet services, voice mail, audio- and video-conferencing, and facsimile messages):**

1. The use of University resources for electronic communications must be related to University business, including academic pursuits, and not for personal or commercial purposes, except for incidental and occasional personal non-commercial use when such use is clearly insignificant, does not generate a direct cost for the University, and does not interfere with or compete with legitimate University business.
2. Only authorized persons may use the University's electronic communications systems.
3. Electronic communications whose meaning, transmission or distribution is illegal, unethical, fraudulent, defamatory, harassing or irresponsible are prohibited. Electronic communications should not contain anything that could not be posted on a bulletin board, seen by unintended viewers, or appear in a University publication. Material that may be considered inappropriate, offensive or disrespectful to others should not be sent or received as electronic communications using University facilities.
4. Appropriate standards of civility and decency should be observed in electronic (as well as all other forms of) communication.

**E. World Wide Web:**

1. "Official" University Web pages are those that provide information about established, University-recognized entities, such as its Schools; patient-care units; administrative offices; research institutes, centers and programs; educational programs; clinical centers, institutes and programs. Information on official University Web pages represents the institution and therefore must be accurate, timely and useful and must conform to this and all other University policies, standards and requirements. Official Web pages shall be held to the same standards as any University, school or unit printed publication.
  - a. The pertinent Dean, Vice President or Department Chair has the ultimate responsibility for official Web pages. These individuals or their designees must authorize the establishment of any official Web page under their purview.
  - b. The University logo must appear on all official Web pages, or their equivalent.
  - c. Official Rutgers Web pages shall be reviewed by the responsible party every six to twelve months and these reviews documented by changing the revision date at the bottom of the page.
  - d. Official Rutgers Web pages may be copyrighted. Official Rutgers Web pages should not contain copyrighted materials without appropriate copyright permission.
2. Faculty professional Web pages and personal Web pages of a faculty member, student or staff member *may not*: promote illegal activities; harass anyone inside or outside the University; include offensive or objectionable material or language or link to other sites that do; distribute copyrighted materials; be used for commercial purposes or personal gain unrelated to the University's missions; contain the University logo; represent the contents as being the official policy or positions of the University. Personal pages from individuals or groups must include the identity of the author, and should contain the following statement: "*The views and opinions expressed in this page are strictly those of the author. The contents have not been reviewed or approved by the Rutgers .*" The University reserves the right to not post or remove posted pages for any reason.

**F. Non-compliance and Sanctions:**

Non-compliance with this policy may result in denial or removal of access privileges to the University's electronic systems; disciplinary action under applicable University policies and procedures; civil litigation; and/or criminal prosecution under applicable state and federal statutes.

**EXHIBIT**

A. UMDnet Account Holder Use Agreement

[http://www.umdnj.edu/opmweb/university\\_policies/information\\_services\\_technology/PDF/00-01-95-10\\_05.pdf](http://www.umdnj.edu/opmweb/university_policies/information_services_technology/PDF/00-01-95-10_05.pdf)

---

<b>Number:</b>	<b>011-004</b>
<b>Section:</b>	<b>Institutional Policies Relative to GME</b>
<b>Title:</b>	<b>Educational Use of Copyrighted Works</b>

**Effective Date:** 4/19/12

**Previous Review & Approval by GMEC:** 1/17/08

**Responsible Office:** NJMS Graduate Medical Education

**Update:** Every five years from effective date or as needed

---

**Purpose:** To establish policy for the use of copyrighted works of others by University faculty, staff and students for educational and other academic purposes.

**Scope:** Under the direction of the Executive Vice President for Academic and Clinical Affairs, the Vice President for Research shall ensure compliance with this policy. The Deans, President/CEOs of the Healthcare Units and Vice Presidents in conjunction with the Director, Office of Patents and Licensing shall implement this policy. This policy applies to all University faculty, staff and students. This policy covers all copyrighted works of others that are incorporated in University documents, publications, courses and computer files. Use of copyrighted works under this policy include, but are not limited to:

1. reproduction of the work;
2. distribution of the work to others by sale, rental, lease or broadcasting;
3. performance of the work in the case of performing arts, audio and audiovisual work; and
4. displaying the copyrighted work, including audiovisual works by broadcasting and on Web sites. Written permission from the owner of the copyright is required in all these instances.

**Definitions:**

1. **Housestaff/House Officer-** refers to all interns, residents and subspecialty residents (fellows) enrolled in a Rutgers New Jersey Medical School (Rutgers NJMS) graduate medical education program. A member of the housestaff may be referred to as a house officer.
2. **Designated Institutional Official (DIO)** – refers to the individual who has the authority and responsibility for the graduate medical education programs.
3. **Program** – refers to the structured medical education experience in graduate medical education which conforms to the Program Requirements of a particular specialty, the satisfactory completion of which may result in eligibility for board certification.
4. **Program Director** – the one physician designated to oversee and organize the activities for an educational program.
5. **Review Committee-** the Accreditation Council for Graduate Medical Education delegates authority to accredit programs/institutions to its Review Committees. The Review Committees are comprised of peer specialists in the field and resident physicians.

