# SOCIAL NETWORKING POLICY

| | |
|---|---|
| APPROVED BY: VICE PRESIDENT FOR Medical Administration and Chief Operating and Strategy Officer | DATE: 06/10/11 |
| LAST REVISION: | DATE: 05/09/11 |
| LAST REVIEWED: | DATE: 05/09/11 |
| POLICY #: SN 01 | REV: A |

## INTRODUCTION

The University of Miami ("University") participates in online communities to promote better communication with the community, including students, alumni, patients, employees, parents, donors, the general public and other community members. Such participation may include, but is not limited to, postings in online forums, blogs, Facebook, LinkedIn, MySpace, YouTube, Twitter, media sites or similar types of online forums. Communications produced by the University or on behalf of the University and/or its affiliates in the online community must comply and be consistent with University standards for business conduct, policies and applicable laws, including laws concerning protected health information, privacy, confidentiality, copyrights and trademarks.

The University and/or its affiliated entities may require that an employee, faculty member, volunteer or other associate discontinue use of the University or affiliate-sponsored online communities or stop acting on behalf of the University /affiliate if it believes such communications are in violation of University policies, values or applicable local, state and federal laws.

## DEFINITIONS

**University:** The University refers to the University Of Miami Miller School Of Medicine, University of Miami Health System and all affiliated entities including, but not restricted to, University of Miami Hospital (UMH), University of Miami Hospitals and Clinics (UMHC), Sylvester Comprehensive Cancer Center (SCCC), Bascom Palmer Eye Institute (BPEI), Diabetes Research Institute (DRI) and the Miami Project to Cure Paralysis.

**PII – Personally Identifiable Information**: Personally Identifiable Information is information that can be used to distinguish or trace an individual's identity. Examples include social security number, medical record number, credit card number, address, phone number or any information that, when combined or used with other identifying information, is linked or linkable to a specific individual.

**PHI – Protected Health Information:** PHI is individually identifiable health which relates to the past, present or future physical health, mental health or condition of an individual. PHI either identifies or could be used to identify the individual and has been transmitted or maintained in any form or medium (electronic, paper or oral). Examples include identifiers such as name, medical record number, social security number or other demographic information used in conjunction with health information such as treatment, diagnosis or medications.

**HIPAA – Health Information Portability and Accountability Act**: A broad-based Federal healthcare-related law which provides the ability to transfer and continue health insurance coverage when employment changes, mandates industry-wide standards for electronic healthcare transactions and requires the protection and confidential handling of protected health information (PHI).

**FERPA - Family Educational Rights and Privacy Act**: A federal law designed to protect the privacy of educational records, to establish the right of students to inspect and review their education records, and to provide guidelines for the correction of inaccurate and misleading data.

**GLBA - Financial Modernization Act, also known as Gramm-Leach-Bliley Act**: A Federal law requiring institutions to design, implement and maintain safeguards to protect personally identifiable financial information.

**PCI – Payment Card Industry**: The Payment Card Industry has created a set of standards designed to ensure that all companies that process, store or transmit credit card information maintain a secure environment. These standards are termed Payment Card Industry Data Security Standards (PCI DSS).

## PURPOSE

The purpose of this policy is to assure:

- Communications in online communities made on behalf of the University are consistent with the University's standards for business conduct, policies and applicable laws, including, but not limited to, laws concerning privacy, confidentiality, copyright and trademarks.
- Uses of the University or affiliate-sponsored online communities are appropriate and such communications are approved for dissemination.
- Employee opinions posted on non-official University online communities represent their own views and are not those of the University and/or its affiliates

**POLICY GUIDELINES:**

## FOR ALL SOCIAL MEDIA SITES, INCLUDING PERSONAL SITES

**Protect confidential and proprietary information**

- Do not post personally identifiable information (PII) or protected health information (PHI), including identifiable photographs of University of Miami patients, students, employees, donors, applicants or alumni unless you have explicit, written permission to do so. Adhere to all applicable University privacy and confidentiality policies including, but not restricted to, HIPAA, PCI, GLBA and FERPA.

- Do not post confidential University information including but not limited to, internal business plans, HR discussions, salary information, research material, financial information and other information not meant for public disclosure.

- Employees who share confidential information do so at the risk of disciplinary action up to and including termination.

**Be respectful of the University, affiliated entities, other employees, students, parents, donors, alumni, partners, and competitors**

- Personal blogs should have clear disclaimers that the views expressed by the author in the blog are the author's alone and not that of the University or its affiliates.

- Be mindful that views expressed can readily be disseminated to a world-wide audience.

- Understand that any material posted can survive indefinitely and attempts to delete or recall such information are presently not technically feasible.

**Respect copyright and fair use**

- Respect the copyright and intellectual property rights of others and of the University. Do not use copyrighted material without permission. Reference or cite sources appropriately.

**Do not use University of Miami logos for endorsements**

- Do not use the University logo or any other official University images on personal social media sites for the purpose of appearing to be an officially sanctioned University or affiliate site without written consent from the UHealth/Miller School of Medicine Office of Marketing.
- Do not use University of Miami's name to promote a product, cause, or political party or candidate.

**Respect University time and property**

- University computers and time on the job are reserved for University-related business as approved by supervisors and in accordance with A046 Use of University Computing Facilities policy

**Terms of service**

- Obey and comply with the Terms of Service of any social media platform employed.

## OFFICIAL UNIVERSITY OF MIAMI/AFFILIATE SOCIAL MEDIA SITES

If you post on behalf of an official University unit, the following policies must be adhered to in addition to all policies and best practices listed above:

- Medical School Departments or business units that have a social media page or would like to start one should contact the UHealth/Miller School of Medicine Office of Marketing at marketing@med.miami.edu or 305-243-3453.

- All University/affiliate social media sites should seek to coordinate with other University sites and their content.

- All University/affiliate pages/posts must have a full-time appointed employee who is identified as being ultimately responsible for content.

- A documented process which explicitly lists who is allowed to post on behalf of the department/business unit as well as the approval process within that unit must exist. This process must be provided to the UHealth/Miller School of Medicine Office of Marketing for input and approval.

- Use of protected health information (PHI), including identifiable photographs of University of Miami patients, students, employees, donors, applicants or alumni may only be used upon completion of the appropriate written authorization and release forms. (Authorization/Release for Photography or Audio/Video Recordings and the Attachment 46 – Authorization for Third Party Disclosure)

- If you have permission to represent the University and/or affiliate on a social media platform, then you should clearly acknowledge that you represent the University.

- All communications/material are property of the University/affiliate and are subject to monitoring. There should be no expectation of privacy. All equipment and internet services are for business use only.

- Departments, business units and affiliates should consider their messages, audiences, and goals, as well as a strategy for keeping information on social media sites current and accurate. The UHealth/Miller School of Medicine Office of Marketing can assist and advise on social media strategy and planning; the Office of HIPAA Privacy & Security, in conjunction with the Office of General Counsel can advise on privacy and security best practices. The Office of HIPAA Privacy and Security serves as the official contact for reviewing and amending this policy.

Related Policies/Forms:

- A046 Use of University Computing Facilities policy
- Authorization/Release for Photography or Audio/Video Recordings
- Attachment 46 – Authorization for Third Party Disclosure