
**UNIVERSITY OF ILLINOIS COLLEGE OF DENTISTRY
MANAGEMENT POLICY AND PROCEDURE**

UIC COD 2.4: Social Media Policy

OBJECTIVE

Social media can be a powerful means to build a community around your clinical service, department, or organization, but social media can pose a risk to our confidential and proprietary information, reputation and brand, and to the privacy rights of employees, students and patients. To minimize these risks, it is expected that all UI Health employees adhere to the following guidelines and rules regarding use of social media. Therefore, UI Health Employees are expected to review this policy before participating in any social media activity.

DEFINITIONS

For the purpose of this policy, the following definitions apply:

A. Channel Definitions (Note: this is not a complete list; this is sample of the more popular social media channels)

1. Facebook: A social media site where users can keep up with friends, upload photos, share links and videos, and learn more about the people and brands that they are connected with.
2. Twitter: A social media and micro-blogging site where users can keep up with friends and brands through the exchange of 140 characters.
3. LinkedIn: A social networking site focused on companies and industry professionals looking to make new business contacts or keep in touch with previous co-workers, affiliates, and clients.
4. YouTube: A video sharing website where users can upload, share and view video content.
5. Yelp: An online community of user reviews and ratings, where you can find information on restaurants, dentists, etc.
6. Tumblr: A site that allows users to post multimedia and other content to a shortform blog. Users can follow other users' blogs.

PROCEDURE

Overview

The full UI Health social media policy is detailed in the following pages. We encourage you to read through the full document, but if you need a quick reference, please refer to these key points:

- 1) Only designated individuals and key departments (e.g. UI Health Marketing, UIC Public Affairs) are authorized to speak on behalf of UI Health online without prior approval.
- 2) *Unauthorized* employees are prohibited from publishing on behalf of any official UI Health pages.
- 3) Service Areas or Departments interested in creating and managing a UI Health-related page must submit a request to UI Health Marketing ([Social Media Request Form](#)), go through the appropriate process (section 1.1 below), and complete media training class prior to any formal UI Health-related page creation (section 1.2 below).
- 4) All authorized employees posting on behalf of UI Health are solely responsible for content, and posts must adhere to all applicable UI Health Policies. When in doubt, please refer to the social media training documents, best practices (section 4), or contact UI Health Marketing (uihealthmktg@uic.edu).
- 5) All HIPAA and State of Illinois privacy laws apply to social media. Employees must not, under any circumstance, share confidential hospital or patient information. This includes pictures of patients, patient information, or medical history (e.g. no ‘selfies’ with patients).
- 6) UI Health employees should have no expectation of privacy in any data in any format or any other kind of information or communications transmitted to, received or printed from, or stored or recorded on any UI Health or University page, site or account.

A. Participation in Social Media as a UI Health Social Media Representative

Social Media can be a valuable tool to build and engage with online communities. Official pages will have the support of the UI Health Marketing department, and individuals will be authorized to manage these pages and speak on behalf of UI Health.

1. UI Health will take the following into consideration when presented with a page proposal, either for brand new pages, or existing pages that would like to be made official:
 - a) The specific goal and target audience of the channel or page.
 - b) Resource availability (i.e. is there an individual with the ability and available time to monitor and update the channel or page at a reasonable frequency). See Section 4: Best Practices for recommendations on update frequency.
 - c) Alignment with UI Health’s brand guidelines and copy standards. See UI Health Marketing’s [Standards and Best Practices Brand Guidelines](#).
 - d) Other considerations to be determined at the discretion of the UI Health Marketing department.
2. Individuals authorized by the UI Health Marketing department will manage official pages. If you are one of these employees authorized to speak on behalf of UI Health online as part of job, you are an official representative of the organization. As such, you must adhere to the following guidelines:

- a) To speak on behalf of UI Health online, you must have approval from the UI Health Marketing Department ([Social Media Request Form](#)).
- b) In order to have an official UI Health social media channel or page, you must attend a UI Health Media Training and Obligations class before you can create or manage any social media pages on behalf of UI Health. Once authorized, you will be personally responsible for all social media activity via your page. Contact UI Health Marketing (uihealthmktg@uic.edu) for a schedule of upcoming Media Training and Obligations classes.
- c) Posts must adhere to all applicable UI Health Policies. When in doubt, please refer to the social media training documents, best practices (section 4), or contact UI Health Marketing (uihealthmktg@uic.edu).
- d) All posts must abide by all other applicable UI Health policies, including, but not limited to:
 - i) **IM 4.17 HIPAA Sanctions:** Ensures the confidentiality and integrity of patient and/or employee Protected Health Information (PHI) as required by law, professional ethics, and accreditation and/or licensure requirements
 - ii) **LD 4.13 Code of Conduct:** All patients and employees treat each other with respect, dignity, and honesty. No harassing, profane, or discriminatory material can be published.
 - iii) **IM 3.15 Acceptable Use of Computer Resources:** Computer resources are the property of the Medical Center and may be used only for legitimate business purposes.
 - iv) **IM 3.02 Confidentiality Agreement and Security Awareness:** Employees may not disclose confidential information they encounter at UI Health.
 - v) All applicable copyright laws. You must have the proper permission to post photos, videos, or other materials owned by others
- e) You must not publish any content that contains any product or service endorsements, or anything that could be construed as political lobbying, solicitations, or contributions.
- f) You must not post information that would infringe on the intellectual property or privacy rights of others.
- g) UI Health and the University restrict employees' use and disclosure of our confidential information and intellectual property. You should treat the UI Health/University trade secrets, confidential information and intellectual property confidentially and not jeopardize them through your use of social media. Further, you should avoid disclosing intellectual property and/or confidential information of third parties that you learned through your employment. Such disclosures may create liability for you, the employee, as well as the University.
- h) By posting content to UI Health social media pages, you grant UI Health the right to reproduce and distribute it, the right to create derivative works, and the right to use it for any purpose.