**Policy:**

- A. The University respects the legal rights of the owners of copyrights. Copyrighted works may be incorporated in University documents, publications and courses only if in compliance with copyright laws.
- B. University faculty, staff and students shall respect the legal rights of owners of copyrights. This includes the use of the materials of others in courses, publications, journals, research projects, videos, computer software, videotapes, conference presentations, etc.
- C. It is the policy of the Rutgers (Rutgers ) to adhere to the requirements of the United States Copyright Law of 1976, as amended (Title 17, United States Code, hereafter referred to as the "Copyright Act"). This policy applies only to copyrighted materials. Uncopyrighted materials may therefore be copied without restriction. Works authored by the United States Government or by some states are not copyrighted. Works published after March 1, 1989 do not require a copyright notice and should therefore be presumed to be under copyright protection. States and their instrumentalities are liable for violations of the Copyright act and all remedies for copyright infringement apply to states as well as to private individuals (PL 101-553). The University does not condone copyright infringement by any Rutgers faculty, staff or student; individuals who violate copyright are not protected by the University and may be subject to University disciplinary actions, civil litigation and/or criminal prosecution. Files belonging to the University or any University employee and containing copyrighted material may be subject to subpoena.
- D. It is the policy of Rutgers to invoke the doctrine of "Fair Use," as defined by Section 107 of the Copyright Act, in order to enable legal copying of copyrighted materials by faculty, staff and students without seeking the permission of a copyright holder and without the payment of royalty fees to the copyright holder. "Fair Use" for educational purposes may not be automatically invoked simply on the basis of copying copyrighted material for neither educational purposes nor on the basis of such copying being made by a non-profit organization. Each claim of "Fair Use" must instead be evaluated against four criteria:
1. the purpose and character of the use;
  2. the nature of the copyrighted work;
  3. the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and
  4. the effect of the use upon the potential market for or value of the copyrighted work.

Guidelines for "Fair Use" are discussed in Section V below.

## **GUIDELINES**

The following guidelines reflecting copyright laws have been adopted by Rutgers to provide faculty, staff and students with general guidance on the use of copyrighted works and to reduce the risk of copyright infringement. Copyright infringement is a criminal act as well as a civil violation and may result in grave consequences to the University and to the individual.

### **A. Faculty and Classroom Copying of Copyrighted Material**

#### **1. Single copying**

A single copy may be made by a faculty member or staff member (or for a faculty or staff member at his/her individual request) of any of the following:

- a. a chapter from a book;
- b. an article from a periodical or newspaper;
- c. a short story, short essay or short poem, whether or not from a collective work;

- d. a chart, graph, diagram, drawing, cartoon or picture from a book, periodical or newspaper.

“Systematic” copying of single articles that has the cumulative effect of copying an entire journal issue or volume without permission from the copyright holder or without payment of royalty fees is a violation of the Copyright Act and constitutes a criminal act.

2. Copies of **copyrighted** material used in slides

Copies of quotations, passages and other material taken from a **copyrighted** material may be used in a classroom electronic slideshow provided that:

- a. the quotations, passages, or other material are linked to the source of the material, if the source material is available on the internet
- b. if the source of the material used is not available on the internet, then the material must be properly attributed to its source or permission for the **use** received from the copyright holder

3. Electronic copies of **copyrighted** material placed online

Copies of **copyrighted** materials for **use** in the classroom, for an assignment, or for a discussion may be posted online by a faculty member for access by students of the class, provide that:

- a. posting of journal articles, magazine articles, book passages or other **copyrighted** material is on a password protected website;
- b. there is a limited period of time allowed for which students may access the material;
- c. the purpose and the character of the **use** is **educational** and noncommercial;
- d. the nature of the **copyrighted works** being posted is predominately factual (such as a paper from a scientific journal);
- e. the effect of the **use** will not be substantially adverse to the potential market for or value of the **copyrighted works**; and
- f. a good faith attempt was made to limit the **use** of the copyright **works** for **educational** purposes

4. Multiple copying for classroom use Multiple copies (no more than one copy per student in a course) for classroom use or discussion may be made by or for a faculty member giving the course, provided that:

- a. the test for brevity and spontaneity as provided in the examples below is met;
- b. the cumulative-effect test as defined below is met; and
- c. each copy includes a notice of copyright.

Any copying of copyrighted material which exceeds these limits must have the written permission of the copyright holder or royalty fees must be paid.

