GUIDELINES FOR APPROPRIATE USE OF INTERNET, ELECTRONIC NETWORKING, AND SOCIAL MEDIA

These guidelines are applicable to all faculty, staff, and students at the Robert C. Byrd Health Sciences Center. The use of the internet or intranet includes, but may not be limited to, postings on blogs, instant messaging (IM), using social networking sites, sending or receiving e-mail, or postings to public media sites, mailing lists, and/or video sites. These guidelines apply whether an individual uses public or private computers or devices. Nothing contained in these guidelines shall supersede other University adopted policies, guidelines, or training relating to Information Technology Resources.

Background:

Faculty, staff, and students at the Robert C. Byrd Health Sciences Center regularly use social and business networking websites and on-line communities to communicate with each other and with others external to the institution. It is expected that members of the HSC community will act with honesty and integrity and will respect the rights, privileges, privacy, sensibilities, and property of others.

The ability to record, store and transmit information in electronic formats brings specific responsibilities to the members of the HSC community with respect to the privacy of patient information. Information that identifies patients that is intentionally or unintentionally placed in the public domain will constitute a breach of the standards of professionalism and confidentiality that apply to our faculty, staff, or students in the HSC schools. All members of the HSC community who are involved in the delivery of health care have an obligation to maintain the privacy and security of patient records under the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

In accordance with HIPAA, FERPA, and WVU Health Sciences Center IT policy, please be advised that faculty, staff, residents, and students are **not permitted** to post confidential patient information, including protected health information (PHI), educational records protected by FERPA, institutionally-owned asset data, confidential, proprietary, or private information on any social networking sites (Facebook, MySpace, Twitter, YouTube, etc.), personal / business related blogs, and/or instant messaging service.

Each member of the HSC community is required to satisfactorily complete the annual HSC Information Technology Security Awareness Training, which includes, but is not limited to, the appropriate usage of information technology resources and various forms of electronic media.

Guidelines:

1) Never post any personal health information (PHI) about an individual patient to any electronic media, other than the patient's electronic health record. "Personal health

information" means information as defined by HIPAA which may identify an individual patient. This guideline applies even if the patient's information has been de-identified so that the only person who may be able to identify the individual is the patient himself.

2) Never post a photograph or image of a patient to any electronic media, other than the patient's electronic medical record. Use of cameras or cell phone cameras in the patient care setting shall be for the sole purpose of assisting in the care and treatment of the patient or for educational purposes. Any photographs taken in the patient care setting must be posted to the patient's electronic medical record.

3) Comply with all applicable institutional policies or guidelines regarding any use of information technology resources, including the use of institutional trademarks or logos. The use of the name "WVU Healthcare" is restricted and may not be used without permission from the office of the Chancellor of Health Sciences.

4) Never post any information about colleagues or co-workers to any electronic media without their explicit written permission. Respect for the privacy of others is an important part of the professionalism of our HSC community.

5) Never become an electronic "friend" of a patient in any electronic media or require that a patient become a "friend" of the health care provider in order to influence or maintain the patient-health care provider relationship.

6) Never misrepresent in any electronic media that an individual faculty, staff, or student is acting on behalf of West Virginia University or the Robert C. Byrd Health Sciences Center.

7) Maintain the professionalism standards of your profession in all aspects in the use of internet, electronic networking or social media.

8) Make sure you understand the permanency of published material on the Web.

9) Finally, please note that Facebook, MySpace, and other social networking sites are increasingly being targeted by cyber-criminals drawn to the wealth of personal information supplied by users. Data posted on the sites (i.e. name, date of birth, address, job details, email and phone numbers) is a windfall for hackers. Viruses on these networks can hijack the accounts of social networking site users and send messages steering friends to hostile sites containing malware, a malicious software often designed to infiltrate a computer system for illicit purposes. Malware can be used to steal bank account data or credit card information once installed on a personal computer. Another

danger of social networking sites are the popular quizzes, horoscopes and games made available for free to users which can sometimes be used to hide links to hostile sites.

Examples of information that should not be shared on social networking, blog sites, and instant messaging services are:

- Reporting on or about official medical activities and/or patient's personal health information.
- Requiring patients to participate in "social networking" activities to influence or maintain the provider/patient relationship.
- Posting of and/or the discussion of student grades, evaluations, course feedback, etc.
- Reviewing profiles of patients.
- Participating in activities that may compromise the provider/patient or faculty/student relationship.
- Providing medical advice on social networking sites.

Enforcement:

All members of the HSC community have a responsibility to ensure that these guidelines are adhered to appropriately. Any individual who becomes aware of a violation of these guidelines should approach his/her immediate supervisor for advice. If the issue is not addressed appropriately, the individual may complain in writing to the Dean of their individual school or to Information Technology Services at ITS@hsc.wvu.edu.