- i) UI Health reserves the right to monitor, prohibit, block, or terminate access to authorized UI Health social media channels at its discretion

- j) As a page manager, you should adhere to social media best practices as outlined in the UI Health Media Training and Obligations class. If you'd like extra tips and insights for social media success, you can attend our Social Media Manager Support Meetings (contact Marketing for schedule uihealthmktg@uic.edu). For a quick reference, please refer to the Social Media Best Practices guide in this document (section 4).

B. Personal Use of Social Media

Occasional personal use of social media is permitted so long as it does not interfere with your employment obligations and complies with the following:

1. Unless you manage an official UI Health social media channel, you should limit your social media usage during work hours to UI Health-related activities. Some examples of acceptable at-work social media use are:
 - a. Positive promotion of UI Health as an organization, related UI Health news, or upcoming UI Health events.
 - b. Joining a conversation related to UI Health.
 - c. "Following" or "liking" the official UI Health Facebook and Twitter.
 - d. Sharing UI Health-related content with coworkers, friends, and family.
 - e. Researching support groups for a service line.

2. Additionally, the following guidelines are important for you to understand, as there are some situations where your personal use of social media and employment with UI Health may overlap.
 - a. The authorized page manager with support from UI Health Marketing and UIC Public Affairs are the only entities authorized to speak officially on behalf of UI Health online.
 - b. You should limit social media activity during work time, as not to negatively impact work performance or required duties.
 - c. You should never post fake negative or positive reviews of UI Health or impersonate an employee authorized to speak on behalf of UI Health.
 - d. You should consider potential conflict of interest issues before establishing an online relationship with a vendor or patient.
 - e. If a blogger or journalist contacts you about UI Health, you should notify your manager, the UI Health Marketing Department, and/or UIC Public Affairs.
 - f. Unless specifically authorized to do so, you should not make public any news about UI Health that is not already public. Only authorized employees are allowed to speak on behalf of UI Health.

You must adhere to [IM 4.17 HIPAA Sanctions](#) (visit HHS.gov for additional information on Health Information Privacy), and the [IM 3.02 Confidentiality Agreement and Security Awareness](#) to ensure patient and hospital privacy at all times, even while using social media for personal use. You are never to reveal confidential information about UI Health or its patients.

3. UI Health and the University restricts employees' use and disclosure of our confidential information and intellectual property, even while using social media for personal purposes. You should treat the UI Health/University trade secrets, confidential information and intellectual property confidentially and not jeopardize them through your use of social media. Further, you should avoid disclosing intellectual property and/or confidential information of third parties that you learned through your employment. Such disclosures may create liability for you, the employee, as well as the University. UI Health employees may not use the University's or UI Health's logos or other trademarks, or post any confidential or proprietary information, without prior written permission.
4. Employees should demonstrate good judgment when using social media (See Section 4: Social Media Best Practices below).

C. No Expectation of Privacy

The UI Health and University's electronic communications systems, and all the information stored thereon, are the property of the University. Employees should have no expectation of privacy in any data in any format or any other kind of information or communications transmitted to, received or printed from, or stored or recorded on any of these systems. The University reserves the right to monitor all employee usage of these systems and to intercept and review any data or communications, in any format, using these systems, including but not limited to social media postings and activities. You consent to such monitoring as part of your employment at the University of Illinois Hospital & Health Sciences System and your use of such assets and systems. You should not use the University's electronic communications assets or systems for any matter that you desire to be kept private or confidential.

The University may store copies of such data or communications for a period of time after they are created, and may delete such copies from time to time without notice.

D. Social Media Best Practices

This best practice list is not meant to be a comprehensive guide to successful social media management. It should serve as a quick reference. For more tips and best practices, visit [Guidelines for All Social Media & networking Sites](#)

- 1) You shouldn't attempt to diagnose and/or give medical advice online. If you are a manager and a potential patient asks a healthcare question, encourage them to visit UI Health in person.
- 2) You shouldn't acknowledge that any patient received care at UI Health. That information is confidential.
- 3) If you are online and communicating about UI Health or anything UI Health-related, you should state your name and position at UI Health. If you are communicating online and your affiliation with UI Health is apparent, you should speak in the first-person and possibly include a disclaimer, such as: *"The views expressed here are my own and do not reflect the views of my employer."*
 - a. This disclaimer may be included in your Facebook or Blog's "About" section or within a Twitter bio.
 - b. The above best practice is recommended so that you don't inadvertently speak on behalf of UI Health.
- 4) You shouldn't post photos of coworkers or any of their personal information without their approval.



- 5) You should utilize the appropriate platform to reach your objectives. For example, Facebook is good for community building and media-sharing. Twitter is good for sharing quick information and having real-time conversations.
- 6) You should follow post frequency best practices. 1-2x/day for Facebook, 1-3x/day for Twitter.
- 7) You should use a voice/tone that reflects UI Health's expertise and high standards. See brand standards ([Standards & Best Practices Brand Guidelines](#))
- 8) You should take into consideration UI Health's goals when posting online. This will be addressed in more detail at the UI Health Media Training and Obligations class

References

[LD 4.13 Code of Conduct](#)

[IM 3.15 Acceptable Use of Computer Resources](#)

[IM 3.02 Confidentiality Agreement and Security Awareness](#)

[IM 4.17 HIPAA Sanctions](#)

Adapted from UI Hospital and Clinics Policy and Procedures 2014

(UI Health Policy Owner- Eric Pitt, Assistant Director of Web and Digital Strategy)