5. Examples of “brevity” are:

- a. Prose: either a complete article, story or essay of less than 2,500 words or an excerpt from any prose work of not more than 1,000 words or 10 percent of the work, whichever is less, but, in any event, a minimum of 500 words. Each of these numerical limits may be expanded to permit the completion of an unfinished line of an unfinished prose paragraph.
- b. Illustration: one chart, graph, diagram, drawing, cartoon or picture per book or periodical issue.
- c. Special works: Certain works in prose often combine language and illustration and fall short of 2,500 words in their entirety. Such special works may not be copied in their entirety, but an excerpt comprising not more than two pages and containing not more than 10 percent of the words found in the text may be copied.

6. Examples of “spontaneity” are:

- a. The copying is an immediate need as a result of the inspiration of the individual faculty member.
- b. The inspiration and decision to use the work and the moment of its use for maximum teaching effectiveness are so close in time that it would be unreasonable to expect a timely reply to a request for permission to copy from the copyright holder.

7. Examples of "cumulative effect" are:

- a. The copying is for only one course in the school.
- b. Not more than one short article, story or essay or two excerpts is copied from the same author, nor more than three from the same collective work or periodical volume during one class semester.

The limitations in and b above shall not apply to current news periodicals, newspapers and current news sections of other periodicals.

- c. There are not more than nine instances of such multiple copying for one course during one class semester.

8. Examples of **prohibitions** based on brevity and spontaneity are:

- a. copying used to create, replace or substitute for anthologies, compilations or collective works, regardless of whether copies of various works or excerpts therefrom are accumulated or are reproduced and used separately;
- b. copying of or from works intended to be "consumable" in the course of study or of teaching. These include workbooks, exercises, standardized tests, test booklets, answer sheets and similar consumable materials.
- c. Copying:
  - (1) to substitute for the purchase of books, publishers' reprints or periodicals;
  - (2) that is directed by higher authority (e.g., a faculty member directing his/her students to copy an article);
  - (3) which is repeated with respect to the same item by the same faculty member from semester to semester.
  - (4) where costs and charges for copying are charged to the student beyond the actual cost of the photocopying.

**B. Music and Audiovisual Use in the Face-to-Face Classroom**

If copyrighted music or audiovisuals are used in a face-to-face conventional class, some utilizations may be made under "Fair Use." No more than ten percent of a copyrighted work of music may be used, but not repeated for the course in the next semester, unless permissions have been obtained from the copyright holder. Under provisions of Section 110 of the Copyright Act, a lawfully obtained copyrighted film or videocassette not labeled "Home Use Only" may be aired in a face-to-face class, provided that such airing is within the scope of the educational intent of the course. No copy of such a film or videocassette may be made without first securing the permission of the copyright holder.

**C. Individual (and Student) Copying of Copyrighted Material**

Rutgers has no mechanisms to monitor photocopying. For this reason, Rutgers photocopy machines (including self-services machines) have posted warnings that the copying of copyrighted materials is subject to the Copyright Act.

**D. Copy-Center Copying of Copyrighted Material**

The Rutgers Department of Supply, Process and Distribution may legally provide faculty and staff with single or multiple copies of copyrighted materials that meet the guidelines outlined in Section V.A above. The Department of

Supply, Process and Distribution reserves the right to refuse to make copies of materials when such copying, in its judgment, is not in compliance with the Copyright Act. Rutgers faculty, staff and students are also advised that they, as individuals, remain responsible for compliance with the Copyright Act when they make use of off-campus copy vendors.

**E. Library Copying of Copyrighted Material**

**1. Internal library copying**

The Rutgers Libraries may legally provide faculty, staff, students and the general public with single copies of copyrighted materials that meet the guidelines outlined in Section V.A above.

Each copy thus made must include either the copyright notice from the material provided or shall be stamped with the following notice:

“This material may be protected by copyright law (Title 17, U.S. Code).” The Rutgers Libraries will not make multiple copies under any circumstances. The Libraries may make one copy of a copyrighted journal article for placement on reserve for class use upon receipt of a written request of the course teacher.

Each copy thus made shall bear the following notice:

“This material may be protected by copyright law (Title 17, U.S. Code).” The Rutgers Libraries will not make multiple copies of articles for placement in the Reserve Collection. The Libraries reserve the right to refuse to make copies of copyrighted materials which are not in compliance with the Copyright Act.

**2. Inter-library loan**

Libraries may also be liable under the law for acquisition of copyrighted materials obtained via inter-library loan from other libraries. The inter-library loan convention permits the securing of, for example, photocopied journal articles from other libraries. This convention, set forth by the Commission on New Technological Uses of Copyrighted Works (CONTU), permits as "Fair Use" the annual request of a maximum of five journal articles per journal title for the then-current five-year period. Paper records and computerized records of inter-library loan requests shall be retained by the Rutgers Libraries for a period of three years.

**F. Copying for Broadcast**

Copying of copyrighted materials for broadcast purposes, including broadcasts utilizing copyrighted printed works, video, music or other recordings, whether for “live” video broadcasts or pre-recorded video programs, presents a special set of problems with regard to copyright compliance. The Rutgers environment has at least four specific areas of broadcast activity which must be considered: closed-circuit, interactive, distance-learning classes; closed-circuit medical consultations and peer conferences; educational offerings or conferences which are broadcast to the external environment by satellite or other broadcast means; and Web-based, distance-learning courses. In the case of closed-circuit broadcasts, it is assumed that such broadcasts are not-for-profit and are aired from a specific classroom, conference room or consultation room at a specific site (e.g., Rutgers Campus). If programs containing copyrighted materials are aired for commercial gain by Rutgers, “Fair Use” may not be invoked and permissions from all copyright holders must be obtained. The guidelines below refer to only those airings, which incorporate copyrighted material.

**1. Closed-circuit, live, interactive, distance-learning classes**

- a. Display or copying of copyrighted materials for closed-circuit, live, interactive, distance-learning classes shall closely follow "Fair Use" guidelines for print materials as described in Sections V.A.1 and 2 above. Each such class shall begin with a text screen that states: “This class session may contain copyrighted material legally available to this class session as set forth in Title 17 of the United States Code.” Copies of such a broadcast may not be made by the host nor by the receiving site unless permission to do so has been granted by the copyright holder.

- b. A teacher having used a specific copyrighted item under terms of "Fair Use" in a closed-circuit, live, interactive, distance-learning class session may not use that item in a following class session, nor from semester to semester, unless specific permission to do so has been granted by the copyright holder.
  - c. As in the case with face-to-face conventional classroom use of copyrighted material, students at both the host classroom and the receiving classroom in a closed-circuit, interactive, distance-learning class may be provided with copies of printed or graphic (but not music nor audiovisual) copyrighted material (one copy per student). Each copy provided must bear the following copyright statement:  
"This material may be protected by copyright law (Title 17, U.S. Code)."
  - d. If copyrighted music or audiovisuals are used in a closed-circuit, interactive, distance-learning class, some utilization may be made under "Fair Use." No more than 10 percent of a copyrighted work of music may be used, but may not be repeated for the course in the next semester unless permission has been obtained from the copyright holder (see Section V.B above). Under provisions of Section 110 of the Copyright Act, a lawfully obtained copyrighted film or videocassette not labeled "Home Use Only" may be aired to a closed-circuit, interactive, distance-learning class, provided that such airing is within the scope of the educational intent of the course. No copy of a closed-circuit, live, interactive, distance-learning class containing such a film or videocassette may be made without first securing permission of the copyright holder.
  - e. In any closed-circuit, live, interactive, distance-learning class session which utilizes copyrighted material; it is the responsibility of the faculty member to assure that such utilization is lawful.
2. Closed-circuit, live, medical consultations and peer conferences
    - a. Closed-circuit, live, peer conferences or medical consultations may make use of print or graphic (but not music or audiovisual) copies (one copy per conference attendee) of copyrighted material. Each copy provided must bear the following copyright statement:  
"This material may be protected by copyright law (Title 17, U.S. Code)."
    - b. Assurance of copyright compliance is the responsibility of the moderator of such closed circuit, live consultations or conferences.
    - c. If copies are to be made of such live consultations and peer conferences, which include copyrighted material, permission must be obtained from the copyright holder.
3. Broadcasts to the external environment  
Broadcasts to the external environment (non-Rutgers or non-Rutgers related), which make use of satellite or other broadcasting technology may fall into two general categories: not-for-profit educational and for-profit commercial (which might be educational).
    - a. In the case of all external-environment, for-profit, live or for-profit, pre-recorded broadcasts, regardless of educational intent, all uses of copyrighted material must be accompanied by permission from the copyright holder or his/her/its royalty-and-permissions agent. Additionally, if copies are to be made of such broadcasts, permission to copy must be obtained. Non- authorized copying of such broadcasts is illegal.
    - b. In the case of external-environment, not-for-profit, educational, live broadcasts, which make use of copyrighted material, the same rights and prohibitions as outline in Section V.F.1 above may apply. If subscription and/or licensing fees are assessed to the recipient of such broadcasts, the broadcasts are for-profit and thus subject to permission and the payment of royalties. In any event, copies may not be made of such broadcasts without the permission of the copyright holder or his/her/its royalty-and-permissions agent.

- c. In the case of all external-environment, pre-recorded broadcasts, permission must be obtained for use of all copyrighted material. A pre-recorded broadcast must include a list of all copyrighted material and the statement of permission for that material. Additionally, copies may not be made of such broadcasts without the permission of the copyright holder or the royalty- and-permissions agent.
4. Web-based, distance-learning courses
  - a. All uses of copyrighted material must be accompanied by permission from the copyright holder or the appropriate royalty-and-permissions agent. Copyright material may include printed works, videos, music or graphics. The document should include a list of all copyrighted material and the statement of permissions for that material.
  - b. If the students involved in the Web-based, distance-learning courses are provided with copies of printed or graphic material, permission to copy must be obtained.
  - c. Permission must be obtained for copying of the digitalized material and any distribution to others.
  - d. Links may be made to other Web sites. However the material on other Web sites may not be copied without permission.
  - e. If the course is given only once, if the copy meets the tests for brevity and cumulative effect, and if each copy has a notice of copyright, then the material may be used without obtaining permission.

#### G. Computer-Related Copying

Computer-related copying may take many forms, such as copying of software, printing of items from computerized files, and downloading of computerized files or items from computerized files to hard disk or to diskette. Many items within computerized files are copyrighted or are subject to licensed control. Users of computers must exercise care in the use of such materials. The following guidelines relate only to the copying of copyrighted or licensed materials.

##### 1. Copying of software

Software operating systems and application programs should be considered copyrighted material unless they are termed "free-ware" or "public domain" by their producers and manufacturers. In most cases, a software program carries a license to which the purchaser agrees upon purchase or at the time of the software's installation. It is customary for software producers to permit the creation of one archival or "back-up" copy for each installation permitted by the license. A license may be for one installation or for multiple installations of a specific software program. Copies of licenses for software programs, which are purchased by Rutgers departments or individuals, shall be kept on file within the department or by the individual as long as the software is in use. Certain basic utility and applications programs are made available to Rutgers individuals and departments as "site license" programs. Such site- licensed programs will generally have only one license for the campus or for the institution as a whole. Licenses for such programs are kept on file centrally at the Campus or University.

Copying, adapting and electronic transmission of computer software is strictly forbidden by Rutgers personnel and students, except:

- a. in strict compliance with Public Law 96-517, Section 10(b) which, in amending Section 117 of Title 17 (U.S. Code) to allow for the making of computer software back-up copies, states (in part) "...it is not an infringement of the owner (purchaser) of a copy of a computer program to make or authorize the making of another copy or adaptation of a computer program provided:

- b. “that such a new copy or adaptation is created as an essential step in the utilization of the computer program in conjunction with a machine and that it is used in no other manner, or
  - c. “that such a new copy and adaptation is for archival purposes only and that all archival copies are destroyed in the event that continued possession of the computer program should cease to be rightful.”
  - d. where appropriate, written consent from the copyright holder is obtained;
  - e. where the software is verified.
    - (1) Illegal copies of software may not be used on Rutgers computers.
    - (2) Software (whether on tape or CD-ROM) may not be installed so as to permit multiple use or multiple-site use unless such permission is granted by the software license itself, or granted by the copyright holder or royalty-and-permissions agent.
2. Copying of computerized files and their contents
- a. Copies (to paper or downloaded to disk) may legally be made of computerized files and their contents, provided that the program license does not forbid such copying. Generally, a computerized file will carry an on-screen warning if copying is not permitted.
  - b. Care must be exercised in the copying of material found in other home pages on the Internet. Some home pages may contain copyrighted materials but may neglect to inform visitors to their Web sites or home pages of the presence of such copyright protection material. It is the position of Rutgers that the presence of such copyrighted material is the responsibility of the owner of the Web site or home page, and liabilities for copyright non-compliance must rest with that owner. Rutgers home pages and Web sites may not include copyrighted material unless permission has been granted by the copyright holder or the royalty-and-permissions agent.
  - c. Legally obtained copies of copyrighted materials may legally be scanned by use of telefacsimile equipment or by use of scanners attached to computers for purposes of transmission. Materials thus copied must bear the following statement: “This material may be protected by copyright law (Title 17, U.S. Code).” Such materials may not be scanned for storage in digital form unless permission to do so has been granted by the copyright holder. If such permission has been granted, the scanned and stored material must bear the following statement: “This material may be protected by copyright law (Title 17, U.S. Code).”
  - d. Rutgers faculty, staff and students may not incorporate copyrighted material into locally-created databases which are installed on Rutgers machines which are housed on Rutgers property unless specific written authorization and permission has been granted to do so by the copyright holder or the royalty-and-permissions agent. Any permitted copyrighted material shall be identified as such on a screen within a body of the program or as a footnote where such display of copyrighted material normally occurs.

#### H. Copyrighted Material Incorporated into Articles, Books, Courseware, Videos

Faculty, staff and students shall carefully consider the use of copyrighted material in all works prepared by them. This includes any copyrighted work of others incorporated in journal articles, books, courseware, software, video and conference material created for academic research as well as educational purposes. Faculty and staff are required to obtain permission and/or licenses from the copyright owner in order to reproduce, publish, distribute or display the copyrighted work.

**I. Legal Advice Regarding Copyright**

Before any Rutgers faculty, staff or student takes action or causes action to be taken that could possibly infringe any "exclusive right in copyrighted works" that are not exempted under the law or are not clearly "Fair Use" under the guidelines delineated above, the matter must be submitted in writing to the Rutgers Office of General Counsel for legal advice. Submissions in writing must include:

1. the work (original, reasonable facsimile or reproduction) which could possibly be infringed;
2. a description of the use/action contemplated or anticipated that could possibly cause the infringement;
3. an explanation as to why the use/action is necessary and how it is of benefit to Rutgers ; and
4. all related pertinent materials, including timelines and deadlines that have a bearing on the amount of time available for rendering the legal advice.

**J. Seeking Permissions**

Permissions for copyrighted materials may be obtained through a variety of mechanisms. For most of the journal literature, permissions information is available at the Copyright Clearance Center, Inc. (CCC), 222 Rosewood Drive, Danvers, MA 01923, telephone (508)750-8400, fax (508) 750-4744. Many book publication permissions may be obtained at CCC as well. Music permissions information may generally be obtained from ASCAP, One Lincoln Plaza, New York, NY 10023, telephone (212) 621-6000, or BMI, 320 W. 57th Street, New York, NY 10019, telephone (212) 586-2000. Information on intellectual property and related matters may be obtained from the International Confederation of Societies of Authors and Composers (CISAC) (home page <http://cisac.org>). Many book and software permissions may be obtained by writing directly to the author. Publishers of books frequently provide addresses for their authors.

**SANCTIONS**

Non-compliance with this policy may result in disciplinary actions under University employee and student policies and procedures, civil litigation, and/or criminal prosecution. \* Sections of this policy are excerpted from the policies of the Texas Tech University Health Sciences Center, with permission.

<b>Number:</b>	<b>011-005</b>
<b>Section:</b>	<b>Institutional Policies Relative to GME</b>
<b>Title:</b>	<b>Management of Potential Occupational/Educational Exposure to HIV, HBV and HCV</b>

**Effective Date: 10/20/2016**

**Previous Review & Approval by GMEC: 1/17/2008, 4/19/2012**

**Responsible Office: NJMS Graduate Medical Education**

**Update: Every five years from effective date or as needed**

**Purpose:** To outline the procedure under which postexposure prophylaxis will be made available to the University's housestaff who in the course of their studies and/or occupational activities are exposed to blood, tissue or other body or laboratory fluids that may contain human immunodeficiency virus (HIV), hepatitis B virus (HBV) and/or hepatitis C virus (HCV). This policy is based upon the available scientific data and Public Health Service recommendations for postexposure management of health-care personnel who have occupational exposure that may place them at risk of acquiring HIV, HBV and/or HCV.

**Scope:** Under the direction of the President, the Executive Vice President for Academic and Clinical Affairs, and the Presidents/CEOs of the Healthcare Units shall ensure compliance with this policy. The Deans, Vice Presidents, Director of Risk Management and Insurance, Director of Rutgers Environmental Health and Safety, and Director of the Occupational Medicine Service shall implement this policy.

**Definitions:**

1. **Housestaff/House Officer-** refers to all interns, residents and subspecialty residents (fellows) enrolled in a Rutgers New Jersey Medical School (Rutgers NJMS) graduate medical education program. A member of the housestaff may be referred to as a house officer.
2. **Designated Institutional Official (DIO)** – refers to the individual who has the authority and responsibility for the graduate medical education programs.
3. **Program** – refers to the structured medical education experience in graduate medical education which conforms to the Program Requirements of a particular specialty, the satisfactory completion of which may result in eligibility for board certification.
4. **Program Director** – the one physician designated to oversee and organize the activities for an educational program.
5. **Review Committee-** the Accreditation Council for Graduate Medical Education delegates authority to accredit programs/institutions to its Review Committees. The Review Committees are comprised of peer specialists in the field and resident physicians.
6. **Bloodborne pathogens-**refer to pathogenic micro-organisms that are present in human blood and can cause disease in humans. These pathogens shall include, but not be limited to, HBV, HCV and HIV.
7. **Occupational Exposure-**refers to reasonably anticipated or inadvertent skin, eye, mucous membrane, or parenteral contact with blood or other potentially infectious materials that may result from the performance of an employee's duties.

**Reference(s):**

1. Kuhar DT, Henderson DK, et al, Updated U.S. Public Health Service Guidelines for the Management of Occupational Exposures to Human Immunodeficiency Virus and Recommendations for Postexposure Prophylaxis. *Infection Control and Hospital Epidemiology* 2013;34(9):875-892.
2. RBHS Policy, Housestaff Immunizations and Health Requirements ([policies.rutgers.edu](http://policies.rutgers.edu))

3. Bloodborne Pathogens ([policies.rutgers.edu](http://policies.rutgers.edu))
4. HIV, HBV and HCV ([policies.rutgers.edu](http://policies.rutgers.edu))

**Policy:**

1. Avoiding occupational/educational exposures is the primary way to prevent transmission of HIV, HBV and HCV in health-care settings. However, hepatitis B immunization and postexposure management are integral components of a complete program to prevent infection following bloodborne pathogen exposure and are important elements of workplace safety.
2. In an attempt to prevent HIV, HBV and/or HCV infection due to occupational/educational exposures, Rutgers shall make postexposure prophylaxis available at no expense to housestaff of the University who have exposures in the course of their educational and/or professional activities at the University's facilities or affiliated institutions which may place them at risk of acquiring HIV, HBV and/or HCV infection.
3. The Deans, Presidents/CEOs of the Healthcare Units and Vice Presidents shall oversee the development of written detailed protocols which must be strictly adhered to following an exposure, and the dissemination of this information to all appropriate individuals on each Campus of the University. Those individuals, services or offices responsible for carrying out these protocols shall be identified and their names published on each Campus. The procedures developed to implement this policy shall ensure timely (within hours of exposure) availability of medical attention and counseling, and of postexposure prophylaxis if requested, 24 hours a day. The goal of these procedures is preparedness to begin postexposure prophylaxis as soon as possible, ideally within hours, following exposure. These protocols and lists of responsible individuals or offices shall be reviewed and updated on a regular basis as often as required. This policy and the references from the Centers for Disease Control and Prevention containing information on postexposure prophylaxis should be used as guidelines for the Campus protocols.
4. Exposed individuals shall be counseled concerning: the risks of their exposure to HIV, HBV and HCV (including considerations of infectivity of exposure source and type of exposure); the known scientific facts, known and unknown risks and potential benefits of postexposure prophylaxis; the need for follow-up medical evaluations whether or not postexposure prophylaxis is elected; the necessity of precautions to prevent transmission of potential HIV, HBV and HCV infection during the follow-up period; and other relevant issues. Such counseling shall continue to be available throughout the medication period if postexposure prophylaxis is requested and during the follow-up period whether or not postexposure prophylaxis is requested.
5. Individuals may accept or decline postexposure prophylaxis on a purely voluntary basis and will not be subject to any discrimination in their studies or job duties as a result of their decision. Exposed individuals shall receive follow-up counseling, postexposure testing and medical evaluation regardless of whether they receive postexposure prophylaxis. Those who become HIV seropositive, whether or not postexposure prophylaxis was taken, HBV seropositive or HCV seropositive should be evaluated, in discussions with appropriate HIV counselors and/or infectious disease experts according to published recommendations for HIV-infected, HBV-infected and HCV-infected health-care personnel.
6. The supervisor for an individual who sustains occupational/educational exposures to blood or other body fluids potentially infected with bloodborne pathogens must complete a Rutgers Accident Report for the Office of Risk Management and Insurance.

7. Individuals electing to receive HIV postexposure prophylaxis who meet all criteria and have signed the required form shall receive medication and follow-up evaluations by health-care providers, health services or offices identified in advance on each campus and available 24 hours a day. At least the first one to three days' supply of medications shall be available in all identified sites where individuals are instructed to report after an exposure so that prophylaxis can be started as soon as possible.
8. Upon report of an exposure, date and time, source, and details of the exposure shall be recorded. These details must include type of procedure being performed, type and brand of device involved, department or work area where the exposure occurred, how the exposure occurred, amount and type of fluid or material, depth of injury and whether fluid was injected, duration and extent of skin or mucous membrane contact, condition of skin, and details about the exposure source (such as HIV/HBV/HCV status and/or risk for these infections). The course of counseling, medical care and medication received shall be documented in writing.
9. Confidentiality will be maintained to the extent possible and permitted by law.
10. If the HIV, HBV and HCV status of the source person is not known, the source person should be informed of the incident and every effort made to obtain this information through appropriate testing. In most cases, this will be the responsibility of the source person's health-care provider. Initiation of postexposure prophylaxis, if elected by the exposed individual, shall begin as soon as possible following exposure regardless of the availability of information about the source person's HIV, HBV and HCV status. However, the results of source-person testing and/or information about the source person's symptoms and risk factors may contribute to the decision to continue postexposure prophylaxis.
11. As part of job orientation and annual training, all Rutgers housestaff with potential exposure to bloodborne pathogens shall be educated concerning the risk for and prevention of bloodborne infections, including the need to be vaccinated against hepatitis B, and to report exposures immediately after they occur, and shall be familiarized with the principles of postexposure management and with their Campus's, School's or Unit's specific procedures for obtaining postexposure care. This shall be the responsibility of the Vice President for Human Resources, Rutgers Environmental Health and Safety, the President/CEOs of the Healthcare Units and the Dean. All housestaff shall receive similar education and information prior to clinical or laboratory studies or duties. The Dean shall ensure that housestaff are so educated and shall assign the direct responsibility for this to appropriate individuals at each School.
12. For Rutgers housestaff at non-Rutgers clinical facilities, the School shall make arrangements concerning immediate care and shall determine cost responsibility in consultation with the affiliated institution. Rutgers housestaff working at non-Rutgers clinical sites and who are exposed may receive medical care, including postexposure prophylaxis and follow up, at Rutgers facilities designated to carry out this policy. Non-Rutgers housestaff working/studying at Rutgers clinical sites and who are exposed may receive immediate medical care, including postexposure prophylaxis, at Rutgers facilities designated to carry out this policy; follow-up care will be at their home institution.
13. Individuals must first submit a claim to their health insurance carrier to be reimbursed for the costs related to the exposure. Following submission of a claim, and presentation of proof thereof (i.e., an explanation of benefits from the insurance carrier) to the appropriate School or University office, unreimbursed costs of the drugs, initial and follow-up laboratory tests for the exposed individual and for the source person (if not already performed), initial and follow-up visits, counseling and record-keeping shall be borne by the University's Workers' Compensation Program in the case of University-employed housestaff.

<b>Number:</b>	<b>011-006</b>
<b>Section:</b>	<b>Institutional Policies Relative to GME</b>
<b>Title:</b>	<b>Pharmaceutical Manufacturers and Other Representatives Policy</b>

**Effective Date:** 4/19/12

**Previous Review & Approval by GMEC:** 2/21/08

**Responsible Office:** NJMS Graduate Medical Education

**Update:** Every five years from effective date or as needed

**Purpose:** To set guidelines for resident interaction with Pharmaceutical and Device Manufacturers Representatives, and all other vendor representatives, that is consistent with Rutgers policy and specific to Graduate Medical Education Programs.

**Scope:** This policy shall apply to Program Directors, Program Coordinators, and all members of the housestaff.

**Definitions:**

1. **Housestaff/House Officer-** refers to all interns, residents and subspecialty residents (fellows) enrolled in a Rutgers New Jersey Medical School (Rutgers NJMS) graduate medical education program. A member of the housestaff may be referred to as a house officer.
2. **Designated Institutional Official (DIO)** – refers to the individual who has the authority and responsibility for the graduate medical education programs.
3. **Program** – refers to the structured medical education experience in graduate medical education which conforms to the Program Requirements of a particular specialty, the satisfactory completion of which may result in eligibility for board certification.
4. **Program Director** – the one physician designated to oversee and organize the activities for an educational program.
5. **Review Committee-** the Accreditation Council for Graduate Medical Education delegates authority to accredit programs/institutions to its Review Committees. The Review Committees are comprised of peer specialists in the field and resident physicians.

**Reference(s):** ACGME Institutional Requirements III.B.13

**Policy:**

- A. Pharmaceutical and Device Manufacturers Representatives and all other vendors (herein after referred as PDMRs) who wish to contact employees of Rutgers NJMS must conform to all Policies and Procedures set forth by Rutgers .
- B. All PDMRs must have approval from the employee(s) with whom they are scheduled to meet, prior to all appointments. Once approval is granted, all PDMRs must sign in with the Department of Public Safety immediately upon entrance to the facility.
- C. While on site and during appointments, all conversations and interaction must take place in a private setting.
- D. PDMRs are proscribed from using the paging system to contact either faculty physicians or housestaff.

- E. Housestaff are not permitted to interact with PDMRs in facilities associated with NJMS, except for approved educational activities.
- F. Educational activities by PDMRs for housestaff are permitted, but only after approval by a faculty member of NJMS. A faculty member must be present during the educational activity.
- G. PDMRs' promotional materials, without substantial educational content, are barred from NJMS facilities. Exhibits and discussion of pharmaceutical and devices as part of medical education programs are permitted in appropriate educational locations.
- H. The receipt of gifts and favors, other than educational materials and grants, from PDMRs by NJMS employees is prohibited under University Policy #00-01-10-05:00 code of Ethics: General Conduct.